



BANK *i* NFO SECURITY®

Course Catalog

Information Security | Risk Management | Compliance | Fraud



From headline-making data breaches to hacktivist attacks, there never have been so many high-profile incidents, which in turn have sparked greater public awareness of information security risks.



Tom Field

Now, more than ever, regulators, board members and even customers are asking smart questions about information security, fraud and compliance. You need to be prepared to give them informed answers.

At Information Security Media Group, we've assembled a broad suite of webinar training programs aimed at giving you the latest information you need about the ever-changing threat, compliance and technology landscape. Among the benefits:

- Relevant Topics – From mobile security to fraud prevention and how to conduct an effective risk assessment, we continue to produce new sessions that reflect today's top priorities.
- Experienced Faculty – For our virtual faculty, we draw upon industry thought-leaders, top consultants, current industry/security leaders, even federal regulators.
- Convenience – You don't need to travel off-site or even to a conference room to experience our programs. They are delivered straight to your desktop.

The ROI on our training programs is three-fold:

1. Cost-effective access to education that will help you in your job today;
2. Access to world-class leaders in our virtual faculty;
3. Ability, through our Membership Program, to gain on-demand access to our training library.

Please check out our latest catalog, and be sure to offer your own suggestions for new course offerings.

Tom Field,
Vice President, Editorial
Information Security Media Group

Table of Contents

4 About ISMG

Whether you deal with strictly compliance initiatives or delve into the intricacies of technology implementation, we have training webinars for you.

6 The Web Advantage

Essential education designed to ensure you meet and exceed your organization's security and risk goals.

8 Board of Advisers

A unique, active group of industry leaders who guide our coverage of banking security, fraud, privacy and risk management issues.

12 Webinar Presenters

We employ actual practitioners at financial services organizations who speak directly from experience.

18 Course Category Matrix

This chart offers guidance to the webinars covering multiple topics of interest.

30 Curriculum Tracks

We've organized several webinars into tracks to help users see the depth of our webinar education for some of today's most popular topics.

42 Course Descriptions

Detailed course descriptions organized by topics that fit your specific responsibilities and goals.

230 Premium Membership

Professionals that understand the need for continuing education know the advantages of a custom experience.

233 Registration Form

Register online, or fill out the form and mail or fax it to our headquarters.

Course Descriptions

Industry-expert practitioners with years of experience develop courses on the topics relevant to your role.

Compliance	42
Anti-Money Laundering	74
Business Continuity	80
Fraud	84
Governance	117
IT Audits	135
Privacy	139
Technology	156
Vendor Management	218



Our Mission

We task an expert faculty of industry professionals to develop a constantly expanding curriculum of exclusive education in the areas that matter most to financial institutions: information security, risk management, fraud, and compliance.

As industry trends change, new threats emerge, and regulations expand, as does our curriculum.

What Differentiates Our Education

Our presenter faculty consists of keynote level industry practitioners with years of experience implementing the areas their webinars focus on. Our experts include regulators and authors of regulations from the FDIC, authorities on risk management from NIST, and c-level information security professionals at financial institutions ranging from multinational to community banks.

A 200+ course curriculum provides a depth and breadth of education that can be found nowhere else. These sessions and accompanying handbooks deliver actionable advice and resources that can be implemented immediately to achieve business goals.

Sessions such as our series on Risk Management Framework: Learn from NIST are not a simple overview of how to conduct a risk assessment. Ron Ross, Sr. Computer Scientist and lead author of SP 800-37, details critical elements of NIST's Risk Management Framework, utilization of ongoing monitoring, and the key inhibitors many institutions face when implementing these procedures. Our webinars provide an insider's insight into the best course of action and how to avoid pitfalls others may become victim to.

Industry Insight

We understand that as the industry, threats, and regulations evolve, so do the needs of our members. We develop at least 15 new courses each quarter to stay ahead of the latest trends. These sessions are based not only on our educational advisory team, which includes experts from the ABA, NACHA, Gartner, and several banking institutions, but also input that comes directly from our current members.

Key Topics

We strive to provide the exclusive custom webinars to meet the needs of each and every member. Our internal staff has years of direct experience in the banking industry so we understand how quickly educational needs expand and how hard it is to rely solely on internal education or industry conferences. Since our key focus is information security, risk management, fraud, and compliance, we can provide a deeper curriculum and industry-specific relevance not found by other providers.

Education with Results

For these reasons, we have developed a comprehensive solution for risk management, information security, fraud and compliance professionals who demand details, not overviews; actionable advice, not checklist briefings; and custom-built, industry-specific education, not one-size-fits-all training. The banking community relies on these educational webinars to provide action items to put to work immediately to satisfy a direct business initiative.



Don't miss out. Join the other 45,000+ satisfied webinar attendees from thousands of organizations worldwide.



The Web Advantage

Essential education designed to ensure you meet and exceed your organization's security and risk goals.

Continually Expanding Curriculum

We task our expert presenters with developing new webinars continually throughout the year. On average, our curriculum increases by approximately 15 new courses each quarter. Coupled with the convenience of our online delivery, the latest education on the most recent threats, trends, and regulations is available as you need it.

A dedicated team of Membership Advisors speak directly with our member community to understand their needs and get custom webinar topics to develop and add to our webinar library.



Convenience

Convenience is essential when it comes to professional education. A volatile threat landscape, constantly changing industry trends, emerging technologies, and periodic regulatory updates make it difficult to stay up-to-date. Annual industry conferences and an aging internal education become outdated quickly.

Premium members gain unlimited OnDemand access to all sessions. They can even watch on mobile devices, including tablets and smartphones, making it easier than ever to stay up-to-date.



Comprehensive Education

We specialize only in the areas of information security, risk management, fraud, compliance, and governance for the financial industry. This is not general security awareness training or industry-generic security best practices. We've developed over 200 webinars by experts for experienced mid/senior-level professionals with core responsibilities in these areas.

The need to respond to regulators, upper management, other business units, and even customers on information security and risk management is ubiquitous. Our curriculum provides the one resource every institution needs to prepare.

Credit eligible articles, interviews, handbooks, and webinars are tracked and Proof of Attendance Certificates can be downloaded to submit to certifying associations for Continuing Professional Education (CPE) hours.

Expert Education & Discussion

We do not have an internal staff of webinar developers who research and create webinars. We rely solely on industry experts who have direct experience implementing the initiatives they are educating on. Regulators and regulation authors also speak directly from an insider's perspective to give insight and instruction on exactly what institutions will be audited on and how to be compliant.

With a Premium Membership, our expert faculty of practitioners can be directly corresponded with. Members can ask questions, provide their educational needs for custom webinar development, and even gain a peer-review of what others in the industry have successfully implemented.



Board of Advisers

The industry's best & brightest at your service.

BankInfoSecurity's Board of Advisers is an unparalleled brain trust.

The BankInfoSecurity Board of Advisers is a unique, active group of industry leaders who guide our coverage of banking security, fraud, privacy and risk management issues. These experts regularly offer input about emerging issues and regularly contribute insight via podcast interviews, blogs and our webinar training programs. They offer practical advice regarding regulatory compliance and emerging fraud risks, as well as provide unique insights on the most effective risk-management strategies and security technologies.

From hands-on security leaders at institutions of all sizes, to recognized industry thought-leaders from banking associations and analyst firms, BankInfoSecurity's Board of Advisers is an unparalleled brain trust. Their experience and insight greatly shape our educational offerings.



Michael Baker
Executive VP, Electronic Banking, Alpine Bank

Baker is the executive vice president of electronic banking for Alpine Bank of Colorado, Junction, Colo. Baker and his team oversee the design, development and deployment of electronic-banking solutions for the bank.



Patti Broer
Information Security Administrator and Business Continuity Plan Coordinator, BankWest

With 25 years experience with BankWest, Broer supports and assists with the bank's Incident Response Plan and Business Continuity Plan, as it relates to breaches of info security, and maintains the bank's Information Security Program, which includes security oversight and administration of most of the bank's software applications.



Doug Johnson
Vice President, American Bankers Association

Johnson leads the ABA's efforts in enterprise risk, cybersecurity, business continuity and resiliency policy, and fraud deterrence. He also represents the ABA on the Financial Services Sector Coordinating Council, serves on the BITS/Financial Services Roundtable Security Steering Committee and is a board member of the Financial Services Information Sharing and Analysis Center.



Jane E. Larimer
General Counsel and EVP of ACH Network services, NACHA

Larimer leads activities that support NACHA's role as administrator of the ACH Network. She also provides legal support for the NACHA Operating Rules and NACHA's activities in the areas of electronic commerce, electronic check initiatives, electronic bill payment and presentment, and electronic benefits transfer.



Avivah Litan
Vice President and Distinguished Analyst, Gartner Research

Litan has more than 30 years of experience in the IT industry, with expertise in financial fraud, authentication, access management, identity proofing, identity theft, fraud detection and prevention applications, as well as other areas of information security and risk. She also covers the security related to payment systems and PCI compliance.



David Navetta
Founding Partner, Information Law Group

Navetta has practiced law for over twelve years, including technology, privacy, information security and intellectual property law. He is also a Certified Information Privacy Professional and currently serves as a Co-Chair of the American Bar Association's Information Security Committee and Co-Chair of the PCI Legal Risk and Liability Working Group.





Matthew Speare
Senior VP, M&T Bank

Matthew Speare is responsible for Information Technology Operations, Telecommunications and Networking, Platform Design and Support, Information Security and IT Risk Management, and Business Continuity Planning and Disaster Recovery.



Lilly Thomas
VP, Independent Community Bankers of America

Thomas specializes in a wide-range of critical community banking issues, including issues pertaining to the Bank Secrecy Act, data security and privacy. Before coming to the ICBA, Thomas was assistant general counsel at the Credit Union National Association. Prior to that, she served as CUNA's federal compliance counsel and director of compliance operations.



George Tubin
Banking/Security Analyst

Tubin has 20 years in the banking and technology industries and is a former Sr. Research Director for TowerGroup's Financial Information Security services, a Sr. Consultant with ADS Financial Services, and has held positions at BayBank, BankBoston, and Fleet in online banking, fraud, ID theft prevention, info security strategy and authentication.



Mike Urban
Senior Director & Fraud Chief, Fraud Product Management, FICO

Urban has 15 years experience in financial fraud management. He analyzes fraud issues and trends to provide continuous improvements in fraud detection technology and fraud management. He regularly works with law enforcement to help prosecute criminals and has been responsible for uncovering several crime rings in the US.



Tom Wills
Senior Risk/Research/Fraud Analyst, Javelin Strategy & Research

Wills leads Javelin's strategic risk management, security, fraud, and compliance advisory services. He spent the last two and a half decades helping large, global enterprises and financial institutions such as NTT Data Corporation, Wells Fargo Merchant Services, PayCycle.com, and Hyundai strategically navigate the challenges of security.

Hear from regulators, congressional staffers and standards bodies – the groups responsible for setting the stage for compliance and other industry requirements.

Webinar Presenters

A who's who of banking and security leaders.

We work with actual practitioners at financial services organizations who speak directly from experience.

Training and education are only as effective as our experts and their expertise. That is why we utilize only the best and brightest in the financial industry to lead our webinars.

All of our presenters are carefully selected and coached to maximize their training effectiveness. Most have hands-on experience at financial institutions or regulatory agencies, and many have faced the same challenges you do. They have successfully navigated their way to a solution – which they will convey to you.

When it comes to the core objective of our training webinars, we stress the “how-to.” After attending our sessions, you will walk away with definitive steps and practical advice that you can utilize at your own institution. Our presenters work hard to go beyond the theory and give solid advice you can immediately put into practice.

Presenter Biographies



Jeff Kopchik

Sr. Policy Analyst, Federal Deposit Insurance Corporation

Jeff Kopchik is a Sr. Policy Analyst in the FDIC's Technology Supervision Branch, Division of Risk Management. As one of the FDIC's senior staff members, he was the Team Leader of the groups that drafted the 2011 FFIEC Supplement to Authentication in an Internet Banking Environment and the original 2005 guidance.



David Matthews

Deputy Chief Information Security Officer for the City of Seattle

David Matthews, deputy chief information security officer for the city of Seattle, co-chairs the U.S.-CERT-sponsored Northwest Alliance for Cybersecurity, which promotes regional cybersecurity programs.



Donald Saxinger

Senior Examination Specialist

Saxinger is the team leader and subject expert for the FDIC's Division of Supervision and Consumer Protection in the area of regulatory IT exams. As lead developer of the FDIC's IT examination standards and procedures, education, and oversight, he has authored policies on business continuity, authentication, ID theft, and emerging tech.



Kevin Sullivan

Investigator, New York State Police

Kevin Sullivan is an Investigator with the NY State Police and is the state investigations coordinator assigned to the NY HIFCA El Dorado Task Force. He has 20 years of police experience. Sullivan possesses a Masters in Economic Crime Management and is both a certified anti-money laundering specialist and certified anti-money laundering professional.



Ron Ross

Senior Computer Scientist & Information Security Researcher, NIST

Ron Ross specializes in security requirements definition, security testing and evaluation and information assurance. He leads the groups focused on the development of key security standards and guidelines for the federal government and critical information infrastructure and efforts for unified information security framework for the federal government.



Melissa E. Hathaway

President, Hathaway Global Strategies

Melissa E. Hathaway, who led President Obama's Cyberspace Policy Review, is a senior adviser at the Belfer Center of Harvard University's Kennedy School of Government.



Joe Rogalski

Security Strategist, Symantec

As a strategist, Rogalski provides key leadership and direction as part of a world-class Security Business Practice organization directly supporting the business goals of a \$6 billion Fortune 500 software company.



Tom Wills

Senior Risk/Research/Fraud Analyst, Javelin Strategy & Research

Tom Wills leads Javelin's strategic risk management, security, fraud, and compliance advisory services. He spent the last two and a half decades helping large, global enterprises and financial institutions such as NTT Data Corporation, Wells Fargo Merchant Services, PayCycle.com, and Hyundai strategically navigate the challenges of security.



Patrick D. Howard

Chief Information Security Officer, Nuclear Regulatory Commission

Howard serves as the CISO for the Nuclear Regulatory Commission. He provides vision, leadership and oversight in developing, promulgating and implementing an agency IT security strategy. This organizational change meets the Federal Information Security Management Act (FISMA) requirements as they relate to IT security.



Tom Walsh, CISSP

President - Tom Walsh Consulting

As president of Tom Walsh Consulting, Walsh has advised healthcare organizations on risk management strategies and conducted numerous courses on HIPAA compliance. Walsh serves as ISO at San Antonio Community Hospital on an outsourced basis and is one of the authors of, “Information Security in Healthcare: Managing Risk.”



Bill Sewall

Information Security, Compliance and Risk Management Specialist

Bill Sewall is an information security, compliance and risk management specialist with 30 years experience as a corporate attorney and general counsel, CIO, ISO, and operational risk manager. Most recently, Sewall spent 10 years as a Senior Executive ISO in Citigroup, managing the IS training and awareness program and IS Policy and Standards.



Matthew Speare

SVP, M&T Bank

Matthew Speare is responsible for Information Technology Operations, Telecommunications and Networking, Platform Design and Support, Information Security and IT Risk Management, and Business Continuity Planning and Disaster Recovery.



Sharon Finney

Corporate Data Security Officer, Adventist Health System

Sharon Finney, CISM, CISSP, is the corporate data security officer for the 37-hospital Adventist Health System, where she sets the data security strategy to ensure the confidentiality, integrity and availability of the organization's information assets.



Christopher Hourihan

Programs & Operations Manager, Health Information Trust Alliance

Hourihan leads the development of the Common Security Framework (CSF) and CSF Assurance Program at HITRUST. The framework helps organizations demonstrate security and compliance with the HITECH Act and HIPAA. Before HITRUST, Hourihan worked at PricewaterhouseCooper's security advisory practice, focusing on healthcare.



Rebecca Herold, CISSP, CISM, CISA, CIPP, FLMI

CEO, The Privacy Professor

Herold has over 20 years of experience in information security, privacy and compliance, including training and awareness. She's publishing her 15th book, "Practical Guide to HIPAA Privacy and Security Compliance," and has written 200+ published articles. Herold was also named Computerworld's #3 best privacy advisor in the world.



Marilyn Lamar

Partner, Liss & Lamar

Lamar has over 20 years of experience in corporate and information technology law including electronic health records, health information exchanges, personal health records and HIPAA and HITECH Act privacy and security. Her practice includes a broad range of services on behalf of hospitals, health plans, and health information exchanges.



Christopher Paidhrin

IT Security Compliance Officer, Southwest Washington Medical Center

Paidhrin has worked in IT and business operations in higher education, the private sector and entrepreneurial environments, where he has held numerous director-level positions. Paidhrin has received awards for IT service excellence and has presented at numerous industry events.



Kate Borten

CISSP, CISM, President - The Marblehead Group

Borten provides technical and management expertise, information security knowledge, and an insider's understanding of the world of healthcare. She is a nationally recognized expert and frequent speaker on topics of HIPAA and health information privacy and security. She is also the author of "Guide to HIPAA Security Risk Analysis" and "HIPAA Security Made Simple."



E.J. Hilbert

Former FBI Special Agent

Hilbert is a former FBI Special Agent specializing in international hacking, carding and fraud teams. Hilbert served as the agent in charge of the investigations into the intrusions of over 300 financial institutions and multiple U.S. government agencies. Hilbert spent his time most recently with the FBI chasing Al Qaeda via their online networks.



Paul Smocer

VP Security, BITS

Paul Smocer leads the security program for BITS, a division of the Financial Services Roundtable. Smocer has over 30 years' experience in security and control functions, most recently focusing on technology risk management at The Bank of NY Mellon and leading information security at the former Mellon Financial.



Mike Urban

Senior Director & Fraud Chief, Fraud Product Management, FICO

Mike Urban has 15 years experience in financial fraud management. He analyzes fraud issues and trends to provide continuous improvements in fraud detection technology and fraud management. He regularly works with law enforcement to help prosecute criminals and has been responsible for uncovering several crime rings in the US.



Markus Jakobsson

Online Security Researcher

Dr. Markus Jakobsson is Associate Professor at Indiana University's School of Informatics, Associate Director of the Center of Applied Cybersecurity Research, Founder of RavenWhite, Inc., has served as the VP of the International Financial Cryptography Association, and is a Research Fellow of the Anti-Phishing Working Group.



Randy Sabett

Privacy Attorney

Sabett is a partner of Sonnenschein Nath & Rosenthal LLP, where he is a member of the Internet, Communications & Data Protection Practice and served as a Commissioner for the Commission on Cyber Security for the 44th Presidency. He counsels on info security, privacy, IT licensing, identity theft and security breaches.



Linda Coven

Head of Online Banking Channel Solutions, Silicon Valley Bank

Ms. Coven is a 20 year veteran of the banking industry with over 7 years experience at SVB serving as strategic advisor to the company's executives and committees related to products and services that help further the bank's strategic objectives. Prior to SVB, Ms. Coven held product manager roles with Imperial Bank and BankBoston.



Evelyn Royer

Vice President Risk Management & Support Services, Purdue Employees Federal Credit Union

Royer joined the credit union in 1994 as the internal auditor until she was promoted to develop the risk management department in 2002. In 2005 Royer became VP to oversee collections, compliance, and internal audit for loans, deposits and plastic products. Royer is also certified by CUNA as a Credit Union Compliance Expert.



William Henley

SVP - Regulation, BITS

At BITS, Henley outlines policy positions on operations and technology issues and provides expertise on regulator issues. Previously, as the Director of IT Examinations for the OTS, he was the principal advisor regarding the development and implementation of policies pertaining to the examination and supervision of savings associations in the area of IT and Technology Risk Management



Anton Chuvakin

Author, PCI Expert

Chuvakin is a recognized security expert in the field of log management and PCI DSS compliance. He is author of books "Security Warrior" and "PCI Compliance" and contributor to "Know Your Enemy II", "Information Security Management Handbook" and dozens of papers on log management, PCI DSS, and security management.



David Garrett

Fraud and Operational Controls Analyst

After stints as a Detective and Corporate Security Investigator, Garrett was recruited to establish a fraud prevention unit for AT&T Universal Card Services (now Citibank). After 10 years, he joined the operational team at ACI Worldwide where he led risk solutions. Garrett also consulted over 40 financial institutions on fraud detection and prevention.



Eric Cole

Security Expert, SANS Institute Faculty Fellow

Eric Cole is an industry-recognized security expert and has authored several books, including “Hackers Beware,” “Hiding in Plain Site,” and “Network Security Bible.” He also serves on the Commission on Cybersecurity for the 44th President and is involved with the SANS Technology Institute and SANS teaching and developing courseware.



David Navetta

Founding Partner, Information Law Group

Navetta has practiced law for over twelve years, including technology, privacy, information security and intellectual property law. He is also a Certified Information Privacy Professional and currently serves as a Co-Chair of the American Bar Association’s Information Security Committee and Co-Chair of the PCI Legal Risk and Liability Working Group.



Dixie Baker, Ph.D.

SVP & Technical Fellow, SAIC

Dixie Baker serves as the chief technology officer of the health and life sciences practice at SAIC. She has worked in high-assurance computing and information protection for more than three decades. In 2009, she became a federal adviser as chair of the Privacy and Security Workgroup at the Health Information Technology Standards Committee.



George Tubin

Banking/Security Analyst

Tubin has 20 years in the banking and technology industries and is a former Sr. Research Director for TowerGroup’s Financial Information Security services, a Sr. Consultant with ADS Financial Services, and has held positions at BayBank, BankBoston, and Fleet in online banking, fraud, ID theft prevention, info security strategy and authentication.



Kim Peretti

J.D., LL.M., CISSP, PricewaterhouseCoopers

Peretti helps clients respond to significant cyber attacks and breaches, as well as advise clients on how to reduce risks related to cybersecurity. Before joining PwC, Peretti was a senior counselor with the Department of Justice’s Criminal Division in the Computer Crime and Intellectual Property Section.



Lester Rosen

President, Employment Screening Resources

Rosen is an attorney at law and President of Employment Screening Resources, a national background screening company. A former deputy District Attorney and criminal defense attorney, he has taught criminal law at the University of California Hastings College of the Law. His jury trials have included murder, death penalty and federal cases.



Mac McMillan

Co-Founder & CEO, CynergisTek Inc.

Mac McMillan is co-founder and CEO of CynergisTek Inc. He has more than 30 years of federal/private sector experience in managing and delivering information security services. He is chair of the Healthcare Information and Management Systems Society’s Privacy and Security Steering Committee.



Philip Alexander

CISSP - ISSMP, MCSE - MCT, MPA

Since beginning his career serving in the U.S. military, Alexander has worked in both the public and private sectors in positions including: engineer, security architect, and IT director. He currently works as an ISO for a major U.S. financial institution, is an avid public speaker, and author of “Data Breach Disclosure Laws - a State by State Perspective.”



Stephen R. Katz, CISSP

President of Security Risk Solutions

Katz has directed info security and privacy functions for over 25 years. In addition to his role at Security Risk Solutions, Katz is an Executive Advisor to Deloitte, on the Board of Directors of nCircle and Avior Computing, the Advisory Boards of Voltage Security and Veracode, and is a member of the (ISC)² Advisory Board for Information Systems Security.



Steven Jones

Vice President, Director Information Security, Synovus Financial Corp.

At Synovus Financial, Jones holds responsibility for organizational policy, risk management, security awareness, identity management, disaster recovery, and other areas of risk management. As a member of senior management, he aids in technology planning, regulatory compliance, business solution delivery, policy, and strategy.



John P. Pironti

Chief Information Risk Strategist for Archer Technologies

In his role at Archer Technologies, Pironti consults with Fortune 1000 executives on IT-GRC and information security issues and initiatives, evangelizes product concepts in the marketplace to gather feedback, and collaborates with Archer’s product experts to translate industry needs into technology solutions.



James Christiansen

CEO of Evantix LLC

Prior to joining Evantix, Christiansen was CISO for Experian Solutions, which he joined after serving as CISO for General Motors. Prior to joining GM, Christiansen leveraged his years of security experience to provide global leadership to Visa International.



Steve Neville

Director of Identity Products, Entrust

Working closely with customers and key departments such as R&D, sales and marketing, Neville is passionate about ensuring that Entrust fields market-driven, innovative products. Neville draws on his more than 15 years’ hi-tech marketing and product management experience to drive the strategic direction of authentication and fraud detection solutions.

#	Course Title	ID	Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
1	2012 Cloud Security Agenda: Expert Insights on Security and Privacy in the Cloud	276	○						○	●	
2	2012 Faces of Fraud Survey: Complying with the FFIEC Guidance	270	○			●				○	
3	5 Critical Data Security Predictions for 2011	205					○		○	●	
4	5 Steps to Managing Security Risk from Your Software Vendors	143	○								●
5	Adaptive Strong Auth & Federated SSO - A Layered Security Model for FFIEC Compliance	249	○							●	
6	Anti-Money Laundering/Fraud Convergence: Why Should I Care?	59	○	●		○		○			
7	Anti-Money Laundering: The Investigator's Guide to the Laws	154	○	●				○			
8	Anti-Money Laundering: The Practitioner's Guide to the Laws	153	○	●				○			
9	Application Security Testing and OCC Bulletin 2008-16 Compliance	110	○						○	●	○
10	Assessing Encryption Standards for Financial Institutions	130						○		●	○
11	ATM Fraud: Strategies to Beat the Skimming Scams	125				●				○	
12	ATM Skimming Fraud: Banking's Growing Billion Dollar Electronic Crime	258				●				○	
13	Automating Security Controls Within Government Information Systems	160					●	○		●	
14	Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks	87					●		○		
15	Banking Fraud: Actual Attacks and Why They Work	295				●				○	
16	Beyond Heartland: How to Prevent Breaches of Security and Trust	129				●			○	○	
17	Beyond Phishing - The Growing Crimeware Threat	29				●			○		
18	Beyond the FFIEC Authentication Guidance: Prepare for Future Threats	238	○			○				●	
19	Big Data & Security: The Management Challenge	294				○	○			●	
20	Board Responsibilities for IT Risk Management: Building Blocks for a Secure System	11					●				
21	Breach Prevention: Fend Off Malicious Attacks	269	○			●				○	
22	Breach Response: Developing an Effective Communications Strategy	288				●	○		○		
23	BSA Compliance: How to Conduct an Anti-Money Laundering Investigation	80	○	●				○			
24	Business Banking Under Attack: How to Fight Back Against Cybercriminals	149				●				○	
25	Business Continuity Planning Best Practices	27			●						
26	Business Continuity Risk Assessment & Resource Allocation	96			●		○	○			
27	Business Impact Analysis — How to Get it Right	95			●		○				
28	BYOD: Manage the Risks and Opportunities	266				○			○	●	
29	Challenges with PCI-DSS Compliance and Security for the Cloud	292	●							○	
30	Check Fraud Management 2.0: A New Approach to a Persistent Challenge	152				●				○	
31	Cloud Computing: Regulatory Security & Privacy Challenges	188	●						●	●	●
32	Complying with the FFIEC Guidance on a Budget	253	●			○				○	
33	Continuous Monitoring: How to Get Past the Complexity	291	○			○		●		●	

#	Course Title	ID	Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
34	Creating a Culture of Responsible Application Security	248					○	○		●	
35	Creating a Culture of Security - Top 10 Elements of an Information Security Program	150	○				●				
36	Data Protection and Incident Response	162					●		●		○
37	Data Protection: The Dirty Little Secret	208						○		●	
38	Debit Fraud: Trends and Typologies	194				●		○		●	
39	Defending Against The Insider Threat	67				●	○		○		
40	Dept. of Health & Human Srvcs: Privacy and Security Strategies for Smaller Healthcare Entities	286							●	○	
41	Developing an Effective Information Security Awareness Training Program - Getting the Word Out	20	○				●				
42	Effective End-to-End Fraud Management: Managing Financial Crime Risks in Today's Banking Climate	168				●			○		
43	Electronic Evidence & e-Discovery: What You Need to Know & Protect	158	●				○	○			
44	Email Security Requirements for Healthcare Providers: HIPAA & Beyond	180	●						○	●	
45	Embezzlement (Part 1): When Everyone Lies, Cheats & Steals	133				●					
46	Embezzlement (Part 2): Conducting Financial Crime Investigations	134				●					
47	Evaluating Security Risks Associated with Banking Vendors	127							○	○	●
48	Evolving Threats, Innovative Responses - How to Effectively Combat Spear-Phishing & Data Leaks	293				●				○	
49	Expert's Guide to Suspicious Activity Reports (SARS): Tips to Avoid Regulatory Pitfalls & Penalties	86	○	●							○
50	FFIEC Authentication Guidance Compliance: Detecting and Responding to Suspicious Activities	251	●	○		○		○			
51	FFIEC Authentication Guidance: Customer Education - Developing a Program That Meets Regulatory Expectations	244	○				●	○			
52	FFIEC Authentication Guidance: Essential Questions You Need to Ask Your Vendors	242	●			○					●
53	FFIEC Authentication Guidance: FDIC on Understanding and Conforming with the 2011 Update	232	●			○		○		○	
54	FFIEC Authentication Guidance: How to Create a Layered Security Strategy	246	○					○		●	
55	FFIEC Authentication Guidance: How to Prepare for Your Next Exam	230	●			○	○			○	
56	FFIEC Authentication Guidance: What Your Vendors Won't Tell You (Unless You Ask)	243	○								●
57	FFIEC Authentication: How to Invest in Anti-Fraud and Operational Controls	245	○							●	
58	FFIEC Authentication: The Myths and Truths of Anomaly Detection	241	○			○				●	
59	FFIEC Guidance: How to Use Layered Security to Fight Fraud	247	○					○		●	
60	Fight Back Against Fraud: Strategies on How to Meet the Multi-Channel Challenge	187	○			●				●	
61	Fighting Fraud Schemes: Education, Response and Defense	40				●	○			○	
62	Fighting Fraud: Stop Social Engineers in Their Tracks	89	○				●		○		
63	Fighting Online Banking Cybercrime with a Holistic Security Strategy	172				●	○			○	
64	Fraud Detection & Prevention Strategies for Financial Institutions: Emerging Technologies Insights	120	○			●				○	
65	Fraud Prevention: Protect Your Customers and Your Institution from Web Vulnerabilities	177				●	○			●	
66	Fraud Prevention: Understand & Mitigate Threats to Global Institutions	213				○				●	

#	Course Title	ID	Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
67	Fraud Prevention: Utilizing Mobile Technology for Authentication & Transaction Verification	260	○			●				○	
68	Fundamental Security: The Power of GLBA and FFIEC Compliance	265	●				○		○		
69	Gaining Control of Compliance Mandates, Security Threats, & Data Leaks	147	●					○			
70	GLBA Privacy Requirements: Building a Program That Meets Compliance Mandates & Ensures Customer Privacy	94	●						●		
71	Hacktivism: How to Respond	287				●	○			○	
72	Hacktivism, BotNets & More: Top Security Trends and Threats from the HP Enterprise Security 2011 Cyber Risk Report	274	○			○					●
73	HIPAA and HITECH Enforcement: How to Secure Health Information	174	●						●		
74	How Identity Fraud is Evolving and Impacting Customer Trust in Your Financial Institution	83				●			○	○	
75	How to Achieve Network Security Without Compromising Performance	225					○			●	
76	How to Build a Successful Enterprise Risk Management Program	250					●	○			
77	How to Develop & Maintain Information Security Policies & Procedures	135	○				●	○			
78	How to Improve Network Security on a Limited Federal Budget	236					○			●	
79	How To Launch a Secure & Successful Mobile Banking Platform	105								●	
80	How to Prepare for Your First Identity Theft Red Flags Rule Exam	113	●					○	●		
81	How to Prevent Data Leakage from Compromising Your Company's Security	50					●				
82	How to Prevent Security Breaches Through Effective Management and Control of USB Devices	148					○	○		●	
83	How to Use Your Mobile Phone for Free Two-Factor Authentication	58								●	
84	ID Theft Red Flags FAQ's: A Guide to the 'Gotchas' of Compliance	142	●			○			●		
85	Identity Theft: How to Respond to the New National Crisis	155				●			●		
86	Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication	81	●						○		○
87	Incident Response: How to React to Payment Card Fraud	144				●			○		○
88	Information Security for Management - What Your Senior Leaders Need to Know	137	○				●				
89	Information Technology Risk Management Program (IT-RMP) Examination Procedures	28	●							○	
90	Innovative Authentication Process Provides the Ultimate Security for Online Banking	165	○			○				●	
91	Insider Fraud - Profiling & Prevention	35				●			○		
92	Insider Threat: 3 Faces of Risk	296				●				○	
93	Insider Threat: Defend Your Enterprise	66					●				
94	Insider Threats - Safeguarding Financial Enterprise Information Assets	85				●					
95	Integrating Risk Management with Business Strategy	176					●				
96	Investigations, Computer Forensics and e-Discovery - A Primer for Every Banking Institution	65	●					○	○		
97	Is Your Device Identification Ready for New FFIEC Guidance?	217	●						●	●	
98	IT Risk Assessments: Understanding the Process	10	○				●	○			
99	Key Considerations for Business Resiliency	151					●				

#	Course Title	ID	Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
100	Legal Considerations About Cloud Computing	159	○				○			●	○
101	Maintaining Compliance with the Gramm-Leach-Bliley Act Section 501b	19	●					○			
102	Maintaining Secure Government Information Systems	173					●			○	
103	Malware, Crimeware, and Phishing - An In Depth Look at Threats, Defenses	30				○				●	
104	Malware, Phishing & Mobile Security: Trending Threats	215	●							○	
105	Malware: Fight Back Using Layered Security	222						○		●	
106	Managing Change: The Must-Have Skills for Security Professionals	283						●	●	○	
107	Managing Shared Passwords for Super-User Accounts	170					○			●	
108	Man-in-the-Browser Attacks: Strategies to Fight the Latest Round in Online Fraud	178				●			○	○	
109	Massachusetts Privacy Law: A Guide to Understanding and Complying with this New Data Protection Standard	132	●						●		○
110	Meeting Federal Compliance to Secure Windows Desktops	189	●					○		●	
111	Mobile Banking: Emerging Threats, Vulnerabilities and Counter-Measures	285				○				●	
112	Mobile Banking: How to Balance Opportunities and Threats	290				○	○			●	
113	Mobile Banking: Trends, Threats and Fraud Prevention Techniques	279	○			●				●	
114	Mobile Technology: How to Mitigate the Risks	256					○			●	
115	Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices	264	○			○	○			●	
116	Money Laundering Update: The Latest Threats to Your Institution	116		●		○		○			
117	No One's Immune to Being Hacked: Strategies for Staying Out of the Headlines	271				○	○			●	
118	Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?	72			○		●	○	●		
119	Pandemic Planning & Response Techniques	77	○		●						
120	PCI Compliance: Tips, Tricks & Emerging Technologies	212	●							○	
121	Power Systems: How to Prevent Unauthorized Transactions	190	○					○		●	
122	Practical User Authentication Strategies for Government Agencies	166				○		○		●	
123	Preparing for an Information Technology Regulatory Exam	18	●							○	
124	Preparing for Your Next Audit: The Five Habits of Successful Security Programs	219	○					●			
125	Preparing Your Institution for an IT Audit	26						●			
126	Preventing Malware: Tips to Staying FFIEC Compliant	223	○							●	
127	Preventing Phone Fraud with Voice Biometric Authentication	36				●				○	
128	Preventing Unauthorized Access To Your Institution's Data	119						○		●	
129	Proactive IT Risk Assessment Strategies	140	○				●				
130	Protect Data in the Cloud: What You Don't Know About the Patriot Act	227	●					○	●	●	
131	Protect IBM i Data from FTP, ODBC and Remote Command	272								●	
132	Protecting CUI: Federal Best Practices for Email Security, Archiving and Data Loss Prevention	185	●					○		●	

#	Course Title	ID	Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
133	Protecting Government Agency Assets Through Improved Software Security	220					○	○		●	
134	Protecting the Exchange of Sensitive Customer Data with Your Vendors	100							●	○	●
135	Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors	97	●								○
136	Red Hat Enterprise Linux 6 Common Criteria	229						○		●	
137	Risk Assessment Framework for Online Channel: Learn from an Expert	261	●			○	○				
138	Risk Management Framework: Learn from NIST	255	○				●				
139	Risk Management, Continuity and Compliance - What All Financial Organizations Need to Know	102	●				○				
140	Risk Management: New Strategies for Employee Screening	282	●			○	○				●
141	Risk Management: Third-Party Breach Impact & Preparedness	289									●
142	Securing Your Email Infrastructure	141	○						○	●	
143	Security Risks of Unified Communications: Social Media & Web 2.0	146								●	
144	Social Networking Compliance for FINRA Regulated Organizations	193	●					○	○	●	
145	Social Networking: Is Your Institution Ready for the Risks?	145							○	●	
146	Sound Risk Management Practices: Enterprise-wide Encryption and Key Management	257						○		●	
147	Synovus Bank Eliminates Cybercrime - A Case Study	277	○			●				○	
148	Taking Fraud Out of Online Banking	44				●			○	○	
149	Testing Security Controls at a Banking Institution: Learn from the Experts	56	○					○		●	
150	The Dirty Little Secret About Network Security	204	●				○			●	
151	The Faces of Fraud: How to Counter 2011's Biggest Threats	196				●	○				
152	The FFIEC Guidance: What You Need to Know Now About Out-of-Band Authentication	263	●							○	
153	The Fraud Deficit: Why Deposit Account Fraud Budgets Need to Shrink	192				●				●	
154	The Fraud Dilemma: How to Prioritize Anti-Fraud Investments	267				●				○	
155	The Future of Banking Enterprise Access Management & Authentication - Emerging Technologies Insights	118								●	
156	The Great Application Security Debate: Static vs. Dynamic vs. Manual Penetration Testing	268	○							●	
157	The Identity Enabled Network: The Future of Secure Cyberspace	163					○			●	
158	The Identity Management Challenge for Financial Institutions	48				○			●	●	
159	The Many Faces of Online Banking Fraud Attacks	259				●				○	
160	The Mobile Environment: Challenges and Opportunities for Secure Banking	216						○		●	
161	The Reality of Cyberattacks: Emerging Solutions for Today's Threats	179								●	
162	The Role of Out-of-Wallet Questions in Meeting the Updated FFIEC Guidelines	237	○					○	●	●	
163	The State of Government Information Security Today	226					●				
164	The State of Print Security 2012	284					○		○	●	
165	Threat Detection, Compliance & Incident Response	181	●				○				

#	Course Title	ID	Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
166	Time: The Hidden Risks - How to Create Compliant Time Practices	161	○							●	
167	Top 20 Critical Controls to Ensure Painless FISMA Compliance	167	○				●				
168	Top 5 Reports IT Auditors Request	214	○				○	●			
169	Top IT Compliance Challenges: Who's Touching Your Data and What Are They Doing With It?	73	●						●	○	○
170	Turn FFIEC Compliance into Customer Loyalty and Retention	252	○				●				
171	U.S. Dept. of Justice on Payment Card Fraud Trends & Threats	169				●				●	
172	Understand How Financial Institutions Can Benefit from Utilizing Tokenization	239	○						○	●	
173	User Authentication: Best Practices for Managing Risk & Compliance	41	○				○			●	
174	Using the NIST HIPAA Security Rule Toolkit for Risk Assessments	262	○				●			○	
175	Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks	98	○					○			●
176	Vendor Management Part II: Assessing Vendors - The Do's and Don'ts of Choosing a Third-Party Service Provider	104	○					○	○		●
177	Vendor Management Part III: Inside the BITS Shared Assessments Program	117						○			●
178	Vendors' Guide to the FFIEC Authentication Guidance	231	●			○					
179	Voice Over IP - Helping Financial Institutions Learn and Mitigate Security Risks	39								●	
180	You & Your Vendors: How to Best Secure Data Exchange	88	○							○	●
181	ZeuS and Other Malware Threats Force Authentication to "Step Out" Of Band	211				●				○	

Education OnDemand

Customize your curriculum by attending sessions specific to the needs of your institution.

1 Register

Our 130+ Premium Webinars cover a wide range of topics including information security, compliance, business continuity, fraud, technology, vendor management, and more. We understand that, at many institutions, this broad spectrum of topics can fall under the responsibility of one team and sometimes even one individual. This extensive curriculum allows users to register for any in-depth webinar and gain actionable advice on any topic they're interested in, not only one focused concentration.

Customize your education – focus on a webinar track or build your own. You decide what training you need and attend as you need to.

Curriculum Tracks	
We've organized several webinars into tracks to help users see the depth of our webinar education for some of today's most popular topics.	
FFIEC Guidance	32
Risk Management	33
Fraud	34
Compliance	36
Payments Security	38
Vendor Management	39
Anti-Money Laundering	40
Governance	41

2 Attend

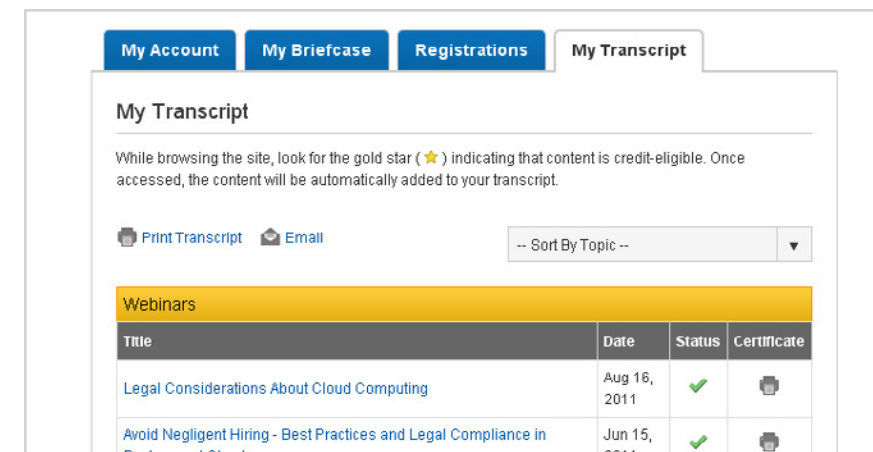
Presented by industry experts with years of experience, these 90 minute sessions provide in-depth actionable advice to implement at your institution. These vital topics warrant so much comprehensive education that our Premium Webinars also come with Presentation Handbooks that include slides and additional research and resources.

In addition, we give our users the added benefit of convenience by providing several ways to attend. Register for a scheduled session on our Webinar Calendar, view Sponsored OnDemand sessions or view any webinar anytime OnDemand as many times as needed with our Premium Annual Membership.

3 Track Your Progress

If required to report to your manager or to an association that provides your certification for your Continuing Professional Education Credits, our system allows tracking for the education you've attended. We can provide Proof of Attendance Certificates for any Premium Webinar attendee.

Premium Annual Members also gain access to a Transcript Tracking interface that shows all Credit Eligible content viewed, including articles, podcasts, handbooks and webinars. Annual Members use this interface to print Proof of Attendance Certificates or their entire educational transcript at any time.



Curriculum Tracks

Pick and choose which courses you attend, or run through some of our pre-selected tracks for your topic area.

FFIEC Authentication Guidance Track

From how to create a layered security program to preparing for your next regulatory exam, our faculty has created a suite of exclusive new training programs designed to help your institution conform with the FFIEC Authentication Guidance. Learn the next steps your institution should take from the industry's top regulators, security leaders and analysts.



Course Title	ID
Adaptive Strong Auth & Federated SSO - A Layered Security Model for FFIEC Compliance	249
Beyond the FFIEC Authentication Guidance: Prepare for Future Threats	238
Complying with the FFIEC Guidance on a Budget	253
FFIEC Authentication Guidance Compliance: Detecting and Responding to Suspicious Activities	251
FFIEC Authentication Guidance: Customer Education - Developing a Program that Meets Regulatory Expectations	244
FFIEC Authentication Guidance: Essential Questions You Need to Ask Your Vendors	242
FFIEC Authentication Guidance: FDIC on Understanding and Conforming with the 2011 Update	232
FFIEC Authentication Guidance: How to Create a Layered Security Strategy	246
FFIEC Authentication Guidance: How to Prepare for Your Next Exam	230
FFIEC Authentication Guidance: What Your Vendors Won't Tell You (Unless You Ask)	243
FFIEC Authentication: How to Invest in Anti-Fraud and Operational Controls	245
FFIEC Authentication: The Myths and Truths of Anomaly Detection	241
FFIEC Guidance: How to Use Layered Security to Fight Fraud	247
Is Your Device Identification Ready for New FFIEC Guidance?	217
Preventing Malware: Tips to Staying FFIEC Compliant	223
The Role of Out-of-Wallet Questions in Meeting the Updated FFIEC Guidelines	237
Turn FFIEC Compliance into Customer Loyalty and Retention	252
Vendors' Guide to the FFIEC Authentication Guidance	231

Risk Management Track

Our vital education for all senior operations and technology professionals covers all aspects of risk mitigation. From Board Responsibilities to employee use of Social Networking, this track helps prepare for the risks and threats every institution faces on a daily basis.

Among our newest sessions: Expert insights on how to manage mobile technologies in the workplace, and an Enterprise Risk Management primer from NIST – the organization that wrote the book on risk management.

FEATURED

**MGMT255
Risk Management Framework: Learn from NIST**

Learn the fundamentals of developing a risk management program from the man who wrote the book on the topic, including: understanding the current cyber threats, developing a multi-tiered risk management approach, and implementing NIST's risk management framework. *Presented by Ron Ross, Sr. Computer Scientist, NIST*



Prepare for the risks and threats every institution faces on a daily basis.

Course Title	ID
Board Responsibilities for IT Risk Management: Building Blocks for a Secure System	11
Business Continuity Risk Assessment & Resource Allocation	96
Business Impact Analysis – How to Get it Right	95
Electronic Evidence & e-Discovery: What You Need to Know & Protect	158
Evaluating Security Risks Associated with Banking Vendors	127
How to Build a Successful Enterprise Risk Management Program	250
IT Risk Assessments: Understanding the Process	10
Information Technology Risk Management Program (IT-RMP) Examination Procedures: How to Satisfy Regulatory Demands	28
Integrating Risk Management with Business Strategy	176
Key Considerations for Business Resiliency	151
Mobile Technology: How to Mitigate the Risks	256
Proactive IT Risk Assessment Strategies	140
Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors	97
Risk Management, Continuity and Compliance - What All Financial Organizations Need to Know	102
Risk Management Framework: Learn from NIST	255
Social Networking: Is Your Institution Ready for the Risks?	145
5 Steps to Managing Security Risk from Your Software Vendors	143
U.S. Dept. of Justice on Payment Card Fraud Trends & Threats	169
Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks	98

Fraud Track

Financial institutions and their customers have been increasingly attacked by incidents of fraud, including: ATM fraud, insider threat, payment card fraud, check fraud, skimming, phishing, and cybercrime. This track focuses on what organizations need to know to prepare, prevent, detect and react to these threats.

These sessions focus not just on external threats, but also on the emerging risk to all organizations – the insider threat.

FEATURED

FR196
The Faces of Fraud: How to Counter 2011's Biggest Threats

Payment card breaches, check fraud and phishing/vishing - these are the most common forms of fraud striking banking institutions today. Join a panel of fraud experts as they look at eye-opening survey results and how institutions can act upon them.

Presented by Mike Urban, Sr. Director & Fraud Chief, FICO; Matthew Speare, SVP, M&T Bank; Tom Field, Vice President - Editorial, ISMG

Course Title	ID
Adaptive Strong Auth & Federated SSO - A Layered Security Model for FFIEC Compliance	249
ATM Fraud: Strategies to Beat the Skimming Scams	125
Beyond Heartland: How to Prevent Breaches of Security and Trust	129
Beyond Phishing - The Growing Crimeware Threat	29
Beyond the FFIEC Authentication Guidance: Prepare for Future Threats	238
Business Banking Under Attack: How to Fight Back Against Cybercriminals	149
Check Fraud Management 2.0: A New Approach to a Persistent Challenge	152
Cross-Border Fraud: How to Spot it, How to Stop it	183
Debit Fraud: Trends and Typologies	194
Defending Against The Insider Threat	67
Effective End-to-End Fraud Management: Managing Financial Crime Risks in Today's Banking Climate	168
Fight Back Against Fraud: Strategies on How to Meet the Multi-Channel Challenge	187
Fighting Fraud Schemes: Education, Response and Defense	40
Fighting Online Banking Cybercrime with a Holistic Security Strategy	172
Fraud Detection & Prevention Strategies for Financial Institutions: Emerging Technologies Insights	120
Fraud Prevention: Protect Your Customers and Your Institution from Web Vulnerabilities	177
Fraud Prevention Strategies for 2010: How to Protect Your Customers...and Your Business	171
How Identity Fraud is Evolving and Impacting Customer Trust in Your Financial Institution	83
Identity Theft: How to Respond to the New National Crisis	155

Course Title	ID
Incident Response: How to React to Payment Card Fraud	144
Insider Fraud - Profiling & Prevention	35
Insider Threats - Safeguarding Financial Enterprise Information Assets	85
Man-in-the-Browser Attacks: Strategies to Fight the Latest Round in Online Fraud	178
Fraud Prevention: Understand & Mitigate Threats to Global Institutions	213
Preventing Phone Fraud with Voice Biometric Authentication	36
Taking Fraud Out of Online Banking	44
The Faces of Fraud: Fighting Back	207
The Faces of Fraud: How to Counter 2011's Biggest Threats	196
The Fraud Deficit: Why Deposit Account Fraud Budgets Need to Shrink	192
U.S. Dept. of Justice on Payment Card Fraud Trends & Threats	169
Zeus and Other Malware Threats Force Authentication to "Step Out" Of Band	211

What organizations need to know to prepare, prevent, detect and react to these threats.



Compliance Track

Government regulation is a key motivator in institutions bolstering their information security and risk management policies and procedures. In many cases the regulatory guidance issued is unclear or vague, making preparation for exams an arduous task. These webinars provide practical advice directly from regulators, examiners and practitioners.

New this year: An entire suite of sessions dedicated to helping financial institutions and their vendors conform with the FFIEC Authentication Guidance.

These webinars provide practical advice directly from regulators, examiners and practitioners.



Course Title	ID
Anti-Money Laundering: The Practitioner's Guide to the Laws	153
Anti-Money Laundering: The Investigator's Guide to the Laws	154
Application Security Testing and OCC Bulletin 2008-16 Compliance	110
ATM Fraud: Strategies to Beat the Skimming Scams	125
Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks	87
Board Responsibilities for IT Risk Management: Building Blocks for a Secure System	11
BSA Compliance: How to Conduct an Anti-Money Laundering Investigation	80
Cloud Computing: Regulatory Security & Privacy Challenges	188
Complying with the FFIEC Guidance on a Budget	253
Electronic Evidence & e-Discovery: What You Need to Know & Protect	158
Expert's Guide to Suspicious Activity Reports (SARS): Tips to Avoid Regulatory Pitfalls & Penalties	86
FFIEC Authentication Guidance Compliance: Detecting and Responding to Suspicious Activities	251
FFIEC Authentication Guidance: Customer Education - Developing a Program that Meets Regulatory Expectations	244
FFIEC Authentication Guidance: Essential Questions You Need to Ask Your Vendors	242
FFIEC Authentication Guidance: FDIC on Understanding and Conforming with the 2011 Update	232

FEATURED

COMP86
Expert's Guide to Suspicious Activity Reports (SARS): Tips to Avoid Regulatory Pitfalls & Penalties

At the core of any good Anti-Money Laundering (AML) program is the Suspicious Activity Report (SAR), which all financial institutions must file when confronting questionable transactions. Learn all SAR writing guidelines and etiquette as well as how and when to properly complete and file a SAR.

Presented by Kevin Sullivan, Investigator, NY State Police

Course Title	ID
FFIEC Authentication Guidance: How to Prepare for Your Next Exam	230
FFIEC Guidance: How to Use Layered Security to Fight Fraud	247
Gaining Control of Compliance Mandates, Security Threats, & Data Leaks	147
GLBA Privacy Requirements: Building a Program That Meets Compliance Mandates & Ensures Customer Privacy	94
HIPAA and HITECH Enforcement: How to Secure Health Information	174
How to Develop & Maintain Information Security Policies & Procedures	135
How to Prepare for Your First Identity Theft Red Flags Rule Exam	113
ID Theft Red Flags FAQ's: A Guide to the 'Gotchas' of Compliance	142
Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication	81
Information Security for Management - What Your Senior Leaders Need to Know	137
Information Security Policies & Standards Development	53
IT Risk Assessments: Understanding the Process	10
Information Technology Risk Management Program (IT-RMP) Examination Procedures: How to Satisfy Regulatory Demands	28
Investigations, Computer Forensics and e-Discovery - A Primer for Every Banking Institution	65
Is Your Device Identification Ready for New FFIEC Guidance?	217
Legal Considerations About Cloud Computing	159
Maintaining Compliance with the Gramm-Leach-Bliley Act Section 501b	19
Massachusetts Privacy Law: A Guide to Understanding and Complying with this New Data Protection Standard	132
Meeting Federal Compliance to Secure Windows Desktops	189
Pandemic Planning & Response Techniques	77
PCI Compliance: Tips, Tricks & Emerging Technologies	212
Preparing for an Information Technology Regulatory Exam	18
Protect Data in the Cloud: What You Don't Know About the Patriot Act	227
Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors	97
Risk Management, Continuity and Compliance - What All Financial Organizations Need to Know	102
Risk Management Framework: Learn from NIST	255
Social Networking Compliance for FINRA Regulated Organizations	193
Threat Detection, Compliance & Incident Response	181
Top IT Compliance Challenges: Who's Touching Your Data and What Are They Doing With It?	73
Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks	98
Vendors' Guide to the FFIEC Authentication Guidance	231

Payments Security Track

Payments make up the majority of transactions at any institution. Millions of debit and credit card, checking, online, and mobile transactions happen every minute of everyday, making payments one of the biggest opportunities for attack. Our Payments Security track provides education on regulations, threats, and the largest cases of breaches to prepare your institution.

Checks, payment cards, online and mobile transactions – payments are the lifeblood of banking and the greatest source of fraud risks.

Course Title	ID
ATM Fraud: Strategies to Beat the Skimming Scams	125
Beyond Heartland: How to Prevent Breaches of Security and Trust	129
Beyond Phishing - The Growing Crimeware Threat	29
Check Fraud Management 2.0: A New Approach to a Persistent Challenge	152
Cross-Border Fraud: How to Spot it, How to Stop it	183
Debit Fraud: Trends and Typologies	194
Encrypting Servers Across the Financial Services Enterprise	257
Fighting Online Banking Cybercrime with a Holistic Security Strategy	172
How To Launch a Secure & Successful Mobile Banking Platform	105
Innovative Authentication Process Provides the Ultimate Security for Online Banking	165
Man-in-the-Browser Attacks: Strategies to Fight the Latest Round in Online Fraud	178
PCI Compliance: Tips, Tricks & Emerging Technologies	212
Preventing TJX Type Data Breaches	33
Taking Fraud Out of Online Banking	44
The Faces of Fraud: Fighting Back	207
The Mobile Environment: Challenges and Opportunities for Secure Banking	216
U.S. Dept. of Justice on Payment Card Fraud Trends & Threats	169

FEATURED

FR169 U.S. Dept. of Justice on Payment Card Fraud Trends & Threats

Credit and debit cards are under increased attack by fraudsters, and organizations need to step up their efforts to protect against threats. Learn trends in debit and other payment card thefts, lessons learned from the biggest breaches, and what you can do to avoid being the next victim. *Presented by Kim Peretti, former senior counsel with the U.S. Dept. of Justice*

Vendor Management Track

When an institution utilizes a vendor, that vendor's vulnerabilities become the institution's vulnerabilities. To ensure your customers' accounts are fully protected from threats, an in-depth vendor management program must be established. Webinars in this track are dedicated to providing you a framework to assess vendors, including what questions to ask and how to best secure sensitive information.

FEATURED

VM98 Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks

The FDIC's Donald Saxinger details exactly what federal regulators are looking for when it comes to managing third-party service provider relationships. Gain a clear understanding of Vendor Management guidance and the four main elements of an effective third-party risk management process. *Presented by Donald Saxinger, Senior Examination Specialist, FDIC and James Christiansen, CEO, Evantix*

Course Title	ID
Evaluating Security Risks Associated with Banking Vendors	127
FFIEC Authentication Guidance: Essential Questions You Need to Ask Your Vendors	242
FFIEC Authentication Guidance: What Your Vendors Won't Tell You (Unless You Ask)	243
How Well Do You Know Your Vendors?	13
Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication	81
Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?	72
Protecting the Exchange of Sensitive Customer Data with Your Vendors	100
Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors	97
5 Steps to Managing Security Risk from Your Software Vendors	143
Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks	98
Vendor Management Part II: Assessing Vendors - The Do's and Don'ts of Choosing a Third-Party Service Provider	104
Vendor Management Part III: Inside the BITS Shared Assessments Program	117
Vendors' Guide to the FFIEC Authentication Guidance	231
You & Your Vendors: How to Best Secure Data Exchange	88



Anti-Money Laundering Track

Anti-money laundering is one of the classic threats to financial institutions, and fighting this complex threat is a key component of Bank Secrecy Act compliance. This webinar track not only provides guidance on becoming BSA compliant and Suspicious Activity Reports but also sheds light onto how AML is evolving into the cross-border risk it is today.

Course Title	ID
Anti-Money Laundering/Fraud Convergence: Why Should I Care?	59
AML: The Practitioner's Guide to the Laws	153
AML: The Investigator's Guide to the Laws	154
BSA Compliance: How to Conduct an Anti-Money Laundering Investigation	80
Cross-Border Fraud: How to Spot it, How to Stop it	183
Expert's Guide to Suspicious Activity Reports (SARS): Tips to Avoid Regulatory Pitfalls & Penalties	86
Money Laundering Update: The Latest Threats to Your Institution	116

FEATURED

AML153
Anti-Money Laundering: The Practitioner's Guide to the Laws

Money laundering is a growing crime that affects numerous organizations. Learn exactly what you need to know to uphold specific statutes and regulations that govern this crime. Gain details on key AML laws, penalties for money-laundering crimes, and how to respond to money-laundering mandates.

Presented by Kevin Sullivan, Investigator, NY State Police

Anti-Money Laundering has evolved into a cross-border concern for all financial organizations.

Governance Track

Senior leaders at institutions require specialized education regarding matters of business continuity, risk management, incident response and preparing the teams and employees they manage. This track highlights the needs of management ultimately responsible for the direction of an institution's course of action in these areas.

Learn the basics of establishing a culture of security within your organization, as well as the latest methods for educating employees, customers and your own senior leaders.

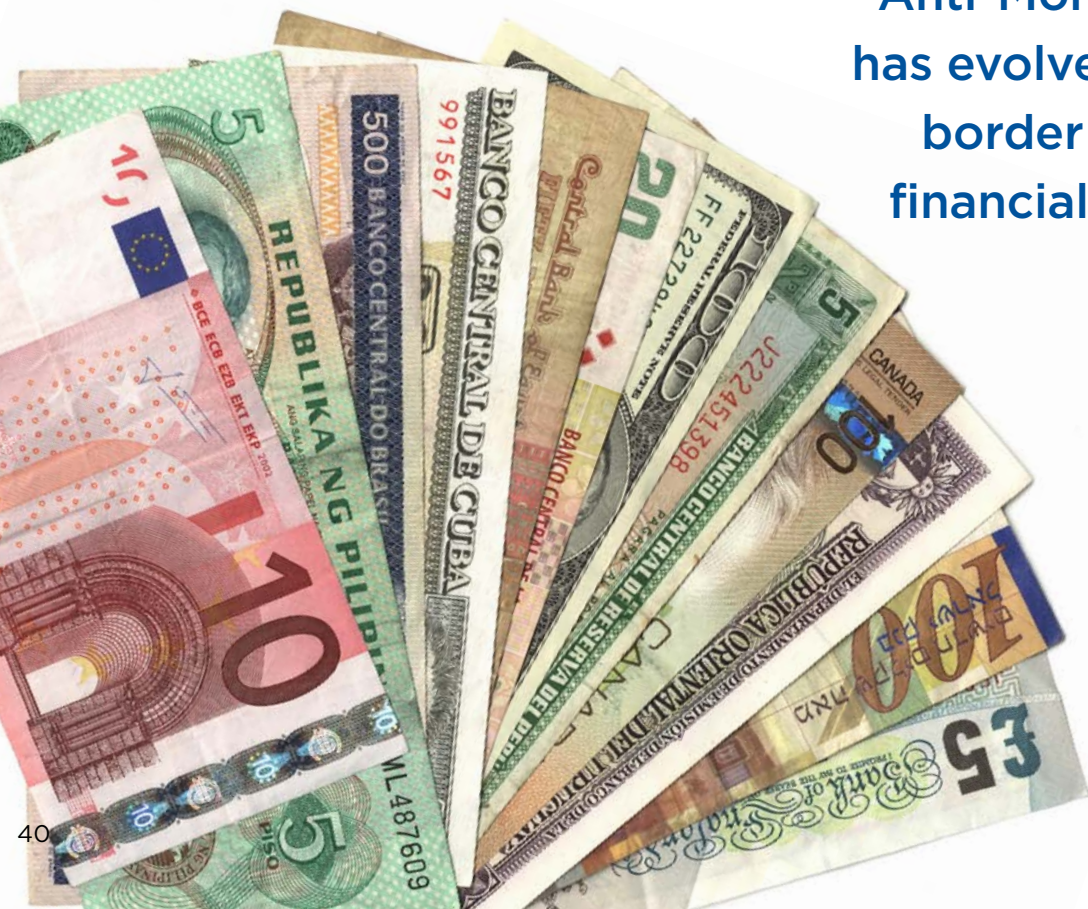
FEATURED

GOV137
Information Security for Management - What Your Senior Leaders Need to Know

By law, senior leaders must know what's at risk, how information is protected and what they are doing to maintain compliance. Learn how to engage senior leaders about their role in enforcing security, creating an information security governance structure, and effective metrics to prepare for an incident.

Presented by Bill Sewall, Information Security Specialist

Course Title	ID
Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks	87
Board Responsibilities for IT Risk Management: Building Blocks for a Secure System	11
Creating a Culture of Security - Top 10 Elements of an Information Security Program	150
Data Protection and Incident Response	162
Electronic Evidence & e-Discovery: What You Need to Know & Protect	158
FFIEC Authentication Guidance: Customer Education - Developing a Program that Meets Regulatory Expectations	244
How to Build a Successful Enterprise Risk Management Program	250
How to Develop & Maintain Information Security Policies & Procedures	135
Developing an Effective Information Security Awareness Training Program - Getting the Word Out	20
Information Security for Management - What Your Senior Leaders Need to Know	137
Information Security Policies & Standards Development	53
IT Risk Assessments: Understanding the Process	10
Insider Threat: Defend Your Enterprise	66
Integrating Risk Management with Business Strategy	176
Key Considerations for Business Resiliency	151
Maintaining Secure Government Information Systems	173
Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?	72
Proactive IT Risk Assessment Strategies	140
Fighting Fraud: Stop Social Engineers in Their Tracks	89
Social Networking: Is Your Institution Ready for the Risks?	145
Threat Detection, Compliance & Incident Response	181



Course Descriptions

Detailed course descriptions organized by topics that fit your specific responsibilities and goals.

188

Cloud Computing: Regulatory Security & Privacy Challenges



Overview

Cloud computing is the hot, new practice that offers a scalable, centralized resource for data and applications that can be available to anyone, anywhere.

But as an emerging trend, cloud computing is also fraught with risk - already we've seen organizations whose data has been compromised.

Register for this session to hear the lessons learned about cloud computing from a panel of experts who will discuss:

- Advantages and disadvantages of storing data or running applications online, as opposed to in-house;
- Current regulatory trends toward better security and privacy standards - and how they impact cloud computing;
- Legal, privacy, records management and ethical challenges that have been identified by cloud pioneers - and strategies to avoid those pitfalls.

Background

Attend any industry event this year, and the term you'll hear most frequently is "Cloud Computing."

But like the old cliché about the weather, one is left to ask: "Everyone is talking about Cloud - but what are they actually doing about it?"

The answer is: More than you might think. Banking institutions for years now have practiced cloud computing without using the term, outsourcing core processing to third-party service providers.

Today, with more banking services to offer and more hosting options from vendors, banking institutions have a broad range of cloud computing opportunities before them. But they also have

significant questions to answer re: scale, security, privacy and true business benefits.

In this session, Matt Speare, veteran technology leader from M&T Bank, will lead our cloud computing discussion - setting the stage with a presentation depicting a banking institution's approach to the cloud. He'll then interact with industry experts, including Jim Reavis of the Cloud Security Alliance, to discuss not just the theory of cloud - but about the real business benefits that pioneer banking institutions are realizing today.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

Michael Smith, Security Evangelist, Akamai

Harold Moss, CTO - Cloud Security Strategy, IBM

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=188>

253

Complying with the FFIEC Guidance on a Budget



Overview

The new FFIEC Guidance is clear. And the deadline to have a plan in place is quickly approaching. Financial institutions need to perform periodic risk assessments of customer authentication controls based on threats and subsequently increase levels of controls based on threats. As part of this risk assessment, financial institutions need to deploy more sophisticated challenge questions as an effective component to their risk management programs.

What is not clear and where many organizations struggle is figuring out exactly where and when to deploy more sophisticated challenge questions and how to do so given budgetary constraints.

This webinar will arm you with the following information:

- Identify the difference between simple challenge questions and sophisticated out-of-wallet questions;
- Clarify when and how to effectively use sophisticated out-of-wallet questions;
- Provide examples of effective usage of out-of-wallet questions;
- Address how to effectively integrate out-of-wallet questions without exceeding your current budget.

Background

The FFIEC Supplement to Authentication in an Internet Banking Environment focuses on the need to perform more frequent and more effective assessments. Following the assessments, financial institutions need to implement layered security techniques to strengthen the security of high-risk transactions, and in particular, utilize more sophisticated challenge questions. This has been highlighted as a weakness in existing systems up to now.

This webinar will discuss authentication techniques based on risk of transaction. We'll explore these techniques in relationship to device identification, dynamic out-of-wallet challenge questions, and out-of-band authentication methods.

We'll specifically delve into the weaknesses of shared secrets and why they are not appropriate for high risk situations. We'll address why the increase of information from social media has limited the effectiveness of this technique. It will clearly become evident why more sophisticated challenge questions are critical to protect your organization and its reputation. The presenters will give concrete examples of effective out-of-wallet questions that are far superior to shared secrets.

Only 11% of respondents have come into conformance with the FFIEC Authentication Guidance since it was released in 2011.

*Source: ISMG's Faces of Fraud Survey 2012

The presentation will also address how to practically integrate challenge questions in, when and where appropriate, to provide the best methods of authentication and risk management possible, without exceeding your budget.

Presented By

Michael Smith, Fraud Market Planning Lead, LexisNexis Risk Solutions

Bryan Knauss, Head of Identity Verification Services, RSA Security

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=253>

292

Challenges with PCI-DSS Compliance and Security for the Cloud

Overview

PCI-DSS compliance has long been a top challenge for financial organizations and their merchant customers. Between understanding what needs to change in order to become PCI compliant, and the complexity of the standard itself, achieving PCI-DSS compliance can have a significant impact on an IT budget.

Financial institutions are rapidly adopting new technologies, such as cloud computing and virtualization, to cut costs; however they end up sacrificing visibility, security controls, data protection standards and compliance requirements in the push to gain the solution benefits.

Register for this session to learn:

- All about the PCI-DSS requirements for adoption of security and virtualization technology;
- Exactly how these requirements apply to financial services organizations.

Background

In June 2011, the PCI Security Standards Council released its PCI DSS Virtualization Guidelines Information Supplement, which offers guidance to merchants, financial institutions and other organizations. As these entities virtualize systems and services, they need to ensure those systems and services comply with payment-card protections outlined within the Payment Card Industry Data Security Standard.

The supplement, drafted by the council's Virtualization Special Interest Group, touches on a number of gray areas, including the different classes of virtualization, how virtualization and cloud computing differ and how mixed mode virtual environments should be implemented under the PCI umbrella.

Specifically, the supplement addresses four principles associated with the use of virtualization in cardholder data environments:

- If virtualization technologies are used in a cardholder data environment, PCI DSS requirements must be applied;
- Virtualization technology introduces new risks that may not be relevant to other technologies;



- Implementations of virtual technologies can vary greatly, and organizations must perform thorough discoveries to identify and document unique characteristics of their virtualized implementations, including all interactions with payment transaction processes and payment card data;
- Specific controls and procedures will vary for each environment, according to how virtualization is used and implemented.

Attend this session to learn from industry experts exactly how these principles apply to financial institutions.

Presented By

John Rostern, Managing Director - Northeast/Southeast Region, Coalfire Systems

Sanjay Raja, Director - Product Marketing, HP Enterprise Security

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=292>

158

Electronic Evidence & e-Discovery: What You Need to Know & Protect

Overview

Federal rules now require institutions to manage their data so it can be produced quickly and completely if demanded by district court cases.

In this session Deputy CISO David Matthews will use his first-hand experience to provide your organization up-to-date information and documents on:

- Compliance with Federal Electronically Stored Information (ESI) standards;
- Real life case studies and examples - do's and don'ts;
- Actual e-discovery documents and samples.

How can your institution be affected? Matthews shares recent case law about e-discovery issues, and he walks you through real situations he's encountered - and how he's responded successfully. He also shares samples of the policies and documents he's prepared to improve ESI procedures in his own organization.

As Matthews emphasizes repeatedly: When it comes down to a court case, it doesn't matter what your policy says - what counts is, 'What procedures did you follow?'

Background

In December of 2006, the Federal Rules of Civil Procedure (FRCP) were revised to require organizations to manage ESI such that it can be produced quickly and completely if required by civil cases in U.S. district courts.

The challenges for organizations are that ESI:

- Is often stored in greater volume than hard documents;
- Is dynamic and often can be modified simply by turning off a computer;
- Can be incomprehensible when taken out of context;
- Often contains meta-data that offers greater context to the information.

And then there are the issues of creating - and enforcing - records retention policies within your organization, so you're prepared to respond effectively when summoned by the law.

In this session, David Matthews, Deputy CISO for the City of Seattle, will walk through electronic evidence issues of which you need to be aware, including:



- Recent case law;
- Case studies from the e-discovery trenches;
- New e-discovery issues inherent in cloud computing and social networking.

Matthews will leave you with strategies for integrating e-discovery into your organization's existing cyber event management procedures.

Presented By

David Matthews, Deputy Chief Information Security Officer for the City of Seattle

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=158>

251

FFIEC Authentication Guidance Compliance: Detecting and Responding to Suspicious Activities



Overview

Since the summer of 2009, financial institutions and their corporate customers have been defrauded by increased incidents of account takeover. These incidents have pitted banks and customers against one another in court, and they were a key impetus behind the release of the new FFIEC Authentication Guidance. So, how can institutions improve their abilities to detect and respond to suspicious activities before fraud is committed? Join a panel of distinguished experts for new insights on:

- Today's most common fraud schemes preying upon institutions and their commercial customers;
- Strategies for improving early detection of account takeover attempts, as well as emerging methods of multifactor authentication;
- How to ensure conformance with this aspect of the FFIEC Authentication Guidance before your next examination.

Background

Since the summer of 2009, financial institutions and their corporate customers have been plagued by a string of ACH and wire fraud incidents that have led to the theft of millions of dollars.

These incidents also have led to a series of high-profile lawsuits between institutions and customers, including the PATCO Construction/Ocean Bank case, which was decided in favor of the bank, and the Experi-Metal/Comerica case, which was decided in favor of the customer.

In preparing the new FFIEC Authentication Guidance, banking regulators point a finger at banks for not detecting and preventing these incidents. "Manual or automated transaction monitoring or anomaly detection and response could have prevented many of the frauds," the guidance says, "since the ACH/wire transfers being originated by the fraudsters were anomalous when compared with the customer's established patterns of behavior."

In discussing how to improve fraud detection and response, the FFIEC Authentication Guidance calls for layered security controls that include processes designed to detect and react quickly to anomalous activity related to:

- Initial login and authentication of customers requesting access to the institution's electronic banking system; and
- Initiation of electronic transactions involving the transfer of funds to other parties.

In this panel discussion, a distinguished thought-leader on financial fraud will discuss current trends in fraud detection and response. He then will lead a panel of industry experts who will delve deeper into topics such as transaction monitoring to improve early detection of account takeover, as well as the use of emerging multifactor authentication methods such as the use of out-of-wallet questions, device identification and geo-location to help prevent identity fraud.

Learn what you can do to improve fraud detection and response and conform with the FFIEC Authentication Guidance prior to your next examination.

Presented By

George Tubin, Banking and Security Analyst

Eli Katz, VP - Enterprise Strategies/Finance, 41st Parameter

Jodi Florence, VP - Marketing, IDology

Mike Byrnes, Director - Customer Authentication & Fraud Detection Solutions, Entrust

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=251>

242

FFIEC Authentication Guidance: Essential Questions You Need to Ask Your Vendors



Overview

Banking regulators, make no bones about it: Your third-party service providers aren't responsible for ensuring that you attain conformance with the FFIEC Authentication Guidance. You are. How do you ensure their ability to aid your efforts towards compliance? Learn the secrets of a vendor management expert, who will share with you the probing questions to ask your vendors, including:

- When and how does your vendor perform external audits checking the security of its products?
- Which authentication controls are built into your vendor's current online banking products - do they conform to the FFIEC Authentication Guidance 2011 update?
- What is your vendor's tactical plan for the remainder of 2011 to ensure its products and services conform to the new guidance in time for 2012?

Background

In a recent interview with BankInfoSecurity, Jeff Kopchik of the FDIC made clear the expectations for banks re: third-party service providers and compliance with the new FFIEC Authentication Guidance.

"The agencies have said many times - and authentication is no different - that it's the financial institution that's ultimately responsible for bringing itself into conformance with the guidance," says Kopchik, one of the principal authors of the guidance. "The buck stops at the financial institution's desk."

For several of the larger banking vendors, the federal regulators conduct their own examinations to ensure compliance. But for the majority of service providers, the responsibility is the banking institution's to ensure that products and services all align with regulatory expectations. This due diligence requires institutions to:

- Sit down with core vendors and ensure mutual understanding of the FFIEC Authentication Guidance;
- Gap analysis to determine which products/services do not currently bring the institution into conformance;

- Creation of a strategic plan with milestones to ensure conformance prior to 2012 regulatory exams.

But two challenges that institutions frequently encounter are:

- What are the specific questions I need to ask my vendors re: FFIEC Authentication Guidance?
- What information will my vendors not offer up unless I know to ask?

To assist you with this due diligence, Philip Alexander, an information security officer at a major U.S. financial institution, will share with you the vendor management tricks he's learned in years of overseeing such relationships for one of the nation's largest banking institutions.

In this exclusive two-part series, Alexander will tackle several key vendor management topics, including:

- Security reviews;
- Vendor's own regulatory compliance;
- Vendor's financial stability;
- Use of 4th-party service providers;
- Liabilities in the event of a breach.

Presented By

Philip Alexander, CISSP - ISSMP, MCSE - MCT, MPA

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=242>

232

FFIEC Authentication Guidance: FDIC on Understanding and Conforming with the 2011 Update



Overview

In the wake of devastating cyber attacks and fraud losses to banking institutions and customers, the FFIEC has issued its first online authentication guidance since 2005. Banking regulators will begin assessing institutions by this new guidance in 2012, so it's imperative to attend this session and gain expert insight from one of the supplement's key authors, Jeff Kopchik of the FDIC, on:

- How the 2011 guidance differs from 2005's;
- The core elements of the new guidance, including risk assessments, layered security, multifactor authentication and customer awareness;
- Strategies for protecting commercial/retail customers and satisfying the guidance.

Following the main presentation, Kopchik will join Matthew Speare of M&T Bank for an open discussion of what this new guidance means for banking institutions.

Background

The Federal Financial Institutions Examination Council has formally released the long-awaited supplement to its "Authentication in an Internet Banking Environment" guidance, which was first issued by the FFIEC in October 2005. Formal assessments for compliance with the new guidance will begin in January 2012.

The purpose of the supplement is to reinforce the risk-management framework described in the original guidance and update the FFIEC member agencies' supervisory expectations regarding customer authentication, layered security, and other controls in the increasingly hostile online environment.

The official supplement highlights the need for:

- Better risk assessments;
- Effective strategies for mitigating known online risks;
- Improved customer and employee fraud awareness.

In this exclusive session, Jeff Kopchik of the FDIC - one of the primary authors of the new guidance - will detail the document's key tenets and the new expectations for banking institutions.

Among his points of discussion:

29% of respondents do not clearly understand the FFIEC Authentication Guidance.

*Source: ISMG's Faces of Fraud Survey 2012

- The FFIEC's intent behind this supplement;
- New expectations for banking institutions;
- What to expect from your examiner in 2012.

Following the main presentation, Kopchik will join Matthew Speare of M&T Bank for an open discussion of what this new guidance means for banking institutions.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

Jeff Kopchik, Federal Deposit Insurance Corp.

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=232>

230

FFIEC Authentication Guidance: How to Prepare for Your Next Exam



Overview

Upon issuing its 2011 update to online authentication guidance, the FFIEC put banking institutions on notice: Examiners will assess how institutions satisfy these enhanced expectations starting in January 2012. So, how best should banking/security leaders go about meeting these new directives and ensuring the security of their retail and commercial customers?

Join a veteran banking/security leader for advice on:

- How to assess your institution's current level of compliance with the new directives;
- What "layered security" means in practical terms;
- Conducting effective risk assessments and customer awareness campaigns;
- How to differentiate security controls between commercial and consumer accounts.

Background

The Federal Financial Institutions Examination Council has formally released the long-awaited supplement to its "Authentication in an Internet Banking Environment" guidance, which was first issued by the FFIEC in October 2005. Formal assessments for compliance with the new guidance will begin in January 2012.

The purpose of the supplement is to reinforce the risk-management framework described in the original guidance and update the FFIEC member agencies' supervisory expectations regarding customer authentication, layered security and other controls in the increasingly hostile online environment.

The official supplement highlights the need for:

- Better risk assessments;
- Effective strategies for mitigating known online risks;
- Improved customer and employee fraud awareness.

In this exclusive session, Matthew Speare of M&T Bank will outline a strategy for how to prepare for your next regulatory examination. Among his points of discussion:

- An overview of the FFIEC update - highlighted items that banks should be concerned about;

- Which technology solutions you should consider to bolster your case for complying with the guidelines;
- Positioning yourself for success with the regulators (ie, how to "prove" you are in compliance).

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=230>

23% of our research respondents did not know if they are in conformance with the FFIEC Authentication Update.

*Source: ISMG's Faces of Fraud Survey 2012

265

Fundamental Security: The Power of GLBA and FFIEC Compliance

Overview

It's been more than 10 years since enactment of the Gramm-Leach-Bliley Act (GLBA). But the fundamental security tenets of GLBA are just as relevant today - especially as banking institutions look to conform to the recently released FFIEC supplement, "Authentication in an Internet Banking Environment."

Join banking and fraud experts George Tubin of GT Advisors and Jeff Multz of Dell SecureWorks for insights on security versus compliance, as they discuss:

- The overarching principles of a comprehensive GLBA information security program;
- How the updated FFIEC Authentication Guidance aligns with GLBA;
- Key recommendations for deploying layered controls to ensure security and compliance.

Background

The adage, "Compliance doesn't ensure good security, but good security almost always ensures compliance," continues to ring true in 2012, as financial institutions seek to comply with the updated FFIEC guidance on online banking.

"Layered security" is a requirement of the new guidance released in 2011, but what does that really mean to banks and credit unions that are preparing for examinations? While financial institutions with an established GLBA information security program and culture most likely were compliant with the new requirements before they were published, many banks and credit unions are still ill prepared to meet the examiners, and as a result may lack fundamental security controls.

Consider the core requirements of GLBA's Safeguards Rule, which requires institutions to:

- Develop a written information security plan;
- Appoint at least one employee to manage the safeguards;
- Conduct a risk assessment of each department handling private information;
- Develop, monitor and test the information security program;
- Amend safeguards as necessary with changes in how information is collected, stored and used.



Risk assessments, security controls and monitoring all are core components of the updated FFIEC Authentication Guidance, as well.

In this session, George Tubin, noted expert in banking security, fraud and compliance, will discuss the key elements of GLBA and the FFIEC guidance with an eye toward offering new insights on:

- Strategies for ensuring both security and compliance;
- A practical approach to layered security;
- Regulatory trends - what to expect next for guidance.

Following Tubin's presentation, Jeff Multz, Director of North America Midmarket Sales for Dell SecureWorks, will discuss the banking and security trends Dell SecureWorks is seeing and how institutions can respond to them.

Presented By

George Tubin, Banking and Security Analyst

Jeff Multz, Director - North America Midmarket Sales, Dell SecureWorks

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=265>

147

Gaining Control of Compliance Mandates, Security Threats, & Data Leaks

Overview

62% of fraud is committed by insiders. Downtime is measured in millions of dollars per minute. Constant security threats and intense scrutiny by regulators and auditors require complete visibility and accountability, both in real-time and historically.

During this session we will cover how you can leverage the logs that you are already collecting to achieve regulatory compliance, protect valuable customer information and improve the efficiency of your IT operations team. This webcast will also feature a real world case study.

During this webcast you'll learn:

- How to easily and cost-effectively automate your log management;
- How log management can be used to achieve compliance;
- How to protect valuable customer data;
- Best practices and tips for simplifying your life.

Background

62% of fraud is committed by insiders. Downtime is measured in millions of dollars per minute. Constant security threats and intense scrutiny by regulators and auditors require complete visibility and accountability, both in real-time and historically. As a financial service organization, you face significant risks and exciting rewards during this period of economic and regulatory change.

To meet the growing demands, you need to make a shift from worrying about the unknown to gaining visibility and control over your operational threats. Top organizations are effectively managing their security threats and compliance requirements by building a foundation for internal investigations, forensics and compliance that allows them to correlate information and detect real-time threats and fraud.

By building pre-defined response plans, they're able to significantly reduce the costs of managing network security and firewall policies. During this session we will cover how you can leverage the logs that you are already collecting to achieve regulatory compliance, protect valuable customer information and



improve the efficiency of your IT operations team. This webcast will also feature a real world case study.

Data integrity and confidentiality is critical for financial services - no other industry is more frequently targeted by cyber-crime and cyber-piracy.

Presented By

Sudha Iyer, Director of Product Management, LogLogic

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=147>

94

GLBA Privacy Requirements: Building a Program That Meets Compliance Mandates & Ensures Customer Privacy

Overview

Preserving the privacy of customer information is a core mandate of Gramm-Leach-Bliley Act (GLBA) compliance - and increasingly an essential for business success.

Banking institutions need strong privacy programs to keep their customers' trust, but also to comply with a growing number of state privacy laws and federal regulations. Beyond regulatory requirements, recent incidents such as the Hannaford data breach have brought to the forefront the need for an effective privacy program.

Register for this webinar for a how-to overview of elements necessary in an effective privacy program, including:

- Overview of GLBA and other regulatory requirements for privacy and security;
- Privacy program components;
- How to establish policies, procedures and technical controls to support and maintain privacy;
- How to align vendor contracts to include privacy-related requirements and outlining vendors' responsibilities;
- Industry "best practices" for customer communications for privacy-related notifications.

Background

Building an effective privacy program is essential for business success. Financial institutions that experience privacy incidents lose the trust of their customers. And lost trust results in lost customers. Institutions need strong privacy programs not only to keep their customers' trust but also to comply with a growing number of privacy laws and regulations worldwide. A growing number of recent privacy related incidents have brought the need for an effective privacy program to the fore-front.

In this exclusive webinar, noted privacy expert Rebecca Herold will lead a discussion of how financial institutions can establish an effective privacy program, outlining the components required to make the program succeed.



Among the points Rebecca will discuss:

- Why a privacy program is necessary;
- Defining personally identifiable information (PII);
- Privacy program components;
- Legal privacy and security requirements;
- Policies, procedures and technical controls;
- Inclusion of privacy program related in the organization's vendor due-diligence process;
- Privacy program maintenance.

Presented By

Rebecca Herold, CEO, The Privacy Professor

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=94>

174

HIPAA and HITECH Enforcement: How to Secure Health Information

Overview

New HIPAA Security Rule enforcement began in February 2010 under the HITECH Act. Healthcare providers and their business associates that fail to secure protected health information are now subject to new penalties. Register for this webinar to learn:

- Strategies for protecting your patients and your business;
- Best-practices from a veteran healthcare/security leader.

Background

After months of discussion, compliance time is here.

Security rules found under HIPAA now enforced by the HITECH Act enable state attorney general's offices to pursue civil charges on behalf of victims. HIPAA violations that result in a data breach are subject to fines of up to \$1.5 million per year.

Faced with the looming threat of serious fines, healthcare providers, plan administrators and other business associates that handle private patient health information are seeking ways to become HIPAA compliant.

But where are the greatest vulnerabilities for healthcare organizations?

What must they do to protect their patients - and themselves?

Where can they pick up practical tips?

In this session, Rapid7, in conjunction with High Point Regional Health System, will spell out exactly how you can protect your patients and secure your business. Get first-hand info from Miles Romello, IT Security Coordinator at High Point Regional Health System.

Presented By

Marcella Samuels, Information Security Solutions Manager, Rapid7

Miles Romello, CISSP, MCSE, MCDBA, IT Security Coordinator, High Point Regional Health System

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=174>

215

Malware, Phishing & Mobile Security: Trending Threats

Overview

Malware, phishing, and the risks to and from mobile devices - these are among today's threats to organizations of all types. And to truly protect your organization requires steps beyond mere checkbox compliance with government and industry regulations.

In this webcast, hosted by Rapid7, the featured speaker, Chenxi Wang, Vice President and Principal Analyst of Forrester Research, leads this discussion on emerging threats and "beyond compliance" strategies, including:

- Why the new threat landscape challenges conventional security;
- How to use compliance as a driver to improve security;
- Recommendations for leading your organization out of the checkbox mentality.

Background

Regulatory compliance is the foundation of any information security program. Government and industry regulations provide the standards by which organizations can be minimally compliant in critical areas such as authentication, payment transactions and privacy.

But the threat landscape is evolving - organized crime continually finds ingenious new ways to sidestep security measures - and so "check-box compliance" isn't enough to ensure true security. Instead, in this age of sophisticated malware, mobile technology and electronic risks such as phishing, information security leaders must build upon regulatory compliance to create an expansive, flexible security program that deals with today's threats and anticipates tomorrow's.

In this session, our speakers will outline the steps you need to take to think and move beyond mere compliance.

Presented By

Chenxi Wang, VP, Principal Analyst, Forrester Research, Inc

Bernd Leger, Senior Director - Marketing, Rapid7

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=215>

113

How to Prepare for Your First Identity Theft Red Flags Rule Exam

Overview

An Insider's Guide to Banking Agencies' Examination Guidelines

The Identity Theft Red Flags Rule compliance deadline was Nov. 1. All banking institutions now must prepare for their first examinations on this important new regulation. Register for this webinar to learn from a senior information security, compliance and risk management specialist:

- How to prepare for examination on this new regulation, which specifies 26 ID theft red flags that institutions must address in their prevention programs;
- The 15 key areas regulators will examine when they assess compliance with Identity Theft Red Flags, Changes of Address and Address Discrepancies standards;
- What your institution can do in advance to help ensure a successful examination;
- What to expect during the exams.

Background

As of Nov. 1, all banking institutions must be in compliance with the Identity Theft Red Flags Rule, which went into effect on Jan. 1, requiring:

- Financial institutions and creditors to implement a written identity theft prevention program;
- Card issuers to assess the validity of change of address requests;
- Users of consumer reports to verify the identity of the subject of a consumer report in the event of a notice of address discrepancy.

To help institutions meet compliance, the banking regulatory agencies have recently released their Red Flags examination procedures, which include 15 key topics that were hammered out and agreed upon by an interagency committee, covering all three aspects of the new rule:

- Identity theft red flags;
- Address discrepancies;
- Changes of address.

In this exclusive new webinar, Bill Sewall, former information security executive with Citigroup, will offer an insider's perspective on how to prepare for a successful Identity Theft Red Flags Rule examination.



Drawing upon his years of experience in risk management and compliance, Sewall will:

Walk Through the Examination Procedures - Explaining each of the 15 aspects and what they mean in regards to how your institution might be examined;

Tell You How to Prepare - Offering insights on risk assessment and scoping tasks you can conduct up front to help ensure a successful examination;

Provide Tips for the Test - Showing how to help manage the examination process, including how to clarify the scope of your exam, as well as how to demonstrate your success at identifying covered accounts and securing board approval for your ID theft prevention program.

Presented By

Bill Sewall, Information Security, Compliance and Risk Management Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=113>

142

ID Theft Red Flags FAQ's: A Guide to the 'Gotchas' of Compliance

Overview

For just over six months now, the banking regulatory agencies have examined institutions for compliance with the ID Theft Red Flags Rule, and they have just released a document addressing frequently asked questions about the regulation.

Register for this exclusive webinar to hear from a former information security executive with Citigroup as he walks you through the FAQs. You'll learn:

- The Deficiencies - Understand the areas other institutions are having a difficult time with and why the FAQs were put together;
- Walk Through the FAQs - Explaining each of the questions and answers contained within the four umbrella topics;
- How to Prepare for Your Exam - Offering insights on risk assessment and scoping tasks you can conduct up front to anticipate any questions and help ensure a successful examination;
- Provide Tips for the Test - Offering a refresher on how to help manage the examination process from start to finish.

Background

As of Nov. 1, 2008, all banking institutions must be in compliance with the Identity Theft Red Flags Rule, which requires:

- Financial institutions and creditors to implement a written identity theft prevention program;
- Card issuers to assess the validity of change of address requests;
- Users of consumer reports to verify the identity of the subject of a consumer report in the event of a notice of address discrepancy.

To help institutions meet compliance, the banking regulatory agencies have recently released a document outlining a series of frequently asked questions about the Red Flags Rule. These questions have arisen from initial examinations and include:

- The ID Theft Red Flags scope;
- The definitions of "covered account," and "service provider";
- Types of notices of address discrepancy that trigger the rule;
- Furnishing a confirmed address to a consumer reporting agency.



In this exclusive new webinar, Bill Sewall, former information security executive with Citigroup, will offer an insider's perspective on how to make sure you answer these questions before the examiner comes calling.

Drawing upon his years of experience in risk management and compliance, Sewall will:

- Walk Through the FAQs - Explaining each of the questions and answers contained within the four umbrella topics;
- Tell You How to Prepare - Offering insights on risk assessment and scoping tasks you can conduct upfront to anticipate any questions and help ensure a successful examination;
- Provide Tips for the Test - Offering a refresher on how to help manage the examination process from start to finish.

Presented By

Bill Sewall, Information Security, Compliance and Risk Management Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=142>

81

Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication



Overview

What happens if your institution suffers an ATM skimming attack and customer accounts have been compromised? Or if a payments processor is hacked and thousands of your credit/debit cardholders are potentially exposed to fraud?

These aren't hypothetical breaches; they've occurred. Repeatedly. And they prove that an incident response plan isn't just a 'nice to have' for a financial institution - it's a must. This webinar outlines the critical components of documenting, testing and updating incident response plans.

Matthew Speare, who created and oversees the incident response program at M&T Bank in New York, will discuss the hottest trends in incident response, including:

- The latest regulatory guidance;
- How to fulfill the elements of a good plan;
- How to handle one of the most critical elements of incident response - customer communications;
- What to do when the incident occurs at one of your vendors.

Background

Incident response by definition refers to the formal reaction to a security breach, i.e. a physical or electronic hack. Every financial institution is required to document, test, update and communicate a formal incident response plan, which may include forensics, e-discovery and other tactics necessary in the wake of a security breach.

Increasingly, incident response plans also include legal and public relations teams as appropriate, as well as customer communications, to ensure the timely release of accurate information.

And then there's the new focus of incident response: third-party service providers. It's one thing to account for incidents at your own institution. As recent breaches have taught us, what if the incident occurs at one of your vendors? The damage can be just as devastating to your business and to customer confidence.

In this webinar, Matthew Speare will discuss the requirements of incident response guidance and the steps that the industry has taken to implement solutions to address the guidance. Among the topics he'll discuss:

- Current regulatory guidance on incident response;
- What today constitutes a security incident;
- What information is considered sensitive customer information;
- How to handle customer communications;
- Steps to take if there is an ongoing investigation;
- How to address incidents that occur at a vendor.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=81>

28

Information Technology Risk Management Program (IT-RMP) Examination Procedures: How to Satisfy Regulatory Demands



Overview

Register for this updated webinar to receive:

- A heads-up on key examination issues;
- Review of the IT Risk Management Program Examination process;
- Overview of IT Examination Officer's Questionnaire;
- What to expect, and how to respond.

Background

Banking regulatory agencies regularly examine banking practices - including information technology - at the institutions they oversee. In this presentation, you will hear about the basic tenants behind the information technology (IT) examinations conducted by the Federal Deposit Insurance Corp. (FDIC) using the Information Technology Risk Management Program (IT-RMP).

Among the key elements examiners are focusing on:

- Vendor management and outsourcing topics;
- An institution's overall information security program.

An important component of IT-RMP framework is the IT Examination Officer's Questionnaire, which was updated in Dec. 2007. This questionnaire must be completed and signed by an officer of the institution and returned to the FDIC examiner-in-charge prior to onsite activities.

During this presentation, we will address amendments to this Officer's Questionnaire, then how the preliminary information gathered via the questionnaire is applied - i) in choosing appropriate work programs suitable for the institution being examined and ii) in identifying the necessary examiner IT skill and experience necessary for conducting each exam. This presentation will prepare the attendees in responding to the pre-examination IT Questionnaire in the most appropriate and accurate manner.

Based on the preliminary information provided by an institution on the technology in use and the applicable practices, and the information available on the previous examinations, bank examiners develop an initial scope for each IT exam. However,

examiners have considerable discretion to expand or contract the scope once onsite, and to utilize any agency-specific or FFIEC-approved work program targeting specific technologies or functions (wire transfer systems, ACH, etc.).

During the course of this presentation, the attendees will gain an understanding of how the regulatory examinations are based on the concepts and guidance provided by the regulatory agencies, information provided in the FFIEC IT Examination Handbook and by industry best-practices.

Presented By

Vincent Pisciotta, Senior Team Member and Security Evangelist, Icons, Inc.

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=28>

65

Investigations, Computer Forensics and e-Discovery - A Primer for Every Banking Institution

Overview

Forensics has become a hot topic for a variety of internal factors, including the importance of the Internet to everyday business and, with it, the rise of electronic fraud.

Externally, financial institutions especially feel regulatory heat in the form of the FFIEC GLBA Notification Rule, SEC/NASD Rule 3010 and even recent VISA/Mastercard PCI requirements, all of which put a premium on forensic and e-discovery capabilities. Add to those pressures recent U.S. litigation trends and the new federal e-discovery rules.

Register for this webinar to learn:

- How to build or enhance a forensics program;
- Proper forensics methodology;
- Federal rules and regulatory requirements that underscore the need for forensics and e-discovery;
- The steps investigators have used to crack tough cases.

Background

Computer forensics is the use of investigative techniques to provide digital evidence of an activity, generally in conjunction with a criminal investigation or civil litigation in cases that include:

- Employee Internet abuse;
- Unauthorized disclosure of corporate information;
- Incident response;
- Fraud.

The forensics process entails:

- Preservation of Evidence - Adherence to a set of procedures that address security, authenticity and chain-of-custody.
- Data Analysis - The ability to locate and recover previously inaccessible documents and files through computer forensic processes.
- Analysis of User Activity - Reports on all user activity including, but not limited to, electronic mail, Internet and Intranet files accessed, files created and deleted and user access times.



Forensics has become a hot topic for a variety of internal factors, including the importance of the Internet to everyday business and, with it, the rise of electronic fraud. Externally, financial institutions feel regulatory heat in the form of the FFIEC GLBA Notification Rule, SEC/NASD Rule 3010 and even the recent VISA/Mastercard PCI requirements, all of which put a premium on forensic and e-discovery capabilities. Add to those pressures recent U.S. litigation trends and the new federal e-discovery rules, and you see why this topic has risen to the top of organizational agendas.

One of the key questions to be tackled in this webinar is whether to establish your own forensics program or outsource it to a third-party provider. Our presenters will explore the factors that go into this decision, including how to:

- Form an internal steering committee of key constituents to evaluate your decisions;
- Establish external relationships with FBI and independent forensics experts;
- Create an e-discovery policy that can be handed down either to an in-house or outsourced forensics team.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

Warren Kruse, Vice President of Data Forensics and Analytics, Encore Legal Solutions

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=65>

217

Is Your Device Identification Ready for New FFIEC Guidance?

Overview

Since the FFIEC guidance in 2005 on “Authentication in an Internet Banking Environment,” cybercriminals have evolved significantly, leading the FFIEC to release new guidance for protecting your business and your customers from fraud. Learn about smart device identification technologies banks will need to adopt to comply with the new FFIEC guidance and meet today’s challenges of widespread identity and password theft, botnets, trojans, coupled with new risks introduced by smartphones and the demise of cookies as an authentication method.

This session will address:

- What smart identification entails;
- The key limitations of simple identification methods;
- Why upgrades to current customer device identification are critical;
- How to initiate transaction authentication and monitoring.

Background

The recent release of FFIEC guidance on authentication heightens focus on the new wave of technologies required to keep up with increasingly sophisticated threats to online banking. However, even before the guidance was finalized, forward-thinking bankers were preparing themselves with new technologies for smart device identification.

The FFIEC’s 2005 guidance on “Authentication in an Internet Banking Environment” ushered in a first generation of device identification technologies. Since that time, cybercriminals have evolved to such a degree that they can decommission nuclear reactors, take down governments and steal billions in online consumer transactions. Yet many online bank accounts are still protected by first generation technologies consisting of little more than a password, a cookie and a simple hash of browser and IP attributes.

Customer device identification remains the most cost effective first perimeter of defense for customer authentication. In addition, banks will need to adopt cookie-less device identification technologies (smart device identification) as part of a multi-factor strategy to protect new account verification, login authentication and transaction authorization. In combination, these solutions will safeguard customer privacy, trust and convenience.



In this webinar, you’ll learn about the smart device identification technologies banks will need to adopt to comply with new FFIEC guidance, specifically, how they can address today’s challenges of widespread identity and password theft, botnets and trojans, as well as new risks introduced by smartphones and the demise of cookies as an authentication method.

All attendees will receive a complimentary copy of ThreatMetrix’ new whitepaper, “Is Your Device Identification Ready for the FFIEC: Smart Device Identification for Online Banking.”

Presented By

Alisdair Faulkner, Chief Products Officer, ThreatMetrix

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=217>

19

Maintaining Compliance with the Gramm-Leach-Bliley Act Section 501(b)

Overview

This workshop will present practical and proven approaches many institutions have adopted in order to comply with Section 501(b) of GLBA and Section 216 of Fair and Accurate Credit Transaction Act. In the course of this workshop, we will provide detailed “best practices” recommendations to help organizations achieve compliance in the following areas, including:

- Determining the board’s role in the creation and oversight of an information security program;
- How to evaluate your risk assessment process;
- How to manage and control risk;
- How to assess the measures taken to oversee third-party service providers.

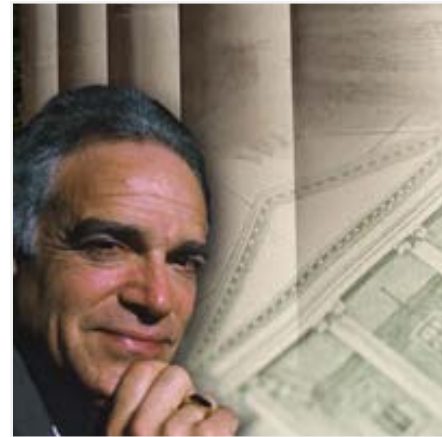
Background

In many ways, the most significant challenges presented by Section 501(b) are those that are non-technical, such as conducting an enterprise-wide information security risk assessment and the requirements to engage the board of directors in the ongoing management of operational risk. This workshop will expand on many of these areas and present practical and proven approaches many institutions have adopted in order to comply with Section 501(b) of GLBA and Section 216 of Fair and Accurate Credit Transaction Act.

FFIEC examination guidelines direct bank examiners to consider the specific review areas listed below. In the course of this workshop, we will provide detailed “best practices” recommendations to help organizations achieve compliance in each of the following important review areas, including how to:

- Determine the involvement of the board;
- Evaluate the risk assessment process;
- Evaluate the adequacy of the program to manage and control risk;
- Assess the measures taken to oversee service providers;
- Determine whether an effective process exists to adjust the program.

In a general memo released soon after GLBA became law, the Federal Deposit Insurance Corp. (FDIC) described to their



examiners that “the (GLBA) guidelines require each institution to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities. While all parts of the institution are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.” This comment succinctly described most of the significant information security challenges presented by GLBA Section 501(b). These challenges will be explored in this session.

Presented By

Susan Orr, CISA, CISM, CRP

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=19>

132

Massachusetts Privacy Law: A Guide to Understanding and Complying with this New Data Protection Standard

Overview

Irrespective of the state you operate in, this privacy law is applicable to any business extending credit to, or processing or storing data on customers in Massachusetts.

Now that the Massachusetts “Standards for the Protection of Personal Information” is in effect, it may well be the toughest privacy law in the nation - and perhaps the new “gold standard” for data security legislation.

Register for this newly refreshed webinar to learn:

- The latest details of the Massachusetts privacy standards;
- How these amended standards may impact your business or agency;
- The potential impact on federal privacy legislation.

Background

Does your business extend credit to or employ Massachusetts residents? Do you or your organization manage, store or process personal information on Massachusetts residents? If “yes,” then you need to be prepared for the Massachusetts “Standards for the Protection of Personal Information.”

Compared to most other state laws covering identity theft, the new Massachusetts “Standards for the Protection of Personal Information” - or Mass Privacy Law -- is sweeping in its scope and impact.

The types of businesses covered by the law are also expansive, since the standards apply to any organization, whether or not it’s located in Massachusetts, as long as it owns, licenses, stores or maintains “personal information about a resident of the Commonwealth.”

In terms of specific requirements, the standards are similar to existing federal laws such as the GLBA and HIPAA that require organizations to establish written information security programs to prevent identity theft. However, in a departure from federal regulations, the Mass Law also contains several detailed technology system requirements, especially for the encryption



of personal information sent over wireless or public networks or stored on portable devices.

This presentation is part of a new series of webinars created by Information Security Media Group to address major federal and state laws covering information security. Each presentation provides:

- An introduction to these specific laws and regulations;
- Detailed materials on the origins, scope, definitions and specific requirements;
- Description of how the laws will be enforced;
- Guidance on the impact of these provisions and what each organization can do to comply.

Presented By

Bill Sewall, Information Security, Compliance and Risk Management Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=132>

189

Meeting Federal Compliance to Secure Windows Desktops

Overview

The federal government mandates that agencies secure their computer desktops, but how can you ensure your lockdown policies are both effective and flexible? Register for this session to learn:



- Best practice tips to ensure your desktop security policies meet federal mandates;
- How to increase user performance on Windows desktops while reducing elevated privileges.

Background

Are you seeking flexible lockdown tips for securing your desktops? Not only are secure desktops a federal mandate for government agencies, but according to Gartner, organizations that properly secure their desktops can save \$1,237 per desktop.

Learn best practices to meet government compliance standards and effectively secure Windows desktops. Derek Melber, author, consultant, and trainer for many Fortune 500 companies on Active Directory, security and group policy, will lead this session focused solely on government agencies and their unique concerns.

In this session, you can learn:

- The benefits of removing administrator rights from end users;
- The combination of technologies needed for effective implementation of this level of security;
- How to best remove the local administrator account, while maintaining the users' access to all applications.

Also, discover how PowerBroker Desktops enables you to achieve government compliance by configuring all users as standard users and enables your users to get more done.

Presented By

Derek Melber, MCSE, MVP, Author of The Group Policy Resources Kit by Microsoft

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=189>

185

Protecting CUI: Federal Best Practices for Email Security, Archiving and Data Loss Prevention

Overview

E-mail continues to be one of the primary risk vectors of exposure of Controlled Unclassified Information and other sensitive data in federal organizations, but most have yet to deploy technology to help prevent costly breaches.



Register for this webinar to learn about:

- The importance of establishing clear and concise messaging policies in today's government enterprise;
- Understanding the results of the recent Task Force report and upcoming Presidential Directive on Controlled Unclassified Information (CUI);
- A summary of the requirements to establish effective data loss prevention (DLP) controls;
- NARA's definitions of, and correct retention policies for, Transitory and Federal Record electronic communications.

Background

The business of the U.S. Federal government presents unique challenges for IT administrators and information security professionals who support and secure complex IT infrastructures - while also meeting the numerous requirements of diverse user communities. As in most industries, e-mail is the most important communications channel, playing a primary role in information exchange, while also being a significant source of risks.

Join security expert Jeff Lake, VP of Federal Operations at Proofpoint, and learn how coming changes to requirements for handling CUI will affect federal agencies, review NARA's guidance on e-discovery for electronic mail archives, and understand how deploying an effective DLP solution can help you better secure private data and your overall e-mail infrastructure.

Presented By

Jeff Lake, VP - Federal Operations, Proofpoint

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=185>

212

PCI Compliance: Tips, Tricks & Emerging Technologies

Overview

Version 2.0 of the Payment Card Industry Data Security Standard is in effect, and already thought-leaders are reviewing emerging technologies and payment card security trends with an eye toward how they may impact PCI's future.

Meanwhile, the single biggest question on the minds of merchants, processors and service providers today is: How do I get - and stay - PCI compliant?

This panel will answer that question with an eye toward PCI's future, exploring:

- PCI's global influence on smaller merchants and service providers with limited IT resources and lack of security expertise;
- The role of emerging technologies such as encryption and tokenization;
- Tips and tricks to make a PCI compliance program a success.

Background

The Payment Card Industry Data Security Standard is a comprehensive standard intended to help organizations proactively protect customer account data.

Before PCI was created, credit card merchants had individual means for organizations to secure customer data. Organizations were forced to perform similar audit reviews for each type of merchant card.

PCI is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

Version 1.0 of the PCI standard was released in Dec. 2004. It subsequently was updated in 2006, 2008 and 2009. Version 2.0 of the PCI standard was announced in late 2010 and went into effect in Jan. 2011.

In November of 2008, payments processor RBS WorldPay was hacked, and fraudsters gained access to as many as 1.5 million consumer accounts.



Then, on Inauguration Day 2009, Heartland Payment Systems (HPY) disclosed that it had been breached, exposing an estimated 130 million credit and debit card holders to potential fraud in what is the largest data compromise ever reported. Heartland maintained it was PCI compliant. But Visa subsequently removed Heartland and RBS WorldPay from its list of PCI compliant vendors until they could be re-assessed for compliance.

The RBS WorldPay and Heartland security breaches raised serious questions about organizations achieving PCI compliance, but still suffering such incidents: How does one attain and sustain PCI compliance?

This question will be explored in this panel discussion, as will:

- What is in scope and out of scope in terms of PCI compliance?
- How can Managed File Transfer help companies achieve PCI compliance?
- How can PCI compliance help an organization consolidate its data security tools?
- How does an organization secure data beyond PCI?

Presented By

Tom Field, Editorial Director, Information Security Media Group

Anton Chuvakin, Author, PCI Expert

André Bakken, Director - Product Management, Ipswitch

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=212>

18

Preparing for an Information Technology Regulatory Exam

Overview

- A look at what the regulatory agencies base IT exams on and how your institution can be best prepared;
- Preparing for the pre-examination IT Questionnaire and the effect your responses will have;
- How do GLBA Section 501(b), the Bank Secrecy Act, Patriot Act and FACTA figure into a regulatory IT exam.

Background

The banking regulatory agencies examine banking practices, including information technology, at the banking institutions they oversee on a periodic basis. In this workshop, you will hear about the basic tenets behind the Information Technology examinations conducted by regulatory agencies and how the preliminary information gathered is applied in choosing appropriate work programs and in identifying the necessary examiner IT skill and experience necessary for conducting each exam. Further, this workshop will prepare the attendees in responding to the pre-examination IT Questionnaire in the most appropriate manner.

Even though the technological advances in the banking sector have been ever-evolving for decades, the last few years have been noteworthy with the advent of the Internet-based banking technologies and a myriad of outsourcing arrangements with Technology Service Providers. On one hand these advances have leapfrogged at the pace banking services are being offered by institutions of ALL sizes, while on the other - it has created a management challenge. In order to keep up with the changing environment and the market conditions, the Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook, which was developed through a collaborative effort of the FFIEC's five member agencies, replaced the 1996 FFIEC Information Systems Examination Handbook. The FFIEC issued the initial 12 booklets that make up the FFIEC IT Examination Handbook. The topics of these booklets include:

- Business Continuity Planning;
- Development and Acquisition;
- Electronic Banking;
- Fedline®;
- Information Security;
- IT Audit;
- IT Management;



- Operations;
- Outsourcing Technology Services;
- Retail Payment Systems;
- Supervision of Technology Service Providers; and
- Wholesale Payment Systems.

These booklets address significant changes in technology since 1996 and incorporate a risk-based examination approach. The Information Security booklet was updated recently in July of 2006.

During the course of this workshop, the attendees will gain an understanding of how the regulatory examinations are based on the concepts and guidance provided in these booklets. We will also discuss how the banking rules and regulations, including GLBA Section 501(b), Bank Secrecy Act, Patriot Act and FACTA among others, are taken into account during the Information Technology examinations.

Based on the preliminary information provided by an institution on the technology in use and the applicable practices, and the information available on the previous examinations, bank examiners develop an initial scope for each IT exam. However, examiners have considerable discretion to expand or contract the scope once onsite, and to utilize any agency-specific or FFIEC approved work program targeting specific technologies or functions (wire transfer systems, ACH, etc.).

Presented By

Susan Orr, CISA, CISM, CRP

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=18>

227

Protect Data in the Cloud: What You Don't Know About the Patriot Act

Overview

As banking institutions seek tremendous cost savings from cloud infrastructure and services, two key factors must be considered: The Patriot Act, which has strict stipulations regarding access to data and where it is stored, and the protection of data - even from third-party service providers.

This webinar explores what these security topics mean to financial institutions:

- The impact from the newly-extended Patriot Act re: sensitive data in the cloud;
- Risks to consumer information stored in the cloud from third parties;
- How to address data sovereignty issues with cloud computing infrastructure.

Background

The virtual nature of cloud computing opens up cost savings that are difficult to ignore, yet two orthogonal but perhaps complimentary issues make having a cohesive data security strategy dramatically more complex.

The first is the recently extended U.S. Patriot Act which provides for sweeping abilities for law enforcement to access data stored in U.S. data centers - regardless of geography. Often in conflict with local, e.g. European Union Data Protection legislation, there are complex issues ahead concerning the protection of data as it crosses international boundaries.

The second issue is that of protecting the data stored in cloud infrastructure - with its virtual nature - it's not possible to know necessarily where a piece of data is being stored in the cloud - nor is it always clear who exactly at the third-party service provider has access to that data.

The question becomes, is it possible to have a strategy where data from international jurisdictions can be stored in the cloud while retaining clear lines of separation? Similarly, is it possible for enterprises to control their data stored in a third-party cloud without knowing exactly where it is?



It turns out that some new advances in key management could help resolve both these scenarios. By using some common examples, e.g. "How to protect sensitive emails in Microsoft BPOS/Office 365 Environments" and "How to enforce sovereignty of data stored in a cloud based infrastructure," we'll help uncover:

- The specific threats to data in the cloud;
- How to segregate data using encryption keys;
- How to protect and control data stored in the cloud.

Presented By

Wasim Ahmad, VP - Marketing, Voltage Security

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=227>

97

Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors



Overview

In the face of regulatory requirements and emerging security threats, banking institutions must consider the policies and procedures necessary for proper retention of audit reports, papers and logs.

Register for this webinar for an overview of the contractual, legal and regulatory compliance requirements for retention of audits, logs and third-party created documentation and reports. Among the key points covered:

- What you need to know about regulatory requirements for record retention;
- How to identify the records retention risks for financial institutions and third-party service providers;
- How to mitigate those risks.

Background

Given the legal and regulatory requirements related to record retention policies - particularly considering such scandals as Enron and WorldCom in the United States - the importance of records retention is in the limelight.

As outsourcing is now commonplace for financial institutions, it's key to consider: When you entrust business partners with your company's confidential data, you place all control of security measures completely into their hands. But:

- Do you know what they are doing with the logs generated as a result of the activities you outsourced to them?
- Do you know what they are doing with the reports that relate to your business?
- Do you know their records retention practices?

As an effect of many recent laws and regulations, it is also common to have third parties perform audits, risk assessments or vulnerability assessments. What happens to these reports following the audit or assessment? How long is it reasonable for the third party to retain your report? What do regulations require with regard to retention?

In this exclusive webinar, noted privacy expert Rebecca Herold will lead a discussion of what financial institutions should know

about the requirements for retaining data, logs and audit reports, as well as the related risks involved with entrusting third parties to retain records for the activities that have been outsourced to them.

Among the points Rebecca will discuss include:

- Retention responsibilities for financial institutions;
- Types of data and reports for which financial institutions and vendors have retention responsibilities;
- Risks involved with data retention within financial institutions and with their business partners;
- Ways to mitigate those risks.

Presented By

Rebecca Herold, CEO, The Privacy Professor

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=97>

261

Risk Assessment Framework for Online Channel: Learn from an Expert



Overview

As part of the updated FFIEC Authentication Guidance, U.S. banking regulators mandate that financial institutions conduct periodic risk assessments of their electronic banking services.

But in the face of evolving threats, a growing online customer base and emerging mobile technology, what's the most effective and flexible framework for conducting regular risk assessments?

Join Joe Rogalski, information security officer at First Niagara Bank, as he details:

- How and when to conduct your risk assessments and meet regulators' expectations;
- How to adapt your internal controls based on what you glean from your periodic risk assessments;
- Case study of his own bank (\$44 billion in assets) and how it responded to the results of its most recent risk assessment.

Background

Risk assessments are the foundation of risk management and information security, and since 2005 U.S. banking regulators have urged institutions to conduct periodic risk assessments of their online banking products and services.

But institutions failed to follow that guidance, and as a result they and their customers were victimized by sophisticated schemes such as ACH/wire fraud and corporate account takeover.

These high-profile fraud incidents helped inspire 2011's updated FFIEC Authentication Guidance, which re-enforces regulators' expectations of periodic risk assessments. Specifically, the guidance says:

"Financial institutions should review and update their existing risk assessments as new information becomes available, prior to implementing new electronic financial services, or at least every twelve months. Updated risk assessments should consider, but not be limited to, the following factors:

- Changes in the internal and external threat environment, including those discussed in the Appendix to this Supplement;
- Changes in the customer base adopting electronic banking;

- Changes in the customer functionality offered through electronic banking; and
- Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry."

In this session, Joe Rogalski, VP and information security officer at New York's First Niagara Bank (\$44 billion in assets), will detail how his institution conducts period risk assessments, including:

- An overview of the FFIEC guidance and what examiners will expect to see in your approach to risk assessments;
- How to conduct an effective risk assessment, including qualitative and quantitative approaches;
- What to do about risks, vulnerabilities and threats identified in your assessments.

Presented By

Joe Rogalski, SVP, First Niagara Bank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=261>

282

Risk Management: New Strategies for Employee Screening

Overview

As part of your risk management strategy, your organization likely conducts pre-employment background checks. But what are your screening strategies after you have made your hires? How would you know, for instance, if:

- An employee's personal finances have crumbled, and that individual is now at risk to embezzle;
- New evidence reveals a senior executive has blatantly falsified academic credentials;
- You uncover a past criminal offense by a current employee - do you have policies to deal with the situation?

Like risk management itself, background screening must be ongoing. In this session, attorney Lester Rosen, renowned expert in employment screening, presents post-hire screening strategies, including:

- How to conduct continual screening of key employees;
- What to do about newly-acquired employees in a merger or acquisition;
- How to proceed when you do uncover past criminal offenses or falsified credentials of current employees.

Additionally, Rosen will offer updates on the latest guidance on use of arrest and conviction records, as well as the do's and don'ts of social media in background screening.

Background

All employers, as part of their risk management strategy, have an obligation to exercise a reasonable duty of care in hiring. In addition, many organizations have a legal duty to not employ individuals with certain enumerated criminal records. There are a number of steps that employers can take in the hiring process to reduce their risk when hiring. But what about after hiring? What role does background screening play in an organization's ongoing risk management framework?

Recently, a prominent online organization made embarrassing headlines with news that its CEO had misrepresented his academic credentials on his resume. Elsewhere, a major U.S. bank fired a longtime employee after a background check revealed two 40-year-old shoplifting arrests.

Incidents such as these - and today's heightened sensitivity to the risks of the insider threat - force organizations to redefine their



screening strategies as part of their risk management approach. No longer is the focus solely on pre-hire background screening. Increasingly, organizations are engaging in continual screening to catch anomalous activity that could be a precursor to actionable behavior. And they also are embracing policies and procedures to handle damaging data when it comes to light about current or acquired employees.

Topics to be discussed in this session include:

- A brief overview of the latest screening trends, including the EEOC's new guidance on the use of arrest and conviction records;
- How to conduct continual screening;
- What to do when you learn about past criminal offenses or falsified credentials of a current employee;
- Proper screening procedures for newly-acquired employees in a merger or acquisition;
- Social media - its proper role in a screening strategy.

Presented By

Lester Rosen, Attorney & President - Employment Screening Resources

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=282>

102

Risk Management, Continuity and Compliance - What All Financial Organizations Need to Know

Overview

Attend this webcast and learn:

- How business results are impacted by ever-higher operational performance requirements;
- What leading institutions are doing to meet regulatory challenges while still achieving business goals;
- How to use technology efficiently in serving the many masters operations, compliance, risk and the marketplace.



Background

Global events and the credit crisis require that financial institutions of all stripes must continue to improve efficiency in the face of regulatory, risk management and business compliance requirements.

Attend this short but important webcast where Rodney Nelsestuen, Research Director for Tower Group, the leading research firm exclusively focused on the financial industry, will share with you best practices deployed by the most successful financial institutions.

Presented By

Rodney Nelsestuen, Research Director, Financial Strategies and IT Investments, Tower Group

Bill Hammond, Director of Product Marketing, Vision Solutions

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=102>

193

Social Networking Compliance for FINRA Regulated Organizations

Overview

Now you can maintain FINRA compliance across Facebook, LinkedIn, Twitter and over 1000 social networks. The secrets are shared during this exclusive webinar.



Control and compliance are key to social media survival in today's regulated industries. So you need a solution for true compliance.

This exclusive webinar will explore the requirements of FINRA with regard to social networking - and how Socialite, a new social media compliance solution from FaceTime Communications, helps you meet them.

- Content and activity archiving;
- Content moderation controls;
- Granular control of features and content;
- Display context of messages posted;
- On-premise, SaaS, or hybrid deployment options.

Background

View this specifically designed webinar for FINRA-regulated organizations. You'll get details on how to securely use social networks, while maintaining FINRA compliance and IT best practices.

- Apply granular controls to Facebook, LinkedIn and Twitter, based on the employee's role in your company;
- Use social networking to engage prospects and build relationships, while maintaining a professional code of ethics;
- Monitor employee social media activity in real time, and block unwanted messages from being posted.

This webcast is critical for financial services companies interested in leveraging social media, while maintaining compliance.

Presented By

Sarah Carter, VP - Marketing, FaceTime Communications

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=193>

263

The FFIEC Guidance: What You Need to Know Now About Out-of-Band Authentication

Overview

As bank examiners begin applying the updated FFIEC Authentication Guidance, many financial institutions will find that their current security practices do not stand up against the strengthened requirements. Arm yourself with the knowledge you need to begin shoring up your authentication controls before your next bank exam.

Register for this webinar from out-of-band authentication provider PhoneFactor to learn:

- Why many of the security measures currently in place are ineffective at protecting against current online banking threats;
- The role of out-of-band authentication and transaction verification as security controls;
- How First Midwest Bank put the FFIEC's recommendations in place, switching from security tokens to out-of-band transaction verification with great success.

Background

The 2011 supplement to the FFIEC Guidance on Internet Banking Security provides an updated view of best practices for securing online banking based on today's threat landscape. The concepts addressed in the supplement are widely recognized by the financial services industry to be critical to preventing online banking fraud.

Examiners began using these enhanced expectations beginning in January 2012. These include:

- **Layered Security:** The concept of layered security extends security controls beyond the initial session login to include online banking transactions and administrative functions. This is driven by an increase in real-time attacks that target transactions, such as ACH, wire transfer and payroll payments. A high level of importance has been placed on identifying suspicious transactions. To minimize the impact on customers, this must be coupled with an easy and effective means for customers to approve legitimate transactions. For many, this involves migrating away from OTP tokens, which the FFIEC points out have proven to be vulnerable to attack. Instead, financial institutions will need to look to methods like fully



- out-of-band technologies that can be used to verify logins, transactions and administrative functions and offer protection from keyloggers and MITM/MITB attacks.
- **Stronger Authentication Methods:** In addition, the updated guidance calls for an overall strengthening of authentication technologies. It notes that out-of-band authentication has taken on a new level of importance given the preponderance of malware running on customer PCs, which can defeat OTP tokens, device identification, challenge questions and many other forms of strong authentication. In particular, closed loop methods that complete the authentication in an out-of-band channel are seen as offering a greater level of security.

This webinar will present real-world examples, starting with a case study from First Midwest Bank, of how financial institutions can leverage out-of-band transaction verification to meet the strengthened requirements set forth in the updated Guidance before their next bank examination.

Presented By

Sarah Fender, VP - Marketing & Product Management, PhoneFactor

Steve Dispensa, CTO & Co-Founder, PhoneFactor

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=263>

181

Threat Detection, Compliance & Incident Response

Overview

Combining and correlating data to meet specific regulatory compliance requirements can prove cumbersome for financial institutions. Combining that data along with real-time threat detection and analysis, and working it into an incident response plan, can prove nearly impossible.

Register for this webinar for insights on:

- How to detect, in real-time, a variety of threats by managing logs, events, databases, and applications;
- Preparing an incident response plan based on advanced analytics and detailed forensics;
- Reducing the manual processes many financial institutions go through when trying to convey compliance with industry regulations;
- Unifying compliance and operations using Security Information and Event Management (SIEM).

Background

Compliance and security are often viewed as two distinct challenges that financial services organizations must address. Multiple regulatory compliance requirements, including PCI-DSS, GLBA and SOX, require the monitoring, collection, archiving and analysis of activity logs from computing and network infrastructure. Organizations typically address these requirements with costly and time-consuming manual processes that are able to capture and store the needed data and generate the minimum set of reports needed to satisfy basic compliance mandates.

Automating these processes can provide effective controls that dramatically increase efficiency of the IT staff and enable them, for the first time, to integrate compliance data with other information as part of their threat detection and incident response processes. Combining and correlating additional data like user activity, real-time events, network flows, session information and application layer data provides the added visibility and deep insight to identify the ever-increasing range of threats and malware relentlessly attempting to penetrate the defense in depth architectures of financial institutions.

Advanced security information and event management (SIEM) technology readily addresses both the scheduled monitoring and reporting needs of compliance officers and the real-time analysis



82% of respondents say they first learn of a fraud incident when they're notified by a customer.

*Source: ISMG's Faces of Fraud Survey 2012

and response demands of security operations center analysts. Pragmatic approaches to the implementation and operations of SIEM solutions can quickly bring these powerful solutions on-line and deliver actionable intelligence that reduce risk.

Presented By

Mel Shakir, CTO, NitroSecurity

Kostas Georgakopoulos, VP & Head of Information Security, Bank of China, USA

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=181>

73

Top IT Compliance Challenges: Who's Touching Your Data and What Are They Doing With It?

Overview

Join in this tactical discussion of how financial institutions are using new technologies to successfully prevent, identify and respond to security threats, no matter where they originate.

- Learn how to identify, prevent and rapidly respond to user threats and data breaches;
- Find out how, while mitigating security threats, you can work towards compliance for PCI and other key mandates.

Do you really know who is accessing your critical data? Do you really know where threats to your data security originate? This webcast features Paul Reymann, one of the nation's leading financial institutions regulatory experts and co-author of Section 501 of the Gramm-Leach-Bliley Act Data Protection regulation.

Background

Today's headlines confirm what will happen to your institution if it does not have effective IT security systems. Financial institutions suffer serious consequences - from stolen customer data and intellectual property to powerful viruses and other malware. Not only are business operations interrupted, but corporate security failures lead to damaged or lost trust, substantial financial loss and lost revenues, as well as high forensics and remediation costs. In addition, PCI, GLBA and SOX mandates present a complex challenge for securing massive amounts of customer data, monitoring complex applications and managing large numbers of users.

To successfully manage threats and compliance challenges, financial institutions need a comprehensive security strategy that can successfully do battle with inside - and outside - threats. Institutions must implement practices that identify, prevent and respond to potential threats and ensure a limited need-to-know access policy.

Companies increasingly leverage new threat-monitoring technologies to build a clean, concise and manageable process for dealing with the tremendous volumes of raw security information from disparate devices, applications and databases.



This webinar examines the key threats financial institutions face today, and how to gain the actionable security intelligence that is required to enable sound risk management and compliance.

Presented By

Paul Reymann, CEO, The Reymann Group

Bob Flinton, VP Product Marketing, netForensics

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=73>

231

Vendors' Guide to the FFIEC Authentication Guidance

Overview

For banking institutions, the release of the 2011 FFIEC Authentication Guidance is a game-changer, handing down new standards for layered security controls, risk assessments, authentication techniques and customer awareness. But what does all this mean to technology vendors and third-party service providers? Attend this session to understand new demands on banking institutions, as well as expert insight on:

- Key tenets of the new guidance and how they may impact banking institutions' technology investments;
- The unique security/risk management challenges facing institutions of all sizes;
- Differences between security controls for commercial and consumer accounts;
- What banking/security leaders need to do to prepare for 2012 regulatory exams.

Background

The Federal Financial Institutions Examination Council has formally released the long-awaited supplement to its "Authentication in an Internet Banking Environment" guidance, which was first issued by the FFIEC in October 2005. Formal assessments for compliance with the new guidance will begin in January 2012.

The purpose of the supplement is to reinforce the risk-management framework described in the original guidance and update the FFIEC member agencies' supervisory expectations regarding customer authentication, layered security, and other controls in the increasingly hostile online environment.

The official supplement highlights the need for:

- Better risk assessments;
- Effective strategies for mitigating known online risks;
- Improved customer and employee fraud awareness.

In this exclusive session, Philip Alexander, information security officer at a major U.S. financial institution, will discuss exactly what technology vendors need to know about the FFIEC guidance and how it impacts their banking customers. Among the topics he will discuss:



- Risk assessments and layered security - what they mean to banking institutions in the context of the guidance;
- Strategies for protecting online banking customers - commercial and consumer;
- Emerging challenges such as mobile banking;
- How you can help your banking customers prepare for 2012 regulatory exams.

Presented By

Philip Alexander, CISSP - ISSMP, MCSE - MCT, MPA

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=231>

154

Anti-Money Laundering: The Investigator's Guide to the Laws

Overview

Money-laundering is one of the most common and complex financial crimes to be committed. Learn exactly what you need to know about the specific statutes and regulations that govern the crime.

Register for this webinar to receive first-hand advice from a veteran anti-money laundering investigator on:

- Key anti-money laundering laws;
- Penalties for money-laundering crimes;
- How your organization can best respond to money-laundering mandates, whether as an investigator or a regulated entity.

Background

Money laundering is the criminal practice of filtering “dirty” money through a series of transactions, so the funds are “cleaned” to look like proceeds from legal activities. The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA), and its implementing regulation, 31 CFR 103, is the main regulatory tool the U.S. government uses to fight drug trafficking, money laundering and other crimes. Law enforcement agencies and financial services organizations of all sizes must be conversant with the letter of this law.

Whether you're a banking executive filing a Suspicious Activity Report, a compliance officer monitoring BSA compliance or a government agent assigned to investigate money-laundering crimes, this BSA overview is applicable.

In this session, Kevin Sullivan, a former investigator with more than 20 years experience in anti-money laundering (AML), shares his insight and understanding of AML legislation, including:

- BSA;
- Money Laundering Control Act;
- Annunzio Wiley Act;
- Money Laundering Suppression Act;
- Wire Transfer Regulations;
- Patriot Act.

In addition to walking through these regulations, Sullivan will discuss money-laundering penalties, the basics of an AML program, as well as regulations governing the establishment of Customer Identification Programs (CIP), which organizations



must implement for identifying and verifying the identity of customers.

This legislative overview is a perfect introduction to the basics of anti-money laundering.

Presented By

Kevin Sullivan, Investigator, New York State Police

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=154>

153

Anti-Money Laundering: The Practitioner's Guide to the Laws

Overview

Money-laundering is one of the most common and complex financial crimes to be committed. Learn exactly what you need to know about the specific statutes and regulations that govern the crime.

Register for this webinar to receive first-hand advice from a veteran anti-money laundering investigator on:

- Key anti-money laundering laws;
- Penalties for money-laundering crimes;
- How your organization can best respond to money-laundering mandates, whether as an investigator or a regulated entity.

Background

Money laundering is the criminal practice of filtering “dirty” money through a series of transactions, so the funds are “cleaned” to look like proceeds from legal activities. The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA), and its implementing regulation, 31 CFR 103, is the main regulatory tool the U.S. government uses to fight drug trafficking, money laundering and other crimes. Law enforcement agencies and financial services organizations of all sizes must be conversant with the letter of this law.

Whether you're a banking executive filing a Suspicious Activity Report, a compliance officer monitoring BSA compliance or a government agent assigned to investigate money-laundering crimes, this BSA overview is applicable.

In this session, Kevin Sullivan, a former investigator with more than 20 years experience in anti-money laundering (AML), shares his insight and understanding of AML legislation, including:

- BSA;
- Money Laundering Control Act;
- Annunzio Wiley Act;
- Money Laundering Suppression Act;
- Wire Transfer Regulations;
- Patriot Act.

In addition to walking through these regulations, Sullivan will discuss money-laundering penalties, the basics of an AML program, as well as regulations governing the establishment of Customer Identification Programs (CIP), which financial



institutions must implement for identifying and verifying the identity of customers.

This legislative overview is a perfect introduction to the basics of anti-money laundering. Other webinars by Kevin Sullivan explore:

- BSA Compliance: How to Conduct an Anti-Money Laundering Investigation;
- Expert's Guide to Suspicious Activity Reports (SARS): Tips to Avoid Regulatory Pitfalls & Penalties;
- Money Laundering Update: The Latest Threats to Your Institution.

Presented By

Kevin Sullivan, Investigator, New York State Police

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=153>

59

Anti-Money Laundering/Fraud Convergence: Why Should I Care?



Overview

During this discussion, attendees will learn:

- What analytics are similar/different in anti-money laundering and fraud;
- Trends for enterprise-wide case management and the combination of anti-money laundering and fraud prevention;
- What the integration areas and data requirement issues are;
- Latest developments in investigations and operations.

Background

The financial industry has started to see a convergence of anti-money laundering and fraud. How will that affect the way financial institutions handle fraud and anti-money laundering in the future? How will that affect you and your company?

This session will take a deep dive and uncover key hidden connections in anti-money laundering and fraud. We will also take a look at the similarities in function, challenges and technology used to combat this.

Many financial institutions have seen the tremendous value add in combining their anti-money laundering and fraud units. What have they combined and how will that help you? This change in the way of combining and fighting anti-money laundering and fraud is gaining in popularity in financial institutions.

Presented By

Amir Orad, Cybersecurity Expert

Neil Katkov, Manager, Asia Research Group, Celent

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=59>

80

BSA Compliance: How to Conduct an Anti-Money Laundering Investigation



Overview

Money laundering is one of the most frequent and frequently-evolving crimes against financial institutions, and regulatory compliance with the Bank Secrecy Act (BSA) is one of the prime directives for banking/security professionals. Register for this webinar to get hands-on advice from a veteran AML investigator on:

- Trends in money-laundering crimes;
- How to conduct an AML investigation;
- Responding to requests from law enforcement.

Background

In March of this year, we saw the Governor of New York fall victim to a scandal that came to light primarily because of banks' anti-money laundering (AML) practices. This huge news story put the focus on a crime that typically is out-of-sight of consumers, but top-of-mind for banking institutions.

Money laundering is the criminal practice of filtering "dirty" money through a series of transactions, so the funds are "cleaned" to look like proceeds from legal activities. The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA), and its implementing regulation, 31 CFR 103, is the main regulatory tool the U.S. government uses to fight drug trafficking, money laundering and other crimes.

BSA requires that all AML personnel have training. This webinar covers some of the key training areas, including:

Money Laundering: The Good, the Bad and the Ugly - the latest trends and patterns that the professional money launderer is concentrating on, i.e.:

- ATMs
- Virtual laundering
- Hawalas
- Micro-structuring

Conducting AML Investigations - Understand the basics of how and when to undertake an investigation. Techniques include:

- Dynamics of investigations

- When to conduct an investigation
- Interviewing techniques
- Reporting

Responding to Law Enforcement Requests - Law enforcement at some point will be drawn to your institution during the course of an investigation. Understand how law enforcement gathers evidence and what you can do to properly respond to requests. Topics include:

- Subpoenas
- National security letters
- Supporting documentation requests
- Section 314a information requests

Presented By

Kevin Sullivan, Investigator, New York State Police

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=80>

86

Expert's Guide to Suspicious Activity Reports (SARs): Tips to Avoid Regulatory Pitfalls & Penalties



Overview

At the heart of the Bank Secrecy Act and the core of any good anti-money laundering program is the suspicious activity report (SAR), which all financial institutions - banks, credit unions, brokers, casinos, insurance companies, etc. - must file when confronting questionable transactions. Register for this webinar for exclusive, hands-on advice from a veteran AML investigator who reviews thousands of SARs each month. Gain insight on how to satisfy regulatory requirements with your SARs, including:

- When a SAR must be filed;
- How to properly complete a SAR;
- SAR writing guidelines and etiquette;
- Where/how to file your SAR.

Background

Under terms of the Bank Secrecy Act, there currently are hundreds of thousands of financial institutions subject to BSA reporting and record keeping requirements, for which the Financial Crimes Enforcement Network (FinCEN) is authorized responsibility. These include:

- Depository institutions, e.g., banks, credit unions and thrifts;
- Brokers or dealers in securities and/or futures;
- Money services businesses (MSBs) [e.g., money transmitters; issuers, redeemers and sellers of money orders and travelers' checks; check cashers and currency exchangers];
- Casinos and card clubs;
- Insurance companies;
- Mutual funds.

Whenever one of these institutions encounters questionable financial activity - a deposit or withdrawal in excess of \$10,000, for instance - it is supposed to file a suspicious activity report, or SAR. These SARs routinely uncover suspected money-laundering activities.

According to FinCEN's publication, The SAR Activity Review, over 4.7 million SARs were filed with FinCEN between 1996 and June 30, 2007. An interesting trend to note: Since January 1, 2003, filings by non-depository institutions - casinos, insurance companies,

etc. - have grown to encompass a greater portion of the SARs filed. In 2001, 96 percent of the SAR database consisted of depository institution suspicious activity reports; today's figure is 64 percent.

Writing an effective SAR to meet regulatory requirements is an essential skill for a financial institution.

In this exclusive webinar, hear from Kevin Sullivan, a renowned AML expert and veteran investigator who has 20 years of police experience and who reviews as many as 4000 SARs per month.

Listen to Sullivan's practical, hands-on advice to help your institution determine:

- Who needs to file these reports?
- When should a SAR be filed?
- What are the reasons to file them?
- How to complete a proper and quality SAR;
- Suitable SAR narrative writing guidelines and appropriate SAR etiquette.

From his years as a state investigation coordinator, you will hear the unique perspective of someone who has seen how all financial institutions prepare their SARs. Sullivan will detail some of the methods that law enforcement use while gathering financial intelligence, such as:

- Desktop bounty hunting;
- Pro-active targeting;
- SAR review meetings.

Presented By

Kevin Sullivan, Investigator, New York State Police

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=86>

116

Money Laundering Update: The Latest Threats to Your Institution



Overview

Mobile Payment Systems, Social Media, Facebook and LinkedIn. These are among the targets of the modern-day money launderer, and it behooves your institution to understand and prepare for them. Register for this webinar to hear directly from money-laundering investigator Kevin Sullivan on:

- The rise of trade-based money laundering, including trade price manipulation and Internet/mobile payment systems;
- The return of classic crimes - how to spot new attempts at old schemes such as ATM's, shared value cards and micro-structuring;
- What you need to know about the risks of money-laundering in virtual communities such as Second Life.

Background

Money laundering is the criminal practice of filtering "dirty" money through a series of transactions, so the funds are "cleaned" to look like proceeds from legal activities. The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA), and its implementing regulation, 31 CFR 103, is the main regulatory tool the U.S. government uses to fight drug trafficking, money laundering and other crimes.

BSA requires that all AML personnel have training. In earlier sessions, we've shown you how to conduct an AML risk assessment, how to conduct a basic money-laundering investigation and we've offered best-practices in preparing Suspicious Activity Reports (SARS).

This webinar covers some of the key new trends in money-laundering, including:

- Virtual Money Laundering - We all know Second Life and other virtual communities are hot spots for people who want to interact socially, play games and even sell/purchase goods and services. But the virtual world is also a playground for the money-launderer, who can commit real fraud in communities with minimal authentication and regulation. Learn how to avoid being tied up in virtual money laundering;
- Trade-Based Money Laundering - U.S. Customs officials define trade-based money laundering as the use of trade to legitimize, conceal, transfer and convert large quantities of illicit cash into less conspicuous assets or commodities. Learn how fraudsters

are practicing this crime via trade price manipulation, Internet/mobile payment systems and digital precious metals;

- Classic Crimes Revived - With the rise of money-laundering crimes, many old schemes are being dusted off and updated. Among them:

- » Shared Value Cards - Prepaid and gift cards have become commonplace in the retail environment, but these cards have no direct ties to individual bank accounts, making them rife for fraud - especially in overseas transaction. Pick up the warning signs of potential fraud;
- » Privately-Owned ATMs - There are 1.6 million ATMs in the world - more than 400,000 in the U.S. alone - and 49 billion ATM transactions annually. How many of them are fraudulent? And what are the warning signs you should look for to indicate potential money-laundering via ATMs? Get the scoop on this complicated network of deceit;
- » Micro-Structuring - Structuring is the old crime of making money deposits that just miss the threshold of suspicious activity within a banking institution (i.e. a transaction of under \$10,000). Micro-structuring is an attempt to get around transaction-monitoring systems by making even smaller deposits that skirt the detection rules embedded in the software systems. Learn how to prevent this tough-to-detect crime.

Presented By

Kevin Sullivan, Investigator, New York State Police

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=116>

27

Business Continuity Planning Best Practices

Overview

Around the globe, natural disasters and man-made incidents and attacks have directly disrupted business operations across all industries. Having a definitive plan and response technique is essential to remain viable, especially in today's rough economic climate. Register to ensure your team is prepared. Session education includes:

- How to develop a comprehensive and strategic plan;
- Key components of a business continuity plan;
- How to avoid common mistakes.

Background

Vital to any critical industry is good business continuity planning where the impacts of delays can be more readily quantified. The need for effective business continuity planning is well-understood by business/security leaders. However, a rise in business interruptions due to natural disasters and other activities has brought the need for business continuity plan development and maintenance to the fore-front.

During the course of this workshop, the attendees will gain an understanding of some of the key requirements for business continuity and disaster recovery. Topics such as the overall planning framework, business impact analysis, operational recovery requirements, recovery strategies, plan development, testing and feedback mechanism and delivering awareness and training throughout an organization will be discussed. The speaker will expand on other topics that were not of any significant concern until very recently, such as terrorist activities and surviving a pandemic flu.

Service disruptions, delays in responding to customer requests, inability to process transactions in a timely manner or being able to resume business in face of a disaster can have a significant impact on an organization's well-being. Recent natural disasters as well as terrorist activities have shown that an organization's resilience to a disaster and being able to resume business was directly related to its preparedness to respond to unforeseen events.



Presented By

Tom Walsh, CISSP, President - Tom Walsh Consulting

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=27>

96

Business Continuity Risk Assessment & Resource Allocation

Overview

Nearly every organization is required to have a business continuity plan. Yet, planners often overlook issues related to resource allocation -- the "people, places and things" necessary for business continuity. Register for this webinar for case studies and insight on how to:

- Identify and describe the components that are most likely to be affected during a disaster;
- Conduct a risk assessment that emphasizes effective resource allocation strategies;
- Assess the impact of this risk assessment upon the organization and its resources;
- Design or recommend appropriate changes to the organization's existing resource allocation process.

Background

Having an institution-wide business continuity (disaster recovery) plan is a regulatory requirement for financial institutions and a must-have for government agencies. Your organization's BCP creates the foundation for your prevention and recovery efforts for both "traditional" and "non-traditional" disasters, including a pandemic. What organizations often overlook are the issues relating to resource allocation - the necessary "people, places and things" that are identified during the risk assessment process. The organization must maintain realistic and practical solutions to resolving the critical resource allocation issues that are likely to impact it, including:

- People: Employees, insiders, affiliated parties (and their families), customers, vendors and third-party service providers;
- Places: Facilities that the organization owns, manages, maintains, leases or controls;
- Things: Assets, equipment, supplies, records and documents.

Register for this session to learn disaster prevention and business recovery strategies, planning techniques and action tactics that you can use to create or modify your organization-wide business continuity plan. You will also learn how to identify the real sources of loss exposure during a disaster; the obvious and not-so-obvious methods for using your resources effectively before and during any type of disaster; and the most successful methods for reinstalling



all of your organization's components in the shortest amount of time.

Among the topics to be discussed:

- How does a disaster plan differ from a pandemic plan?
- What resource allocation issues should the business continuity plan address?
- Your institution's business continuity scenario test;
- Business continuity planning & implementation guidelines;
- Hypothetical disasters: Could these happen to you?

Presented By

Dana Turner, Security Practitioner, Security Education Systems

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=96>

95

Business Impact Analysis — How to Get it Right



Overview

A business impact analysis is an integral part of developing a business continuity plan for any type of disaster, and the Federal Financial Institutions Examination Council has released recent guidance about enhancements to the BIA and testing discussions.

Register for this webinar to learn:

- Updated regulatory requirements for a business impact analysis;
- How to conduct an effective BIA;
- How to improve business continuity/disaster recovery planning through the BIA process.

Background

What if there was a terrorist attack, ala Sept. 11, and your institution could not create and deliver account statements in an acceptable timeframe? Potentially damaging to your business.

Or, say, if there was a natural disaster that disabled a key vendor that manages your Internet banking system - what impact might that loss have on you and your customers?

Business impact analysis is a necessary - and often overlooked - part of business continuity/disaster recovery planning. Done right, a BIA needs to look at the consequences that could result from an interruption in core elements of the banking institution's infrastructure - both within the institution and within the elements controlled by third-party service providers.

According to the latest update to the FFIEC's Business Continuity Planning Booklet, a BIA must:

- Include a work flow analysis that involves an assessment and prioritization of those business functions and processes that must be recovered;
- Identify the potential impact of uncontrolled, non-specific events on these business functions and processes;
- Consider the impact of legal and regulatory requirements;
- Estimate the maximum allowable downtime for critical business functions and processes and the acceptable level of losses (data, operations, financial, reputation, and market share) associated with this estimated downtime.

According to FFIEC guidelines, once the BIA is complete, it should be evaluated during the risk assessment process, incorporated into,

and tested as part of the BCP. The BIA should be reviewed by the board and senior management periodically and updated to reflect significant changes in business operations, audit recommendations and lessons learned during the testing process. In addition, a copy of the BIA should be maintained at an offsite location so it is easily accessible when needed.

A well-planned BIA must take into account the specific business needs for areas such as:

- Call center operations,
- Item processing,
- Loan processing,
- Back-office operations for both recovery and continuity.

When determining a financial institution's critical needs, all functions, processes and personnel should be analyzed, and each department should answer a series of critical questions, including:

- What critical interdependencies exist between internal systems, applications, business processes and departments?
- What specialized equipment is required and how is it used?
- How would the department function if the mainframe, network and/or Internet access were not available?
- What single points of failure exist and how significant are those risks?
- What are the critical outsourced relationships and dependencies?

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=95>

77

Pandemic Planning & Response Techniques



Overview

Think the pandemic threat isn't real, or that you needn't prepare a thorough plan to account for it? Your organization's regulators disagree. Pandemic planning is a significant regulatory requirement for every financial institution and a key component in government agency requirements. Register for this webinar to receive expert advice on:

- What regulators expect from your pandemic plan;
- How your organization can prevent or mitigate a pandemic's effects;
- Resource allocation issues your pandemic plan should address;
- How to calculate risks to each business function;
- How to test your pandemic plan;
- Documentation to prepare.

Background

A traditional business continuity plan is developed to serve as the foundation for recovering and managing business operations that may be affected by traditional, short-lived disasters caused by natural, human-caused or technological disasters.

Addressing the likely effects of a pandemic, however, becomes a complex subset of the business continuity plan. A pandemic is often defined as an epidemic or outbreak in humans of infectious diseases that has the ability to proliferate rapidly throughout a widespread geographical area. Unlike natural, human-caused or technological disasters, which have limited life spans, pandemics are predicted to affect a significant geographical area in cycles for up to 18 months - and affect the health of more than 40% of the area's population. A smart organization uses its existing business continuity plan as the foundation for incorporating more complex measures that responding to a pandemic will likely require.

What organizations overlook most frequently are the non-traditional issues relating to resource allocation during a pandemic -- the necessary "people, places and things" that are identified during the risk assessment process. The organization must maintain realistic and practical solutions to resolving the critical resource allocation issues that are likely to impact the institution, including:

- People: Employees, insiders, affiliated parties (and their families), customers, vendors and third-party service providers;

- Places: Facilities that the organization owns, manages, maintains, leases or controls; and
- Things: Assets, equipment, supplies, records and documents.

This presentation focuses on the core components of the FFIEC's Interagency Statement on Pandemic Planning and the lessons learned by more than 2,700 organizations during the FBIIC/FSSCC's Pandemic Flu Exercise of 2007.

Those core components include:

- Developing a program of prevention;
- Documenting a strategy for responding to various stages of pandemic outbreak;
- Constructing a comprehensive framework of facilities, systems and procedures to insure the continuing operation of critical functions;
- Creating a testing program; and
- Managing an oversight program to ensure that ongoing reviews and updates are in place.

You will learn pandemic prevention and business recovery strategies, planning techniques and action tactics that you can use yourself - and that you can then teach to others within your organization. You will also learn how to identify the real sources of pandemic-related loss exposure; the obvious and not-so-obvious methods for using your resources effectively -- before and during any type of disaster; and the most successful methods for managing the maintenance and recovery effort until you can reinstall all of your organization's components.

Presented By

Dana Turner, Security Practitioner, Security Education Systems

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=77>

125

ATM Fraud: Strategies to Beat the Skimming Scams

Overview

ATM fraud is one of the primary crimes committed against banking institutions, and skimming alone adds up to billions in annual losses. How can you fight back?

Learn:

- Evolving attack methods of the fraudsters;
- Effective anti-skimming strategies from banking and law enforcement leaders;
- New anti-skim solutions that help deter criminals.

Background

Late last year, ATM skimming operations in Maryland, Illinois and Georgia netted thieves more than \$120,000.

In January, one Houston area bank reported it lost more than \$200,000 to skimming.

And in February, the U.S. Secret Service broke up an alleged ring of ATM skimmers in Massachusetts, announcing the arrests of three suspects - including one man who was in possession of nearly \$100,000.

As one law enforcement officer commented about these crimes: "Word among criminals on the street is that skimming is a much more profitable crime to commit, not only because the amount of money they are able to steal very quickly, but also because it is less likely that they will be detected."

Clearly, ATM skimming has emerged as one of banking's fastest-growing electronic crimes - and at a time when financial institutions can ill afford any further loss of consumer confidence. With over 250,000 bank-managed ATMs in operation throughout North America, banking/security leaders are challenged by savvy cyber criminals with an inventory of readily available skimming technology, executing their ATM fraud action plans upon institutions of all sizes.

How vulnerable are banking operations to ATM skimming attacks? Without an understanding of the crime, the skimming process and proactive protective strategies, virtually any institution - any customer -- could be the next victim.

In this 60-minute session, you will hear keen insight from a U.S. Secret Service agent, a former bank/security leader and a security solutions provider, presenting:



- How Skimming Works - Detailed examination of the crime, the rapidly-changing skimming technology used on ATMs, and the criminal process of ATM skimmers as documented by federal and local law enforcement.
- Prevention Strategies - including security and loss prevention strategies deployed in institutions' campaigns to alter skimming's impact on identity theft losses. Learn more about rising direct and indirect costs, notification procedures, loss-cost analysis and prevention-mitigation tactics.
- Emerging Technologies - that are now a part of effective ATM security practices. Understand the four-step layered security approach that can help banking operations detect and deter ATM skimming crime and fraud losses.

Presented By

P. Kevin Smith, CPP

Jeff Rinehart, Special Agent, United States Secret Service, Criminal Investigative Division

Christopher Carney, Business Development Manager, Financial & Banking, ADT Security Services, Inc.

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=125>

258

ATM Skimming Fraud: Banking's Growing Billion Dollar Electronic Crime

Overview

ATM fraud is one of the fastest-growing electronic crimes committed against banking institutions, with card skimming fraud alone adding up to billions in annual losses. How can your institution fight back and mitigate this growing form of ATM fraud, cardholder identity theft and credit card losses?

In this 60-minute webinar, you will learn:

- Evolving attack methods of skimming fraudsters and their sophisticated technologies, now impacting ATMs and ATM vestibules;
- Effective anti-skimming strategies from banking and law enforcement leaders;
- New anti-skim technologies that are an important part of effective ATM security practices;
- The four-step layered security approach that can help ATM operations detect and deter ATM skimming crime and fraud losses before they become your institution's negative press.

Background

Recent 2011 news headlines and electronic crime alerts highlight just how pervasive and sophisticated skimming methods have become and their impact in losses to financial institutions:

- In September, the Secret Service made numerous arrests in a skimming crime ring that accounted for more than \$1 million in losses to banks and ATM cardholders in Washington, Idaho and Arizona.
- In October, authorities were investigating suspects in the Denver area who had skimmed more than \$100,000 - accessing over \$11,000 from one person's account alone.
- Also in October, several Bronxville, New York ATM cardholders using one common ATM reported unauthorized withdrawals on their accounts ranging from \$400-\$1,000 each. Ironically, recent skimming victims even included U.S. Attorney Jenny Durkan - the chair of the Justice Department's Cybercrime Subcommittee - stealing \$1,000 from her bank account.

Clearly, ATM skimming has emerged as one of banking's fastest-growing electronic crimes - and at a time when financial institutions can ill afford any further loss of consumer confidence. With over 250,000 bank-managed ATMs in operation throughout



North America, banking/security leaders are challenged by savvy cyber criminals with an inventory of readily available skimming technology, executing their ATM fraud action plans upon institutions of all sizes.

Presentations include:

- How Skimming Works - Detailed examination of the crime, the rapidly changing skimming technology used on ATMs and ATM vestibule card readers, and the criminal process of ATM skimmers as documented by federal and local law enforcement.
- Prevention Strategies - These include security and loss prevention strategies deployed in institutions' campaigns to alter skimming's impact on identity theft losses. Learn more about rising direct and indirect costs, notification procedures, loss-cost analysis and prevention-mitigation tactics.
- Emerging Technologies - More specifically, those that are now a part of effective ATM security practices. Understand the multi-layered security approach that can help banking operations detect and prevent ATM skimming crime and fraud losses.

Presented By

Steve McMahon, Special Agent, United States Secret Service, Criminal Investigative Division Sector Specialist - Banking and Finance

Stephen Lattanzio, VP, Sun National Bank

Tracie Gerstenberg, Business Development Manager - ATM Security, Financial Services, ADT Security

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=258>

295

Banking Fraud: Actual Attacks and Why They Work

Overview

You can't prevent fraud if you don't understand the attacks.

This webinar dissects recent, real-world online and mobile banking fraud attacks. We will present a step-by-step view of the fraudsters' activities and behaviors, their use of malware and how they were able to successfully compromise the accounts and circumvent the fraud prevention solutions that were in place. Only by understanding how these sophisticated schemes actually work can financial institutions decide on the most effective defenses.

In this research-based webinar, Guardian Analytics' fraud experts will present:

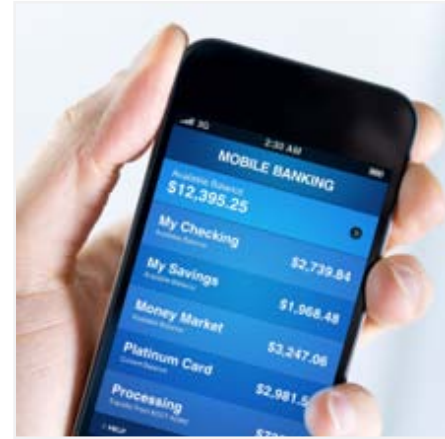
- Specific attack schemes, including the automated attacks recently discovered by Operation High Roller, and how they were able to avoid detection;
- Examples of how fraudsters are able to use one channel to set up fraud attacks in other channels;
- Data from recent research that highlights why fraud prevention is strategically important for financial institutions;
- What's working today for preventing online and mobile banking fraud.

Background

In June, Guardian Analytics and McAfee announced the results of a joint fraud investigation. Operation High Roller describes a new breed of automated attack that uses cloud-based servers to control the attacks instead of running off of the victim's computer. This is just one example of the highly sophisticated schemes that we'll describe in detail during this webinar. The conclusions are clear: financial institutions must continue to improve their fraud prevention capabilities.

We'll reinforce the fraud threat content with highlights from our recent Business Banking Trust Study that reports on the impact fraud can have on an organization's relationship with its financial institution. For example:

- 74 percent of businesses have experienced online fraud - 52 percent in just the past 12 months;
- 56 percent indicate that it takes only one fraud incident for them to lose confidence in their FI;



- 40 percent of businesses that were hit by fraud took all or some of their banking business elsewhere.

The bottom line business impact for FIs - which makes fraud prevention such a strategically important issue - is lost dollars, lost trust and lost customers.

Presented By

Chris Silveira, Manager of Fraud Intelligence, Guardian Analytics

Tiffany Riley, VP - Marketing, Guardian Analytics

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=295>

129

Beyond Heartland: How to Prevent Breaches of Security and Trust

Overview

It may be the biggest data breach we've ever seen - and an eerie harbinger of crimes to come. The Heartland Payment Systems (HPY) hack involves scores of financial institutions and tens of thousands of consumers who've had their accounts compromised by fraudsters. Crimes against processors are on the rise, and in this panel discussion you'll gain insights from:

- A banking/security leader, who describes the impact of such breaches on community banking institutions;
- A noted privacy attorney, who discusses the legal impact of these crimes and how to fight them;
- A trusted leader of on-demand information security services, who will share market insights on the latest fraud trends and what companies need to do to prevent, manage and respond to the growing security threats.

Background

When Heartland Payment Systems (HPY) revealed in January 2009 that it had been the victim of a malicious hack sometime in 2008 - that an unknown number of consumers had their account names and numbers pilfered - the payments processor became the unwitting face of fraud.

Since that crime, more than 600 financial institutions have volunteered to Information Security Media Group that they and their customers - tens of thousands of individuals - were affected and in some cases defrauded as a result of the Heartland breach.

Although no one knows for certain how big the breach was, the Heartland case nevertheless caused:

- Customers to join in class action suits against the processor;
- Banking institutions to band together to buck the trend of having to replace cards and placate customers after crimes committed on other organizations' watch;
- The security and payments industry to re-evaluate the systems and solutions in place to protect personally identifiable information at all stops along the transaction route.

Merchants, banks, customers and vendors - they all have been affected by the Heartland breach, and their perspectives will be represented in this panel discussion about the crime and how to prevent future incidents.



Register for this webinar to see these perspectives:

- An overview of the Heartland breach and its impact on banking institutions, as portrayed by Tom Field, Editorial Director of Information Security Media Group;
- How one community banking institution was struck and is now fighting back, as told by Stephen Wilson, VP of McGehee Bank;
- The legal perspective: what consumers, institutions and states can do to respond, with insight from noted privacy attorney Randy Sabett;
- Beyond Heartland - ways financial institutions can address the growing complexity, cost and compliance pressures of protecting their customers' most critical information, with advice from Kevin Prince, Chief Architect of Perimeter eSecurity.

Security experts say Heartland-style breaches are the wave of the future in fraud, but financial institutions now have the opportunity to buck that trend. This panel discussion is step one toward preventing further breaches.

Presented By

Stephen Wilson, VP, McGehee Bank

Randy Sabett, CISSP, Privacy Attorney

Kevin Prince, Chief Architect, Perimeter eSecurity

Tom Field, Editorial Director, Information Security Media Group

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=129>

29

Beyond Phishing - The Growing Crimeware Threat

Overview

- Hear about the trends you need to know in malware/crimeware as it continues to evolve;
- Learn new ways to approach the crimeware problem;
- Find out how to protect your institution, customers and brand name.

Background

If you think your customers and your brand are protected from attacks with anti-phishing measures, you may be surprised. While phishing continues to be an ever-present problem, other threats continue to evolve, with crimeware at the forefront of the external threats landscape.

Uriel Maimon from RSA, The Security Division of EMC, and Vanja Svajcer from Sophos come together for this webinar to share with you their joint knowledge of this problem. Uriel Maimon is the Senior Researcher in the Office of the CTO, Consumer Solutions Business Unit, at RSA. Uriel specializes in the technology research of financial fraud, crimeware analysis and cyber-forensics.

Vanja Svajcer is a Principal Virus Researcher at SophosLabs, UK. Vanja joined Sophos as a virus analyst in 1998 after graduating from the Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia. His interests include automated analysis, honeypots and research of malware for mobile devices. He's a frequent speaker at conferences related to malware research and computer security.

Join us to learn from industry experts:

- How these types of attacks work;
- What is the full impact of a Trojan attack;
- How to use a layered approach to combat these evolving threats.

Presented By

Uriel Maimon, Senior Researcher in the Office of the CTO, RSA

Vanja Svajcer, Principal Virus Researcher, SophosLabs, UK

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=29>

44

Taking Fraud Out of Online Banking

Overview

- Evolution of identity fraud techniques, including man-in-the-middle;
- The authentication solution landscape for financial institutions - what are some of the choices banks have to fight fraud (e.g., risk-based authentication, strong authentication, PKI, OTP, smart cards);
- Life in the trenches - implementing FFIEC guidelines and banking industry best practices for strong authentication.

Background

Over the last few years, the online threats targeting financial institutions and their customers have undergone some significant advancements. The threats have become very sophisticated, and they continue to succeed in spite of customer education and significant investment in security technology. At the same time, banks are under pressure to implement the FFIEC guidelines requiring stronger authentication.

One example of the sophisticated attacks banks face is a new type of phishing attack called man-in-the-middle. This threat can succeed in spite of stronger authentication techniques that satisfy FFIEC guidelines, including OTP tokens, grid pads and site authentication techniques like pictures.

Financial institutions looking to protect their online customers from identity fraud have a wide range of technologies from which to choose. Traditional hardware-based solutions, such as OTP tokens or smart cards, require changes to user behavior and/or are prohibitively expensive to push out to all online customers.

Arcot has created software-only strong authentication solutions that make it easy and affordable to protect millions of online bank customers from identity fraud. Our authentication solutions eliminate the need for hardware tokens and complex login processes. We deliver authentication solutions that provide the strength of hardware yet with the simplicity of a password.

Presented By

R. 'Doc' Vaidhyanathan, Vice President, Product Management, Arcot

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=44>

288

Breach Response: Developing an Effective Communications Strategy

Overview

How an organization communicates in the wake of a major breach incident can play an important role in maintaining the organization's reputation and minimizing the financial impact.

But how can your organization avoid mismanaging post-breach communication and potentially wasting millions of dollars?

Join us for this webinar, featuring an attorney who advises clients on breach resolution and other security matters who will:

- Discuss how to prepare a breach response plan, including a communication strategy;
- Review the do's and don'ts of post-breach communication, outlining best practices;
- Offer insights on when to hire and how to select a breach resolution or public relations firm.

Background

Making the quick communication decisions needed to mitigate the potential harm of a data breach is challenging. Too many organizations in all business sectors mismanage data breach response efforts, making decisions without complete knowledge and lacking a clear and forthright message.

Recent breach responses provide examples of how confusing, inconsistent post-breach communication can do more harm than good. Examples include: Sony's announcement that it had initially underestimated the number of consumers affected by a breach; Hannaford's use of a single notice letter to 4.2 million consumers even though only 1,800 individuals had fraudulent charges; and the inconsistencies between the information released by Global Payments about its breach and the updates on the incident provided by VISA.

Carefully planned communication in the wake of a major breach incident can play a major role in maintaining the organization's reputation and minimizing the financial impact of a breach. Good communication also can help mitigate or prevent unnecessary litigation or government investigations.

In this webinar, our speaker, a legal expert who has advised organizations that have experienced breaches, will review the essential components of a successful post-breach communication strategy, including:



- Preparing proactively for data breaches by conducting compliance and security assessments, designating an internal breach response team, establishing relationships with key vendors and developing breach response communication plans;
- Testing a breach response plan, including the communications component;
- Providing accurate and timely notice communications by quickly and efficiently collecting the facts to understand the breach, developing methods to identify all relevant audiences, crafting the right message and identifying the best means of communication;
- Determining when to hire a breach resolution or public relations firm to help with post-breach communications;
- Planning how to inform appropriate regulators, such as state attorneys general, before issuing a breach notice.

Attendees also will learn about how to avoid mistakes, including:

- Providing inaccurate or confusing notice communications, including communications that provide a limited, legalistic or formulaic response;
- Failing to develop proper remediation and mitigation processes and using a process that frustrates consumers;
- Ignoring certain audiences that should be contacted regarding a data breach.

Presented By

Ronald Raether, Partner, Faruki Ireland & Cox PLL

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=288>

269

Breach Prevention 2012 & Beyond: Fend Off Malicious Attacks

Overview

Today's cyber-culture causes financial institutions to rely heavily on the use of electronic information, which can be a gold mine for hackers. Malicious individuals are constantly searching for security vulnerabilities and weaknesses to gain access to electronic information. Are you taking the proper steps to protect that private information? During this session, ATTUS Technologies, a trusted compliance advisor for risk and information security, will look at:

- Different methods of attacks;
- Risks of social engineering and network perimeter attacks;
- Common high-risk flaws;
- How to prepare for, identify and defend against these risks.

Background

Your institution houses private information for your clients, but what would happen if that information fell into the wrong hands? An information breach not only affects the clients whose information is leaked, but diminishes the integrity of your institution.

Understanding all the threats to your information security is the first step in protecting it. Hackers and malicious individuals exist in many guises. From recreational, to organized crime rings, to disgruntled ex-employees, the list goes on. You need to ensure that not only your electronic systems are adequately secure, but that your employees are properly trained.

In this session, Tyler Leet will discuss:

- Breach statistics;
- Common findings and benefits of security testing;
- Social engineering tactics, findings and prevention methods.

Presented By

Tyler Leet, RISC Services Manager, ATTUS Technologies

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=269>

270

2012 Faces of Fraud Survey: Complying with the FFIEC Guidance

Overview

The FFIEC Authentication Guidance update has been in circulation since mid-2011. But as banking examiners begin testing for conformance, we find:

- Only 11% of surveyed institutions have come into conformance since the guidance was issued;
- Nearly 30% don't fully understand the guidance;
- 88% do not believe the guidance will result in a significant reduction of online fraud.

Join a distinguished panel of fraud experts for an exclusive first look at the eye-opening survey results and how institutions can act upon them, including:

- A look at 2012's top fraud threats;
- How banking institutions are countering these threats;
- Top security investments to fight fraud and conform to the FFIEC Authentication Guidance.

Background

A follow-up to ISMG's 2011 Faces of Fraud Survey, this webinar looks not only at the latest fraud trends and how institutions are fighting back, but also at their progress in putting together layered security controls in conformance with the FFIEC Authentication Guidance.

- Chart the latest fraud trends, including account takeover, skimming and payment card breaches;
- Gauge institutions' preparedness to conform to the FFIEC Authentication Guidance, including where they are prioritizing their efforts;
- Predict the top areas of focus for 2012, from real-time fraud monitoring tools to new layered security controls.

Presented By

George Tubin, Banking and Security Analyst

Matthew Speare, SVP - Information Technology, M&T Bank

Tom Field, Vice President, Editorial

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=270>

149

Business Banking Under Attack: How to Fight Back Against Cybercriminals

Overview

Cybercriminals are on the attack, and as a recent FDIC alert shows, business banking accounts are in their crosshairs. Learn first-hand how one leading business bank fights back by:

- Spotting fraudsters before they commit crimes;
- Educating customers about fraud prevention;
- Balancing security needs with costs and customer convenience.

This complementary BankInfoSecurity presentation will use real-life fraud examples to detail why traditional techniques are not enough to prevent fraud, and how one leading business bank is successfully monitoring individual online account holder behavior with predictive analytics to catch suspicious activity before fraud can occur.

Background

Business online banking accounts are under attack by sophisticated fraud rings that coordinate elaborate account takeover, distributed mules and under-the-radar money transfer schemes. Unsuspecting business employees, high account balances and online payments features attract these criminals to businesses and banks of all sizes. As the industry creates new methods to thwart fraudsters, these criminals devise new techniques that void these innovations. Today's fraudsters easily defeat yesterday's multi-factor authentication, transaction monitoring and other controls requiring banks to constantly reassess their countermeasures.

This complementary BankInfoSecurity presentation will use real-life fraud examples to detail why traditional techniques are not enough to prevent fraud, and how one leading business bank is successfully monitoring individual online account holder behavior with predictive analytics to catch suspicious activity before fraud can occur.

During this one-hour event, you will learn:

- Real-life case studies of catching fraudsters before fraudulent transactions can occur;
- Techniques used by today's cybercriminals and how to identify them;



- How to balance customer convenience, costs and improved security;
- The role of customer education in fraud prevention efforts;
- Best practices in preventing online-related fraud.

Presented By

Linda Coven, Head of Online Banking Channel Solutions, Silicon Valley Bank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=149>

152

Check Fraud Management 2.0: A New Approach to a Persistent Challenge

Overview

Check fraud, a decades-old problem, continues to grow despite a decrease in the number of checks written and paid each year. Current defenses have major shortcomings that allow check fraud to flourish and losses to mount as high false positive rates plague even the best efforts of fraud analysts and investigators.

New approaches to data management, next generation analytics and visual alert disposition techniques can fundamentally improve the efficiency and success of check fraud management efforts at banks of all sizes. This session explores these new approaches and what they offer to banks and credit unions of all sizes.

Register for this webinar to learn:

- Why check fraud is an important problem requiring a new approach;
- How and why existing approaches to check fraud fall short;
- How new approaches to check fraud enable loss prevention teams to catch more fraud, more accurately and more efficiently.

Background

Check fraud remains in the top three loss areas for most banks and credit unions. It's a damaging, ongoing challenge, causing record losses that continue to grow annually. In the latest available comprehensive survey of U.S. banks alone, check fraud resulted in close to \$1 billion in losses. Many financial institutions treat check fraud as a cost of doing business. Why? Because a new approach to systematically solving check fraud has not emerged in decades.

Institutions using check fraud detection solutions know their challenges and shortcomings all too well. Inaccurate detection analytics yield a large number of alerts, mostly false positives. Those committed to reducing check fraud losses have no choice but to review these alerts in a short time period, an approach that requires an inefficient, manpower-intensive approach.

It's time for a new approach - one that produces a manageable number of actionable alerts, enables fast, efficient disposition of those alerts and provides a comprehensive view of fraud so that



more sophisticated cross-channel and collusive schemes can be stopped.

Attendees to this webinar will learn:

- Why simple, flawed analytics lead to a flood of false positives;
- How a siloed view of check transactions can leave analysts blind to complex fraud events;
- How next-generation analytics can dramatically reduce false positives while still identifying fraud;
- How better tools for alert management and forensic research can drive faster, more accurate disposition and higher rates of fraud detection - and, ultimately, prevention.

Presented By

Mike Mulholand, Director, Fraud Solution Strategy - Memento, Inc.

Tim Brady, Director, Investigation Services - Memento, Inc.

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=152>

194

Debit Fraud: Trends and Typologies

Overview

Skimming, tsunamis, chameleons - debit fraud schemes are on the rise. Join us for a free webinar where we'll talk about the latest in debit card fraud, and share our experiences in how to detect it. This webinar will deliver:

- An overview of debit fraud;
- Current & forecasted trends;
- Typologies & sample scenarios;
- Things to look for in a fraud solution.



Background

Debit card fraud, the act of using debit card information to fraudulently obtain money or goods, is front and center in the minds of Americans. The March 2009 Unisys Security Index reported that credit and debit card fraud is the number one fear for Americans, surpassing terrorism, computer and health viruses and personal safety.

Fraudsters are constantly on the attack, with no concern for the consequences or fall-out from their actions. Financial institutions are continuously left to fight from a defensive position, reacting to attacks while trying to limit damage and clean up the resulting mess.

This webinar discusses current debit card use and debit card fraud trends. It examines several specific debit fraud scenarios that represent a sample of both common and emerging debit card fraud trends faced by card holders and financial institutions today. Finally, it offers a number of features that make an anti-fraud software solution effective.

Presented By

Charles Robertson, Verafin

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=194>

67

Defending Against The Insider Threat

Overview

The insider threat - it may be the hardest to detect, yet it poses the greatest risk to information security and regulatory compliance. And with recent, high-profile data breaches resulting from insider abuses, the topic is hotter than ever.



Register for this webinar to learn:

- How to identify and mitigate insider threats;
- The different types of threats - accidental & malicious;
- How to spot authorized users handling information in unauthorized ways;
- Proper procedures and tools to help maintain regulatory compliance and protect against the insider threat.

Background

Organizations must constantly balance access to information for the purpose of conducting business, while protecting this information from unauthorized users. While many well-established methods and products exist for tracking external attacks on information, less oversight and protection is made for identifying authorized users handling information in unauthorized ways - the insider threat.

Jerald Murphy will lead a discussion about how proper procedures and tools can be implemented to comply with regulatory guidelines, while at the same time identifying and mitigating internal data leakage. He will also discuss how to organize roles between data management and security/compliance, so that information workers can have the most flexibility, while still ensuring protection of data.

Among the topics to be discussed in this webinar:

- The current business security environment;
- The different types of insider threat;
- How to respond to & report data loss from an inside threat.

Presented By

Jerald Murphy, Senior Vice President and Director of Research, The Robert Frances Group

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=67>

168

Effective End-to-End Fraud Management: Managing Financial Crime Risks in Today's Banking Climate

Overview

In this webinar, jointly presented by Norkom and IBM, attendees will learn and hear:

- Discussion on the latest market trends, threats and issues banks face in dealing with the increasing frequency and sophistication of fraud attacks and intensifying regulatory landscape;
- The value of an expanded view of financial crime management as a true 'end-to-end' process;
- Benefits of properly managing financial crime risks during the 'upstream' phases of financial operations such as origination and loan application;
- Why effective fraud management is much more than just 'good detection' - and must include sophisticated methods to aggregate information across multiple channels, assess risk and investigate suspicious activity in a holistic manner across the entire financial institution;
- What IBM and Norkom Technologies offer to optimize fraud defenses in a cost-effective and efficient manner and how Norkom's top-rated Enterprise Investigation Management solution enables financial institution to achieve the promise of effective fraud management.

Background

Financial institutions all across the world share a common cause in the fight against financial crime. All financial institutions, irrespective of their size or geographies, are being targeted by the same sophisticated, target-driven criminals across multiple channels, business lines and financial products. However, this is where the similarities end. Financial institutions vary widely in their approaches to managing financial crimes, in particular the spiraling levels of fraud. Indeed, the phrase 'effective fraud management' has many connotations, but the question is - what does it actually mean and how can it be achieved?

This webinar offers expert commentary and analysis on the growing fraud threats facing financial institutions in today's climate, and the strategies leading financial institutions are employing to manage these threats effectively.



In this webinar, you'll hear from Celent's Neil Katkov, a leading industry expert on financial crime and compliance, who will share his insights into the world of financial crimes, outline the issues facing financial institutions and their need to manage fraud as a true 'end-to-end' process.

You'll also hear from Robert Snider, Financial Industry Solutions Architect with IBM, who will discuss how financial institutions can strengthen account origination processes using an integrated risk management strategy. Snider will highlight current and pending challenges in terms of regulatory compliance, fraud risk and credit risk management procedures. He will explain how the IBM Banking Industry Framework provides a unified banking framework that delivers software and accelerates smarter solution deployment, providing end-to-end banking solutions.

Finally, David Dixon, Norkom's Managing Director of Financial Crime, will discuss the growing recognition by leading financial institutions that, while fraud detection is indeed an important component in the fraud management process, it is only one element of a true end-to-end fraud management solution, and to prevent future fraud from taking place, financial institutions need to effectively and efficiently manage the investigation and resolution processes.

Presented By

Robert L. Snider, IBM Financial Services Sector Industry Senior Solutions Architect

Neil Katkov, PhD, Senior Vice President, Celent

David Dixon, Managing Director of Global Solutions, Norkom Technologies

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=168>

133

Embezzlement (Part 1): When Everyone Lies, Cheats & Steals

Overview

Embezzlement has become the nation's favorite financial crime - and losses attributed to embezzlement are greater than those from all other financial crimes combined.

Register for part one of this two-part series to learn:

- Where embezzlers look for opportunities;
- Identifying embezzlement offenders;
- The differences between men & women embezzlers.

Background

Embezzlement is often the most complicated crime to discover or to investigate. Embezzlement is the intentional misuse or misappropriation of funds or property entrusted to an employee or some other person who has power, control, trust or authority over money or property.

Embezzlement is often involved with banks, conservatorships, home health care workers, insurance companies - just about any industry you can imagine. If they commit their crimes often enough, serial killers, pedophiles, rapists and burglars all settle upon a distinct pattern of behavior - the method of operation that works best for them. Embezzlers are among the most habitual offenders - and they either choose a distinct method of operation or they must adhere to a business rhythm that is beyond their control.

Understanding the crime of embezzlement is critical to every investigator. To plan any strategy, you have to understand the unique "people, places and things" involved, so that you can identify potential witnesses and suspects and know where to look for evidence. Embezzlement crimes usually contain an abundant evidence trail that most other crimes do not. But you have to know where to look and what you're actually looking for. While this presentation isn't so much about conducting a financial crime investigation, your participation will help you to plan and execute a professional one.

Embezzlement is a crime that involves:

- Trust;
- Ego;
- Rationalization;



- Greed;
- Habits;
- Patterns.

This presentation provides a basic methodology and appropriate techniques for identifying embezzlers, and it's appropriate for both law enforcement officers and private security personnel. Useful for pre-employment screening, audit work and internal investigations, these techniques focus on the steps that an investigator may take to identify these crimes and the offenders.

This presentation is designed to help you:

- Understand why embezzlement has become the nation's favorite financial crime;
- Show the proven links between an organization's structure and its vulnerability to loss -- and the critical areas of risk;
- Craft an alliance between the security, audit and human resources functions to work together to resolve embezzlement issues;
- Demonstrate who embezzles, how much they steal - and why - within your own organization;
- Learn what motivates an embezzler, where they look for opportunities - and why this is such a rhythmic, cyclical and predictable crime;
- Chart a person's characteristics and a person's habits to identify potential and practicing embezzlers.

Presented By

Dana Turner, Security Practitioner, Security Education Systems

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=133>

134

Embezzlement (Part 2): Conducting Financial Crime Investigations

Overview

Conducting any kind of investigation can be risky. Conducting an investigation that involves people's character, finances and relationships within a family or employee's workplace is even riskier because it likely changes the lives, careers and relationships forever.

Register for this session to learn:

- Components of a financial crime investigation;
- How to plan a financial crime investigative strategy;
- When to justify further investigation.

Background

Many financial crimes are also emotional crimes, and the investigator must be particularly careful that the investigation does not raise more negative issues with victims. The crime of embezzlement committed against a family member or a business owner is among the most emotionally devastating crimes for the victims. There are two very simple goals for every investigator - to find the truth and to determine the responsibility for results. Even an inexperienced embezzler will do his/her best to make this simple goal unattainable. After learning about and understanding the unique habits that embezzlers practice, any investigator may plan for and execute a successful financial crime investigation.

This presentation is designed for those people who are responsible for investigating and documenting events regarding financial crimes: law enforcement agents, private security personnel, auditors and more. Although this presentation addresses any type of financial crime investigation, the crime of embezzlement - one of the most frequent and misunderstood offenses - is given special attention. The seminar components focus upon the six key functions that every investigator must consider when conducting an investigation, including:

- Identifying and interviewing victims, witnesses, informants and suspects;
- Gathering and cataloging appropriate evidence;
- Documenting the facts and opinions gathered during the investigation;
- Coordinating law enforcement agency and private resources to insure the speedy apprehension of offenders;



- For non-law enforcement agency personnel, working with your legal counsel to prosecute offenders -- civilly and criminally;
- Recovering funds and investigative costs.

This presentation provides a logical and strategic model that's designed to help both private and public investigative personnel to understand the true scope of the processes used to conduct professional, comprehensive and effective financial crime investigations. By understanding the cause-and-effect relationships between the investigator's strategy and the investigative result, any investigator may use this model to design and implement a standardized, company or agency-wide investigative process.

This presentation is designed to help you:

- Determine each investigator's and external resources' duties and responsibilities - legal, moral and ethical;
- Comply with current regulations and emerging practices affecting industry standards of care for financial crime investigators;
- Develop an investigation policy and procedure that makes the best use of the victim's and agency's resources;
- Locate and understand the significance of the primary sources of information that are accessible to the investigator - including physical evidence and testimony;
- Prepare reports that will likely be examined in either civil or criminal actions.

Presented By

Dana Turner, Security Practitioner, Security Education Systems

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=134>

293

Evolving Threats, Innovative Responses - How to Effectively Combat Spear-Phishing & Data Leaks

Overview

Targeted e-mail attacks represent one of the most significant IT threats facing healthcare and financial services today from a data security perspective. Many of the large, widely publicized data breaches in recent years have started with a single, carefully crafted and personalized e-mail that tricked the targeted recipient and ultimately resulted in malware infections or exposure of their login credentials which was followed by data theft or other damage. These attacks are highly-targeted and seemingly innocent to traditional reputation, content scanning and sender verification techniques used today. Enterprises have no method, tool or process to detect or effectively manage such attacks until it is too late.

Join this webcast and learn about:

- The anatomy of a targeted attack and how they're stealing not only financial information but sensitive corporate data;
- How big data technologies are being used to address the challenges of detecting and defeating highly-targeted attacks;
- Effective methods to protect your sensitive healthcare and financial data anywhere you go - even on mobile devices and public terminals;
- Best practices for creating the right policies for data privacy and encryption including risk analysis;
- How to extend a protection strategy to protect sensitive data, in all formats, across the entire organization.

Background

Healthcare and financial service organizations have volumes of sensitive data making them prone to an ever-broadening range of IT security threats: from basic annoyances such as auto-emailed viruses, to targeted social network informed phishing-style attacks that trick employees into giving up private credentials or clicking on dangerous links that install polymorphic malware. New approaches to threat detection and remediation have become necessary for organizations that are at risk.

Join this webcast for a lively discussion on what companies can do to spot and respond to targeted attacks. We will touch on topics



including: the anatomy of a targeted attack, big data phish-finding, anomalytics, sandboxing, follow-me protection, and defense beyond the gateway.

Presented By

Kevin Epstein, VP - Product Marketing, Proofpoint

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=293>

187

Fight Back Against Fraud: Strategies on How to Meet the Multi-Channel Challenge

Overview

ACH and wire fraud. ATM skimming. Payment card compromises. Mortgage fraud. Phishing.

Financial institutions are besieged by fraud threats today - and not just via one dominant channel, but through all of them. Simultaneously.

How can institutions fight back - as well as educate & enlist their consumer and business customers to do their parts, too? Join this panel discussion to hear new insights from industry thought-leaders on:

- The multi-channel fraud threats facing financial institutions today;
- Successful strategies for mitigating these threats;
- New tactics for educating and protecting customers;
- Emerging technologies to fight fraud.

Background

From ATM skimming to bogus wire transfers, 2010 has been the “Year of the Fraudster” for banking institutions and their customers.

According to the latest Verizon Business Data Breach Investigations Report, financial services far and away is the most commonly breached industry, accounting for 85% of the 143 million records breached in 2009. The most common types of fraud:

- Insiders;
- Social engineering schemes;
- Hacks by organized crime.

Symptoms of these crimes have dominated the news: ATM skimming sprees, increased incidents of ACH fraud, aka corporate account takeover, attacks against merchant point-of-sale devices.

More daunting for banking institutions: These incidents aren't occurring in isolation. Rather, they tend to strike across multiple channels, testing for every possible vulnerability.

The cost to financial institutions? It breaks down two ways:



- Financial - The time, expense and human resources necessary to respond to breaches, notify customers, monitor accounts and, when necessary, replace payment cards and lost funds;
- Reputational - Perhaps the biggest toll of all - the loss of customer confidence when an account has been breached. The customer doesn't necessarily care who committed the breach; they just know it happened on their bank's watch.

So, how can financial institutions fight back? First they must know their enemy and the guises it wears. That's the main point of this session. Matt Speare of M&T Bank will lead the discussion, walking attendees through an overview of the types of fraud schemes institutions such as his see every day. From there, our panel of industry experts will discuss current trends and the threat landscape, as well as proven solutions to detect and deter fraud.

Presented By

Reed Taussig, President & CEO, ThreatMetrix

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

Kim Peretti, J.D., LL.M., CISSP, PricewaterhouseCoopers

Ori Eisen, Founder, Chairman and Chief Innovation Officer, 41st Parameter

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=187>

40

Fighting Fraud Schemes: Education, Response and Defense

Overview

- Learn in detail the current financial scams in circulation from phishing and lottery scams, ATM and credit card skimming, among many others;
- Learn proactive defenses to prevent consumers and employers from falling victim.

Background

In today's world financial institutions and their customers are under increasing attacks by criminal elements attempting to obtain financial information to conduct identity theft, account takeovers, ATM fraud, debit and credit card fraud, and numerous other types of check fraud and electronic crimes.

These types of crimes amount to losses of over \$20 billion per year to financial institutions, businesses and consumers. FBI statistics reported in Wired Magazine in 7/2006 reveal that 71% of all online fraud originated from within the U.S. in 2005.

Average losses to the most common online scams were: Nigerian Letter - \$5,000; Check Fraud - \$3,800; Confidence Scams - \$2,025; Investment - \$2,000; Non-Delivery of Merchandise - \$410; Auction - \$385; Credit/Debit Card - \$240. In contrast, the average loss to a bank robbery is approximately \$2,400, with a 75 to 85 percent apprehension rate. Internet-based and identity theft crimes have approximately a 6 percent apprehension rate for those criminals.

This webinar will describe many of the current financial scams that are circulating in our society right now, and will offer proactive defenses to prevent consumers and employers from falling victim to these scams, and what rights and resources are available should you become a victim of these type of crimes.

Among the types of frauds and scams that will be discussed are phishing, lottery scams, work-from-home scams, ATM and credit



card skimming, counterfeit check schemes, auction fraud scams and social engineering methods used by scammers.

With the onslaught of these types of crimes and the ever changing world of technology, criminals are increasingly attacking the human factor which is probably the weakest link in the chain. The best defense against these crimes is consumer education so that these scams can be recognized and avoided.

Presented By

Kirk McGee, CPP, AVP, Regional Security Officer, TD Banknorth N.A.

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=40>

58% of Faces of Fraud Survey respondents expect to see an increase in fraud-fighting resources in 2012.

*Source: Information Security Media Group's Faces of Fraud Survey 2012

172

Fighting Online Banking Cybercrime with a Holistic Security Strategy

Overview

In this webinar, Jerry Silva, former Tower Group analyst now principle of PG Silva Consulting Company, and Terry Austin, President and CEO of Guardian Analytics, will present why the dynamic landscape of online banking and payments demands a strategic and holistic security strategy designed for the long haul, one that can withstand the ever-evolving threats against online banking.

In this 60 minute session, these two experts will present:

- The opportunities for banks and credit unions to use online banking to capture increased wallet share, grow customer loyalty and grow revenue;
- The latest trends in cyber attacks against online banking and where fraudsters have the advantage;
- Why a bank's strategic advantage - deep knowledge of the customer - is the centerpiece of a holistic security strategy and how it can be used to stop new and emerging attacks like man-in-the-browser attacks;
- How a layered approach built on behavioral analytics and risk scoring makes other security technologies like MFA, OOB, and secure clients more effective and more valuable and create an environment that can withstand ever-evolving threats against institutions.

Background

In the war against cyber criminals, financial institutions are presented with an arsenal of different solutions designed to secure access, detect fraud and authenticate users. These point solutions may individually address specific threats, but on their own are likely to be defeated by tomorrow's new and improved attacks.

Experts from the FS-ISAC, FBI, Gartner, ABA and others recommend institutions implement a layered security strategy with a long-view of protection in mind. But most institutions are implementing point solutions, rather than building layers with a holistic, integrated security strategy in mind that offers powerful protection balanced with customer convenience.



Presented By

Jerry Silva, Founder, PG Silva Consulting

Terry Austin, President & CEO, Guardian Analytics, Inc.

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=172>

120

Fraud Detection & Prevention Strategies for Financial Institutions: Emerging Technologies Insights

Overview

Third in a series of new roundtable events showcasing emerging technologies.

- Hear about the top fraud threats facing financial institutions - from inside and out - including examples such as the Heartland Payment Systems breach;
- Learn best-practices for detecting suspicious behavior and high-risk activities;
- Discuss strategies for defending against fraudsters without negatively impacting your systems or the customer experience.

The recent Heartland Payment Systems data breach exposed hundreds of banking institutions and thousands of customers to potential credit and debit card fraud. But Heartland is only one example of the many fraud risks that threaten institutions from the inside and out.

Background

The Heartland Payment Systems data breach so far has been the biggest story of the year.

Hundreds of banking institutions and thousands of their customers were exposed to potential credit/debit card fraud when the payment processor's information systems were hacked in 2008. No one knows the full extent of the damage yet, but we do know that the Heartland breach represents only one type of fraud threat to institutions and consumers.

Across the globe, online criminals and rogue insiders have focused their funds, time and resources to perpetrate fraud - and they're getting very good at it. The result has been a dramatic increase in online fraud that specifically targets banking institutions and their customers. Every data breach or costly identity-theft case reported in the media erodes the public's confidence in the security of online financial transactions. This loss of confidence could jeopardize the ability of organizations to conduct transactions online. And for an industry such as banking, which is built on trust, the loss of confidence could endanger the very institutions.

Beyond the emerging threats are new, global regulations such as the U.S.-based FFIEC and FACTA Red Flags, the UK-based Faster



Payments Initiative, Europe's SEPA directives and others - all focused on providing specific guidelines in response to online fraud.

While the intent of online security is clear - to better protect individuals and businesses from online crime - the implementation details are often far from transparent. And today, many organizations around the globe struggle with the question, "Where should we begin?" Importantly, these same organizations are concerned with the next critical question as well: "What do we do next?"

In this webinar, hear the latest market research on fraud threats against banking institutions, as well as expert insight on strategies and solutions these institutions are deploying. Register now to learn:

- The top fraud threats facing financial institutions and their end users, including examples such as Heartland Payment Systems;
- Best practices for detecting suspicious behavior and high-risk activities;
- Strategies for defending against fraudsters without invasive back-end integration or unnecessary disruption of the customer experience.

Presented By

Tom Wills, Senior Risk and Fraud Analyst, Javelin Strategy & Research

Steve Neville, Director of Identity Products, Entrust

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=120>

177

Fraud Prevention: Protect Your Customers and Your Institution from Web Vulnerabilities

Overview

Fraud is the #1 risk to banking institutions, and the chief victims are their customers - consumers and businesses who lose vast sums of money to web-based scams.

Register for this webinar for expert insights on:

- Current fraud trends, including ACH and social networking;
- Top vulnerabilities for your employees and customers alike;
- How to enhance protection through the latest technology solutions.

Background

The headlines tell it all:

In Michigan, a small business has sued its bank after a phishing attack left the business vulnerable to fraudulent ACH transactions that added up to over \$500,000.

In Texas, a bank sued its customer - and then was countersued - over a dispute involving \$800,000 worth of ACH fraud and the question of, "What is reasonable security?"

ACH fraud has become one of the most insidious crimes preying upon banking institutions and their customers, eroding the trust that's so fundamental to the banking relationship. The FDIC, FBI and American Banking Association all have sent out alerts warning banks and businesses of the dangers of ACH fraud, and the Department of Justice now is investigating the extent and roots of these crimes.

But ACH isn't the only form of fraud that is bilking banking institutions and businesses. ATM and payment card crimes are also on the rise, and social networking sites now provide a new venue for fraudsters to prey upon consumers and organizations.

In all, the FDIC estimates that banking customers lost \$120 million to fraud in 2009. How will 2010's statistics compare?

Register for this webinar for unique insight into the legal implications of current fraud trends, as well as potential solutions to prevent these crimes. David Navetta, Co-Chair of the American Bar Association's Information Security Committee, will lead the discussion of:



- The latest fraud trends targeting banking institutions and businesses;
- Current court cases and their implications for information security organizations.

Then Matthew Speare of M&T Bank will discuss how banking institutions should approach ACH fraud and social networking, including:

- Changing attack venues;
- Policies;
- What to monitor and how.

Following Navetta and Speare, thought-leaders from Websense, sponsor of this session, will discuss emerging technology solutions and their roles.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

Patrik Runald, Senior Manager of Security Research, Websense

David Navetta, Founding Partner, Information Law Group

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=177>

260

Fraud Prevention: Utilizing Mobile Technology for Authentication & Transaction Verification

Overview

It's no longer just about mobile banking. Mobile technology today is deployed by leading-edge institutions for out-of-band user authentication, transaction verification and to help prevent fraud via real-time security alerts.

How can your institution crack down on fraud and maximize its mobile investment?

Join Tom Wills, internationally-recognized banking and mobility expert, as he discusses:

- Online authentication and security, and how mobile technology can be used as an additional security layer;
- Mobile's role in preventing and detecting ACH/wire fraud;
- Lessons learned from the case study of an Asian bank that deploys mobile as an element of its layered security controls.

Background

Because fraud knows no boundaries, banking institutions worldwide now deploy new layered security controls to authenticate online transactions.

In the U.S., the Federal Financial Institutions Examination Council (FFIEC) has issued authentication guidance that specifically lists out-of-band verification among recommended security controls. As the FFIEC details in its guidance: "Out-of-band authentication means that a transaction that is initiated via one delivery channel [e.g., Internet] must be re-authenticated or verified via an independent delivery channel [e.g., telephone] in order for the transaction to be completed. Out-of-band authentication is becoming more popular given that customer PCs are increasingly vulnerable to malware attacks. However, out-of-band authentication directed to or input through the same device that initiates the transaction may not be effective since that device may have been compromised."

With mobile technology, institutions can instantly verify user ID by sending out confirmation messages to the account holder via text message or mobile app -- an out-of-band authentication solution that user two devices, two channels.

But mobile has uses beyond authentication, says Tom Wills, global banking/security strategist. Mobile is also an effective tool



for transaction verification and for issuing customer alerts. And as an out-of-band security control, it falls within the FFIEC's recommendations for methods to help detect and prevent fraudulent ACH/wire transactions.

In this session, Wills shares his insights about mobile technology as a security control, including:

- How out-of-band authentication works and why it's critical to today's banking relationship;
- How mobile compares to other emerging out-of-band authentication methods, such as biometric voice recognition;
- Case study of OCBC Bank in Singapore, where mobile is already being used for out-of-band authentication, transaction verification and customer alerts;
- Strategies for evaluating vendors of mobile technology solutions.

Presented By

Tom Wills, Senior Risk and Fraud Analyst, Javelin Strategy & Research

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=260>

287

Hacktivism: How to Respond

Overview

Is your organization at risk of a hacktivist attack? If so, are you prepared to respond?

The past two years have seen entities such as Sony, the FBI and the Egyptian government fall victim to data leaks, denial-of-service attacks and plain public embarrassment by hacktivist groups such as Anonymous, LulzSec and WikiLeaks.

Hacktivism is a moving target. They are loosely aligned, capable of swift action, and their motivations are less to make a profit than to make a political statement about individuals and organizations with whom they disagree.

So, what needs to happen if your organization becomes a target for hacktivist attack?

The global Information Security Forum has studied the recent surge in hacktivist attacks, and in this session Gregory Nowak of the ISF draws upon the latest research to show:

- How to determine when your organization is at immediate risk of a hacktivist attack;
- How to identify which systems or information might be most at risk;
- Which changes you must initiate in your information security program to protect against hacktivist attacks;
- Ways in which security leaders can raise awareness and cross-organizational response to the hacktivist threat.

Background

Hacktivism - the use of internet technology as a medium of social activism - has been around for years, but emerged as a steady, significant threat in late 2010, when Wikileaks released secret U.S. Department of Defense documents.

Since then, groups such as Anonymous and LulzSec have stepped forward to claim responsibility for hacktivist attacks against entities such as Sony, the CIA, the U.S. Senate and PBS. These attacks - often distributed denial-of-service attacks or network penetration leading to exposure of proprietary information - are meant to express a variety of grievances by the hacktivists.

In 2011 alone, Verizon tracked 855 incidents for its 2012 Data Breach Investigations report, and 58% of all data thefts were tied to activist groups. E-mails, password lists, proprietary documents - hacktivists are after any data they can grab.



“Doubly concerning for many organizations and executives was that target selection by these groups didn’t follow the logical lines of who has money and/or valuable information,” says Verizon in its 2012 report. “Enemies are even scarier when you can’t predict their behavior.”

And while organizations often are prepared to defend against technology-driven attacks such as denial-of-service and e-mail bombs, they are unprepared for the public relations assault that accompanies a hacktivist attack. Hacktivists want publicity, and they will use their attacks - even the mere threat of attack - as a means to increase exposure.

In this session, drawn from the ISF’s latest research on hacktivism, Nowak demonstrates:

- The evolutions of hacktivism, and why your organization must be concerned;
- Steps information security and risk management teams should take to raise awareness about hacktivist attacks;
- Proactive measures every organization should put in place to mitigate hacktivist risks;
- How proper incident response in the wake of a hacktivist attack can preserve, and sometimes enhance, an organization’s reputation.

Presented By

Gregory Nowak, Principal Research Analyst, Information Security Forum

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=287>

83

How Identity Fraud is Evolving and Impacting Customer Trust in Your Financial Institution

Overview

Learn about the latest findings on the impact of identity fraud on your financial institution and your customers:

- Why banking customers are shying away from the online banking channel;
- How stolen identities are used to defraud your customers and damage your brand;
- Which banking channels are most vulnerable to identity fraud;
- How financial institutions are empowering customers to prevent identity fraud;
- The latest phishing trends and tactics to commit identity theft;
- The techniques financial institutions use to protect their brands and customers from identity fraud.

Background

In 2008, over 8 million U.S. adults will be victims of identity fraud. Even more alarming is the fact that over 150 million U.S. consumers don’t bank online out of fear of identity theft.

Learn about the latest findings on the impact of identity fraud on your financial institution and your customers, including:

- Why banking customers are shying away from the online banking channel;
- How stolen identities are used to defraud your customers and damage your brand;
- Which banking channels are most vulnerable to identity fraud;
- How financial institutions are empowering customers to prevent identity fraud;
- The latest phishing trends and tactics to commit identity theft;
- The techniques financial institutions use to protect their brands and customers from identity fraud.

Presented By

John LaCour, Director of AntiPhishing Solutions for MarkMonitor

Rachel Kim, Associate Analyst, Javelin Strategy & Research

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=83>

155

Identity Theft: How to Respond to the New National Crisis

Overview

Your identity - it’s the gold standard of the Internet, and fraudsters are out to capture it. Smart card technology provides one potential solution to the identity theft crisis. Watch this video to hear Neville Pattinson, VP of Government Affairs at Gemalto, discuss:

- The advantages of smart card technology;
- How to apply these solutions specifically in e-government and healthcare reform;
- How to take back control of your identity in the real and virtual worlds.

Background

With the advent of the Social Security number in the 20th century, U.S. citizens were given one single, digital identifier that would distinguish them in their financial, medical and government interactions. Like fingerprints, no two Social Security numbers were alike, and as long as your physical card was secure, so was your identity.

But with the advent of the Internet era, our former strength is now a vulnerability. Fraudsters target people’s personal information, and if they are able to net a Social Security number - they’ve gained the keys to your kingdom.

So, how does one respond with a new solution in this new era?

Smart card technology is one answer, and during this video you will hear from an industry expert on the advantages of smart card technology as a solution to what has become a national identity crisis. Neville Pattinson, VP of Government Affairs at Gemalto, will discuss applicable uses of smart card technology in:

- e-Government 2.0;
- Healthcare reform;
- Immigration.

Presented By

Neville Pattinson, VP of Government Affairs & Standards, NA., Gemalto

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=155>

144

Incident Response: How to React to Payment Card Fraud

Overview

As TJX, Hannaford and Heartland have taught us, incident response isn't just about reacting to your own institution's security breaches - it's about what happens when your card processors, merchants and vendors are compromised.

Register for this session for insight on:

- How to immediately respond to a payment card breach - yours or a partner's;
- Lessons learned from Heartland and other incidents;
- Customer protection: You suspect a customer has been compromised - what do you say and when?

Background

TJX, Hannaford, Heartland. The scenario has played itself out all too frequently in recent years. Fraudsters have gained access to payment card data - not from the banking institutions' own systems, but from their card processors, merchants or third-party service providers. And you know what happened next: fraud perpetrated against thousands of consumers.

In each of these cases, who was left to respond to the incidents by identifying potentially compromised customers, reaching out to them and then mitigating the situations, either by monitoring the accounts or replacing the cards? Answer: The banking institutions that issued the cards.

Payment card fraud is one of the fastest-growing crimes, and fraudsters are constantly searching for new ways to gain illegal access to card data, whether in your hands or those of a third-party service provider.

So what lessons have we learned from these incidents? What new strategies can we employ not just to respond to such incidents after they occur, but perhaps catch them even before they occur, or before damage is done?

In this exclusive webinar, Matthew Speare, a banking/security leader at a major U.S. institution, will share his experience in payment card incident response, focusing on:

- The threat landscape: Where is your institution exposed;
- How to prepare your team to respond immediately to a payment card incident;



- What can be done to help prevent incidents and mitigate fraud;
- Lessons learned from Heartland and other incidents - especially how to handle customers whose accounts may be at risk.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=144>

35

Insider Fraud - Profiling & Prevention

Overview

- Why is insider fraud on the rise now? What are the trends?
- What is the strategy of how to deal with it? Controls, analytics?
- What is the "day in the life" of a case/attack? What process does it typically go through?
- How can one systemize the investigations? Technology, policy, responsibility, priorities, etc.?

Background

The improvement of internal banking systems and data warehousing has made it easier for banking professionals to service customers, but has also created a new set of challenges for information and corporate security managers.

The same data and account access that is required to conduct the day-to-day business of servicing customers can be used to launch an extraordinary range of attacks. As much as we talk about the risk posed by external threats, insider access to customer data and accounts represents a point of compromise that far exceeds that posed by external attacks on sensitive information such as phishing.

Although efforts to protect the customers via review of access policies, scanning for sensitive data and securing external network defenses are necessary, they are not sufficient to protect against attacks perpetrated by malicious insiders.

Countering the employee fraud threat requires a system that can be deployed quickly to leverage the considerable knowledge of these attacks that exists across the industry and in the heads of individual security professionals and investigators. These systems must proactively identify known fraud, allow nimble investigations of suspicious activity and provide a proven path to deploy more advanced profiling and analysis to protect against less frequent but potentially devastating attacks perpetrated by the more sophisticated malicious insider.

Presented By

Kirk McGee, CPP, AVP, Regional Security Officer, TD Banknorth N.A., Springfield, Massachusetts

Paul Henninger, Actimize

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=35>

36

Preventing Phone Fraud with Voice Biometric Authentication

Overview

- Hear about the current state of call center authentication;
- Learn how to apply voiceprint technology to strong authentication for your financial institution;
- Find out how the FFIEC guidelines apply to telephone banking and call centers.

Background

Although FFIEC Guidelines were put in place to help financial institutions secure the online channel, fraudsters have not given up. In fact, they are migrating to channels that aren't as well protected. With cross-channel fraud becoming a growing concern, and FFIEC guidelines being extended to telephone banking, many institutions are looking for solutions to protect their institution, brand and customers across ALL channels.

Nuance, the leader in speech technology, and RSA, the leader in security solutions, join forces to discuss how voice biometric technology can be used as an effective tool in using authentication to protect your institution from phone banking fraudsters.

Dan Faulkner, Director of Product Marketing at Nuance, will join Chuck Buffum, Senior Evangelist for Phone Authentication at RSA, in this timely and topical presentation. Join us to learn from these industry experts:

- The current state of authentication in call centers;
- The implications of the FFIEC guidance on call centers;
- Voice biometric technology and its role in caller authentication;
- Multi-factor risk-based authentication for financial institutions.

Presented By

Dan Faulkner, Director of Product Marketing, Nuance Communications

Chuck Buffum, Senior Product Evangelist, Phone Authentication, RSA, The Security Division of EMC

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=36>

296

Insider Threat: 3 Faces of Risk

Overview

IT sabotage. Intellectual property theft. Employee fraud. These are the three most common insider threats to organizations. But what are the successful solutions for detecting and preventing these crimes? Register for this session to hear first-hand from leading researchers and authors Dawn Cappelli and Randy Trzeciak, as well as security expert and author Christine Meyers:

- What motivates insiders to commit crimes;
- Most common methods of attack;
- Solutions you can use to stop these incidents before they cause damage.

Background

The insider threat: It's a top challenge for any organization, and it's one that Dawn Cappelli and Randy Trzeciak have studied for over a decade.

Cappelli and Trzeciak are both leaders with the CERT Program at Carnegie Mellon University's Software Engineering Institute, and they are the author of a new book, *The CERT Guide to Insider Threats*.

In their work, these researchers have uncovered the three most common types of insider crimes:

IT Sabotage: An insider's use of IT to direct specific harm at an organization or an individual. Common crimes: Deletion of information; bringing down systems; website defacement to embarrass an organization.

Theft of Intellectual Property: An insider's use of IT to steal intellectual property from the organization. This category includes industrial espionage involving insiders, and among the criminals' targets: Proprietary engineering designs; scientific formulas; source code; confidential customer information.

Fraud: An insider's use of IT for the unauthorized modification, addition or deletion of an organization's data (not programs or systems) for personal gain, or theft of information that leads to fraud (identity theft, credit card fraud). Typical crimes: Theft and sale of confidential information (SSN, credit card numbers, etc.); modification of critical data for pay (driver's license records, criminal records, welfare status); stealing of money (financial institutions, government organizations).



In this session, Cappelli and Trzeciak will discuss each of these models of insider crimes, including case studies that detail potential indicators that your organization is at risk.

They will be joined by Christine Meyers, Director of Attachmate's Enterprise Fraud Management solutions, and overseer of the Luminet product. She will discuss security controls that will help detect and prevent these costly insider crimes. She will also provide a 6-step guide to reducing risk across the enterprise.

Presented By

Dawn Cappelli, Technical Manager, CERT Insider Threat Center

Randy Trzeciak, Insider Threat Research Team Technical Lead, CERT

Christine Meyers, Director - Enterprise Fraud Management, Attachmate

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=296>

85

Insider Threats - Safeguarding Financial Enterprise Information Assets

Overview

LendingTree, Societe Generale, TD Ameritrade. These are just a few of the most recent high profile examples of fraud and theft perpetrated by trusted insiders - and its costing these organizations billions of dollars. How is this happening?

- Do you have more employees than active accounts?
- Do you know who is accessing your applications?
- Can you enforce password policy across all your users?
- Do you have visibility into all access activities across disparate systems?

Background

Societe Generale being a prime example - in a business environment, 32% of all fraud and theft is perpetrated by trusted employees, so enforcing and monitoring employee access to information assets is critical. In fact, it's not only critical, it's also a legal requirement in a growing number of government regulations and industry mandates.

Through seamless integration of discrete security and identity management systems, Imprivata manages the risks and consequences inherent with ensuring networks and applications are only accessed by authorized employees.

This Imprivata webinar will help you strengthen your enterprise security posture by:

- Enforcing who gets access to corporate networks and applications;
- Enforcing password policy across all users;
- Providing visibility into all user access activities across disparate systems;
- Locking down all user network and application access;
- Providing a more comprehensive security infrastructure by integrating physical access with IT and data access.

Presented By

Geoff Hogan, SVP - Business Development & Product Management/Marketing, Imprivata

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=85>

169

U.S. Dept. of Justice on Payment Card Fraud Trends & Threats

Overview

Credit and debit cards are under increased attack by fraudsters, and organizations need to step up their efforts to protect their customers - and themselves.

Join Kimberly Peretti, former senior counsel with the U.S. Dept. of Justice, for her insider's tips on:

- Trends in debit and other payment card thefts;
- Lessons learned from the TJX, Hannaford and Heartland breaches;
- What you can do to avoid being the next victim.

Background

Ten years ago, the Department of Justice was prosecuting mischief-makers for defacing web pages. Today, federal prosecutors are targeting international crime rings behind high-profile hacks.

Kimberly Peretti, former senior counsel in the department's computer crime section, who played a prominent role in prosecutions against notorious international hackers such as Albert Gonzalez, offers an insider's view of financial data breaches. In this session, she will cover:

- Background on carding: discussion on the current "carding scene," carding forums and carding activity (online, in-store, gift cards, PIN cashing);
- Evolution of prosecutions: From carding forums in 2004 to major resellers in 2006, and now the new, international hacking rings - including the Gonzalez case;
- What we know: Lessons learned from the breaches and the criminals, as well as emerging methods - and victims;
- How we can respond: Emerging technologies and steps organizations can take today to minimize their exposure to financial data breaches.

Presented By

Kim Peretti, J.D., LL.M., CISSP, PricewaterhouseCoopers

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=169>

178

Man-in-the-Browser Attacks: Strategies to Fight the Latest Round in Online Fraud

Overview

Business banking account fraud cases have dramatically increased in 2010. In order to remain secure, it is essential for banks to understand new strategies fraudsters are implementing and the latest trends and threats. Attend this session to discover:

- The current state of online fraud in 2010 - latest threats, trends, and vulnerabilities;
- How to protect against attacks - including “man-in-the-browser”;
- Steps to secure your largest and most lucrative business account customers.

Background

Man-in-the-browser attacks are the state of the art in online banking fraud. And the criminal community is heavily focusing these attacks on business-banking customers, where the available funds are often greater, transaction limits are higher and the business customer has a lucrative target with access to a wire transfer or automated clearing house (ACH) services through its online-banking interface.

While many safeguards are deployed within financial institutions, criminals are evolving their techniques rapidly, and many of the security methods are simply not effective against man-in-the-browser attacks - particularly when the business customer is the target.

In this timely session, Eric Skinner, CTO of Entrust, will look at:

- The current state of online fraud;
- How the evolution of these threats affects online transactions;
- Approaches that can be effective in addressing the latest online threats - and in particular, man-in-the-browser attacks.

Presented By

Eric Skinner, CTO, Entrust

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=178>

279

Mobile Banking: Trends, Threats and Fraud Prevention Techniques

Overview

As financial institutions expand their mobile banking services, fraudsters certainly will be close behind. This webinar will cover the expanding use of mobile banking and the fraud threats that are lurking, including:

- The explosive growth of smartphone ownership and the resulting demand for improved mobile services;
- Trends in mobile banking services, and the inherent risks associated with smartphone usage;
- The threats that lurk as fraudsters escalate attacks against the mobile channel;
- Fraud detection and prevention techniques based on each user’s unique mobile banking behavior.

Background

Over half of U.S. adults already have smartphones, and Forrester Research predicts that by 2015 one in five U.S. adults will be using mobile banking. If a financial institution doesn’t offer the desired mobile services, it runs the risk of losing clients. But with such growth, we all know that the fraudsters won’t be far behind. So, how will account holders be using their mobile devices, how does that increase fraud threats and how do financial institutions mitigate the resulting risk? Register for this webinar and learn:

- The state of smartphone ownership and mobile banking adoption and functionality;
- Usage patterns and behaviors that make smartphones particularly attractive to cyber criminals;
- Fraud threats that have already been spotted in the wild and how they take advantage of unique smartphone characteristics;
- Behavior-based techniques that some financial institutions are already using to detect mobile banking fraud attacks;
- Anomaly detection solutions that prevent fraud and also conform to the FFIEC Guidance.

Presented By

Chris Silveira, Manager of Fraud Intelligence, Guardian Analytics

Tiffany Riley, VP - Marketing, Guardian Analytics

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=279>

277

Synovus Bank Eliminates Cybercrime - A Case Study

Overview

Synovus Bank rolled-out Trusteer Rapport to their customers to protect them against online banking fraud and meet regulatory requirements.

This webinar will detail:

- Synovus Bank’s challenges, layered security strategy and the impact of online banking fraud;
- The solution selection process and criteria;
- The various promotional, educational and awareness tools used to drive end-user adoption;
- The results - zero fraud instances since implementing Trusteer Rapport;
- Trusteer’s Cybercrime Prevention Architecture - adaptive protection, layered security and real time cybercrime intelligence.

Background

Synovus Bank, one of the largest community banks in the southeast, offers Online Cash Management services to its commercial clients with a simple pledge: “The freedom to manage your cash position anytime, anywhere.” After witnessing relentless cyber-attacks on the endpoints of end users, Synovus Bank knew that meeting this pledge required them to take action. The bank’s product development team carefully selected an endpoint security solution that met their requirements:

- Satisfying FFIEC Guidelines;
- Low customer impact/Ease of installation;
- Proven effective, quick to implement and easy to manage;
- Complement the bank’s two tier security architecture.

Hear how Synovus Bank proactively prevents fraud. Kevin Gibson, Director of Product Development at Synovus Bank, explains the challenges they faced, why Trusteer Rapport was the right fit, and its ease-of-deployment. He also discusses how Trusteer’s layered security helps them protect against cybercrime, as well as Trusteer’s role in enabling compliance with the latest FFIEC guidance. Trusteer’s Director of Product Marketing, Oren Kedem, will describe Trusteer’s Cybercrime Prevention Architecture and how it stops online banking fraud.



Presented By

Oren Kedem, Director - Product Marketing, Trusteer

Kevin Gibson, Director - eCommerce, Synovus Financial Corp

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=277>

256

The Many Faces of Online Banking Fraud Attacks

Overview

Cyber criminals are continually advancing their techniques to defeat modern online banking defenses. This puts financial institutions in the position of defending against an ever-growing set of attacks. Identifying the best fraud prevention strategy requires an understanding of the wide array of schemes and how they work from start to finish.

Craig Priess, Guardian Analytics Founder and Vice President of Products, will describe the newest fraud attack schemes, how they're able to defeat today's defenses, and anomaly detection as a proven solution that financial institutions can use to defend themselves and their account holders.

You will learn:

- The latest advances in malware that are enabling fraudsters to move faster than ever to avoid detection;
- How typical controls, such as dual controls, are being defeated;
- How anomaly detection can prevent fraud regardless of what scheme the fraudsters are using;
- Why the FFIEC included anomaly detection as a minimum requirement of a layered security program.

Background

Cyber criminals are aggressively advancing their techniques for defeating online banking defenses while continuing to use tried and true methods to execute online banking fraud and steal money undetected. This puts financial institutions in the position of defending against an ever-expanding mix of attacks.

Identifying the best strategy for protecting account holders and your institution requires an understanding of the wide array of malware and human-based attacks against online banking and how they work from start to finish.

Craig Priess, Guardian Analytics Founder and Vice President of Products, has analyzed data from hundreds of banks to understand the latest wire, ACH and other payments fraud attacks. Based on his findings, as well as recent fraud research, Craig will present:

- The newest malware schemes that are enabling fraudsters to move faster than ever to avoid detection;
- Why "low-tech" fraud attacks are still successful;
- How typical defenses, such as dual controls, are being routinely defeated;



- How malware is directly attacking end-user security;
- The methods criminals use to get account holders themselves to unknowingly execute fraud.

Craig also will discuss how financial institutions can use anomaly detection to stop the widest array of attacks because it detects fraud based on online banking behavior, regardless of the fraud scheme that's in play. Its proven ability to detect fraud that other solutions miss is a big part of why the FFIEC is now requiring anomaly detection as a minimum element of a layered security program.

Presented By

Tiffany Riley, VP - Marketing, Guardian Analytics

Craig Priess, Founder & VP - Products, Guardian Analytics

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=256>

196

The Faces of Fraud: How to Counter 2011's Biggest Threats

Overview

Payment card breaches, check fraud and phishing/vishing - these are the most common forms of fraud striking banking institutions today. Yet, what form of fraud do institutions feel most prepared to prevent? Money laundering.

This is just one of the sobering results from the Faces of Fraud: Fighting Back study conducted by BankInfoSecurity. Join a distinguished panel of fraud experts for an exclusive look at the eye-opening survey results and how institutions can act upon them, including:

- How to ensure you're prepared to defend against the most common fraud threats;
- Bridging institutional silos that stand in the way of fighting fraud;
- How to improve employee and customer awareness, ensuring that fraud prevention is a shared responsibility.

Background

Payment cards, bogus checks, phishing and vishing scams - we know what today's top fraud threats are to financial institutions. But how are these organizations fighting back? What are the most successful strategies for detecting and deterring threats, as well as educating customers and obtaining resources? These questions - and answers - are the basis of this webinar exploring the results of the survey, The Faces of Fraud: Fighting Back.

Administered electronically by Information Security Media Group (ISMG), publisher of BankInfoSecurity, this survey was crafted with guidance from industry thought-leaders, with a mission to:

- Gauge the scope of the multi-faceted fraud threat to U.S. banking institutions;
- Measure the industry's preparedness for evolving threats;
- Identify specific strategies and solutions employed by banking/security leaders to fight fraud;
- Predict the emerging technologies and strategies where institutions are investing their resources.

From bogus ACH transactions to ATM skimming and to identity theft via payment cards and deposit accounts, the forms of fraud haven't changed in recent years. But the scale and coordination of these attacks has evolved, and banking institutions today find



themselves facing not just individual fraudsters, but sophisticated criminal rings that are constantly probing for new ways to hack into consumer and commercial accounts via all available channels.

News headlines have been dominated by ATM skimming sprees, the ACH epidemic and the aftermath of the Heartland Payment Systems breach - the largest financial hack ever reported. But behind the scenes, institutions are just as concerned with check, first-party and mortgage fraud, malware proliferation, as well as emerging threats in mobile banking and social media. Beyond the actual threats, institutions are similarly challenged by a lack of resources to fight fraud, as well as a dearth of guidance from regulators and associations re: common threats, successful strategies and emerging solutions.

The discussion of the Faces of Fraud survey will review this complex threat landscape, analyzing:

- Which are the most common forms of fraud being experienced today?
- Where do institutions feel most - and least - prepared to fight fraud?
- What are the technology solutions that organizations need now to help detect and prevent fraud?

Presented By

Mike Urban, Director of Portfolio Management, Fiserv

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

Tom Field, Editorial Director, Information Security Media Group

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=196>

192

The Fraud Deficit: Why Deposit Account Fraud Budgets Need to Shrink

Overview

To effectively manage fraud prevention teams, processes and technology, banks and credit unions must establish annual fraud “budgets” to predict, measure and account for losses and other related costs. Explore the impact of thinking of fraud as a budgeted expense which is “under control” as long as the budget is met and how new approaches can shrink fraud budgets and increase bank profits.

Join industry experts Andy Schmidt, George Tubin and Shirley Inscoe as they discuss:

- The true cost of deposit account fraud;
- Why many fraud budgets are too high;
- Why check fraud losses continue to go up;
- How to effectively engage senior management.

Background

The most recent American Bankers Association Survey reports >\$1B in deposit account fraud losses at banks in North America and nearly \$12B in attempts. The amount is significant, as are the considerable resources dedicated to containing the problem. What’s surprising is the fact that many institutions consider deposit account fraud - specifically check fraud - a “covered” problem or a “budgeted expense,” when reducing these costs could have a material impact on profitability and free up resources to strengthen defenses against other fraud threats.

Join TowerGroup analysts Andy Schmidt and George Tubin, and industry veteran Shirley Inscoe, as they explore how many banks are rethinking deposit account fraud and making it a focal point of their cross-channel fraud management strategy. Hear early results from a TowerGroup survey regarding current perspectives towards fraud management. Learn about the tools and techniques required to reduce fraud budgets with confidence and to secure executive support in the effort to rethink fraud.

Register for this webinar to learn:

- Why the decline in check volume will not lead to a decline in check fraud losses or attempts;



- Why deposit account fraud defenses are a critical component of a cross channel fraud management strategy;
- How new approaches to check, deposit and kiting fraud enable loss prevention teams to catch more fraud, more accurately and more efficiently;
- What steps can be taken to help senior management “rethink fraud.”

Presented By

George Tubin, Banking and Security Analyst

Andy Schmidt, Research Director - Global Payments, TowerGroup, Inc.

Shirley Inscoe, Director - Financial Services Solutions, Memento

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=192>

267

The Fraud Dilemma: How to Prioritize Anti-Fraud Investments

Overview

Device identification. Anomaly detection. Transaction verification. When it comes to fraud prevention, there are nearly as many options as there are threats. So, how do you best prioritize your own investments in anti-fraud solutions?

Join this panel of experts, led by financial fraud expert George Tubin, as they explore:

- Today’s top fraud threats;
- How to plan your technology investments;
- Tips to secure internal buy-in for anti-fraud investments.

Background

In light of increasingly sophisticated fraud techniques - everything from account takeover attempts to ATM skimming and increasingly sophisticated phishing attacks - financial institutions are under constant pressure to protect customer assets.

Further, embodied by the FFIEC Authentication Guidance, they face heightened regulatory pressure to assess risks, deploy layered security controls and to improve customer awareness of this ever-evolving threat landscape.

And a single misstep could result in a data breach that carries heavy financial, regulatory, customer, shareholder and reputational implications.

Among the anti-fraud options available to banks:

- Device authentication/identification, which has a wide spectrum of approaches, some better than others.
- Malware detection and mitigation, operating either from the cloud or on a user’s device to reduce Man-in-the-Browser fraud from compromised endpoints.
- Anomaly detection, which can take the form of simple rules to complex cross-channel behavioral analysis.
- Transaction verification, which can be rules-based or triggered by anomaly detection and can then take several forms (token, SMS, phone verification, dual authorization).

So, how does an institution go about evaluating all of these options and deciding which fits its own risk profile best?

In this panel discussion, banking/fraud expert George Tubin will lead a lively discussion of today’s top fraud threats and solutions.

Among the topics to be tackled:



- Regulatory Requirements - What are the basic expectations for assessing and mitigating fraud risks?
- Investment Planning – What’s your institution’s fraud loss profile, and how can you best match mitigation approaches to your identified risks?
- Selling the Solution - Once you’ve identified your anti-fraud solutions, how do you demonstrate value to stakeholders, and then win support for a prioritized investment plan?

Presented By

George Tubin, Banking and Security Analyst

Alisdair Faulkner, Chief Products Officer, ThreatMetrix

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=267>

211

ZeuS and Other Malware Threats Force Authentication to “Step Out” Of Band

Overview

Malware like ZeuS has rapidly outpaced all other banking security threats, and, according to a survey by PhoneFactor, is regarded as the greatest threat to online banking today. Because malware has evolved to defeat most security measures currently in place, financial institutions must likewise evolve their security practices to stay ahead of these threats. Regulators are following suit with an update to the FFIEC guidance on Authentication in an Internet Banking Environment expected soon.

As malware has become more pervasive and more sophisticated, out-of-band authentication and transaction verification have taken on a new level of importance for financial institutions and regulators. Instead of trying to rid the world of malware, institutions can simply circumvent malware by “stepping out” of band to authenticate transactions.

Join PhoneFactor CTO Steve Dispensa and Vice President of Marketing & Product Management Sarah Fender for this empowering webcast as they:

- Share insights from their latest research on online banking security;
- Dissect current malware threats and present the latest best practices for mitigating them;
- Explore the role of out-of-band authentication and transaction verification in preventing fraud.

Background

Real-time attacks from malware like ZeuS have rapidly become online banking’s number one security threat. As malware continues to evolve so must the security measures employed by financial institutions to protect online banking customers. Countless banks have learned the hard way - many unfortunately after a successful attack - that the security they had in place was not sufficient. A number of banks have already added measures, such as out-of-band authentication and transaction verification, to their online banking applications, realizing the importance these methods have in preventing online fraud.

The FFIEC is expected to endorse these practices in an upcoming update to the Guidance on Authentication in Online Banking. In addition to calling for a strengthening of authentication



mechanisms, such as out-of-band, the updated FFIEC Guidance is likely to recommend a layered security approach that applies security controls to both logins and transactions.

PhoneFactor CTO Steve Dispensa and Vice President of Marketing & Product Management Sarah Fender will explain to you why “stepping out-of-band” is so important. They will start by sharing data from PhoneFactor’s recent Survey on Online Banking Security, which polled financial services professionals from more than 70 financial institutions regarding the threats facing online banking today, what banks are doing to protect their customers and perceptions about the role security plays in customer loyalty.

Dispensa and Fender will also talk in depth about ZeuS, SpyEye and other malware prevalent in the banking industry. This includes how these attacks work, how they continue to transform and how you can mitigate against them. They will also explain why phone-based out-of-band authentication is a best practice in the fight against malware.

This discussion will leave you with an understanding of the value of layering transaction verification on top of out-of-band authentication to prevent online banking fraud. It is well worth your time to learn why you should “step out” of band.

Presented By

Sarah Fender, VP - Marketing & Product Management, PhoneFactor

Steve Dispensa, CTO & Co-Founder, PhoneFactor

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=211>

160

Automating Security Controls Within Government Information Systems

Overview

In this webcast you’ll learn how to:

- Help automate the testing and reporting of all of the technical controls found in the NIST 800-53A framework;
- Use file integrity checks to assure your systems are in a desired state;
- Provide snapshots allowing side comparisons of a system at different time stamps;
- Test system configurations against external and/or internal policies;
- Automate documentation and report on failures for internal/external audit teams, system administrators and/or agency executives.

Background

The nation’s federal and private-sector infrastructure systems are at risk because adequate cyber security controls are not in place. FISMA required agencies to enhance their security posture by instituting a process for assessing, testing and managing IT security. However, this requirement is not enough to protect organizations’ IT systems.

A new approach is needed to fully secure data and access to IT systems, an approach that clarifies requirements and uses automated solutions that manage configuration assessment. Tripwire helps simplify the task of automating compliance by combining change detection and reporting with configuration assessment capabilities.

Presented By

Chris Orr, Systems Engineer, Tripwire

Brian Clark, Account Executive, Tripwire

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=160>

162

Data Protection and Incident Response

Overview

Public and private sector organizations alike are charged with protecting critical data and responding to incidents that put information security at risk. In this session, David Matthews, deputy CISO for the City of Seattle, reveals:

- Data protection challenges;
- Tools to meet those challenges;
- How to respond to security incidents.

Background

Hackers. Insiders. Man-made or natural disasters. These are among the forces that threaten data critical to private and public sector organizations. And they force information security leaders to constantly be vigilant in data protection and incident response.

In this webinar, David Matthews, deputy CISO for the city of Seattle, will give an inside view into the challenges he faces every day - from the benign and accidental to the intentional and potentially devastating.

Offering a unique government perspective, Matthews will discuss:

- The specific data protection issues that face local governments;
- Which tools, procedures and training are used to address those issues;
- How to respond when data is lost or systems are compromised.

Matthews also will offer first-hand insight on incident response procedure, as well as roles and responsibilities for information security staff.

And how does a real security incident unfold? Matthews will take you inside a real case study from his experience.

Presented By

David Matthews, Deputy Chief Information Security Officer for the City of Seattle

Geoff Glave, Product Manager, Absolute Software

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=162>

87

Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks



Overview

Minimize your insider threat.

Can your organization afford the potential cost of one bad hire? We're talking:

- Negligent hiring cases in which employers lose 60% of the time, with average verdicts of \$3 million;
- Average out-of-court settlements of \$500,000 and attorney fees.

And what is the one question everyone will ask you if there is a bad hire? "Did you conduct a background check?"

Avoid financial and reputational risk from bad hires. Register for this session to learn:

- Best-practices to keep your organization productive and out of court when hiring the best possible candidates;
- How to obtain and utilize criminal records and background information on job applicants;
- Lessons from case studies to demonstrate what steps employers should take and mistakes to avoid;
- 10 steps a firm can take immediately at NO COST to avoid a bad hire.

Background

All employers have an obligation to exercise a reasonable duty of care in hiring. In addition, many organizations have a legal duty to not employ individuals with certain enumerated criminal records. There are a number of steps that employers can take in the hiring process to reduce their risk when hiring.

First, organizations must carefully review and audit their hiring program, including their application, interview and past employment checking practices, as well as procedures for performing criminal record checks. In addition, employers need to consider a host of legal considerations when screening applicants, including the federal Fair Credit Reporting Act (FCRA), state laws, Sarbanes-Oxley and discrimination laws, as well as privacy implications.

Topics to be discussed in this session include:

- The "Parade of Horrible" facing employers that hire without screening, and why background checks are mission-critical for financial institutions;
- The essential elements of negligent hiring lawsuits, employer defenses and why they are on the rise;
- Why "gut" instinct is not an effective hiring tool;
- The essential elements of a screening program;
- Compliance with the federal Fair Credit Reporting Act (FCRA) and State laws;
- The impact of discrimination laws and privacy laws;
- Best practices for hiring, including the application interview and past employment checking processes;
- How to legally obtain and utilize criminal records;
- Issues affecting past employment, education and credentials verification;
- The use and limitations of credit reports;
- A brief introduction to international background checks and terrorist screenings;
- The use of the Internet and social networking sites such as Facebook and MySpace to screen applicants;
- An introduction to drug testing.

Presented By

Lester Rosen, Attorney & President, Employment Screening Resources

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=87>

11

Board Responsibilities for IT Risk Management: Building Blocks for a Secure System



Overview

Board members and senior management are responsible for planning and implementing an IT risk management system that works. But they must understand the risks and safeguards - and in these challenging times they especially must know their legal accountability, as dictated by such regulations as the Gramm-Leach-Bliley Act (GLBA) and the ID Theft Red Flags Rule.

Register for this webinar to learn:

- Comprehensive guidance on information security specifically for board members;
- The board's role in planning, researching and implementing an information security program;
- Tips and techniques for information security administration and management.

Background

Safeguarding information assets might sound like a task for the technical team. However, when it comes to information security breaches, your board of directors is ultimately accountable. Board members and senior management are responsible for planning and implementing an IT risk management system that works. To do so, they must understand the risks and safeguards required to govern and maintain a secure environment.

Customer confidence and trust is one key to banking success. That trust is only as secure as the IT risk management system board members and senior management decide to implement. By implementing a system that identifies, measures, manages and controls risks to data and systems, you can protect your institution's reputation and adhere to regulatory mandates and laws. The Gramm-Leach-Bliley Act and section 216 of the Fair and Accurate Credit Transactions Act require strict administrative, technical and physical safeguards. Is your institution in compliance or at risk?

Does your board of directors have a firm understanding of the institution's information security programs and policies? What methods will they use to assess how well the institution is adhering to these policies? Better understanding and tools for risk management success are just a click away.

Our "Board Responsibilities for IT Risk Management" workshop will help ensure that board members have a firm understanding of risk assessment, security controls, monitoring, testing and training techniques.

Presented By

Bill Sewall, Information Security, Compliance and Risk Management Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=11>

150

Creating a Culture of Security - Top 10 Elements of an Information Security Program

Overview

The Obama Administration has a heavy emphasis on information security, and already we're seeing greater attention paid to cybersecurity and FISMA reform. Now is the time for government agencies to benchmark and strengthen their information security programs.

Learn from security veteran Patrick Howard, CISO of the Nuclear Regulatory Commission, on how to:

- Develop the security program and policy;
- Manage security risks;
- Provide user awareness, training and education;
- Respond to incidents.

Background

The Federal Information Security Management Act of 2002 (FISMA) mandates that each federal agency develop a program to provide information security for data and systems that support the agency's functions.

And while agencies have had varying success meeting the demands of FISMA, the Obama Administration has ushered in a new wave of information security proponents eager to bolster these programs and create a new, higher level of cybersecurity throughout government.

But how does an agency first benchmark, then strengthen, its information security program?

Patrick Howard, a veteran security leader who currently oversees information security operations at the Nuclear Regulatory Commission (NRC), proposes a 10-step program to ensure solid protection. In this exclusive webinar, Howard will outline these 10 critical steps, including:

Develop the Security Program and Policy - How to define the security program, adopt best practices, assign roles and responsibilities.

Manage Security Risks - How to determine what needs to be protected, identify threats to security and privacy of information assets, manage remediation of weaknesses.



Provide User Awareness, Training and Education - How to offer new employee training, ongoing user awareness, security staff education/certification.

Respond to Incidents - How to create an effective incident response plan, law enforcement notification, customer breach notification, forensics and preservation of evidence.

Other areas Howard will touch upon include:

- Planning for security;
- Organizing for security;
- Establishing and enforcing system access controls;
- Implementing configuration management process;
- Monitoring security posture;
- Planning for contingencies.

Presented By

Patrick Howard, Chief Information Security Officer, Nuclear Regulatory Commission

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=150>

20

Developing an Effective Information Security Awareness Training Program - Getting the Word Out

Overview

From GLBA to the ID Theft Red Flags Rule, information security awareness is a lynchpin of banking regulatory guidance. Register for this webinar to learn:

- Fundamentals of an information security education program;
- How to structure your program to satisfy the requirement and the need;
- How to prepare and deliver an effective training program.

Background

The Interagency Guidelines Establishing Information Security Standards, per Gramm-Leach-Bliley Act (GLBA) of 2001, require each banking institution to have a comprehensive written information security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the bank. This program must include security awareness training to inform personnel of information security risks associated with the activities of personnel, as well as responsibilities of personnel in complying with bank policies and procedures designed to reduce such risk.

The ID Theft Red Flags Rule requires proof of ID theft awareness programs for institution employees and customers.

So, how does an institution deploy an education program that meets both the regulatory and workplace needs? Attend this presentation for hands-on advice on:

- Fundamental components of an information security education program;
- Setting goals, creating content and leveraging media effectively;
- How to prepare and deliver good awareness materials.

Presented By

Bill Sewall, Information Security, Compliance and Risk Management Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=20>

50

How to Prevent Data Leakage from Compromising Your Company's Security

Overview

In this webinar we will cover:

- Four sources of potential abuse and four advanced technologies that can eliminate internal threats to data;
- Using the Internet equivalent of credit scores to identify and stop cyber-criminals;
- Web 2.0 threats that can compromise your company's and your customers' security;
- The importance of bi-directional gateway security in protecting customer-critical information.

Background

Industry and government regulations such as PCI, GLBA and SOX can provide guidance on data protection, but they don't go far enough. Even with these rules in place, identity theft, data breaches and data theft are the fastest growing crimes in the U.S.

Studies of identity theft between 2000-2006 found 1.8 billion records have been compromised. Hundreds of thousands of computers are turned into zombies every day, creating vast networks of spam and malware cannons.

Listen to this webinar on turning your network, messaging and web gateways into security gateways, using strong bi-directional technologies that can ferret out infected computers, prevent data loss and eliminate Internet threats. If you are responsible for e-mail, messaging, web or network security for a financial institution of any size, then this webinar is for you. After all, if you don't control the data that's entrusted to you ... someone else certainly will.

Presented By

Elan Winkler, Director of Messaging Product Marketing, Secure Computing Corporation

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=50>

244

FFIEC Authentication Guidance: Customer Education - Developing a Program That's Effective and Meets Regulatory Expectations

Overview

For too long, banking institutions have paid only lip service to the need for developing information security awareness and education programs for their customers.

But now, as directed by the FFIEC Authentication Guidance, institutions as of January 2012 are expected to manage a robust awareness and education effort for retail and commercial customers alike.

But what is an effective awareness/education program, and how can it be rolled out online and in person to the customers who need it most?

Join an information security leader at a major U.S. bank for practical insights on how to:

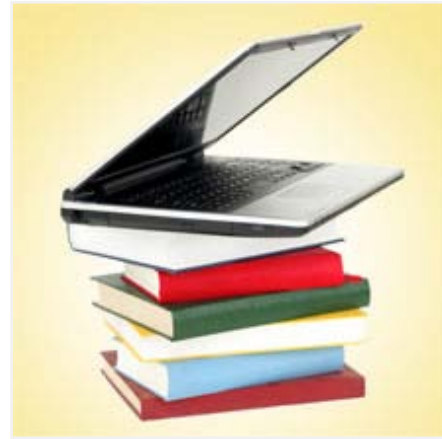
- Assess the awareness/education needs of retail and commercial customers;
- Create an effective program that includes online, print and in-person components;
- Develop an education and awareness strategy that is regularly updated and improved by customer feedback;
- Develop a program that meets the regulatory requirements.

Background

When it comes to information security risks to retail and commercial customers, awareness and education programs have been much like the proverbial weather. Many institutions talked about these programs, but few implemented successful ones.

But now, with the advent of the 2011 supplement to the FFIEC Authentication Guidance, banking regulators are putting institutions on notice that they now will be examined on the efficacy of their customer education programs.

In part, this new emphasis is in response to the recent spate of ACH/wire fraud incidents, which defrauded unsuspecting commercial customers - many of whom did not realize their losses were not automatically reimbursed by the institutions. The new guidance calls for customer awareness and educational



efforts tailored for retail and commercial account holders and, at a minimum, to include these elements:

- An explanation of protections provided - and not provided - to account holders;
- An explanation of how and why the institution might contact a customer on an unsolicited basis and ask for the customer's electronic banking credentials;
- Advice for commercial online banking customers to perform periodic risk assessments;
- A listing of risk control mechanisms that customers may consider implementing to mitigate their own risk, or at the very least a listing of available resources where such information can be found;
- A contact list for customers to use if they notice suspicious account activity or experience any security-related events.

To offer practical tips from his own institution's experience, Joe Rogalski of First Niagara Bank will outline his robust customer education/awareness program and show how - and where - it touches retail and commercial customers in multiple forms.

Presented By

Joe Rogalski, SVP, First Niagara Bank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=244>

89

Fighting Fraud: Stop Social Engineers in Their Tracks

Overview

Social engineering is the ultimate con - the bag of tricks employed by fraudsters who will lie, cheat and steal their way past your organization's security controls. Their goals: theft, fraud or espionage. Your best line of defense: Your people.

Fraud incidents are on the rise, especially in financial services and healthcare, and many of these crimes result from social engineers pulling off deception in person, via the telephone and through popular social networking sites.

Register for this webinar to hear directly from a former FBI Special Agent on:

- What social engineering is;
- The latest scams;
- Why social engineering is so effective;
- Steps to take to prevent "being socialized."

The presenter, E.J. Hilbert, is a former FBI Special Agent specializing in international hacking, carding and fraud teams. He has trained law enforcement representatives throughout the U.S., Canada, the United Kingdom, Belarus, Russia and the Ukraine.

Background

Despite all the media hype about hackers and viruses, the greatest threats to an organization's information security are the employees of the company. They're the ones who too often, too willingly, fall victim to social engineering ploys and open the doors wide to slick-tongued fraudsters.

When an intruder targets an organization for attack, be it for theft, fraud, or economic espionage, the first step is reconnaissance. They need to know their target. The easiest way to conduct this task is by gleaning information from those that know the company best. Their information gathering can range from simple phone calls to dumpster diving. It's not beyond an attacker to use everything at their disposal to gain information.

Being cognizant of these types of attacks, educating your employees about the methodologies of the attacks and having a plan in place to mitigate them are essential to surviving these manipulations.



This presentation focuses on the core issues of social engineering's methodologies, effectiveness and prevention - as well as how to test the effectiveness of your training efforts. These core components include:

- Identifying the many forms in which the attack may occur;
- Understanding the intention of the attack;
- Educating the potential victims;
- Creating a policy to minimize the impact of the attack;
- Testing employees' abilities to sniff out social engineering scams;
- Managing a program to ensure that ongoing reviews and updates are in place;
- Regular testing to ensure the effectiveness of your training initiatives.

You will understand social engineering methodologies, why it is the most effective tool in attacking a company and why so many people fall victim. You will also learn how the importance of effective corporate communication and incident response planning can prevent attacks from occurring in the first place. You will discover new ways to test the effectiveness of your awareness efforts. And finally you will learn what to do "next" after the attack has occurred. Can you put the genie back in the bottle? Yes, if you know where the genie is likely to go next.

Presented By

E.J. Hilbert, Former FBI Special Agent

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=89>

250

How to Build a Successful Enterprise Risk Management Program



Overview

An enterprise risk management program is more than a collection of organizational functions. ERM integrates all risk efforts under one set of common definitions, process framework and system solutions. Join a banking/security leader to hear how she developed and grew her institution's ERM program, including how to:

- Determine your organization's risk appetite;
- Initiate an ERM program;
- Monitor on an ongoing basis your alignment of strategy, risks, controls, compliance, incentives and people.

Background

Enterprise risk management is not just a function of an organization. It's a culture that can be developed and enhanced. Each leader already plays a risk management role for its organization. ERM is the organization's umbrella effort of risk management, and it is three dimensional because it:

- Integrates all risk efforts under one set of common definitions, process framework and system solutions;
- Brings together the different types of risks, the time spectrum and the organization's decision frame;
- Is a continuous process and evolves and matures with the organization.

A common set of definitions, process framework and system solutions allows the ERM team to bring all risk management efforts together to set the appropriate risk tolerance levels for the organization and each function, bring transparency on risk management efforts and resource allocations and create synergy in risk management efforts and renders more effectiveness.

Each function will identify and treat risks associated with its functional orientation. There's a benefit in synchronizing the risk types, with its time character and the organization's decision frame to provide a more holistic and integrated coverage.

And finally, risk management is a process, not a project. Thus, it should be customized to your organization's culture and risk appetite. Just like any process, it needs to continuously refine

and reevaluate its approaches, seek feedback, be supported by a common system solution and celebrate successes along its journey.

GRC programs promote the timely, consistent and accurate capture and maintenance of all material issues, arising during the course of business, in an auditable system of record. GRC, like ERM, is three dimensional, and is comprised of:

- Performance management, which addresses reliable achievement of objectives through effective management of business processes that are visibly and objectively measured;
- Risk management, which addresses managing the uncertainty associated with the pursuit of objectives;
- Compliance, which addresses voluntary promises that must be kept and laws and regulations that must be obeyed as objectives are pursued.

Together, ERM and GRC promote transparency, contingency and risk appetite aspects of the corporate planning and strategy process by:

- Addressing considerations that fall beyond the boundaries of business/economic scenarios;
- Substantiating, or eliminating, any contingencies;
- Helping to accurately shape objectives to ensure the board-directed risk return trade-offs are reflected.

Presented By

Mona Leung, CFO, Alliant CU

Clark Abrahams, Director - Global Marketing, SAS

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=250>

135

How to Develop & Maintain Information Security Policies & Procedures



Overview

Information security policies and procedures are the cornerstone of any information security program - and they are among the items that typically receive the greatest scrutiny from examiners and regulators. Cursory, disconnected or poorly communicated security policies will fail and likely drag down the overall information security program with them.

Register for this webinar to learn:

- How to ensure your policies map to your own institution's risk profile;
- How to structure your policies and presentations to senior management and board members;
- The basics of information security policies and what they must cover.

Background

Information security policies and procedures are the cornerstone of any information security program - and they are among the items that typically receive the greatest scrutiny from examiners and regulators.

But beyond satisfying examiners, clear and practical policies and procedures define an organization's expectations for security and how to meet those expectations. With a good set of policies and procedures, employees, customers, partners and vendors all know where you stand and where they fit in re: information security.

The key to creating effective policies and procedures is to start with a solid risk assessment, and then follow a measured program that includes:

- Implementation;
- Monitoring;
- Testing;
- Reporting.

This webinar is designed for IT professionals, risk managers, auditors or compliance officers who are responsible for writing, approving or reviewing security policies or procedures.

It's a daunting task to create effective policies and procedures, and it's ongoing work to monitor and maintain them. But in this age of endless information security threats, please remember: Policies and procedures aren't just a "nice to have" - they're a must.

Presented By

Bill Sewall, Information Security, Compliance and Risk Management Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=135>

137

Information Security for Management – What Your Senior Leaders Need to Know

Overview

In most cases, especially in this time of financial crisis, information security should not be the most important issue for a financial institution or government agency -- but if neglected, it will inevitably become a critical factor in the organization's continuing viability.

This "Information Security for Management" webinar focuses on helping managers understand the importance and impact of information security on their organization and their role in setting the direction for good security practices. In particular, the presentation provides guidance on:

- Instituting an efficient information security governance structure;
- Ensuring all employees are aware of their responsibilities;
- Anticipating and mitigating risks from third-party service providers;
- Assessing the organization's risks - including the insider threat;
- Setting up an effective metric reporting process and preparing for security incidents.

Background

Information security is one of several business risks that management must address as part of its day-to-day responsibilities.

The simplest and most efficient solution to avoiding a major incident is incorporating information security into the day-to-day operations of the institution and making it part of the culture. The success of this approach is directly dependent on management's commitment to set the "tone from the top" and provide effective leadership for the program.

When it comes to information security, what you don't know can hurt you and your organization. Senior leaders must understand what's at risk, how information is protected and what their institutions or agencies are doing to maintain regulatory compliance.

Register for this webinar to learn:

- How to engage senior leaders about security and their role in enforcing it;



- How to create an information security governance structure;
- How to set up effective metrics to prepare for an information security incident.

Presented By

Bill Sewall, Information Security, Compliance and Risk Management Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=137>

66

Insider Threat: Defend Your Enterprise

Overview

Studies show that nearly 80% of publicized data breaches come from internal sources. View this on-demand webinar to gain insight from key industry leaders and take away actionable steps on:



- What insider threats are real and present in today's environment;
- How to keep your enterprise from becoming a news headline;
- Establishing a holistic approach to your enterprise security.

Background

Companies of all sizes and industries have recently learned the hard way about costly and irreparable data breaches - enough proof that every company is susceptible to insider threat. Today, management teams are faced with the reality of insider threat and what affect it can have on their company, including:

- Damage to their brand;
- Loss of customer trust;
- Loss of customers - be it existing base or potential new ones;
- Loss of trade secrets;
- Reduced company valuation/stock price.

This Imprivata webinar, featuring industry leaders David Ting, Founder and CTO of Imprivata, and Dan Mocerri, Co-Founder and CEO of Convergent, discusses the reality of insider threat and explains how a converged physical access and IT security strategy, with Imprivata® OneSign, can ensure that you are actively defending your enterprise from insider threat while also addressing regulatory compliance.

Presented By

David Ting, Founder and CTO, Imprivata

Dan Mocerri, Co-founder and CEO, Convergent

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=66>

10

IT Risk Assessments: Understanding the Process

Overview

- Examination of IT risk assessments and how they are vital to financial institutions;
- A look at why IT risk assessments are important to your organization;
- How an IT risk assessment is performed;
- Sample assessment matrix included.



Background

Performing a thorough enterprise-wide risk assessment is essential to ensure compliance with regulatory mandates and guidance, like section 501 (b) of GLBA, AML/BSA, BCP, and stronger authentication. A risk assessment is also fundamental to developing an audit program and imperative for developing a strong security program.

A review of the institution's risk assessment is a key element of FFIEC IT examinations and IT audits. Examiners will not only review the outcome of your risk assessment, but will want to see documentation to support the process you used and the reports provided to the board.

This workshop will focus on the risk assessment process for a community bank, including a sample matrix that can be adapted for your institution.

Presented By

Susan Orr, CISA, CISM, CRP

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=10>

176

Integrating Risk Management with Business Strategy

Overview

Key business decisions impact both the strategy definition and the execution. Without integrating risk management frameworks within the decision making process, organizations will always struggle to align risk management with their business strategy and objectives.

This seminar will cover:

- Key stages of a business decision making process;
- Key stages of a risk management framework;
- Integrating risk management stages within the business decision making process;
- Examples where failure to align risk management with business strategy can have unexpected adverse consequences.

Background

In the wake of the global financial crisis, as well as recent information security incidents such as the Heartland Payment Systems data breach, banking institutions are re-dedicating themselves to the sound principles of risk management. But with a difference. Now the primary focus is on improving alignment of risk management with business strategies.

Example: A recent risk management survey by Ernst & Young highlights that 85% of the respondents would like to focus on “improving the alignment of our risk management approach with our business strategy and business activities.”

In another survey, prepared by the Economist Intelligence Unit on behalf of SAS, more than half of respondents say that they have conducted, or plan to conduct, a thorough overhaul of their own risk management practices. Among the key focus areas:

- Improvements to data quality and availability;
- Stronger risk governance;
- A move toward a firm-wide approach to risk;
- Deeper integration of risk within business lines.

But how do organizations improve their risk management practices and achieve that level of integration? That question is the foundation of this webinar.

This session will focus on integrating a risk management framework within the business decision-making process. Leading



this discussion will be Clark Abrahams, a former bank executive who now is Chief Financial Architect at SAS, and Manoj Kulwal, Global Product Manager for Governance, Risk and Compliance (GRC) Solutions at SAS. Together, these thought-leaders will lay out a discussion and examples of risk management/business alignment that touches upon:

- The key stages of business decision-making and the risk management framework;
- How to integrate risk management in business strategy;
- What’s at risk if you fail to align?

Presented By

Manoj Kulwal, Global Product Manager for SAS Governance, Risk and Compliance

Clark Abrahams, Director - Global Marketing, SAS

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=176>

128

Register Now: Visit www.bankinfosecurity.com or Call (800) 944-0401

151

Key Considerations for Business Resiliency

Overview

Organizations understand the need for business continuity and disaster recovery in the face of natural, man-made and pandemic disasters. But what about business resiliency, which brings together multiple disciplines to ensure minimal disruption in the wake of a disaster?

Register for this webinar to learn:

- How to assemble the business resiliency basics;
- How to craft a proactive plan;
- How to account for the most overlooked threats to sustaining your organization - and how to then test your plan effectively.

Background

Business resiliency is the combination of crisis management, incident response, business continuance and disaster recovery into one succinct set of processes and capabilities.

This combination allows organizations to have minimal disruption in the event of a business-impacting incident that affects the entire organization.

When evaluating business resiliency capabilities, it’s important to understand that they only are as effective as the proactive planning and considerations that go into their development. Too often, planning does not incorporate essential considerations that have the most impact, including:

- Information infrastructure requirements;
- Remote workforce/pandemic preparation;
- Overlooked threat scenarios;
- Table top vs. actual tests.

This session will discuss the key elements of business resiliency and the considerations which should be made when developing or maturing this capability.

Presented By

John P. Pironti, Chief Information Risk Strategist, Archer Technologies

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=151>

Register Now: Visit www.bankinfosecurity.com or Call (800) 944-0401

173

Maintaining Secure Government Information Systems

Overview

Join us for a webinar to learn how to effectively support environments that require the highest levels of security, including Common Criteria, STIG, FIPS 140-2 and DCID 6/3. Topics will cover:

- Industry leading protection with SELinux - a mandatory access control system based on collaboration with the National Security Agency;
- User authentication and access control with industry standard management and identity products;
- Ease in automated provisioning, patching, and configuration management;
- Flexibility in logging, monitoring, and auditing.



Background

Government computer systems continue to be targets for attack by a variety of enemies - whether they are foreign intelligence, sport hackers, terrorists or malcontents. As computers increase in capability and functionality, and as more data is produced and stored, this problem will only get worse.

Red Hat Enterprise Linux was built from the ground up to be secure and recognized by numerous certifications, including the federally sponsored Common Criteria. Through its history, Red Hat Enterprise Linux has passed the Common Criteria process 12 times on four different hardware platforms. It’s the most certified operating system available today.

Presented By

Rick Ring, Senior Solutions Architect, Red Hat

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=173>

129

72

Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?

Overview

Just because you aren't directly offshoring any of your core systems or processes doesn't mean your third-party service provider isn't.

It's a given that most organizations outsource critical functions - particularly technology - as a means to reduce IT expense. Yet, even if organizations outsource these functions to U.S.-based service providers, many of these vendors in turn outsource work to offshore partners. As these offshore service providers take on additional responsibilities, it becomes paramount that their information security programs be held to the same standards - or higher - as those of the clients.

So, as vendor management peaks in importance, it makes good business sense for organizations to take a good, hard look at the true costs and benefits of offshore outsourcing.

Register for this webinar and learn:

- The impact of political & cultural realities of overseas outsourcing;
- The logistical difficulties involved;
- The differences between direct & indirect outsourcing;
- In country limitations surrounding background checks; A general lack of data privacy laws in many nations providing outsourcing services;
- Responsible outsourcing (maximizing your returns while minimizing risk);
- Patriotism as a competitive advantage;
- The law of diminishing returns.

Background

This webinar takes a comprehensive look at the costs of offshoring. This is not strictly a CFO decision limited to the fact that foreign labor is cheaper than their domestic counterparts.

Overseas outsourcing introduces a slew of complexities related to logistics which can negatively impact the availability of your company's critical systems. BCP and general system up-time issues will be impacted by the fact that foreign countries just don't have the infrastructure that is on par with that of the United States.



Security is a major issue, due to the fact that in many cases, it's the foreign-based company that is charged with the administration of their own security.

Be aware of situations where your vendor might have vendors, sending your data to fourth parties without your knowledge. Do you know if your domestic vendor is sending your data to yet another vendor located in a foreign country - companies with whom you do not have a contractual relationship with and that may not meet your security standards?

Foreign countries are not 'mini-Americas'. The cultural and political differences of the specific country your company is considering establishing an outsourcing relationship need to be taken into account.

There are also in-country limitations that you need to be aware of, ranging from background checks to a general lack of data security laws.

The presenter, Philip Alexander, is an Information Security Officer for a major financial institution, and is the author of the book, "Data Breach Disclosure Laws: A State-by-State Perspective."

Presented By

Philip Alexander, CISSP - ISSMP, MCSE - MCT, MPA

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=72>

140

Proactive IT Risk Assessment Strategies

Overview

Please join distinguished analyst John Pescatore, of leading analyst firm Gartner, and Andre Gold, founder of Gold Risk Management & former security head at ING, for an exclusive on-demand webcast: "Staying Ahead of Changing Threats."

View this on-demand webinar now to learn:

- Which attacks are happening now and what's projected over the next couple years;
- How multistaged threats are necessitating new vulnerability management practices;
- Why continual risk assessment is increasingly seen as standard due diligence;
- Where penetration testing and red teaming fits into proactive IT risk assessment strategies.

Background

As cyber attacks have grown in sophistication and complexity, they've evolved from simple experimentation and vandalism to costly financial crime and state-sponsored information warfare. View this 40-minute webcast to get viewpoints from two industry thought leaders on how IT security practices must evolve to mitigate the risks posed by today's prolific threat environment.

Presented By

John Pescatore, Vice President and Research Fellow in Gartner Research

Andre Gold, Information Security Strategist and Business Development Consultant

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=140>

167

Top 20 Critical Controls to Ensure Painless FISMA Compliance

Overview

Regulatory requirements can become a burden and paperwork drill. Regulatory compliance does not always mean more secure systems. We are fighting a cyberwar and need to focus our efforts and attention. Well-managed systems are inherently more secure systems. Focus on the "Top 20 Critical Controls" and hear how Safend can help you do that.

Join this webinar to learn:

- What the controls are and who they apply to;
- How you can cut down on efforts to comply with the endpoint data protection specific requirements;
- How to protect your sensitive data, ace compliance checks and keep your customers happy.

Background

Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Safend Data Protection Suite helps you control your endpoints and address data leakage and targeted attack threats.

Presented By

Steve Trebbe, Director, Government Sales at Safend

Mark P. Williamson, Chief Technology Officer and co-founder of Conquest Security

Edy Almer, VP - Product Management, Safend

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=167>

255

Risk Management Framework: Learn from NIST



Overview

From heightened risks to increased regulations, senior leaders at all levels are pressured to improve their organizations' risk management capabilities. But no one is showing them how - until now.

Learn the fundamentals of developing a risk management program from the man who wrote the book on the topic: Ron Ross, computer scientist for the National Institute of Standards and Technology. In an exclusive presentation, Ross, lead author of NIST Special Publication 800-37 - the bible of risk assessment and management - will share his unique insights on how to:

- Understand the current cyber threats to all public and private sector organizations;
- Develop a multi-tiered risk management approach built upon governance, processes and information systems;
- Implement NIST's risk management framework, from defining risks to selecting, implementing and monitoring information security controls.

Background

Cyber threats can destroy any organization or its reputation, and recent incidents prove they can come from anywhere - malware in a security vendor's e-mail attachment, a lost laptop with critical health data or a rogue employee who commits financial fraud.

In a landscape filled with new threats and new regulations, risk management has never been more critical to senior leaders in all sectors. Whether you are maintaining an online banking system, sharing healthcare data with a business associate or rolling out a new mobile device policy to agency staff, you are tasked with understanding the information security risks and the management of controls.

To guide risk managers, NIST has developed a Risk Management Framework (NIST SP 800-37), which aims to improve organizations' abilities to manage information system-related security risks in today's ever-changing environment of sophisticated cyber threats, system vulnerabilities and rapidly changing business requirements.

Among the characteristics of the Risk Management Framework, it:

- Promotes near real-time risk management and ongoing information system authorization through the implementation of continuous monitoring processes;
- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions;
- Provides emphasis on the selection, implementation, assessment and monitoring of security controls.

Leading this session is one of the world's foremost risk management experts, Ron Ross, NIST's senior computer scientist and lead author of SP 800-37, NIST's widely-embraced Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans. In this session, Ross will walk through the critical elements of the Risk Management Framework. But he also will offer expert insight on:

- The current cyber threats targeting critical public and private sector information systems;
- The fundamentals of the risk management approach, including risk assessments, response and ongoing monitoring;
- Potential inhibitors to security success, including cultural barriers, lack of senior leadership commitment, and failure to follow a true risk-based approach.

Presented By

Ron Ross, Senior Computer Scientist & Information Security Researcher, National Institute of Standards and Technology (NIST)

View the complete outline and register for this webinar at: <http://www.bankinfosecurity.com/webinars.php?webinarID=255>

226

The State of Government Information Security Today



Overview

What are the top leadership challenges facing government information security leaders today? Where are agencies most vulnerable and how are they tackling challenges such as the move to cloud computing?

For answers to these questions and more, check out The State of Government Information Security Today webinar. Eric Chabrow presents an overview of the survey's top findings, then leads an expert panel in a discussion of key topics such as:

- Federal government's commitment to cybersecurity;
- Budget challenges for government security leaders;
- The future of cloud computing and other top initiatives.

Background

President Obama made cybersecurity a priority and named a senior White House cybersecurity coordinator. But do those charged with safeguarding government IT systems feel they're more secure than in the past? What staffing and technology investments must they make to improve security in 2011?

Among the topics to be tackled in this overview of the 2011 Government Information Security Today survey:

State of Security:

- Are government IT systems more or less secure since President Obama's inauguration on Jan. 20, 2009?
- What poses the greatest threat to the security of government agencies' IT systems?
- How do leaders assess their agency's ability to defend itself against a major digital assault?

Staff & Training:

- How vulnerable are government IT systems because of a dearth of qualified IT security professionals?
- How do leaders grade the effectiveness of their agency's security training and awareness activities for IT and IT security personnel, including contractors?

Compliance:

- How effective is the Federal Information Security Management Act in securing agencies' IT systems?

Emerging Technologies:

- What is the biggest reservation about cloud computing?
- What security services or technologies do agencies plan to add in the coming year?

Spending:

- How do leaders expect their agency's information security budget for the next fiscal year to differ from the current budget?

Following the survey overview, Chabrow convenes a panel discussion of the findings. Panelists include:

- Melissa Hathaway, who ran President Obama's cyberspace review;
- Chris Ipsen, chief information security officer of the State of Nevada;
- Karen Evans, national director of the U.S. Cyber Challenge, as well as the federal government's former top IT executive;
- Tom Soderstrom, chief technology officer at NASA's Jet Propulsion Laboratory.

Presented By

Eric Chabrow, Executive Editor, GovInfoSecurity, InfoRiskToday

View the complete outline and register for this webinar at: <http://www.bankinfosecurity.com/webinars.php?webinarID=226>

252

Turn FFIEC Compliance into Customer Loyalty and Retention

Overview

Within the FFIEC Authentication Guidance, one provision - strong authentication - stands out as an opportunity to make security conveniently visible to customers. Join two banking security thought-leaders and a solution provider for insights on:

- How to satisfy a crucial FFIEC mandate within the overall layered security model;
- How to also establish greater customer confidence - and loyalty - in online transactions.



This solution is an integral component of the complete security suite offered by Intel, McAfee and Nordic Edge to deliver the broadest suite of integrated technologies that address the full range of FFIEC mandates, including:

- SSO bundled with strong authentication;
- Web services (XML) security to inspect and limit backend transactions;
- Threat and compliance reporting.

Presented By

George Tubin, Banking and Security Analyst

Jesper Tohmo, CTO, Nordic Edge

Christopher Beier, IT Security & Product Consultant

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=252>

Background

Even as the security landscape surrounding Internet financial transactions becomes more hostile, banking executives are still primarily concerned with customer satisfaction, loyalty and retention. Until now, security for financial transactions has been thought of as an add-on or afterthought, in which traditional security measures have been considered by management to be an impediment to positive customer relationships.

In this session, two banking experts will interpret the FFIEC authentication guidance in the context of the user experience. They will discuss the foundations of the guidelines and the impending paradigm shift that can lead the customer into a security partnership with the bank, making the customer a willing (and eager) participant in the high risk transaction security process.

By providing easy to deploy and easy to use strong authentication technology, customers can now see themselves as “in charge” of their secure transactions, creating a trusted bond between themselves and their bank. Furthermore, the same communications mechanism that provides secure out-of-band authentication can also be utilized to seamlessly and securely transmit transaction confirmation messages, reinforcing the customer’s confidence in the transaction.

In the final module, the CTO from a leading identity and access solutions provider, Nordic Edge, an Intel subsidiary, joins to demonstrate the user authentication experience, in which smartphones deliver true out-of-band secure authentication in the most convenient way possible. Learn how to take advantage of the latest thinking in Internet financial transaction security in your customer outreach and retention programs.

291

Continuous Monitoring: How to Get Past the Complexity

Overview

What exactly is continuous monitoring - and why is it so hard for organizations to get it right?

It is one of the most discussed and least understood concepts in enterprise risk management today. Fundamentally, continuous monitoring is about deploying systems to examine all of the transactions and data processed in different applications and databases, ensuring that patches are updated, proper controls are in place and that all known (and even unknown) vulnerabilities have been addressed within an acceptable risk threshold.

But in this session, you will go beyond the fundamentals and learn first-hand from a leading expert:

- How to establish a successful continuous monitoring program;
- Technology and personnel requirements that might be easily overlooked;
- How to overcome the obstacles that have prevented other organizations from achieving maximum benefits from continuous monitoring.

Background

Continuous monitoring fits into the six steps of the Risk Management Framework described in guidance issued by the National Institute of Standards and Technology, which defines its objective to determine if deployed security controls continue as changes inevitably occur to IT systems.

The concept traces its roots to traditional auditing processes, but goes further than a periodic snapshot audit by putting in place frequent examination of transactions and controls so weaknesses can be corrected or replaced before they can do damage. Continuous monitoring systems should examine all of the transactions and data processed in different applications and databases, testing for inconsistencies, duplication, errors, policy violations, missing approvals, incomplete data and other possible breakdowns in internal controls.

A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static and occasional security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information. That information can be used to take appropriate risk mitigation actions and make



cost-effective, risk-based decisions regarding the operation of their information systems. A continuous monitoring program allows an organization to track the security state of an information system on an ongoing basis and maintain the security authorization for the system over time. Understanding the security state of information systems is essential in highly dynamic environments of operation with changing threats, vulnerabilities, technologies and missions/business processes.

Presenter Dwayne Melancon, an industry expert on continuous monitoring, will discuss:

- NIST’s view of continuous monitoring as well as guidelines and requirements for government agencies and specific industries to implement it;
- How to establish a continuous monitoring strategy;
- A step-by-step roadmap to integrate continuous monitoring into your organization’s Risk Management Framework;
- How continuous monitoring will help your organization defend against breaches, gain IT systems’ efficiencies, improve availability and prepare for audits.

Presented By

Dwayne Melancon, CTO, Tripwire

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=291>

219

Preparing for Your Next Audit: The Five Habits of Successful Security Programs

Overview

Institutions must enhance their security infrastructure and protect their customers' data in order to keep up with the demands of new and more stringent regulations. But how do you select the right providers for your institution to ensure compliance in your next audit?



This webinar will present:

- The five habits of successful security programs;
- Know your regulators;
- Internal controls - why they are important.

Background

Compliance and increased security challenges from regulators continue to increase the costs and risks to regulated businesses. Institutions must enhance their security infrastructure and protect their customers' data in order to keep up with the demands of new and more stringent regulations.

But how do you select the right providers for your institution to ensure compliance in your next audit?

In this webinar, Andrew Jaquith, Chief Technology Officer, and Tara Tate, Internal Controls Officer, present:

- The five habits of successful security programs;
- Know your regulators;
- Internal controls - why are they important;
- Q&A with Andrew Jaquith and Tara Tate.

Presented By

Andrew Jaquith, CTO, Perimeter E-Security

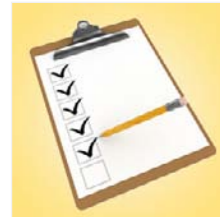
View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=219>

214

Top 5 Reports IT Auditors Request

Overview

Meeting regulatory compliance is essential for financial institutions, but can be a time consuming process to validate. Knowing the most common reports requested by auditors can help to make this process more efficient.



In this webinar, we will examine:

- The top five reports auditors request;
- The critical information contained in these reports;
- How you can develop the processes which can easily satisfy 80% of your audit requirements.

Background

Compliance is a critical business issue for financial institutions. While there are costs associated with becoming and maintaining compliance, there are also costs associated with non-compliance, including large fines.

Going through regulatory IT auditing is a stressful situation for any organization. Lack of security processes or insufficient knowledge about the auditor's expectations can hamper the IT team's ability to go through regulatory audits.

By knowing the most common reports requested by auditors, your organization will be able to prepare for the audit process faster, and make it as painless as possible.

In this webinar, you will learn:

- Which five reports are most commonly requested;
- The information these reports contain;
- How you can develop the processes which can easily satisfy 80% of your audit requirements.

Presented By

Jagat Shah, CTO & Co-Founder, EventTracker by Prism Microsystems, Inc.

A.N. Ananth, CEO, EventTracker by Prism Microsystems, Inc.

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=214>

283

Managing Change: The Must-Have Skills for Security Professionals

Overview

In healthcare, financial services and other sectors, information breaches are an epidemic. More than 400 major healthcare breaches have been reported since late 2009. And headline-grabbing breaches in the financial services sector, such as the Sony and Global Payments incidents, illustrate why preventing breaches - and their potentially astronomical costs - is more important than ever.

Creating a corporate culture that values privacy is an essential component of breach-prevention efforts. Breach prevention is destined to fail unless everyone at a company buys into the importance of protecting sensitive information.

But how does a leader help create that culture? That's the challenge.

Senior executives who want to help create a new corporate culture must develop the skills needed to manage change. In this webinar, a nationally known expert will offer timely strategies, including:

- A detailed three-step change process;
- How to overcome resistance to change;
- How using "emotional intelligence" can help assure success.

Background

Building a corporate culture that makes privacy and regulatory compliance a top priority is hard work. Managing change is never easy. Too many senior leaders try to lead an effort to change their organizations with the same approach that works for other major initiatives, only to quickly discover that this top-down approach won't work.

A successful effort to manage change requires a hands-on strategy that engages many people in the process. It requires a vision of the future, a realistic assessment of current functioning and an open-ended plan to move the organization forward.

Understanding the resistance to change that emerges is critical to identifying the appropriate techniques to overcoming the problems that invariably arise during a change initiative.

Attendees at this webinar will gain practical insights on applying proven techniques to help ensure the success of an effort to build a corporate culture that values privacy.

This webinar will describe:



- Why a project that involves managing a change in corporate culture is different from other major initiatives;
- The three vital steps involved in the change process;
- Why "management by committee" is doomed to fail;
- The role of leadership in a major change initiative;
- The change vision value proposition;
- The inevitable emergence of resistance, both institutional and individual;
- Techniques for overcoming resistance to change;
- The use of a concept called "emotional intelligence" to help change behaviors and transform the culture.

To help illustrate a practical approach to managing change, our speaker will offer an example of how a hospital can apply the concepts to help create a culture of compliance.

Presented By

Jan Hillier, Clinical Asst Professor of Management, Kelly School of Business - Indiana University-Bloomington

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=283>

26

Preparing Your Institution for an IT Audit

Overview

- Understand why IT audit is needed and what it will achieve;
- Gives attendees tools to use in preparing for IT audit;
- Learn to identify, evaluate and improve IT controls;
- Learn how to continuously collect and categorize information for year round availability.

Background

Would you be prepared if your IT auditor called right now and wanted last year's audit report and a current status of the recommended changes? Getting your institution ready for an IT audit needs preparation and planning and a sharpened knowledge of what systems really are running in your institution. Do you know what IT controls are in place? It doesn't matter whether you manage or work in an information technology function, the IT audit is, if you're not ready for it, a daunting task. An IT audit can actually be a very useful exercise if you know why the audit is taking place and what the audit is expected to realize when completed.

This webinar will provide attendees with the tools to prepare the IT audit, and will help the institution not just survive the audit but thrive from the changes made in the audit's recommendations. It will help identify, evaluate and improve the IT controls that your auditors are looking at during their work.

Institutions are increasingly looking at their information technology as a key part of their business strategy. As a result, controls to ensure the efficiency and effectiveness of an organization's operations, reliable financial statements and compliance with laws and regulations are often provided by automated systems. Indeed, in recent years, the passage of regulations such as Gramm-Leach-Bliley, Sarbanes-Oxley and HIPAA have made the need for effective IT controls an absolute necessity. As a result, IT auditors, like their internal financial and operational audit counterparts are charged by the institution's most senior management to evaluate the controls in an organization to ensure that risks are managed and controls are in place and operating effectively.

The webinar will start by discussing the need for IT controls as a way of mitigating the various risks. It will then continue on management's responsibility for ensuring that proper controls are



in place, and some of the governance frameworks - including the COBIT framework designed specifically for IT - that help them design the control structure for the organization. We will cover different types of controls including:

- Entity-level controls, which are the controls put in place by executive management that set the tone for the organization. These may include policies and procedures, risk assessment, quality assurance and board committees;
- Application controls, which are controls embedded in computer programs and related manual processes that help ensure the completeness and accuracy of data processing;
- General controls, which are controls to ensure the continued proper operation of computer systems. These include controls over data center operations, software acquisition and maintenance, systems security, disaster recovery.

We continue with a discussion on the IT auditor's role in documenting, evaluating and testing these controls. We will review the audit process from the risk assessment to determine what to review all the way through to the final report and follow-up on audit recommendations. Finally, we will discuss ways to survive in an audited environment including how the IT department can continuously collect and categorize this evidence so that it is always available for your auditor.

Presented By

Adam Losner, President and Founder, Finance Technology and Controls Consulting

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=26>

129

Beyond Heartland: How to Prevent Breaches of Security and Trust

Overview

It may be the biggest data breach we've ever seen - and an eerie harbinger of crimes to come. The Heartland Payment Systems (HPY) hack involves scores of financial institutions and tens of thousands of consumers who've had their accounts compromised by fraudsters. Crimes against processors are on the rise, and in this panel discussion you'll gain insights from:

- A banking/security leader, who describes the impact of such breaches on community banking institutions;
- A noted privacy attorney, who discusses the legal impact of these crimes and how to fight them;
- A trusted leader of on-demand information security services, who will share market insights on the latest fraud trends and what companies need to do to prevent, manage and respond to the growing security threats.

Background

This is the fraud that got everyone's attention.

When Heartland Payment Systems (HPY) revealed in January 2009 that it had been the victim of a malicious hack sometime in 2008 - that an unknown number of consumers had their account names and numbers pilfered - the payments processor became the unwitting face of fraud.

Since that crime, more than 600 financial institutions have volunteered to Information Security Media Group that they and their customers - tens of thousands of individuals - were affected and in some cases defrauded as a result of the Heartland breach.

Although no one knows for certain how big the breach was, the Heartland case nevertheless caused:

- Customers to join in class action suits against the processor;
- Banking institutions to band together to buck the trend of having to replace cards and placate customers after crimes committed on other organizations' watch;
- The security and payments industry to re-evaluate the systems and solutions in place to protect personally identifiable information at all stops along the transaction route.

Merchants, banks, customers and vendors - they all have been affected by the Heartland breach, and their perspectives will be represented in this panel discussion about the crime and how to prevent future incidents.



Register for this webinar to see these perspectives:

- An overview of the Heartland breach and its impact on banking institutions, as portrayed by Tom Field, Editorial Director of Information Security Media Group;
- How one community banking institution was struck - and is now fighting back - as told by Stephen Wilson, VP of McGehee Bank;
- The legal perspective - what consumers, institutions and states can do to respond, with insight from noted privacy attorney Randy Sabett;
- Beyond Heartland - ways financial institutions can address the growing complexity, cost and compliance pressures of protecting their customers' most critical information, with advice from Kevin Prince, Chief Architect of Perimeter eSecurity.

Security experts say Heartland-style breaches are the wave of the future in fraud, but financial institutions now have the opportunity to buck that trend. This panel discussion is step one toward preventing further breaches.

Presented By

Stephen Wilson, VP, McGehee Bank

Randy Sabett, CISSP, Privacy Attorney

Kevin Prince, Chief Architect, Perimeter eSecurity

Tom Field, Editorial Director, Information Security Media Group

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=129>

188

Cloud Computing: Regulatory Security & Privacy Challenges

Overview

Cloud computing is the hot, new practice that offers a scalable, centralized resource for data and applications that can be available to anyone, anywhere.

But as an emerging trend, cloud computing is also fraught with risk - already we've seen organizations whose data has been compromised.

Register for this session to hear the lessons learned about cloud computing from a panel of experts who will discuss:

- Advantages and disadvantages of storing data or running applications online, as opposed to in-house;
- Current regulatory trends toward better security and privacy standards - and how they impact cloud computing;
- Legal, privacy, records management and ethical challenges that have been identified by cloud pioneers - and strategies to avoid those pitfalls.

Background

Attend any industry event this year, and the term you'll hear most frequently is "Cloud Computing."

But like the old cliché about the weather, one is left to ask: "Everyone is talking about Cloud - but what are they actually doing about it?"

The answer is: More than you might think. Banking institutions for years now have practiced cloud computing without using the term, outsourcing core processing to third-party service providers.

Today, with more banking services to offer and more hosting options from vendors, banking institutions have a broad range of cloud computing opportunities before them. But they also have significant questions to answer re: scale, security, privacy and true business benefits.

In this session, Matt Speare, veteran technology leader from M&T Bank, will lead our cloud computing discussion - setting the stage with a presentation depicting a banking institution's approach to the cloud. He'll then interact with industry experts, including Jim Reavis of the Cloud Security Alliance, to discuss not just the theory of cloud - but about the real business benefits that pioneer banking institutions are realizing today.



Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

Michael Smith, Security Evangelist, Akamai

Harold Moss, CTO - Cloud Security Strategy, IBM

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=188>

162

Data Protection and Incident Response

Overview

Public and private sector organizations alike are charged with protecting critical data and responding to incidents that put information security at risk. In this session, David Matthews, deputy CISO for the City of Seattle, reveals:

- Data protection challenges;
- Tools to meet those challenges;
- How to respond to security incidents.

Background

Hackers. Insiders. Man-made or natural disasters. These are among the forces that threaten data critical to private and public sector organizations. And they force information security leaders to constantly be vigilant in data protection and incident response.

In this webinar, David Matthews, deputy CISO for the city of Seattle, will give an inside view into the challenges he faces every day - from the benign and accidental to the intentional and potentially devastating.

Offering a unique government perspective, Matthews will discuss:

- The specific data protection issues that face local governments;
- Which tools, procedures and training are used to address those issues;
- How to respond when data is lost or systems are compromised.

Matthews also will offer first-hand insight on incident response procedure, as well as roles and responsibilities for information security staff.

And how does a real security incident unfold? Matthews will take you inside a real case study from his experience.

Presented By

David Matthews, Deputy Chief Information Security Officer for the City of Seattle

Geoff Glave, Product Manager, Absolute Software

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=162>

180

Email Security Requirements for Healthcare Providers: HIPAA & Beyond

Overview

E-mail continues to be a main source of exposure of protected health information and other private data in today's enterprise, but most organizations have yet to deploy technology to prevent costly breaches of PHI.

Register for this webinar to learn:

- How policy-based encryption can help protect private healthcare information and mitigate the risks associated with data loss and corporate policy violations;
- New provisions of the U.S. economic stimulus legislation that expand the scope of HIPAA security rules and the impact on your organization's e-mail security/compliance strategy;
- New HIPAA violation penalties and the impact of the breach notification requirements enforced by the FTC;
- Technology requirements for protecting the confidentiality of healthcare information in both outbound and archived e-mail messages.

Background

Healthcare regulations for IT security - such as HIPAA and HITECH - are now broader than ever. And they apply not just to healthcare organizations, but to all kinds of companies that handle or store private health information. Today's penalties for data breaches are increasingly onerous: Fines are bigger, notification requirements are more stringent and enforcement organizations have new incentives for taking action against organizations that fail to protect healthcare privacy.

Learn what to look for in a secure e-mail solution for complying with the web of regulations that now apply to so many companies. You'll also learn how automatic, policy-based e-mail encryption can provide effective protection for sensitive health information in e-mail.

Presented By

Rami Habal, Director of Product Marketing, Proofpoint

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=180>

67

Defending Against The Insider Threat

Overview

The insider threat - it may be the hardest to detect, yet it poses the greatest risk to information security and regulatory compliance. And with recent, high-profile data breaches resulting from insider abuses, the topic is hotter than ever.

Register for this webinar to learn:

- How to identify and mitigate insider threats;
- The different types of threats - accidental & malicious;
- How to spot authorized users handling information in unauthorized ways;
- Proper procedures and tools to help maintain regulatory compliance and protect against the insider threat.



- Further actions to mitigate insider threat;
 - » Policy;
 - » Procedure;
 - » Compliance.

Presented By

Jerald Murphy, Senior Vice President and Director of Research, The Robert Frances Group

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=67>

Background

Organizations must constantly balance access to information for the purpose of conducting business, while protecting this information from unauthorized users. While many well-established methods and products exist for tracking external attacks on information, less oversight and protection is made for identifying authorized users handling information in unauthorized ways - the insider threat.

In some cases, the insider threat is inadvertent, while in other cases authorized access to data is being taken advantage of for malicious purposes. Organizations must understand the impact of these threats, both for regulatory compliance and overall business risk.

Jerald Murphy will lead a discussion about how proper procedures and tools can be implemented to both comply with regulatory guidelines, while at the same time identifying and mitigating internal data leakage. He will discuss how to organize roles between data management and security/compliance, so that information workers can have the most flexibility, while still ensuring protection of data and adherence to regulatory guidelines.

Among the topics to be discussed in this webinar:

- The current business security environment;
- The different types of insider threat:
 - » Intentional;
 - » Unintentional;
- How to respond to & report data loss from an inside threat;

127

Evaluating Security Risks Associated with Banking Vendors

Overview

Regulatory change is coming - fueled by the ever present news of breaches within the credit card payment networks degrading the faith in today's financial institutions. A new approach is needed to secure, make compliance easier, and enhance the operating efficiency for critical financial datacenters and those processing sensitive cardholder information or personally identifiable information (PII).

Attend this webinar to learn to:

- Facilitate PCI compliance and go beyond to provide demonstrable security for critical financial datacenters;
- Decrease the burden of proof and yet provide the verification of operational controls in a new way that will increase confidence for vendor management due diligence;
- Reduce your risk and secure your infrastructure against emerging threats to ensure that only authorized changes are allowed.

Background

Regulatory change is coming - fueled by the ever present news of breaches within the credit card payment networks degrading the faith in today's financial institutions. PCI-DSS is a step in the right direction toward thwarting 'smash and grab' attacks but is weak against zero day attacks and low 'n slow attacks that are designed to persist under the radar of common controls. A new approach is needed to secure, make compliance easier, and enhance the operating efficiency for critical financial datacenters and those processing sensitive cardholder information or personally identifiable information (PII).

As the industry continues to outsource to vendors and rely on multiple parties, those who evaluate risk need better visibility and reporting of the operational controls of these contracted entities as mandated by the regulations and standards of FFIEC and PCI-DSS. Due diligence today encompasses stronger contracts, data center visits and keeping up-to-date on vendor performance. How does a vendor keep up with these requests and provide demonstrable measures of how they secure not only IT infrastructure but applications and critical data? How can vendor management be easier for enterprises beyond submitting lengthy assessments that they can only trust reflect the true operations of the vendor? Being able to provide protection from



device to datacenter systems provides the deep visibility, control enforcement and system integrity needed to go beyond today's standards and be prepared for addressing future regulation changes.

In this webinar, hear about how:

- SecureNet Payment Systems, a leader in supplying cutting-edge payment processing technologies, plans to demonstrate and verify operational controls to ease the due diligence process of vendor management requests and compliance with Solidcore.
- MTXEPS, leader in electronic payments software and solutions, provides end-to-end protection of card holder data going above and beyond today's Data Security Standards (PCI-DSS) from device to datacenter through branded Connected Payments for Retailix retail solutions secured with S3 Control from Solidcore Systems.

Presented By

Kim Singletary, Director of OEM & Compliance Solutions, Solidcore Systems

Ken Harris, Vice President, MTXEPS Inc.

Preetham Gowda, CIO, SecureNet Payment Solutions

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=127>

94

GLBA Privacy Requirements: Building a Program That Meets Compliance Mandates & Ensures Customer Privacy

Overview

Preserving the privacy of customer information is a core mandate of Gramm-Leach-Bliley Act (GLBA) compliance - and increasingly an essential for business success.

Banking institutions need strong privacy programs to keep their customers' trust, but also to comply with a growing number of state privacy laws and federal regulations. Beyond regulatory requirements, recent incidents such as the Hannaford data breach have brought to the forefront the need for an effective privacy program.

Register for this webinar for a how-to overview of elements necessary in an effective privacy program, including:

- Overview of GLBA and other regulatory requirements for privacy and security;
- Privacy program components;
- How to establish policies, procedures and technical controls to support and maintain privacy;
- How to align vendor contracts to include privacy-related requirements and outlining vendors' responsibilities;
- Industry "best practices" for customer communications for privacy-related notifications.

Background

Building an effective privacy program is essential for business success. Financial institutions that experience privacy incidents lose the trust of their customers. And lost trust results in lost customers. Institutions need strong privacy programs not only to keep their customers' trust but also to comply with a growing number of privacy laws and regulations worldwide. A growing number of recent privacy related incidents have brought the need for an effective privacy program to the fore-front.

In this exclusive webinar, noted privacy expert Rebecca Herold will lead a discussion of how financial institutions can establish an effective privacy program, outlining the components required to make the program succeed.



Among the points Rebecca will discuss:

- Why a privacy program is necessary;
- Defining personally identifiable information (PII);
- Privacy program components;
- Legal privacy and security requirements;
- Policies, procedures and technical controls;
- Inclusion of privacy program related in the organization's vendor due-diligence process;
- Privacy program maintenance.

Presented By

Rebecca Herold, CEO, The Privacy Professor

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=94>

174

HIPAA and HITECH Enforcement: How to Secure Health Information

Overview

New HIPAA Security Rule enforcement began in February 2010 under the HITECH Act. Healthcare providers and their business associates that fail to secure protected health information are now subject to new penalties. Register for this webinar to learn:

- Strategies for protecting your patients and your business;
- Best-practices from a veteran healthcare/security leader.

Background

After months of discussion, compliance time is here.

Security rules found under HIPAA now enforced by the HITECH Act enable state attorney general's offices to pursue civil charges on behalf of victims. HIPAA violations that result in a data breach are subject to fines of up to \$1.5 million per year.

Faced with the looming threat of serious fines, healthcare providers, plan administrators and other business associates that handle private patient health information are seeking ways to become HIPAA compliant.

But where are the greatest vulnerabilities for healthcare organizations?

What must they do to protect their patients - and themselves?

Where can they pick up practical tips?

In this session, Rapid7, in conjunction with High Point Regional Health System, will spell out exactly how you can protect your patients and secure your business. Get first-hand info from Miles Romello, IT Security Coordinator at High Point Regional Health System.

Presented By

Marcella Samuels, Information Security Solutions Manager, Rapid7

Miles Romello, CISSP, MCSE, MCDBA, IT Security Coordinator, High Point Regional Health System

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=174>

83

How Identity Fraud is Evolving and Impacting Customer Trust in Your Financial Institution

Overview

Learn about the latest findings on the impact of identity fraud on your financial institution and your customers:

- Why banking customers are shying away from the online banking channel;
- How stolen identities are used to defraud your customers and damage your brand;
- Which banking channels are most vulnerable to identity fraud;
- How financial institutions are empowering customers to prevent identity fraud;
- The latest phishing trends and tactics to commit identity theft;
- The techniques financial institutions use to protect their brands and customers from identity fraud.

Background

In 2008, over 8 million U.S. adults will be victims of identity fraud. Even more alarming is the fact that over 150 million U.S. consumers don't bank online out of fear of identity theft.

Learn about the latest findings on the impact of identity fraud on your financial institution and your customers, including:

- Why banking customers are shying away from the online banking channel;
- How stolen identities are used to defraud your customers and damage your brand;
- Which banking channels are most vulnerable to identity fraud;
- How financial institutions are empowering customers to prevent identity fraud;
- The latest phishing trends and tactics to commit identity theft;
- The techniques financial institutions use to protect their brands and customers from identity fraud.

Presented By

John LaCour, Director of AntiPhishing Solutions for MarkMonitor

Rachel Kim, Associate Analyst, Javelin Strategy & Research

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=83>

113

How to Prepare for Your First Identity Theft Red Flags Rule Exam

Overview

An Insider's Guide to Banking Agencies' Examination Guidelines

The Identity Theft Red Flags Rule compliance deadline was Nov. 1. All banking institutions now must prepare for their first examinations on this important new regulation. Register for this webinar to learn from a senior information security, compliance and risk management specialist:

- How to prepare for examination on this new regulation, which specifies 26 ID theft red flags that institutions must address in their prevention programs;
- The 15 key areas regulators will examine when they assess compliance with Identity Theft Red Flags, Changes of Address and Address Discrepancies standards;
- What your institution can do in advance to help ensure a successful examination;
- What to expect during the exams.

Background

As of Nov. 1, all banking institutions must be in compliance with the Identity Theft Red Flags Rule, which went into effect on Jan. 1, requiring:

- Financial institutions and creditors to implement a written identity theft prevention program;
- Card issuers to assess the validity of change of address requests;
- Users of consumer reports to verify the identity of the subject of a consumer report in the event of a notice of address discrepancy.

To help institutions meet compliance, the banking regulatory agencies have recently released their Red Flags examination procedures, which include 15 key topics that were hammered out and agreed upon by an interagency committee, covering all three aspects of the new rule:

- Identity theft red flags;
- Address discrepancies;
- Changes of address.

In this exclusive new webinar, Bill Sewall, former information security executive with Citigroup, will offer an insider's perspective on how to prepare for a successful Identity Theft Red Flags Rule examination.



Drawing upon his years of experience in risk management and compliance, Sewall will:

- Walk Through the Examination Procedures - Explaining each of the 15 aspects and what they mean in regards to how your institution might be examined;
- Tell You How to Prepare - Offering insights on risk assessment and scoping tasks you can conduct upfront to help ensure a successful examination;
- Provide Tips for the Test - Showing how to help manage the examination process, including how to clarify the scope of your exam, as well as how to demonstrate your success at identifying covered accounts and securing board approval for your ID theft prevention program.

Presented By

Bill Sewall, Information Security, Compliance and Risk Management Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=113>

142

ID Theft Red Flags FAQ's: A Guide to the 'Gotchas' of Compliance

Overview

For just over six months now, the banking regulatory agencies have examined institutions for compliance with the ID Theft Red Flags Rule, and they have just released a document addressing frequently asked questions about the regulation.

Register for this exclusive webinar to hear from a former information security executive with Citigroup as he walks you through the FAQs. You'll learn:

- The Deficiencies - Understand the areas other institutions are having a difficult time with and why the FAQs were put together;
- Walk Through the FAQs - Explaining each of the questions and answers contained within the four umbrella topics;
- How to Prepare for Your Exam - Offering insights on risk assessment and scoping tasks you can conduct upfront to anticipate any questions and help ensure a successful examination;
- Provide Tips for the Test - Offering a refresher on how to help manage the examination process from start to finish.

Background

As of Nov. 1, 2008, all banking institutions must be in compliance with the Identity Theft Red Flags Rule, which requires:

- Financial institutions and creditors to implement a written identity theft prevention program;
- Card issuers to assess the validity of change of address requests;
- Users of consumer reports to verify the identity of the subject of a consumer report in the event of a notice of address discrepancy.

To help institutions meet compliance, the banking regulatory agencies have recently released a document outlining a series of frequently asked questions about the Red Flags Rule. These questions have arisen from initial examinations and include:

- The ID Theft Red Flags scope;
- The definitions of "covered account," and "service provider";
- Types of notices of address discrepancy that trigger the rule;
- Furnishing a confirmed address to a consumer reporting agency.



In this exclusive new webinar, Bill Sewall, former information security executive with Citigroup, will offer an insider's perspective on how to make sure you answer these questions before the examiner comes calling.

Drawing upon his years of experience in risk management and compliance, Sewall will:

- Walk Through the FAQs - Explaining each of the questions and answers contained within the four umbrella topics;
- Tell You How to Prepare - Offering insights on risk assessment and scoping tasks you can conduct upfront to anticipate any questions and help ensure a successful examination;
- Provide Tips for the Test - Offering a refresher on how to help manage the examination process from start to finish.

Presented By

Bill Sewall, Information Security, Compliance and Risk Management Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=142>

155

Identity Theft: How to Respond to the New National Crisis

Overview

Your identity - it's the gold standard of the Internet, and fraudsters are out to capture it. Smart card technology provides one potential solution to the identity theft crisis. Watch this video to hear Neville Pattinson, VP of Government Affairs at Gemalto, discuss:

- The advantages of smart card technology;
- How to apply these solutions specifically in e-government and healthcare reform;
- How to take back control of your identity in the real and virtual worlds.

Background

With the advent of the Social Security number in the 20th century, U.S. citizens were given one single, digital identifier that would distinguish them in their financial, medical and government interactions. Like fingerprints, no two Social Security numbers were alike, and as long as your physical card was secure, so was your identity.

But with the advent of the Internet era, our former strength is now a vulnerability. Fraudsters target people's personal information, and if they are able to net a Social Security number - they've gained the keys to your kingdom.

So, how does one respond with a new solution in this new era?

Smart card technology is one answer, and during this video you will hear from an industry expert on the advantages of smart card technology as a solution to what has become a national identity crisis. Neville Pattinson, VP of Government Affairs at Gemalto, will discuss applicable uses of smart card technology in:

- e-Government 2.0;
- Healthcare reform;
- Immigration.

Presented By

Neville Pattinson, VP of Government Affairs & Standards, NA., Gemalto

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=155>

35

Insider Fraud - Profiling & Prevention

Overview

- Why is insider fraud on the rise now? What are the trends?
- What is the strategy of how to deal with it? Controls, analytics?
- What is the "day in the life" of a case/attack? What process does it typically go through?
- How can one systemize the investigations? Technology, policy, responsibility, priorities, etc.?

Background

The improvement of internal banking systems and data warehousing has made it easier for banking professionals to service customers, but has also created a new set of challenges for information and corporate security managers.

The same data and account access that is required to conduct the day-to-day business of servicing customers can be used to launch an extraordinary range of attacks. As much as we talk about the risk posed by external threats, insider access to customer data and accounts represents a point of compromise that far exceeds that posed by external attacks on sensitive information such as phishing.

Although efforts to protect the customers via review of access policies, scanning for sensitive data and securing external network defenses are necessary, they are not sufficient to protect against attacks perpetrated by malicious insiders.

Countering the employee fraud threat requires a system that can be deployed quickly to leverage the considerable knowledge of these attacks that exists across the industry and in the heads of individual security professionals and investigators. These systems must proactively identify known fraud, allow nimble investigations of suspicious activity and provide a proven path to deploy more advanced profiling and analysis to protect against less frequent but potentially devastating attacks perpetrated by the more sophisticated malicious insider.

Presented By

Kirk McGee, CPP, AVP, Regional Security Officer, TD Banknorth N.A, Springfield, Massachusetts

Paul Henniger, Actimize

<http://www.bankinfosecurity.com/webinars.php?webinarID=35>

81

Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication

Overview

What happens if your institution suffers an ATM skimming attack and customer accounts have been compromised? Or if a payments processor is hacked and thousands of your credit/debit cardholders are potentially exposed to fraud?

These aren't hypothetical breaches; they've occurred. Repeatedly. And they prove that an incident response plan isn't just a 'nice to have' for a financial institution - it's a must. This webinar outlines the critical components of documenting, testing and updating incident response plans.

Matthew Speare, who created and oversees the incident response program at M&T Bank in New York, will discuss the hottest trends in incident response, including:

- The latest regulatory guidance;
- How to fulfill the elements of a good plan;
- How to handle one of the most critical elements of incident response - customer communications;
- What to do when the incident occurs at one of your vendors.

Background

Incident response by definition refers to the formal reaction to a security breach, i.e. a physical or electronic hack. Every financial institution is required to document, test, update and communicate a formal incident response plan, which may include forensics, e-discovery and other tactics necessary in the wake of a security breach.

Increasingly, incident response plans also include legal and public relations teams as appropriate, as well as customer communications, to ensure the timely release of accurate information.

And then there's the new focus of incident response: third-party service providers. It's one thing to account for incidents at your own institution. As recent breaches have taught us, what if the incident occurs at one of your vendors? The damage can be just as devastating to your business and to customer confidence.



In this webinar, Matthew Speare will discuss the requirements of incident response guidance and the steps that the industry has taken to implement solutions to address the guidance. Among the topics he'll discuss:

- Current regulatory guidance on incident response;
- What today constitutes a security incident;
- What information is considered sensitive customer information;
- How to handle customer communications;
- Steps to take if there is an ongoing investigation;
- How to address incidents that occur at a vendor.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=81>

65

Investigations, Computer Forensics and e-Discovery - A Primer for Every Banking Institution

Overview

Forensics has become a hot topic for a variety of internal factors, including the importance of the Internet to everyday business and, with it, the rise of electronic fraud.

Externally, financial institutions especially feel regulatory heat in the form of the FFIEC GLBA Notification Rule, SEC/NASD Rule 3010 and even recent VISA/Mastercard PCI requirements, all of which put a premium on forensic and e-discovery capabilities. Add to those pressures recent U.S. litigation trends and the new federal e-discovery rules.

Register for this webinar to learn:

- How to build or enhance a forensics program;
- Proper forensics methodology;
- Federal rules and regulatory requirements that underscore the need for forensics and e-discovery;
- The steps investigators have used to crack tough cases.

Background

Computer forensics is the use of investigative techniques to provide digital evidence of an activity, generally in conjunction with a criminal investigation or civil litigation in cases that include:

- Employee Internet abuse;
- Unauthorized disclosure of corporate information;
- Incident response;
- Fraud.

The forensics process entails:

- Preservation of Evidence - Adherence to a set of procedures that address security, authenticity and chain-of-custody.
- Data Analysis - The ability to locate and recover previously inaccessible documents and files through computer forensic processes.
- Analysis of User Activity - Reports on all user activity including, but not limited to, electronic mail, Internet and Intranet files accessed, files created and deleted and user access times.



Forensics has become a hot topic for a variety of internal factors, including the importance of the Internet to everyday business and, with it, the rise of electronic fraud. Externally, financial institutions feel regulatory heat in the form of the FFIEC GLBA Notification Rule, SEC/NASD Rule 3010 and even the recent VISA/Mastercard PCI requirements, all of which put a premium on forensic and e-discovery capabilities. Add to those pressures recent U.S. litigation trends and the new federal e-discovery rules, and you see why this topic has risen to the top of organizational agendas.

One of the key questions to be tackled in this webinar is whether to establish your own forensics program or outsource it to a third-party provider. Our presenters will explore the factors that go into this decision, including how to:

- Form an internal steering committee of key constituents to evaluate your decisions;
- Establish external relationships with FBI and independent forensics experts;
- Create an e-discovery policy that can be handed down either to an in-house or outsourced forensics team.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

Warren Kruse, Vice President of Data Forensics and Analytics, Encore Legal Solutions

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=65>

283

Managing Change: The Must-Have Skills for Security Professionals

Overview

In healthcare, financial services and other sectors, information breaches are an epidemic. More than 400 major healthcare breaches have been reported since late 2009. And headline-grabbing breaches in the financial services sector, such as the Sony and Global Payments incidents, illustrate why preventing breaches - and their potentially astronomical costs - is more important than ever.

Creating a corporate culture that values privacy is an essential component of breach-prevention efforts. Breach prevention is destined to fail unless everyone at a company buys into the importance of protecting sensitive information.

But how does a leader help create that culture? That's the challenge.

Senior executives who want to help create a new corporate culture must develop the skills needed to manage change. In this webinar, a nationally known expert will offer timely strategies, including:

- A detailed three-step change process;
- How to overcome resistance to change;
- How using "emotional intelligence" can help assure success.

Background

Building a corporate culture that makes privacy and regulatory compliance a top priority is hard work. Managing change is never easy. Too many senior leaders try to lead an effort to change their organizations with the same approach that works for other major initiatives, only to quickly discover that this top-down approach won't work.

A successful effort to manage change requires a hands-on strategy that engages many people in the process. It requires a vision of the future, a realistic assessment of current functioning and an open-ended plan to move the organization forward.

Understanding the resistance to change that emerges is critical to identifying the appropriate techniques to overcoming the problems that invariably arise during a change initiative.

Attendees at this webinar will gain practical insights on applying proven techniques to help ensure the success of an effort to build a corporate culture that values privacy.

This webinar will describe:



- Why a project that involves managing a change in corporate culture is different from other major initiatives;
- The three vital steps involved in the change process;
- Why "management by committee" is doomed to fail;
- The role of leadership in a major change initiative;
- The change vision value proposition;
- The inevitable emergence of resistance, both institutional and individual;
- Techniques for overcoming resistance to change;
- The use of a concept called "emotional intelligence" to help change behaviors and transform the culture.

To help illustrate a practical approach to managing change, our speaker will offer an example of how a hospital can apply the concepts to help create a culture of compliance.

Presented By

Jan Hillier, Clinical Asst Professor of Management, Kelly School of Business - Indiana University-Bloomington

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=283>

132

Massachusetts Privacy Law: A Guide to Understanding and Complying with this New Data Protection Standard



Overview

Irrespective of the state you operate in, this privacy law is applicable to any business extending credit to, or processing or storing data on customers in Massachusetts.

Now that the Massachusetts “Standards for the Protection of Personal Information” is in effect, it may well be the toughest privacy law in the nation - and perhaps the new “gold standard” for data security legislation.

Register for this newly refreshed webinar to learn:

- The latest details of the Massachusetts privacy standards;
- How these amended standards may impact your business or agency;
- The potential impact on federal privacy legislation.

Background

Does your business extend credit to or employ Massachusetts residents? Do you or your organization manage, store or process personal information on Massachusetts residents? If “yes,” then you need to be prepared for the Massachusetts “Standards for the Protection of Personal Information.”

Compared to most other state laws covering identity theft, the new Massachusetts “Standards for the Protection of Personal Information” - or Mass Privacy Law -- is sweeping in its scope and impact.

The types of businesses covered by the law are also expansive, since the standards apply to any organization, whether or not it’s located in Massachusetts, as long as it owns, licenses, stores or maintains “personal information about a resident of the Commonwealth.”

In terms of specific requirements, the standards are similar to existing federal laws such as the GLBA and HIPAA that require organizations to establish written information security programs to prevent identity theft. However, in a departure from federal regulations, the Mass Law also contains several detailed technology system requirements, especially for the encryption

of personal information sent over wireless or public networks or stored on portable devices.

This presentation is part of a new series of webinars created by Information Security Media Group to address major federal and state laws covering information security. Each presentation provides:

- An introduction to these specific laws and regulations;
- Detailed materials on the origins, scope, definitions and specific requirements;
- Description of how the laws will be enforced;
- Guidance on the impact of these provisions and what each organization can do to comply.

Presented By

Bill Sewall, Information Security, Compliance and Risk Management Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=132>

72

Offshore Outsourcing: Do You Know Where Your Data is and How it’s Managed?



Overview

Just because you aren’t directly offshoring any of your core systems or processes doesn’t mean your third-party service provider isn’t.

It’s a given that most organizations outsource critical functions - particularly technology - as a means to reduce IT expense. Yet, even if organizations outsource these functions to U.S.-based service providers, many of these vendors in turn outsource work to offshore partners. As these offshore service providers take on additional responsibilities, it becomes paramount that their information security programs be held to the same standards - or higher - as those of the clients.

So, as vendor management peaks in importance, it makes good business sense for organizations to take a good, hard look at the true costs and benefits of offshore outsourcing.

Register for this webinar and learn:

- The impact of political & cultural realities of overseas outsourcing;
- The logistical difficulties involved;
- The differences between direct & indirect outsourcing;
- In country limitations surrounding background checks;
- A general lack of data privacy laws in many nations providing outsourcing services;
- Responsible outsourcing (maximizing your returns while minimizing risk);
- Patriotism as a competitive advantage;
- The law of diminishing returns.

Background

This webinar takes a comprehensive look at the costs of offshoring. This is not strictly a CFO decision limited to the fact that foreign labor is cheaper than their domestic counterparts.

Overseas outsourcing introduces a slew of complexities related to logistics which can negatively impact the availability of your company’s critical systems. BCP and general system up-time issues will be impacted by the fact that foreign countries just don’t have the infrastructure that is on par with that of the United States.

Security is a major issue, due to the fact that in many cases, it’s the foreign-based company that is charged with the administration of their own security.

Be aware of situations where your vendor might have vendors, sending your data to fourth parties without your knowledge. Do you know if your domestic vendor is sending your data to yet another vendor located in a foreign country - companies with whom you do not have contractual relationship with and that may not meet your security standards?

Foreign countries are not ‘mini-Americas’. The cultural and political differences of the specific country your company is considering establishing an outsourcing relationship need to be taken into account.

There are also in-country limitations that you need to be aware of, ranging from background checks to a general lack of data security laws.

The presenter, Philip Alexander, is an Information Security Officer for a major financial institution, and is the author of the book, “Data Breach Disclosure Laws: A State-by-State Perspective.”

Presented By

Philip Alexander, CISSP - ISSMP, MCSE - MCT, MPA

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=72>

100

Protecting the Exchange of Sensitive Customer Data with Your Vendors

Overview

For financial institutions, data security is both an operational and regulatory imperative. A bank or financial services provider that fails to protect a customer's financial data faces the threat of losing customers, tarnishing their reputation and eventually losing competitive advantage.

Register for this exclusive webinar to answer:

- How does regulatory compliance, like GLBA, affect the way your data needs to be handled and audited?
- Who has access to your sensitive files?
- What would the impact be if these files, including sensitive customer data, were compromised?
- Where and when is this data being sent?
- Why would you let employees/partners share your files over insecure FTP, e-mail or IM?

Background

For financial institutions, data security is both an operational and regulatory imperative. A bank or financial services provider that fails to protect a customer's financial data faces the threat of losing customers, tarnishing their reputation and eventually losing competitive advantage. There are some key questions you should think about when it comes to securing your customers' important financial data, including:

- How does regulatory compliance, like GLBA, affect the way your data needs to be handled & audited?
- Who has access to your sensitive files?
- What would the impact be if these files, including sensitive customer data, were compromised?
- Where and when is this data being sent?
- Why would you let employees/partners share your files over insecure FTP, e-mail or IM?

Questions still linger on how to meet compliance regulations that affect financial institutions, like GLBA, PCI and SOX.

With increased government regulation and oversight in the form of mandates such as GLBA, PCI, etc., no organization that deals with financial information can afford to ignore the very real challenge of ensuring data security, integrity and privacy.



Learn more about how your organization can meet these compliance challenges as it relates to financial data security as well as how to manage your partners to ensure that they are also following acceptable data sharing practices. And hear how other financial institutions are tackling these very important data security issues.

Presented By

Greg Shields, Microsoft MVP in Terminal Services

Kevin Gillis is Vice President, Product Management at Ipswitch

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=100>

154

Register Now: Visit www.bankinfosecurity.com or Call (800) 944-0401

73

Top IT Compliance Challenges: Who's Touching Your Data and What Are They Doing With It?

Overview

Join in this tactical discussion of how financial institutions are using new technologies to successfully prevent, identify and respond to security threats, no matter where they originate.

- Learn how to identify, prevent and rapidly respond to user threats and data breaches;
- Find out how, while mitigating security threats, you can work towards compliance for PCI and other key mandates.

Do you really know who is accessing your critical data? Do you really know where threats to your data security originate? This webcast features Paul Reymann, one of the nation's leading financial institutions regulatory experts and co-author of Section 501 of the Gramm-Leach-Bliley Act Data Protection regulation.

Background

Today's headlines confirm what will happen to your institution if it does not have effective IT security systems. Financial institutions suffer serious consequences - from stolen customer data and intellectual property to powerful viruses and other malware. Not only are business operations interrupted, but corporate security failures lead to damaged or lost trust, substantial financial loss and lost revenues, as well as high forensics and remediation costs. In addition, PCI, GLBA and SOX mandates present a complex challenge for securing massive amounts of customer data, monitoring complex applications and managing large numbers of users.

To successfully manage threats and compliance challenges, financial institutions need a comprehensive security strategy that can successfully do battle with inside - and outside - threats. Institutions must implement proactive practices that identify, prevent and respond to potential threats and ensure a limited need-to-know access policy.

Companies increasingly leverage new threat-monitoring technologies to build a clean, concise and manageable process for dealing with the tremendous volumes of raw security information from disparate devices, applications and databases.



This webinar examines the key threats financial institutions face today, and how to gain the actionable security intelligence that is required to enable sound risk management and compliance.

Presented By

Paul Reymann, CEO, The Reymann Group

Bob Flinton, VP Product Marketing, netForensics

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=73>

Register Now: Visit www.bankinfosecurity.com or Call (800) 944-0401

155

276

2012 Cloud Security Agenda: Expert Insights on Security and Privacy in the Cloud

Overview

Nearly three-quarters of surveyed professionals say concerns regarding data security prevent their organizations from adopting cloud services. And more than half of the respondents say their own services are more secure than those offered by cloud providers.

These are among the findings of the new 2012 Cloud Security Survey. Join a distinguished panel of cloud computing experts for the first look at the findings of this perceptive study and how organizations can improve the security of their cloud computing initiatives, including:

- Understanding risks cloud computing presents;
- Mitigating these risks;
- Steps to take to employ cloud computing securely and effectively.

Background

What are organizations' top cloud security concerns, and how are security leaders addressing these concerns through policy, technology and improved vendor management?

No longer just an emerging technology practice, cloud computing today is embraced globally as a means of gaining efficient access to critical applications, processes and storage. It's now common for organizations to rely on cloud service providers for functions and business applications such as customer relationship management, messaging or storage via a public, private or hybrid cloud. Further, industry-specific cloud-based applications such as electronic health records or mobile banking and payment applications are emerging at an unprecedented pace.

But these engagements come with questions about risks:

- What are your cloud service provider's security and privacy measures, and have they been audited?
- Where geographically is cloud data being stored, and how do operational practices comply with government, industry and organizational privacy regulations?
- How is a multi-tenant cloud environment managed, and, in the event of system compromise, what will be the incident response escalation process?



The 2012 Cloud Security Survey was crafted with assistance from leading experts in cloud computing, security and privacy, with a mission to:

- Chart the latest cloud trends, including types of cloud implementations most common by industry and region;
- Gauge organizations' top cloud security concerns, from vendor security to data governance and breach preparedness;
- Predict the top areas of investment for organizations most concerned about cloud security.

This webinar will draw upon survey results and expert insight from a special roundtable panel to discuss:

- Top Security Concerns - Are organizations more concerned about where their data is stored, or whether a malicious insider might be a threat to it?
- Success Factors - On a scale with cost savings and availability of services, how does security now rank among elements critical to a successful cloud computing implementation?
- Protective Measures - What are some of the practices organizations are employing, from instituting more stringent contracts to enforcing third-party audits and even participating in mock security exercises with cloud service providers?

Presented By

Tomas Soderstrom, IT/CTO, NASA's Jet Propulsion Laboratory

David Matthews, Deputy Chief Information Security Officer for the City of Seattle

Françoise Gilbert, Founder & Managing Partner, IT Law Group

Eric Chabrow, Executive Editor, GovInfoSecurity & InfoRiskToday

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=276>

205

5 Critical Data Security Predictions for 2011

Overview

There were a number of lessons to learn from the data security mistakes in 2010. In this webinar, Andrew Jaquith, CTO for Perimeter E-Security, presents:

- Top security stories of 2010;
- Key incidents and lessons learned;
- Predictions for 2011.



Background

In 2010, enterprises of all sizes saw an exponential increase in the information risks they face. The term "data leak prevention" entered common usage among security professionals, while new buzzwords like "advanced persistent threat" gave them more things to worry about.

Listen to Andrew Jaquith, Chief Technology Officer for Perimeter E-Security and recent Forrester analyst, as he wraps up the year's top security stories, looks forward to the year ahead, and predicts five security trends for 2011. Offering a unique security perspective, Andrew will discuss:

- Another year of living dangerously: a look back;
- Three key incidents from 2010 and lessons learned;
- Take it to the bank: five data security predictions for 2011;
- Questions and answers with Andrew.

Presented By

Andrew Jaquith, CTO, Perimeter E-Security

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=205>

160

Automating Security Controls Within Government Information Systems

Overview

In this webcast you'll learn how to:

- Help automate the testing and reporting of all of the technical controls found in the NIST 800-53A framework;
- Use file integrity checks to assure your systems are in a desired state;
- Provide snapshots allowing side comparisons of a system at different time stamps;
- Test system configurations against external and/or internal policies;
- Automate documentation and report on failures for internal/external audit teams, system administrators and/or agency executives.



Background

The nation's federal and private-sector infrastructure systems are at risk because adequate cyber security controls are not in place. FISMA required agencies to enhance their security posture by instituting a process for assessing, testing and managing IT security. However, this requirement is not enough to protect organizations' IT systems.

A new approach is needed to fully secure data and access to IT systems, an approach that clarifies requirements and uses automated solutions that manage configuration assessment. Tripwire helps simplify the task of automating compliance by combining change detection and reporting with configuration assessment capabilities.

Presented By

Chris Orr, Systems Engineer, Tripwire

Brian Clark, Account Executive, Tripwire

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=160>

249

Adaptive Strong Auth & Federated SSO - A Layered Security Model for FFIEC Compliance

Overview

In the wake of today's evolving threat landscape, the FFIEC recommends a robust, layered security program that includes the use of dual customer authorization through different access devices. Strong authentication, when combined with federated single sign on standards, can strengthen, accelerate and provide key security components to build a layered security model that addresses FFIEC mandates. Learn from Forrester Research Speaker Eve Maler and Intel experts how on-premise or cloud-hosted financial applications now require a more convenient, adaptive and portable strong authentication model.

In this expert session, learn:

- Unique value prop of federated SSO combined with strong auth;
- An overview on software OTP authentication components and flows;
- How SAML based SSO provides a rich authentication audit trail for compliance;
- How mobile-based software OTP compares to other strong auth methods;
- Adaptive authentication & SSO use cases decomposed;
- How to deliver one-time passwords over various channels such as smartphone apps, SMS, e-mail and Yubikeys.

Background

Enterprises are adopting federated single sign-on (SSO) to cloud SaaS applications such as Google Apps and Salesforce to reduce helpdesk costs associated with password resets.

But there's another good reason to centralize authentication in the enterprise: it lets you perform two-factor strong authentication to enable secure access to these cloud applications. With the advent of rootkit-based malware that gets surreptitiously installed on personal computers and can compromise some of the most robust online authentication techniques, financial institutions should not rely solely on any single control for authorizing high risk transactions.

Given these newer threats, the new supplement to the FFIEC Authentication Guidance recommends a layered security program that includes the use of dual customer authorization through



different access devices that can help provide a level of security that customers expect and that can protect institutions from financial and reputation risk.

Strong authentication via hardware tokens has been used to secure internal application access for some time, but recent events have shown this method to have serious downsides. As the cloud, partners and a remote workforce drive demand for access to sensitive applications outside the traditional firewall, clearly a more convenient, adaptive, and portable strong authentication model is required. The emergence of federated SSO and mobile-based software tokens provide a more powerful, flexible approach.

In this expert session with Forrester Research, learn:

- Unique value prop of federated SSO combined with strong auth;
- An overview on software OTP authentication components and flows;
- How SAML based SSO provides a rich authentication audit trail for compliance;
- How mobile based software OTP compares to other strong auth methods;
- Adaptive authentication & SSO use cases decomposed;
- How to deliver one-time passwords over various channels such as smartphone apps, SMS, e-mail and Yubikeys.

Presented By

Eve Maler, Principal Analyst, Forrester Research

Vikas Jain, Director - Product Management, Intel - Cloud Identity & Security

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=249>

110

Application Security Testing and OCC Bulletin 2008-16 Compliance

Overview

Manage your application security risk and comply with OCC Bulletin 2008-16 cost-effectively.

- Hear about how leading organizations are leveraging Bulletin 2008-16 as a blueprint for securing third-party applications;
- Learn about contract language you can use in SLAs to demand secure software from third parties;
- Learn how you can cost-effectively manage the risk of built, bought or outsourced code without additional hardware, software or personnel investments.

Your IT organization - no matter what the size - is learning to do more with less. Yet whether you choose to build applications internally, purchase third-party software or outsource your needs, the burden of managing IT security risk - and specifically application security risk - has not reduced.

This webinar will discuss cost-effective measures your organization can take to secure your applications, comply with OCC Bulletin 2008-16 and develop an effective, comprehensive application security strategy.

Background

Recently, the Comptroller of the Currency (OCC) took the extraordinary step of issuing a bulletin (OCC Bulletin 2008-16) to alert financial institutions of the risks posed by insecure software and recommend steps banks should take to reduce risk and protect their critical data.

This follows on new industry regulations from the Payment Card Industry requiring application security testing for merchants, service providers and payment application vendors, along with a recent advisory from Gartner that "application security testing should be mandatory for outsourced development and maintenance."

Perhaps most notable in the OCC Bulletin is the scope of the recommendations. Not only are banks advised about internally developed applications, but they need to mitigate risk from commercial software, outsourced development and contracted software for both internal and web-facing applications.

This webinar will discuss cost-effective means you can comprehensively assess your entire portfolio of software



applications, whether bought, built internally or outsourced without the addition of new hardware, software or time-consuming (and costly) manual testing.

Special guest presenter, John Jacott, PCI-QSA, IRCA Lead Auditor for ISMS, will provide insights as to what auditors may be looking for and how to generally leverage the framework of Bulletin 2008-16 as an overall blueprint for application security.

Presented By

Mike Puglia, Veracode Director of Product Marketing

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=110>

130

Assessing Encryption Standards for Financial Institutions

Overview

Critics of the Heartland Payment Systems data breach have called out for tougher encryption standards for financial institutions and their third-party service providers. Applications for encryption are all around us, from encrypting e-mail traffic to board communications, remote access and mobile & Internet banking.

Register for this webinar to learn the encryption basics and to understand recent advances, including:

- Which data every financial institution should consider encrypting;
- Technological and business process challenges of encrypting data;
- Things you should ask ALL of your vendors about encryption technologies used in their products or services;
- Regulatory mandates regarding data encryption.

Background

Encryption is the process of obscuring information to make it unreadable without special knowledge.

In the mid-1970s, strong encryption -- the process of turning computer data into code that can be read only by someone with a key to the information -- emerged from the sole preserve of secretive government agencies into the public domain, and is now used in protecting widely-used systems, such as Internet e-commerce, mobile telephone networks and bank automatic teller machines.

In financial services, the adoption of distributed computing has radically increased the speed and amount of customer data being transmitted, stored or shared with business partners.

As a result, in 2005 the Federal Financial Institutions Examination Council (FFIEC) set a 2006 deadline for U.S. banking institutions to implement two-factor authentication to secure their transactions - a move that encouraged many institutions to increase interest in encryption. Today, encryption is used by institutions for the transmission of information across networks, as well as for storage of information on computers.

The purpose of this webinar is to provide the practical information on the basics of encryption, answering fundamental questions such as:



- What should my institution encrypt - and where?
- What technological challenges will we face in encryption?
- Where is the best place to get started when encrypting critical information?

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=130>

238

Beyond the FFIEC Authentication Guidance: Prepare for Future Threats

Overview

Cyber crime against financial institutions has evolved dramatically since 2005. This evolution is what inspired the FFIEC Authentication Guidance update. But how will cyber threats evolve in the years ahead and what can banking institutions do today to protect themselves tomorrow?

Join banking security experts and a former regulator to learn:

- What FIs need to do before the deadline to conform with the new guidance;
- Why the leaders in the banking space are taking the initiative to go above and beyond the guidance recommendations;
- Why compliance does not equal true security: what FIs should be doing to achieve real security.

Background

Several recent cases involving ACH-related fraud and corporate account takeover have proved once again that cyber crime in the electronic banking environment is still a reality, despite the security measures implemented over the years. The explanation is simple: cyber crime against financial institutions and customers is evolving almost daily while the regulation is often lagging behind. With millions of dollars lost to e-banking fraud every year, many FIs are now looking hard at their security practices as well as their vendor recommendations and the new Authentication Guidance Supplement.

The Second Annual Cost of Cyber Crime Study, conducted by the Ponemon Institute, revealed that the median annualized cost of cybercrime is \$5.9 million a year, which is 56 percent higher than the year before. The organizations are paying anywhere from \$1.5 million to \$36.5 million a year to combat cyber crime, according to the study.

As a financial institution, how can you minimize your risk and your customers' risk of becoming victims of cyber crime? Does the new Authentication Guidance offer enough direction for future-proofing security? Surely, being in compliance with the guidance will help you today, but what about the future?

How vulnerable is your institution to the next man-in-the-middle attack? Are you prepared to handle real-time attacks? Will



community banks and credit unions become targets? In order to implement a successful security strategy, it is imperative to have a thorough understanding of the cyber attacks' mechanisms and the protection offered by common technology solutions.

In this session, you will hear the recommendations from the industry experts on how to implement adequate security mechanisms to protect your institution and your customers from cyber fraud and future-proof your security, including:

- The new guidance and recommended strategies for protecting commercial/retail customers;
- What to do and when to start;
- A case study presented by Bank of America about their best practices in securing commercial e-banking customers: above and beyond the guidance;
- Evolving fraud and required countermeasures: how to ensure true, future-proof security;
 - » MITM and MITB delivery mechanisms and risks
 - » Out-of-band authentication: myth vs. fact
 - » Transaction signatures
 - » Layered approach

Presented By

Benjamin Wyrick, Director - Sales, VASCO Data Security

Milton Santiago, SVP - Portal Strategy & eChannels, Bank of America

William Henley, SVP - Regulation, BITS

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=238>

294

Big Data & Security: The Management Challenge

Overview

The massive growth of data within today's enterprise overwhelms traditional security controls. How can organizations inventory, manage and secure big data at every stage of its lifecycle? How can they turn the security challenge into a security advantage? Join this panel of experts for a discussion of big data and security - the challenges and opportunities, including:

- How to define big data and address security concerns;
- How to achieve business efficiencies from big data;
- The impact of consumer devices and removable USB drives, and how to ensure secure enterprise mobility.

Background

Big data is truly a challenge that stretches the boundaries of the enterprise.

According to a new report from the Information Security Forum (The Information Security Forum [ISF] is an independent, not for profit association of leading organisations from around the world. It's dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management), data volumes are growing at an alarming rate - around 2.5 million terabytes every day.

From structured and unstructured data within the network of enterprise PCs and servers to the consumer devices - smart phones, laptops and removable storage devices that introduce new data management challenges - organizations are easily overwhelmed by the questions posed by big data:

- What does big data look like, and where can it be found?
- How can we leverage big data to improve operational efficiencies?
- How do we address the inherent security concerns and, in fact, use big data analytics to improve our security posture?
- What new challenges - and opportunities - are posed by mobility?

In this session, leading experts in big data will define the challenges and offer hands-on advice for how to tackle them.

Steve Durbin, Global VP of the ISF, will set the stage with a big data overview, offering context on today's challenges, as well as introducing topics such as:



- The impact of cyber crime;
- Privacy concerns;
- The skills shortage - do we need data scientists to manage big data?

Gary Gerber, Sr. Product Marketing Manager of Imation Mobile Security, then will discuss how to secure enterprise data, with an emphasis on best practices for secure mobility. Among his key points:

- How enterprises secure the vast amounts of data workers are moving through unsecured devices out of the network everyday;
- Teleworking trends and how they impact big data management;
- Tips for improved identity & access management;
- How to develop an effective organizational approach for securing removable storage devices.

Following the short presentation will be an engaging panel discussion addressing the audience's key questions about big data and security.

Presented By

Steve Durbin, Global VP, Information Security Forum

Gary Gerber, Senior Product Marketing Manager, Imation

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=294>

266

BYOD: Manage the Risks and Opportunities

Overview

From smart phones to tablets, laptops to USB devices, consumer technologies are ubiquitous in the workplace - and so is the 'bring-your-own-device' (BYOD) practice of allowing employees to conduct work on their own personal electronics.

But how do these consumer technologies change organizations' approaches to securing corporate information assets?

Join this panel of mobile technology experts for a thorough discussion of the risks and rewards of enabling BYOD, with an emphasis on how to manage the mix of consumer devices in the workplace, as well as enforcing key tenets of your mobile policy. Among the discussion points:

- How to properly inventory your employees' personal devices;
- Technology solutions to protect your corporate systems and data, as well as the end-point devices;
- Strategies and tactics for enforcing mobile policies and maintaining compliance in regulated industries;
- How to use BYOD as an opportunity to enable further proliferation of data and access security.

Background

From home computers and laptops to cellphones and PDAs, employees have always lobbied to introduce consumer technologies in the workplace.

But with the advent of smart phones, tablets, portable storage and a variety of laptops - powerful computing devices that often rely on unsecured wireless networks - the push today is even greater. Example: Intel, the global computer technologies manufacturer, reports that connected mobile devices grew from 10,000 to 30,000 over the first 10 months of 2011. And by 2014, Intel expects 70% of its employees to use personal devices for some aspect of their job.

So, it's no longer a question of whether to allow employees to use their own devices - no corporate policy can stem the tide of consumerization. The questions now are about:

- Inventory - How do you properly account for all of the consumer devices introduced by your employees? Know how to lock down your corporate wireless networks and desktop computers, so you'll also know when employees are trying to access corporate resources via connecting new devices.



- Security - How do you protect your systems and data from unauthorized access - and in the event of lost or stolen devices? From identification to proper authentication, appropriate access control, data storage and detecting unauthorized activities - all controls implemented by an organization on 'corporate-owned' resources over the last decade can potentially be rendered useless on an employee-owned device. Learn the importance of each control and the implementation challenges in a large-scale environment.
- Opportunity - Beyond securing devices, BYOD is an opportunity to improve data and access security in the enterprise, web, mobile and SaaS applications. The opportunity is for organizations to still have strong security and authentication, but in a way that is "outsourced" to the device owner for all of their applications. This outsourcing can save the company IT budget, as well as reduce help desk support.

In this session, mobile security experts will discuss these topics and more, sharing insights on how today's leading-edge organizations are embracing BYOD as a means of improving employee productivity and creating new business value.

Presented By

Benjamin Wyrick, Director - Sales, VASCO Data Security

Malcolm Harkins, CISO, Intel

Dan Ford, Chief Security Officer, Fixmo

Ahmed Dattoo, Chief Product Officer, Zenprise

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=266>

188

Cloud Computing: Regulatory Security & Privacy Challenges

Overview

Cloud computing is the hot, new practice that offers a scalable, centralized resource for data and applications that can be available to anyone, anywhere.

But as an emerging trend, cloud computing is also fraught with risk - already we've seen organizations whose data has been compromised.

Register for this session to hear the lessons learned about cloud computing from a panel of experts who will discuss:

- Advantages and disadvantages of storing data or running applications online, as opposed to in-house;
- Current regulatory trends toward better security and privacy standards - and how they impact cloud computing;
- Legal, privacy, records management and ethical challenges that have been identified by cloud pioneers - and strategies to avoid those pitfalls.

Background

Attend any industry event this year, and the term you'll hear most frequently is "Cloud Computing."

But like the old cliché about the weather, one is left to ask: "Everyone is talking about Cloud - but what are they actually doing about it?"

The answer is: More than you might think. Banking institutions for years now have practiced cloud computing without using the term, outsourcing core processing to third-party service providers.

Today, with more banking services to offer and more hosting options from vendors, banking institutions have a broad range of cloud computing opportunities before them. But they also have significant questions to answer re: scale, security, privacy and true business benefits.

In this session, Matt Speare, veteran technology leader from M&T Bank, will lead our cloud computing discussion - setting the stage with a presentation depicting a banking institution's approach to the cloud. He'll then interact with industry experts, including Jim Reavis of the Cloud Security Alliance, to discuss not just the theory of cloud - but about the real business benefits that pioneer banking institutions are realizing today.



Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

Michael Smith, Security Evangelist, Akamai

Harold Moss, CTO - Cloud Security Strategy, IBM

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=188>

291

Continuous Monitoring: How to Get Past the Complexity

Overview

What exactly is continuous monitoring - and why is it so hard for organizations to get it right?

It is one of the most discussed and least understood concepts in enterprise risk management today. Fundamentally, continuous monitoring is about deploying systems to examine all of the transactions and data processed in different applications and databases, ensuring that patches are updated, proper controls are in place and that all known (and even unknown) vulnerabilities have been addressed within an acceptable risk threshold.

But in this session, you will go beyond the fundamentals and learn first-hand from a leading expert:

- How to establish a successful continuous monitoring program;
- Technology and personnel requirements that might be easily overlooked;
- How to overcome the obstacles that have prevented other organizations from achieving maximum benefits from continuous monitoring.

Background

Continuous monitoring fits into the six steps of the Risk Management Framework described in guidance issued by the National Institute of Standards and Technology, which defines its objective to determine if deployed security controls continue as changes inevitably occur to IT systems.

The concept traces its roots to traditional auditing processes, but goes further than a periodic snapshot audit by putting in place frequent examination of transactions and controls so weaknesses can be corrected or replaced before they can do damage. Continuous monitoring systems should examine all of the transactions and data processed in different applications and databases, testing for inconsistencies, duplication, errors, policy violations, missing approvals, incomplete data and other possible breakdowns in internal controls.

A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static and occasional security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information. That information can be used to take appropriate risk mitigation actions and make



cost-effective, risk-based decisions regarding the operation of their information systems. A continuous monitoring program allows an organization to track the security state of an information system on an ongoing basis and maintain the security authorization for the system over time. Understanding the security state of information systems is essential in highly dynamic environments of operation with changing threats, vulnerabilities, technologies and missions/business processes.

Presenter Dwayne Melancon, an industry expert on continuous monitoring, will discuss:

- NIST's view of continuous monitoring as well as guidelines and requirements for government agencies and specific industries to implement it;
- How to establish a continuous monitoring strategy;
- A step-by-step roadmap to integrate continuous monitoring into your organization's Risk Management Framework;
- How continuous monitoring will help your organization defend against breaches, gain IT systems' efficiencies, improve availability and prepare for audits.

Presented By

Dwayne Melancon, CTO, Tripwire

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=291>

248

Creating a Culture of Responsible Application Security

Overview

Software applications are the lifeblood of every organization, and today's #1 IT security threat is vulnerabilities in these applications.



Register for this session to learn:

- How to arm developers with the right security controls so that they can create secure applications from the outset;
- The concept of 'responsible application security,' which means coding correctly from the start;
- How, through training/education, developers will be able to get their applications into production more quickly and securely.

Background

The applications we entrust with our healthcare, financials and national defense are just as vulnerable as other code. The problem is that while our threat environment has changed dramatically, the way in which we write code has not.

Security doesn't have to weigh down software development.

In this session, we'll share stories from large organizations that have standardized their application security controls, raised the awareness of their personnel and transitioned away from punitive penetration testing programs to a positive verification approach.

Register for this webinar to learn:

- How to foster/create a culture of responsible application security;
- The top 3 security mistakes in creating custom applications;
- Financial models that make the case for ROI in application security;
- Real-world success stories, including a large mutual fund and a branch of the U.S. military.

Presented By

Jeff Williams, CEO, Aspect Security

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=248>

194

Debit Fraud: Trends and Typologies

Overview

Skimming, tsunamis, chameleons - debit fraud schemes are on the rise. Join us for a free webinar where we'll talk about the latest in debit card fraud, and share our experiences in how to detect it. This webinar will deliver:



- An overview of debit fraud;
- Current & forecasted trends;
- Typologies & sample scenarios;
- Things to look for in a fraud solution.

Background

Debit card fraud, the act of using debit card information to fraudulently obtain money or goods, is front and center in the minds of Americans. The March 2009 Unisys Security Index reported that credit and debit card fraud is the number one fear for Americans, surpassing terrorism, computer and health viruses and personal safety.

Fraudsters are constantly on the attack, with no concern for the consequences or fall-out from their actions. Financial institutions are continuously left to fight from a defensive position, reacting to attacks while trying to limit damage and clean up the resulting mess.

This webinar discusses current debit card use and debit card fraud trends. It examines several specific debit fraud scenarios that represent a sample of both common and emerging debit card fraud trends faced by card holders and financial institutions today. Finally, it offers a number of features that make an anti-fraud software solution effective.

Presented By

Charles Robertson, Verafin

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=194>

208

Data Protection: The Dirty Little Secret

Overview

Think your data is secure? Think again.

If you are sending data over a service provider's network, then you need to know: Current Wide Area Network (WAN) technologies offer no inherent data protection. It's time for you to take matters into your own hands to ensure your data is secure.

View this FREE webinar to learn about:

- The importance of data-centric security and the latest findings on how/where data is stolen;
- The truth about the lack of security with MPLS and other WAN technologies;
- A groundbreaking data protection method that secures data without impacting network or application performance.

Background

Many network and security executives believe data is secure as it traverses the Wide Area Network (WAN). This myth is often perpetuated by service providers who claim their networks are "private" - insinuating that your data is safe from attack, theft, or redirection as it traverses over network backbone.

The truth is that your data may be more vulnerable on the MPLS/Metro-E backbone than anywhere else. Since your data is most often sent in clear text (unencrypted), your data can be viewed, replicated, modified or redirected without detection. To make matters worse, there are readily available video instructions on the Internet on how to tap data lines for data replication.

And if your data is breached, it's your company that bears the financial and legal burden. Nearly all standard service level agreements (SLA) specify only availability rather than data security and integrity (another little truth the providers are not keen on sharing).

The good news is that with recent technological advancements, it is now possible to protect data in motion over the WAN, without the complexity, cost and performance issues of IPsec tunnels. With this latest breakthrough in data protection, your information can be secured quickly and easily while maintaining high availability, disaster recovery and any-to-any connectivity -- all with performance that meets the standards for voice, video and other high speed applications.



Among the topics to be discussed are:

- How threats to networks and data have changed over the past 15 years;
- The difference between "virtual privacy" and actual security;
- A revealing look at the lack of security within wide area networks;
- Network encryption case studies - how several companies are protecting their data without using performance killing IPsec tunnels.

Presented By

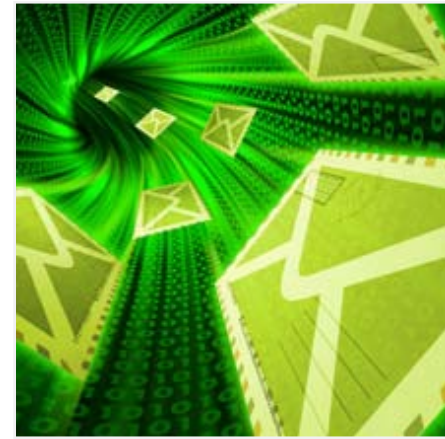
Jim Doherty, Chief Marketing Officer (CMO), Certes Networks

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=208>

180

Email Security Requirements for Healthcare Providers: HIPAA & Beyond



Overview

E-mail continues to be a main source of exposure of protected health information (PHI) and other private data in today's enterprise, but most organizations have yet to deploy technology to prevent costly breaches of PHI. Join this discussion to find out what you need to know about the latest security, privacy and data breach regulations for health information.

Register for this webinar to learn:

- How policy-based encryption can help protect private healthcare information and mitigate the risks associated with data loss and corporate policy violations;
- New provisions of the U.S. economic stimulus legislation (ARRA) that expand the scope of HIPAA security rules, and the impact on your organization's e-mail security and compliance strategy;
- New HIPAA violation penalties and the impact of the breach notification requirements enforced by the FTC;
- Technology requirements for protecting the confidentiality of healthcare information in both outbound and archived e-mail messages.

Background

Healthcare regulations for IT security - such as HIPAA and the new HITECH provisions of HIPAA - are now broader than ever. And they apply not just to healthcare organizations, but to all kinds of companies that handle or store private health information, from web hosting firms to accountants. Today's penalties for data breaches are increasingly onerous: Fines are bigger, notification requirements are more stringent and enforcement organizations have new incentives for taking action against organizations that fail to protect healthcare privacy.

Learn what to look for in a secure e-mail solution for complying with the web of regulations that now apply to so many companies.

By attending, you'll also learn how automatic, policy-based e-mail encryption can provide effective protection for sensitive health information in e-mail and why it should be a central part of your approach to HIPAA compliance.

Presented By

Rami Habal, Director of Product Marketing, Proofpoint

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=180>

246

FFIEC Authentication Guidance: How to Create a Layered Security Strategy



Overview

With the FFIEC Authentication Guidance update, regulators have raised the bar: Traditional security controls are insufficient. Banking institutions now must adopt a layered approach.

But how does one choose among all of the layered security options? Then, what are the elements of an effective layered security strategy that satisfies the guidance and enhances security?

Join George Tubin, a foremost industry analyst, for his expert insights on:

- FFIEC Authentication Guidance and expectations for layered security controls;
- Strengths/weaknesses of most popular controls, from out-of-band authentication to voice-based biometrics;
- An effective layered security framework that includes the device, user, transaction and network.

Background

Device identification. One-time password tokens. Out-of-band authentication. When it comes to layered security controls, there are countless options available to help banking institutions comply with the FFIEC Authentication Guidance. But how does a banking/security leader make the right choices?

To answer this question, one first must understand the FFIEC's definition: "Layered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control."

And while banking regulators don't endorse any specific controls, they do offer these options as elements of a layered security program:

- Fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
- Dual customer authorization through different access devices;
- Out-of-band verification for transactions;
- "Positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;

- Enhanced controls over account activities, such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows;
- Internet protocol [IP] reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;
- Policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud;
- Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels; and
- Enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

Analyst George Tubin leads a discussion on crafting an effective layered security program, including:

- FFIEC Authentication Guidance - What the update says about layered security and what's no longer sufficient;
- Fraud Prevention Technologies - An in-depth look at the most popular security controls, reviewing strengths and weaknesses of each. Included: Out-of-band authentication, anomaly detection, account-based restrictions, voice biometrics and more;

Layered Security Strategy - How to put the pieces in place to secure the transaction, user, device and network.

Presented By

George Tubin, Banking and Security Analyst

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=246>

245

FFIEC Authentication: How to Invest in Anti-Fraud and Operational Controls

Overview

In reviewing recent ACH/wire fraud incidents that have plagued banks and commercial customers, the FFIEC Authentication Guidance minces no words: Institutions could have and should have detected and prevented these incidents with proper layered security controls.

But what constitutes appropriate controls, as described by the new supplement to the guidance, and how can an institution evaluate the options and make smart, secure investments?

Join a veteran anti-fraud expert to learn how to:

- Conform with anti-fraud and operational controls expectations expressed by the FFIEC Authentication Guidance;
- Analyze anti-fraud options and assess them with operational controls in mind;
- Anticipate future expectations for fraud prevention, based on the FFIEC Authentication Guidance and recent court rulings.

Background

In part, these fraud cases inspired the FFIEC to revisit its original 2005 online banking guidance. But in issuing the 2011 supplement to the FFIEC Authentication Guidance, banking regulators were openly critical of banking institutions.

“Based upon the incidents the agencies have reviewed,” the guidance reads, “manual or automated transaction monitoring or anomaly detection and response could have prevented many of the frauds since the ACH/wire transfers being originated by the fraudsters were anomalous when compared with the customer’s established patterns of behavior.”

To help detect and prevent future incidents, the FFIEC Authentication Guidance calls for new layered security programs that include two core elements:

- The ability to detect and respond to suspicious activity in an account;
- Enhanced controls of administrative functions.

In the appendix to the guidance, the FFIEC recommends that institutions investigate several different security controls, including:



- Anti-malware software;
- Transaction monitoring/anomaly detection software;
- Out-of-band authentication;
- USB devices to enhance online banking session security;
- Use of restricted funds transfer recipient lists.

Layered security controls do not need to be complex, the FFIEC says. But they cannot be one-dimensional - not in today’s ever-evolving threat landscape.

In this session, David Garrett, an experienced anti-fraud expert, will walk through the relative merits of various security controls, operational and anti-fraud controls, and he’ll show you how to develop a strategy to invest in the controls that are right for your institution and its risks - financial and reputational.

Presented By

David Garrett, Fraud and Operational Controls Analyst

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=245>

241

FFIEC Authentication: The Myths and Truths of Anomaly Detection

Overview

On page five of the 2011 FFIEC Authentication Guidance Supplement, the Agencies state that an institution’s layered security should include the ability to detect anomalies and effectively respond to suspicious or anomalous activity. Anomaly detection is a proven approach to defending against the array of threats facing online banking and institutions using anomaly detection today are experiencing a wide range of business and operational benefits. This presentation will provide a practical view of anomaly detection from experts who have designed and implemented anomaly detection solutions at a broad array of institutions.

In a unique Q&A format, the presenters will provide rich details on:

- What anomaly detection is and how it identifies compromise and fraudulent wire, ACH, bill pay and external transfer fraud in the face of current and future threats;
- How to technically and operationally implement anomaly detection;
- Real-world case studies illustrating operational and fraud prevention successes;
- Answers to the most common questions about anomaly detection.

Background

In response to the evolving threats against online banking and the growth in fraud stemming from the online channel, the FFIEC updated its guidance to financial institutions on Internet banking security. The guidance raised the bar for risk assessments, layered security and customer education.

In the 2011 Guidance, the Agencies are very specific about the need for layered security and provide explicit directions for the minimum elements every layered security stack should have. On page five of the 2011 FFIEC Authentication Guidance Supplement, the Agencies state that an institution’s layered security should include the ability to detect anomalies and effectively respond to suspicious or anomalous activity. Anomaly detection is a proven approach to defending against the array of threats facing online banking. Institutions of all sizes on a variety of different platforms are successfully using anomaly detection to address today’s sophisticated threats including Man-in-the-Browser threats.



This presentation will provide a practical view of anomaly detection from experts Craig Priess and Terry Austin. In a unique Q&A format, the presenters will cover the most commonly asked questions about anomaly detection. Their discussion will cover:

- Why anomaly detection has been so successful at stopping online fraud;
- Real-world fraud cases stopped by anomaly detection;
- How anomaly detection compliments other security solutions;
- Time and effort required to implement anomaly detection solutions;
- Operational considerations;
- ROI drivers for anomaly detection.

Presented By

Craig Priess, Founder & VP - Products, Guardian Analytics

Terry Austin, President & CEO, Guardian Analytics, Inc.

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=241>

247

FFIEC Guidance: How to Use Layered Security to Fight Fraud

Overview

Layered security is one of the core tenets of the new FFIEC Authentication Guidance - and it's perhaps the most effective strategy for detecting and preventing banking fraud schemes. But what are some of today's most mature approaches to layered security, and how are banking institutions employing them?

Join a distinguished panel of industry experts to learn:

- The types of layered security controls prescribed by the FFIEC, and what examiners will be looking for from institutions starting in January 2012;
- Tips from banking institutions that are already deploying layered controls such as knowledge-based authentication, device identification, behavioral monitoring, anomaly detection and cross-channel pattern analysis;
- Emerging technologies that will enable more efficient and effective ways to know their customers, improve fraud detection and create layered protection across all maintenance activities and customer devices.

Background

In response to heightened incidents of fraud, the Federal Financial Institutions Examination Council has formally released the long-awaited supplement to its "Authentication in an Internet Banking Environment" guidance, first issued in October 2005.

Among the most prominent topics in the new guidance is "layered security," which the FFIEC defines as "the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control." But layered security controls also are appropriate in all customer interactions.

Starting in January 2012, banking regulators will examine institutions for conformance with this new guidance, looking for how institutions have:

- Improved their abilities to detect and respond to suspicious activity;
- Enhanced controls for system administrators of business accounts.

Among the layered security methods recommended by the FFIEC:



- Fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
- Dual customer authorization through different access devices;
- Out-of-band verification for transactions;
- "Positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;
- Enhanced controls over account activities, such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows;
- Internet protocol [IP] reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;
- Policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud.

In this session, Matthew Speare of M&T Bank will discuss how his institution has tackled the layered security strategy in all aspects of electronic banking. He then will lead a panel of industry experts in an open discussion on best-practices in fraud prediction and detection and how to improve the analysis of suspicious behavior.

Presented By

- Matthew Speare, SVP of Information Technology, M&T Bank
- Michael Smith, Fraud Market Planning Lead, LexisNexis Risk Solutions
- Alisdair Faulkner, Chief Products Officer, ThreatMetrix
- Mark Benoit, Security Specialist, Attachmate Corporation

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=247>

187

Fight Back Against Fraud: Strategies on How to Meet the Multi-Channel Challenge

Overview

ACH and wire fraud. ATM skimming. Payment card compromises. Mortgage fraud. Phishing.

Financial institutions are besieged by fraud threats today - and not just via one dominant channel, but through all of them. Simultaneously.

How can institutions fight back - as well as educate & enlist their consumer and business customers to do their parts, too? Join this panel discussion to hear new insights from industry thought-leaders on:

- The multi-channel fraud threats facing financial institutions today;
- Successful strategies for mitigating these threats;
- New tactics for educating and protecting customers;
- Emerging technologies to fight fraud.

Background

From ATM skimming to bogus wire transfers, 2010 has been the "Year of the Fraudster" for banking institutions and their customers.

According to the latest Verizon Business Data Breach Investigations Report, financial services far and away is the most commonly breached industry, accounting for 85% of the 143 million records breached in 2009. The most common types of fraud:

- Insiders;
- Social engineering schemes;
- Hacks by organized crime.

Symptoms of these crimes have dominated the news: ATM skimming sprees, increased incidents of ACH fraud, aka corporate account takeover, attacks against merchant point-of-sale devices.

More daunting for banking institutions: These incidents aren't occurring in isolation. Rather, they tend to strike across multiple channels, testing for every possible vulnerability.

The cost to financial institutions? It breaks down two ways:



- Financial - The time, expense and human resources necessary to respond to breaches, notify customers, monitor accounts and, when necessary, replace payment cards and lost funds;
- Reputational - Perhaps the biggest toll of all - the loss of customer confidence when an account has been breached. The customer doesn't necessarily care who committed the breach; they just know it happened on their bank's watch.

So, how can financial institutions fight back? First they must know their enemy and the guises it wears. That's the main point of this session. Matt Speare of M&T Bank will lead the discussion, walking attendees through an overview of the types of fraud schemes institutions such as his see every day. From there, our panel of industry experts will discuss current trends and the threat landscape, as well as proven solutions to detect and deter fraud.

Presented By

- Reed Taussig, President & CEO, ThreatMetrix
- Matthew Speare, Senior Vice President of Information Technology, M&T Bank
- Kim Peretti, J.D., LL.M., CISSP, PricewaterhouseCoopers
- Ori Eisen, Founder, Chairman and Chief Innovation Officer, 41st Parameter

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=187>

177

Fraud Prevention: Protect Your Customers and Your Institution from Web Vulnerabilities

Overview

Fraud is the #1 risk to banking institutions, and the chief victims are their customers - consumers and businesses who lose vast sums of money to web-based scams.

Register for this webinar for expert insights on:

- Current fraud trends, including ACH and social networking;
- Top vulnerabilities for your employees and customers alike;
- How to enhance protection through the latest technology solutions.

Background

The headlines tell it all:

In Michigan, a small business has sued its bank after a phishing attack left the business vulnerable to fraudulent ACH transactions that added up to over \$500,000.

In Texas, a bank sued its customer - and then was countersued - over a dispute involving \$800,000 worth of ACH fraud and the question of, "What is reasonable security?"

ACH fraud has become one of the most insidious crimes preying upon banking institutions and their customers, eroding the trust that's so fundamental to the banking relationship. The FDIC, FBI and American Banking Association all have sent out alerts warning banks and businesses of the dangers of ACH fraud, and the Department of Justice now is investigating the extent and roots of these crimes.

But ACH isn't the only form of fraud that is bilking banking institutions and businesses. ATM and payment card crimes are also on the rise, and social networking sites now provide a new venue for fraudsters to prey upon consumers and organizations.

In all, the FDIC estimates that banking customers lost \$120 million to fraud in 2009. How will 2010's statistics compare?

Register for this webinar for unique insight into the legal implications of current fraud trends, as well as potential solutions to prevent these crimes. David Navetta, Co-Chair of the American Bar Association's Information Security Committee, will lead the discussion of:



- The latest fraud trends targeting banking institutions and businesses;
- Current court cases and their implications for information security organizations.

Then Matthew Speare of M&T Bank will discuss how banking institutions should approach ACH fraud and social networking, including:

- Changing attack venues;
- Policies;
- What to monitor and how.

Following Navetta and Speare, thought-leaders from Websense, sponsor of this session, will discuss emerging technology solutions and their roles.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

Patrik Runald, Senior Manager of Security Research, Websense

David Navetta, Founding Partner, Information Law Group

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=177>

213

Fraud Prevention: Understand & Mitigate Threats to Global Institutions

Overview

In this webinar you will learn current and next-generation methodologies being deployed by global organized crime rings, and effective techniques to analyze and disrupt them. You will also gain insights on conducting global due diligence operations on international individuals and companies, which has never been more crucial than now.

In today's financial industry, threats to your sensitive information are diverse and are growing in volume, sophistication and intensity. To protect your organization, your assets and your customers from fraudsters takes both an understanding of their capabilities and techniques, and knowing as much as you can about who you are doing business with. By attending this webinar, you will increase your situational awareness from both a technology and business perspective. Don't miss this important webinar for bank and financial information and security professionals.

Attend this webinar to learn about:

- Current and emerging methodologies employed by organized crime to defraud financial institutions;
- Structure and methodologies for black-market malware distribution and money laundering through physical and virtual money mules;
- Advanced information on international due diligence and compliance issues that will benefit financial organizations;
- Successful cases of investigation and arrest.

Background

The webinar will expose current and emerging methodologies deployed by Russian and Romanian organized crime to deploy Zeus variants and other malware to compromise consumer credentials. The speakers will expose the underground black market that exists for financial institution-specific malware creation, distribution, BotNet utilization and money laundering via the recruitment of both physical and virtual money mules.

The speakers will also relate successful cases of investigation and arrest where law enforcement stopped fraudsters who were using Zeus malware to target banks.



Beyond understanding of fraudsters and their methodologies, banks and financial institutions will further benefit from a proactive stance achieved by knowing more about who they are doing business with. The importance of conducting international due diligence on individuals and companies has never been more prominent that it is today, and implementing a compliant due diligence department is vital in today's corporate environment. With a plethora of regulations enacted and numerous multi-million dollar fines levied, it has become apparent that responsible companies should strive toward implementing a compliance program that allows them to be proactive and compliant in their international business dealings. Regulators are investigating and pursuing companies who are not compliant, and to this point, this webinar will also convey recent regulatory issues surrounding situations that webinar attendees would not want their company or reputation to be associated with.

Presented By

Ronald Plesco, CEO, National Cyber Forensic Training Alliance

William News, Director - Investigative Resources, NFC Global

Brandt Heatherington, Global Director - Commercial Marketing, i2 Group

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=213>

225

How to Achieve Network Security Without Compromising Performance

Overview

Historically, it has been a trade-off. Securing the information network has required organizations to settle for solutions that have diminished network performance. But how - at a time when government agencies place greater demands than ever on their networks - can you deliver security and performance?

This webinar offers methods and suggestions for implementing security without sacrifices. If you think security can only be accomplished by compromise, this is a must-see webinar.

Topics include:

- Security best practices for modern networks;
- Methods for quickly creating secure communities of interest without impacting performance;
- A primer on an advanced IPSec technology that eliminates tunnels and dramatically improves the performance of encrypted networks.

Background

The tradeoffs that used to come with improved security are no longer required. For those still securing their networks with performance killing IPSec tunnels, find out how you can improve security, reliability and visibility without compromising the security of the network.

“In addition to the increased network security required for individual government networks, the nature of today’s national and cybersecurity threats have increased the need for secure collaboration between agencies and organizations,” said retired Vice Admiral Jerry O. Tuttle, a highly distinguished Navy officer and acknowledged IT technology visionary. “The ability to quickly create Secure Enclaves and Communities of Interest without impacting network performance is a welcome advance in secure network communications.”

Secure Enclaves have become an essential part of government networks - whether to create secure communities of interest, segment data for compliance, or to create electronic perimeters for critical network isolation. Until now, creating these Secure Enclaves required setting up cumbersome IPSec tunnels that



downgraded performance, restricted visibility and often violated network security best practices. Fortunately, a new technology has emerged that allows security personnel to quickly and easily create Secure Enclaves that adhere to security best practices.

Topics to be discussed include:

- Network security best practice;
- The difference between “virtual privacy” and actual security;
- A revealing look at the lack of security within wide area networks;
- Group encryption case studies;
- Group encryption and TIC compliance;
- Cloud security strategies with group encryption.

Presented By

Jim Doherty, Chief Marketing Officer (CMO), Certes Networks

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=225>

236

How to Improve Network Security on a Limited Federal Budget

Overview

It’s the common challenge: Federal budgets are level-funded or cut. But as critical data becomes ever-more mobile and regulatory mandates grow, how do you use your limited resources to actually improve network security?



Join Jeff Schafer of the USGS Fort Collins Science Center in Colorado as he explains:

- How to cost effectively and efficiently secure your network;
- The real definition of continuous compliance and remediation;
- How to stay ahead of government IT regulations.

Background

Government computer systems continue to be targets for attack. As IT assets increase in capability and functionality and as more data is produced and stored, this problem will only get worse. Government agencies are struggling with implementing efficient and rapidly deployable technologies to protect against these growing threats while at the same time ensuring conformance to current and future IT governance laws and requirements.

A single management server can provide the asset visibility, control and real-time remediation needed for highly distributed systems and security management to hundreds of thousands of endpoints, regardless of their location or connection type. Single management servers have saved many public sector organizations costs through reduced power usage, decreased software license fees, fewer compliance costs and penalties, improved information security process efficiencies and infrastructure consolidation.

Join Jeff Schafer from the USGS Fort Collins Science Center in Colorado as he explains how he’s efficiently securing his network to solve multiple challenges cost effectively and efficiently. He will demonstrate what continuous compliance, remediation and accountability really mean, while staying on top of all the various government IT regulations, directives and guidance.

Presented By

Jeff Schafer, Lead IT Specialist, USGS Fort Collins Science Center

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=236>

148

How to Prevent Security Breaches Through Effective Management and Control of USB Devices

Overview

In this Lumension webinar, you will learn:

- How USB devices are used to transfer data;
- About the federal government ban on USB devices and its impact;
- How to effectively manage USB devices to secure data and networks without impacting productivity.



Background

The DoD has banned the use of USB devices after an unauthorized device containing “agent.btz”, a variation of the Storm Worm, was connected to a sensitive DoD network causing massive outages. To ensure security without impeding government business, a new policy is forthcoming that will require the management and reporting of USB device usage on government networks. Listen to Steve Antone, Lumension Vice President of Federal Solutions Group, as he discusses how to prevent security breaches through effective management and control of USB devices.

Presented By

Steve Antone, VP - Federal Solutions Group, Lumension Security

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=148>

105

How To Launch a Secure & Successful Mobile Banking Platform

Overview

If you're not at least investigating mobile banking now, you can bet your competitor is.

Worldwide, there are 3.3 billion mobile devices -- vs. 950 million PCs - and four people are born every second, while 32 mobile phones are sold.

Mobile banking is the immediate future of financial institutions of all sizes and geographies. Even in this down economy, 41% of respondents to a recent banking survey said they intend to invest in new/enhanced services such as mobile banking in 2009. By 2012, says another study, 40 million U.S. consumers will be mobile banking users.

Register for this webinar to hear first-hand how and why New York-based M&T Bank launched its mobile banking pilot program, including:

- Why institutions of all sizes are getting into mobile banking;
- How to use mobile banking to your competitive advantage;
- The pros and cons of popular mobile solutions in the marketplace;
- Whether to build your program with internal or outsourced resources;
- How to measure your pilot program's success;
- How to prepare for future regulations/examinations for mobile banking.

Background

Increasingly, banking institutions are developing new mobile banking initiatives, enabling customers to perform activities such as performing balance checks, account transactions, payments, etc. via a cell phone or PDA.

For M&T Bank, a \$65 billion institution based in Buffalo, N.Y., late 2008 was absolutely the wrong time to get into mobile banking:

- The economy was crazy;
- Joblessness was high;
- Spending was down; budgets tight.

And yet, for many reasons, it also was the perfect time to launch this new initiative:

- Tech-savvy customers are demanding the service;



- Institutions nationwide are rolling out their own mobile products;
- M&T could gain a competitive edge if it launched mobile banking - and stand to lose that edge if it didn't.

Ultimately, M&T took the plunge and is rolling out its mobile banking pilot project this December. By this time next year, the institution hopes to have 10% of its customer base enrolled in mobile banking.

Register for this webinar to learn first-hand from M&T executive Matthew Speare about how he sold, launched and expects to benefit from this pilot project, including:

- How he pitched and sold the pilot to skeptical senior leaders;
- The types of solutions and service-providers he evaluated;
- Unique risks that needed to be assessed and mitigated;
- How to derive lessons learned from other institutions' mistakes;
- The pros and cons of different approaches to mobile banking.

Over the course of this 90-minute webinar, Speare will detail his own institution's case study, from the drawing board to the beta test, and he also will answer real-time questions from session registrants.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=105>

58

How to Use Your Mobile Phone for Free Two-Factor Authentication

Overview

Listen to this webinar to learn more about PhoneFactor and how it simplifies two-factor authentication, including:

- How PhoneFactor compares to other two-factor authentication methods;
- The pros and cons of each type of system;
- Issues to consider when choosing a strong authentication solution.

This Webcast also features case studies about real-world companies that are using PhoneFactor to meet their authentication needs.

Background

- Usernames and passwords alone are no longer secure, with the number of hackers attacking banks jumping 81% versus last year;
- Regulations are increasing for banks - FFIEC and PCI compliance;
- U.S. consumers are concerned about online security losing more than \$7B over last two years;
- Strong authentication is the solution, however traditional solution like tokens, biometrics and card readers are a hassle and expensive;
- PhoneFactor is a phone-based authentication solution that solves all these issues.

One reason many banking institutions are reluctant to adopt two-factor authentication is the hassle and expense of purchasing and managing costly tokens. But with regulatory compliance and increasing security risks, you can't afford not to use strong, two-factor authentication.

Presented By

Jason Sloderbeck, VP of Security & Service Delivery, Positive Networks

Evan Conway, Executive Vice President of Channel Management, Positive Networks

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=58>

159

Legal Considerations About Cloud Computing

Overview

Organizations are leaping to embrace "cloud computing" - accessing virtualized resources via the Internet. But are they jumping too soon without weighing all the legal considerations regarding security and privacy? Register for this webinar to hear a government security leader's expert insights on:

- e-Discovery and records retention challenges;
- Security and privacy risks;
- What it takes to ensure safe, secure cloud computing.

Background

Cloud computing is among the hottest topics in both private and public sectors. Business and technology leaders are enamored with the notion of accessing virtualized resources via the Internet. Cloud's efficiencies promise to save significant money for organizations and consumers.

Yet, despite cloud's attractiveness, few government agencies have implemented any type of cloud computing initiative, mostly because of IT security concerns.

This session tackles those IT security concerns head-on, as David Matthews, Deputy CISO for the City of Seattle, discusses key legal considerations such as:

- eDiscovery - Where is the data? Who owns it? If requested, how does one retrieve, analyze or protect this data?
- Records Retention - Again, who is responsible for the data? How does one enforce retention rules and who is responsible for the disaster recovery plan?
- Pain Points for Organizations - Including accessibility issues, confidentiality concerns, verification of data integrity, risk identification and mitigation, as well as insider threats from cloud provider staff.

Presented By

David Matthews, Deputy Chief Information Security Officer for the City of Seattle

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=159>

165

Innovative Authentication Process Provides the Ultimate Security for Online Banking

Overview

VirtualBank, Money Magazine's "Best Online Bank," recently implemented out-of-band authentication to protect its customers from the myriad attacks targeting online banking today. By enabling phone-based authentication, VirtualBank can offer their customers both unparalleled protection and a superior user experience.

Learn how VirtualBank did it and how phone-based authentication fits with your online banking security objectives. Join this webcast to see:

- Why out-of-band authentication is critical to protecting online banking users from today's threats;
- How VirtualBank selected and implemented an out-of-band authentication solution;
- VirtualBank's goals for their new online banking authentication system, and the positive outcomes.

Background

Securing online banking just gets harder every day. With new threats from malware and man-in-the-middle attacks making traditional authentication methods obsolete and customers suing their banks for failing to protect them, banks are searching for solutions that add the necessary level of security without negatively impacting their customer's online banking experience.

VirtualBank, Money Magazine's "Best Online Bank," takes great pride in offering their customers the very best security available. But equally important to them is the customer's online experience. Their Internet banking model relies on impeccable security and incredible ease-of-use.

That's why they have partnered with PhoneFactor, who was recently named to Bank Technology News' FutureNow List, to offer out-of-band, two-factor protection that truly differentiates VirtualBank from their competitors.

Join Frank Barbato, VirtualBank CIO, and Steve Dispensa, PhoneFactor CTO, to learn more about this fascinating case study in the next generation of online banking security.



Presented By

Steve Dispensa, CTO & Co-Founder, PhoneFactor

Frank Barbato, Chief Information Officer, VirtualBank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=165>

217

Is Your Device Identification Ready for New FFIEC Guidance?

Overview

Since the FFIEC guidance in 2005 on "Authentication in an Internet Banking Environment," cybercriminals have evolved significantly, leading the FFIEC to release new guidance for protecting your business and your customers from fraud. Learn about smart device identification technologies banks will need to adopt to comply with new FFIEC guidance and meet today's challenges of widespread identity and password theft, botnets, trojans, coupled with new risks introduced by smartphones and the demise of cookies as an authentication method.

This session will address:

- What smart identification entails;
- The key limitations of simple identification methods;
- Why upgrades to current customer device identification are critical;
- How to initiate transaction authentication and monitoring.

Background

The recent release of FFIEC guidance on authentication heightens focus on the new wave of technologies required to keep up with increasingly sophisticated threats to online banking. However, even before the guidance was finalized, forward-thinking bankers were preparing themselves with new technologies for smart device identification.

The FFIEC's 2005 guidance on "Authentication in an Internet Banking Environment" ushered in a first generation of device identification technologies. Since that time, cybercriminals have evolved to such a degree that they can decommission nuclear reactors, take down governments and steal billions in online consumer transactions. Yet many online bank accounts are still protected by first generation technologies consisting of little more than a password, a cookie and a simple hash of browser and IP attributes.

Customer device identification remains the most cost effective first perimeter of defense for customer authentication. In addition, banks will need to adopt cookie-less device identification technologies (smart device identification) as part of a multi-factor strategy to protect new account verification, login authentication and transaction authorization. In combination, these solutions will safeguard customer privacy, trust and convenience.



In this webinar, you'll learn about the smart device identification technologies banks will need to adopt to comply with new FFIEC guidance, specifically, how they can address today's challenges of widespread identity and password theft, botnets and trojans, as well as new risks introduced by smartphones and the demise of cookies as an authentication method.

All attendees will receive a complimentary copy of ThreatMetrix' new whitepaper, "Is Your Device Identification Ready for the FFIEC: Smart Device Identification for Online Banking."

Presented By

Alisdair Faulkner, Chief Products Officer, ThreatMetrix

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=217>

30

Malware, Crimeware, and Phishing - An In Depth Look at Threats, Defenses

Overview

- Describe malware, crimeware intrusions and how they relate to phishing;
- Overview of current attacks and help to anticipate likely trends;
- Describe different ways clients are attacked, understanding of proactive defenses;
- Describe traditional and current malware, and different types of phishing;
- The human factor as increasing factor in phishing solutions.

Background

The evolution of malware and crimeware has produced more insidious and harmful intrusions to networks and systems. This webinar will show how these types of intrusions relate to phishing and will help put current attacks into perspective and help organizations anticipate likely trends.

The webinar will also describe the different ways by which clients may be attacked, and their machines may become infected. While many of these threats aren't yet seen in the wild, a thorough understanding of the threats allows for proactive defenses to be deployed against them when they do occur.

The presentation will cover traditional and current malware, the relevance of configuration vulnerabilities, the relevance of deceit, social malware and social phishing, how deceit works in phishing and why mutual authentication techniques such as SiteKey may not be as secure as they may seem.

It will continue and cover spear phishing, and the presentation will give examples of the different types of spear phishing methods.

A very important aspect of this problem is the human factor, as an increasing number of vulnerabilities arise due to deceit, configuration errors and neglect. While many security solutions and user interfaces may appear to be equally secure - in a pure technical sense - the human factor creates large security differences between approaches. The presentation will explain why, and describe what to do and not to do, both in terms of technical and design aspects, and in terms of consumer education.



Attendees will learn what organizations should do, and what the best proactive approaches are to crimeware and phishing. The different kinds of services that are available to react to attacks will be covered. Attendees will learn how to evaluate their organization's vulnerabilities to existing attacks and potential future threats, and equally will also learn what should not be done.

Presented By

Markus Jakobsson, Associate Professor, Indiana University's School of Informatics

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=30>

222

Malware: Fight Back Using Layered Security

Overview

The onslaught of ACH/wire fraud incidents confirms what the researchers have long said: We're in a new wave of malicious code. This new wave is run by organized crime, and it's focused on one objective: stealing personally identifiable information and ultimately money through fraudulent ACH and wire payments. So, how can organizations adopt a layered security approach to protecting themselves and their customers - and at the same time comply with FFIEC's new online authentication guidance?

Join a panel of industry experts for a frank discussion about:

- Beyond Zeus: the current malware landscape and the threats it poses;
- Tools and technologies to achieve layered security;
- How to educate consumers and corporate customers without scaring them away.

Background

In the summer of 2009, criminals from the Ukraine stole \$415,000 from the government payroll account of Bullitt County, Kentucky. The criminals used a version of the "Zeus" keystroke logging Trojan to steal the online credentials, log-in to the Bullitt County bank account and steal payroll funds.

This incident is considered to be the first of the recent epidemic of ACH/wire fraud incidents that have led to corporate account takeover. Since that time, countless small-to-midsized businesses, government agencies and even a Catholic Church diocese have been victimized by organized crime and ever-evolving strains of malicious software.

Financial institutions and regulators continue to fight back against fraudsters. Banking institutions of all sizes have stepped up their fraud detection and prevention efforts, as well as their customer awareness campaigns.

U.S. banking regulators, meanwhile, have issued alerts, education and even a new FFIEC online authentication guidance that calls, in part, for institutions to adopt new, layered security controls and to improve their customer awareness efforts.

In this session, two industry experts shares insights on:

- The evolution of malware;
- What is in FFIEC's new guidance;



- The definition of layered security;
- Importance of cross-channel fraud protection;
- Other business benefits of improved detection.

Following short presentations on malware and layered security, the presenters will engage in a panel discussion tackling today's top questions on how to protect banks and their customers.

Presented By

George Tubin, Banking and Security Analyst

Shirley Inscoc, Director - Financial Services Solutions, Memento

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=222>

170

Managing Shared Passwords for Super-User Accounts

Overview

Security best practices and regulations such as FISMA require that access to sensitive data and servers be granted only to those who need it, and that those individuals are granted only the privileges they need. This “least-privilege” model is challenging to implement, particularly in Linux and UNIX environments, where administrators commonly share passwords to root or other superuser accounts. View this webinar now to learn:

- How to tie UNIX and Linux entitlements to individuals by leveraging Microsoft Active Directory;
- Why tools such as sudo are not sufficient in delivering the world-class security IT managers need;
- What the baseline requirements are for implementing a least-privilege security model based on user roles.

Background

Security best practices and regulations such as FISMA share some common requirements: that access to sensitive data and servers be granted only to those whose job function requires it, and that those individuals are granted only the privileges they need to perform their duties. This “least-privilege” security model has obvious merits in theory, but in practice it can be challenging to implement, particularly in Linux and UNIX environments, where it is still all too common for administrators to share passwords to root or other superuser accounts.

How, for example, do you give backup administrators the superuser privilege to copy a database and move it to another volume without giving them access to the database itself? While sudo and other tools provide some help, they can be cumbersome to manage and implement and become unworkable in complex environments with hundreds of heterogeneous servers and multiple administrators with widely varying job roles and authority.

This webinar will:

- Examine the real-world challenges around tying entitlements to individuals instead of to root or generic accounts;
- Describe the baseline requirements for implementing a least-privilege security model based on user roles;
- Explain why existing tools such as sudo fall short in delivering enterprise-class security and manageability;



- Show you the value of leveraging Active Directory’s centrally managed identities and its rich group- and role-based management capabilities to provide access control and privilege management services to Linux and UNIX systems;
- Demonstrate how the Centrify Suite provides an integrated, consistent and cost-effective solution for least-privilege security management across some 200 of the most widely used versions of Linux and UNIX.

Presented By

Dr. Eugene Schultz, CISM, CISSP, Chief Technology Officer at Emagined Security

David McNeely, Director of Product Management at Centrify Corporation

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=170>

189

Meeting Federal Compliance to Secure Windows Desktops

Overview

The federal government mandates that agencies secure their computer desktops, but how can you ensure your lockdown policies are both effective and flexible? Register for this session to learn:

- Best practice tips to ensure your desktop security policies meet federal mandates;
- How to increase user performance on Windows desktops while reducing elevated privileges.

Background

Are you seeking flexible lockdown tips for securing your desktops? Not only are secure desktops a federal mandate for government agencies, but according to Gartner, organizations that properly secure their desktops can save \$1,237 per desktop.

Learn best practices to meet government compliance standards and effectively secure Windows desktops. Derek Melber, author, consultant, and trainer for many Fortune 500 companies on Active Directory, security and group policy, will lead this session focused solely on government agencies and their unique concerns.

In this session, you can learn:

- The benefits of removing administrator rights from end users;
- The combination of technologies needed for effective implementation of this level of security;
- How to best remove the local administrator account, while maintaining the users’ access to all applications.

Also, discover how PowerBroker Desktops enables you to achieve government compliance by configuring all users as standard users and enables your users to get more done.

Presented By

Derek Melber, MCSE, MVP, Author of The Group Policy Resources Kit by Microsoft

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=189>

185

Protecting CUI: Federal Best Practices for Email Security, Archiving and Data Loss Prevention

Overview

E-mail continues to be one of the primary risk vectors of exposure of Controlled Unclassified Information and other sensitive data in federal organizations, but most have yet to deploy technology to help prevent costly breaches.

Register for this webinar to learn about:

- The importance of establishing clear and concise messaging policies in today’s government enterprise;
- Understanding the results of the recent Task Force report and upcoming Presidential Directive on Controlled Unclassified Information (CUI);
- A summary of the requirements to establish effective data loss prevention (DLP) controls;
- NARA’s definitions of, and correct retention policies for, Transitory and Federal Record electronic communications.

Background

The “business” of the U.S. Federal government presents unique challenges for busy IT administrators and information security professionals who support and secure complex IT infrastructures - while also meeting the numerous requirements of diverse user communities including war-fighters, tele-workers and office workers. As in most industries, e-mail is the most important communications channel, playing a primary role in information exchange, planning and budgeting, while also being a significant source of risks.

Join security expert Jeff Lake, VP of Federal Operations at Proofpoint, and learn how coming changes to requirements for handling CUI will affect federal agencies, review NARA’s guidance on e-discovery for electronic mail archives, and understand how deploying an effective DLP solution can help you better secure private data and your overall e-mail infrastructure.

Presented By

Jeff Lake, VP - Federal Operations, Proofpoint

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=185>

285

Mobile Banking: Emerging Threats, Vulnerabilities and Counter-Measures

Overview

The banking industry has never seen such a fundamental change as mobile banking. Globally, millions of consumers are already using a wide array of mobile devices to conduct banking - and millions more are expected to go mobile in the coming months.

But with that growth come a whole new set of threats: mobile malware, third-party apps, unsecured Wi-Fi networks, risky consumer behavior. And it does not matter whether an institution uses a proprietary or third-party mobile banking application - the bank owns the risks.

So, how do banking/security leaders mitigate their risks and protect their customers from evolving mobile threats? Join Tom Wills, renowned expert in global mobile trends, for insights into how global banking institutions can navigate the mobile threat landscape, including:

- Emerging external threats to mobile banking and payments;
- How to influence the riskiest wildcard - user behavior;
- Anti-fraud solutions and strategies to thwart mobile attacks and maintain customer trust.

This session is for banking institutions of all sizes, from any global region.

Background

According to Javelin Strategy & Research, mobile banking usage grew 63 percent in 2011, and the adoption rate is expected to swell globally over the next 18 months.

But how prepared are banking institutions to handle this growth - and the corresponding growth of mobile threats?

The mobile threat landscape is ever-evolving, and institutions and consumers alike are wary of the risks. Among today's growing concerns:

- Mobile Malware - Trojans, viruses and rootkits migrating from traditional online banking and designed specifically for the mobile marketplace. Researchers see an increase in mobile malware development - in pace with market growth.
- Third-Party Apps - Consumers love their smart phone and tablet applications, but often these apps come from third



- parties with questionable security practices. Or worse, the apps are created by fraudsters and loaded with malware.
- Unsecured Wi-Fi - The unsecured wireless network is a toll-free highway for fraudsters to gain access to mobile devices, either to seize control of or gain access to account information.
- User Behavior - Consumers are prone to download third-party apps, use unsecured wireless networks, open and click links in SMS text messages and e-mails, and lose their mobile devices. Mobile-use behavior is creating a suite of vulnerabilities, and fraudsters are eager to take advantage.

While mobile banking and payments are still relatively young in the U.S., adoption is more mature in international markets such as Asia, where presenter Tom Wills currently resides. In this session, Wills walks through the attack methods cyber-fraudsters are pursuing and offers steps banking institutions can take to reduce their risks. During this presentation, Wills offers insights about:

- The latest mobile malware and the technology solutions aimed at stopping it;
- Why secure application development matters, and how institutions can provision their risks;
- How consumers' risky behavior makes them prey for social engineers;
- Why consumer privacy is a growing concern, and how to address it;
- How institutions can leverage mobile to improve customer trust and loyalty.

Presented By

Tom Wills, Senior Risk and Fraud Analyst, Javelin Strategy & Research

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=285>

290

Mobile Banking: How to Balance Opportunities and Threats

Overview

Whether by smart phone, tablet or laptop, mobile banking is where customers and their institutions are headed - and so are the fraudsters.

As banking institutions globally roll out more services through the mobile channel, security leaders are challenged to stay a step ahead of the evolving risks. But what are today's top threats, and what are the emerging security components institutions must put in place to take advantage of new mobile opportunities?

Register for this session to learn first-hand from a leading banking/security practitioner, as well as the CTO of a major security solutions vendor:

- Top security considerations when rolling out a mobile strategy;
- The truth about mobile malware and other fraud threats;
- How to influence end-user behavior;
- Emerging trends in mobile payments, authentication and regulation.

Background

Mobile banking may be the single biggest innovation the global banking industry has seen. From smart phones to tablets and laptops, banking customers are pushing their institutions to roll out more mobile services.

But these same customers also represent one of the biggest threats to mobile banking. Having no control over what customers do on their mobile device - from the third-party apps they download to potentially dangerous links in e-mails and SMS text messages they click on - security leaders must find a delicate balance between growing their mobile channel while managing fraud risk.

And user behavior is only one threat vector. Mobile banking is also threatened by the proliferation of third-party apps, unsecured wireless networks and the evolution of mobile malware.

At the same time, the mobile landscape is evolving with new opportunities in mobile payments (including P2P) and authentication (such as biometrics).

How does the banking/security leader balance the mobile banking demand, threats and future business opportunities?



In this webinar, Matthew Speare of M&T Bank - a pioneer in mobile banking - will discuss how he achieves this delicate balance, offering insights on:

- What to consider when rolling out a mobile strategy;
- How to understand - and respond to - user behavior;
- Future trends, including the question: Will U.S. regulators issue mobile guidance?

Joining Matt will be Sam Curry, CTO of RSA. He will offer bleeding-edge insight on:

- The evolving payments landscape;
- The facts on mobile malware such as Citadel;
- Emerging mobile authentication options, including biometrics.

Presented By

Matthew Speare, SVP - Information Technology, M&T Bank

Sam Curry, CTO, RSA

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=290>

279

Mobile Banking: Trends, Threats and Fraud Prevention Techniques

Overview

As financial institutions expand their mobile banking services, fraudsters certainly will be close behind. This webinar will cover the expanding use of mobile banking and the fraud threats that are lurking, including:

- The explosive growth of smartphone ownership and the resulting demand for improved mobile services;
- Trends in mobile banking services, and the inherent risks associated with smartphone usage;
- The threats that lurk as fraudsters escalate attacks against the mobile channel;
- Fraud detection and prevention techniques based on each user's unique mobile banking behavior.



Tiffany Riley, VP - Marketing, Guardian Analytics

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=279>

Background

Over half of U.S. adults already have smartphones, and Forrester Research predicts that by 2015 one in five U.S. adults will be using mobile banking. If a financial institution doesn't offer the desired mobile services, it runs the risk of losing clients. But with such growth, we all know that the fraudsters won't be far behind. So, how will account holders be using their mobile devices, how does that increase fraud threats and how do financial institutions mitigate the resulting risk?

This webinar will answer these and many more questions about what will surely be the year's hot financial services topic. Learn about:

- The state of smartphone ownership and mobile banking adoption and functionality;
- Usage patterns and behaviors that make smartphones particularly attractive to cyber criminals;
- Fraud threats that have already been spotted in the wild and how they take advantage of unique smartphone characteristics;
- Behavior-based techniques that some financial institutions are already using to detect mobile banking fraud attacks without disrupting legitimate activity;
- Anomaly detection solutions that prevent fraud and also conform to the FFIEC Guidance.

Presented By

Chris Silveira, Manager of Fraud Intelligence, Guardian Analytics

264

Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices

Overview

When it comes to employee-owned mobile devices, many organizations want to run away from the security risks of the bring-your-own-device-to-work trend. Intel chose to run toward them.

In an exclusive case study, Intel CISO Malcolm Harkins details the security challenges and business opportunities of BYOD. And he explains how the move forced the company to re-think enterprise security to accommodate employees' smart phones, tablets and other mobile devices. Learn how to:

- Involve employees in developing an effective mobile policy;
- Create a layered security approach to manage the risks;
- Build the BYOD business case and calculate ROI.

Background

At Intel, the BYOD trend started in 2009, when employees began using their own smart phones, tablets and mobile storage devices on the job. Rather than reject the trend, as many organizations initially attempted, Intel's senior leaders were quick to embrace it as a means to cut costs and improve productivity.

Since Jan. 2010, the number of employee-owned mobile devices on the job has tripled from 10,000 to 30,000, and by 2014 Intel CISO Malcolm Harkins expects that 70 percent of Intel's 80,000 employees will be using their own devices for at least part of their job.

The payback so far:

- Better Productivity - Employees who use their own devices respond faster to communication and over a greater percentage of the day;
- Improved Security - Mobility improves Intel's time to respond, contain and recover from incidents;
- Greater Control - Because personally-owned devices are encouraged, Intel now has markedly fewer unauthorized devices on its network.

And while there are heightened risks that come with having employees carry sensitive data on their personal devices, Harkins says organizations must tackle these risks head-on. "Doing nothing is not an option" when it comes to BYOD, he says. "Employees will work around and unknowingly expose the enterprise."



In this presentation, Harkins tells how Intel came to embrace and benefit from the BYOD trend, including insights on:

- Bottom-up Approach - Intel from the outset involved employees in mobile policy creation, making the process open to input and constructive criticism. The result: an effective Employee Service Agreement for personally-owned devices.
- Risk Management - There is no 'one size fits all' so Intel developed a five-tier risk management model that provides enhanced security capabilities depending on the employee's access to sensitive data such as line of business applications, filtered e-mail and the corporate intranet.
- Beyond Technology - Intel quickly discovered that BYOD impacts more than the IT and security groups. HR and legal play huge roles in helping to define policy, enforce compliance and ensure adequate attention is paid to details regarding privacy, appropriate use and software licensing.

Presented By

Malcolm Harkins, CISO, Intel

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=264>

256

Mobile Technology: How to Mitigate the Risks

Overview

Smart phones, laptops, tablet PCs, optical discs and USB devices. There are many new mobile devices and emerging technologies to help today's professionals do their jobs in any location - and increasingly private business is being conducted on personal digital and storage devices. Yet, these technologies create new risks to the security of information systems and privacy of protected data.

How do you ensure that critical information remains secure on personal mobile devices - even when the devices are lost or stolen?

Join this expert panel for insights on:

- Proper inventory management of mobile devices - and remember, mobile means more than just smart phones;
- Creating and enforcing mobile security policies;
- Strategies for encryption, data loss prevention and other elements of layered security to protect devices and systems;
- Unique mobile challenges for regulated industries such as financial services, government and healthcare.

Background

In the fall of 2011, the U.S. Department of Veterans Affairs launched a "go-slow" approach to enabling physicians and others to use Apple iPhones and iPads for limited purposes. In this pilot program, a limited number of VA staff members will use the smart phones and tablets primarily for encrypted e-mail and as viewers to access a VA clinical information system, but not to store patient information.

"We're being careful to not increase our breach exposure as we roll these devices out," said Roger Baker, the VA's CIO. The VA's experience mirrors what is happening to public and private sector organizations in every global marketplace. They are all trying to get a secure handle on the mobile revolution, which is driven by consumer-friendly technologies and threatened by a range of security risks. Employees and customers alike want to conduct business via mobile technologies, including optical discs and USB devices, so information security leaders are forced to grapple with questions such as:

Who Owns the Devices? Do organizations issue their own devices in the workplace, or do they allow their employees to bring their own devices to work - if they follow prescribed policies?



What Are the Elements of a Sound Mobile Policy? Organizations need minimum security standards, and they need to articulate clear uses, data management principles and the fundamentals of mobile security awareness.

What are the Risks? Each organization must assess the relative risks of mobile against other electronic channels - for employees and customers alike. But there are unique mobile security risks, including controls in mobile applications, the growing threat of mobile malware and the ever-present prospect of device loss or theft.

In this session, mobile security experts will discuss these topics and more, sharing insights on how today's leading-edge organizations are enabling safe, secure mobile computing inside and outside the workplace.

Presented By

Paula Skokowski, VP - Products & Marketing, Accellion

Terrell Herzig, CISO, UAB Medicine

Robert Hamilton, Senior Product Marketing Manager - Data Loss Prevention, Symantec

Scott Ashdown, Director - Products and Solutions, Imation

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=256>

271

No One's Immune to Being Hacked: Strategies for Staying Out of the Headlines

Overview

Join Q1 Labs' CSO Chris Poulin to hear how security intelligence - delivered via next-generation SIEM and log management technology - provides the visibility needed to detect anomalies inside and outside your organization. With risk coming from all directions, including an increasing number of insider theft cases, targeted hacktivism and the evolving complexity of external vulnerabilities, the pressure to protect IT resources and gain better network and application visibility is only getting more intense.

Attend and learn:

- Why context and situational awareness are necessary for advanced threat detection and behavioral analysis;
- How enterprises are using security intelligence to combat insider threats and protect critical customer information;
- How to detect threats (zero-day) that many security solutions miss.

Background

The security model of 10-12 years ago is no longer adequate to meet contemporary challenges, as "Internet hooliganism" has given way to organized criminal activity. It's outmoded and does not scale in the face of today's threats and IT environment. Perimeter-based security has evolved to a highly distributed model, as employees, partners and customers conduct business remotely across the Internet and criminals exploit new attack vectors and misplace user trust.

Government and industry regulatory mandates emerged and/or were given "teeth" through stronger penalties and more diligent enforcement.

The security industry has responded with new and enhanced products to meet each threat. All of these tools add value to overall enterprise security, but they are, in effect, islands of security technology. They're not conducive to a risk-based enterprise-wide security program, and the overall effort tends to be fragmented.

In many cases, organizations have to deal with incomplete data because a given security tool may not recognize a threat or risk



for what it is without correlation from other data sources. On the other hand, even when data is collected from disparate sources, analysts are challenged by the sheer volume, making it extremely difficult to distill actionable information.

Security intelligence addresses these problems across the spectrum of the security lifecycle, centralizing data from disparate silos, normalizing it and running automated analysis. This enables organizations to prioritize risk and cost-effectively deploy security resources for detection, prevention, response and remediation.

Presented By

Chris Poulin, CSO, Q1 Labs, an IBM company

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=271>

190

Power Systems: How to Prevent Unauthorized Transactions

Overview

Your Guide to Compliance Assessments & Network Security

Many organizations don't prevent unauthorized users from modifying or downloading application data. In addition, modern interfaces, like FTP, allow users access to data even when menu and command restrictions are in place.

How do you ensure the security and integrity of your Power Systems and gauge your true network security status?

Attend this webinar to:

- Receive data on detailed audit trends from over 1,500 IBM servers;
- Learn best practices for auditing network access (including FTP), user profiles and events;
- Determine your organization's true network security status.

SPECIAL NOTE: All attendees will be eligible to use a compliance assessment tool after the webinar.

Background

For the past seven years, PowerTech has compiled audit trends from over 1,500 servers into the annual State of IBM i Security study. Each year, the study identifies many of the same vulnerabilities, suggesting that IBM i shops aren't where they should be in terms of security and auditing.

Application programs often rely on outdated security models that can leave data vulnerable. Many environments don't prevent unauthorized users from modifying or downloading application data. And, modern interfaces, like FTP, allow users to access data even when menu and command restrictions are in place.

Join us for this webinar to learn how to get inside the security configuration of your Power Systems server (System i, iSeries, AS/400) using PowerTech's Compliance Assessment.

You'll learn about auditing these critical configuration areas:

- System values;
- Network access, including FTP and ODBC;
- User profiles;
- Special authorities;
- Event auditing.



Attendees are eligible to use the Compliance Assessment for FREE on their own system.

Presented By

Robin Tatam, Director - Security Technologies, PowerTech Group

Jill Martin, Product Support Manager, PowerTech Group

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=190>

166

Practical User Authentication Strategies for Government Agencies

Overview

Government agencies at all levels (federal, state and local) face unprecedented IT security threats from an increasingly organized and well-funded community of cybercriminals. Add stringent regulatory requirements to this and government agencies are faced with a daunting task of managing risk and adhering to compliance standards.

Register for this webinar to:

- Gain a clear understanding of today's threat landscape;
- Learn how to transfer private business best practices to the public sector with rapid compliance and a low total cost of ownership;
- Compare the most popular two-factor solutions, including tokenless phone-based authentication.

Background

With government agencies entrusted to protect citizens' personal, financial and health records, as well as data vital to national security, the risks are incredibly high.

And with sophisticated cyber criminals constantly probing for access to this information, the threats are constant and real.

Add to this threat landscape the realities of regulatory requirements, which mandate that access to this information be secured with multi-factor authentication, despite the burdensome costs and time required to implement these solutions.

Clearly, government agencies are challenged.

In this session, learn how public and private sector organizations are adopting phone-based, two-factor authentication to mitigate risk for a fraction of the cost of security tokens and smart cards.

With a discussion led by industry thought-leaders, you will learn how to:

- Assess today's top risks;
- Weigh pros and cons of two-factor solutions;
- Transfer private business best practices to the public sector with rapid compliance and a low total cost of ownership.



Presented By

Sarah Fender, VP - Marketing & Product Management, PhoneFactor

Steve Dispensa, CTO & Co-Founder, PhoneFactor

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=166>

223

Preventing Malware: Tips to Staying FFIEC Compliant

Overview

With the recent release of the new online authentication guidance, the Federal Financial Institutions Examination Council (FFIEC) directs banking institutions to provide a more air-tight defense against risks to their networks and customers.

The barrage of recent high-profile data breaches confirms what experts have been saying all along: Fraudsters are generating more sophisticated and persistent malware to steal your institution's confidential data for profit.

The new approach to customer data security entails a layered security strategy for the endpoints, addressing increasingly sophisticated attacks. Layered security consists of multiple protection solutions working together to achieve complete endpoint protection.

This webinar will explore how to:

- Comply with pending FFIEC mandates;
- Stay up-to-date with the latest malware and breach trends;
- Secure employee workstations and other data points;
- Accelerate IT efficiency and support.

Background

With the release of the new online authentication guidance, the Federal Financial Institutions Examination Council (FFIEC) is mandating that financial institutions provide customers with recommendations on alternative risk control strategies to mitigate their own risk.

Increasingly sophisticated malware attacks are on the rise, targeting confidential customer information. Customers expect credit unions to protect their personal and financial information at all costs. The new approach to customer data security entails a layered security strategy for the endpoints. Layered security consists of multiple protection solutions working together to achieve complete endpoint protection. Financial institutions implementing a layered security solution can achieve a competitive advantage over the competition by providing their customers peace of mind.

Early adopters will build a reputation synonymous with security and foster stronger customer relationships that translate into higher customer retention. Join Certified Information Systems Security Professional Byron Hynes, and Carlos Santamaria,



Product Manager for Faronics, as they share the latest research and trends in customer data breaches. They will explore examples of emerging threats, and divulge the best practices for ensuring complete security in your financial institution, as well as:

- Latest data breaches and their implications;
- Roundup of malware threats;
- The evolution of malware in 2011;
- Beyond transactional security: protecting your endpoints where data resides;
- Tools and technologies to achieve layered security.

Presented By

Carlos Santamaria, Product Manager, Faronics

Byron Hynes, Infrastructure & Security Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=223>

119

Preventing Unauthorized Access To Your Institution's Data

Overview

Data loss. Information leak. Content monitoring and filtering. Data Loss Prevention (DLP) has been called many things, but what it comes down to for financial institutions is this: Security controls to detect and prevent the unauthorized transmission of information from your institution to outsiders.

Register for this webinar to learn from industry thought-leaders:

- Today's biggest DLP threats to the financial services industry;
- The threats' potential impact on your institution and consumer confidence;
- How DLP solutions should fit into your security strategy.

It could be from a hack - like the recent Heartland Payment Systems breach - or it could be from a lost PC or a malicious insider. Whatever the cause of data loss, DLP is about the strategies and products you can deploy to minimize your institution's risk.

Background

No one wants to be where Heartland Payment Systems found itself in January 2009: explaining how hackers managed to penetrate their systems sometime in 2008 and gain access to an undetermined number of consumer names and credit card numbers.

To prevent hacks and minimize the damage that can be done by malicious insiders or loss/theft of information-critical devices, many financial institutions now are rallying around the strategies and solutions of Data Loss Prevention.

DLP goes by different names: data leak, information leak, content monitoring and filtering. Whatever the term, the concept still boils down to deploying security controls to detect and prevent the unauthorized transmission of sensitive information to outsiders.

In the past, DLP efforts have focused mainly on potential losses to hackers - i.e. the criminals who breached not just the Heartland systems, but also TJX and Hannaford Brothers prior to the latest high-profile hack.

And it's true: rapidly evolving malware and fraudulent attacks are a constant challenge to financial institutions and their customers.



But other recent cases such as the Bank of New York Mellon, Countrywide and France's Societe Generale have shown us that inattention and incomplete monitoring can lead to significant data loss through benign accident or through the activities of malicious insiders.

Add to those threats the impacts of organization change, consolidation and acquisitions to an institution's data security as a result of the current economic upheaval, and you gain a sense of the scope of the DLP challenge.

In this webinar, we tackle the topic of DLP by:

- Defining DLP in today's context;
- Showing where data breaches are increasing, and why financial institutions are especially vulnerable to the insider threat;
- Spelling out specific strategies aimed at helping institutions prevent, detect and, if necessary, resolve costly data breaches;
- How to protect your critical information assets from external and internal threats via:
 - » Cloud/client security model;
 - » Securing e-mail;
 - » Data leak prevention.

Presented By

Tom Wills, Senior Risk and Fraud Analyst, Javelin Strategy & Research

Victor Lee, Director, Data Protection Marketing, Trend Micro, Inc.

Tom Field, Editorial Director, Information Security Media Group

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=119>

227

Protect Data in the Cloud: What You Don't Know About the Patriot Act

Overview

As banking institutions seek tremendous cost savings from cloud infrastructure and services, two key factors must be considered: The Patriot Act, which has strict stipulations regarding access to data and where it is stored, and the protection of data - even from third-party service providers.

This webinar explores what these security topics mean to financial institutions:

- The impact from the newly-extended Patriot Act re: sensitive data in the cloud;
- Risks to consumer information stored in the cloud from third parties;
- How to address data sovereignty issues with cloud computing infrastructure.

Background

The virtual nature of cloud computing opens up cost savings that are difficult to ignore, yet two orthogonal but perhaps complimentary issues make having a cohesive data security strategy dramatically more complex.

The first is the recently extended U.S. Patriot Act which provides for sweeping abilities for law enforcement to access data stored in U.S. data centers - regardless of geography. Often in conflict with local, e.g. European Union Data Protection legislation, there are complex issues ahead concerning the protection of data as it crosses international boundaries.

The second issue is that of protecting the data stored in cloud infrastructure - with its virtual nature - it's not possible to know necessarily where a piece of data is being stored in the cloud - nor is it always clear who exactly at the third-party service provider has access to that data.

The question becomes, is it possible to have a strategy where data from international jurisdictions can be stored in the cloud while retaining clear lines of separation? Similarly, is it possible for enterprises to control their data stored in a third-party cloud without knowing exactly where it is?



It turns out that some new advances in key management could help resolve both these scenarios. By using some common examples, e.g. "How to protect sensitive emails in Microsoft BPOS/Office 365 Environments" and "How to enforce sovereignty of data stored in a cloud based infrastructure," we'll help uncover:

- The specific threats to data in the cloud;
- How to segregate data using encryption keys;
- How to protect and control data stored in the cloud.

Presented By

Wasim Ahmad, VP - Marketing, Voltage Security

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=227>

272

Protect IBM i Data from FTP, ODBC and Remote Command

Overview

The IBM i server is one of the most secure and reliable business computers available today. But, no system is completely safe from the people who know how to access it. Organizations need to understand how to protect their critical systems and data from unauthorized access through common services such as ODBC, JDBC, FTP and remote command.

In this session, Robin Tatam, Director of Security Technologies for PowerTech, covers:

- An overview of IBM i security;
- Protecting your system in today's wide-open environment;
- Tools to help you secure your system.

Background

Each year, PowerTech releases its "State of IBM i Security" study, documenting how well organizations manage their security. And, each year, the study shows that the vast majority of organizations still rely on menu security to protect their data. Unfortunately, today's users have access to interfaces (such as FTP, ODBC, JDBC, and remote command) that completely bypass these controls and make it easy to view, update and delete data in the database. If you need to comply with government or industry regulations, or if you simply want to ensure the integrity of your application data, understanding these interfaces is critical.

In this webinar, Robin Tatam, Director of Security Technologies for PowerTech, discusses:

- What you need to know about IBM i security;
- How to close the "back doors" not covered by traditional menu security schemes;
- How to implement policies that restrict access to only those users who need it.

Tatam also demonstrates PowerTech's Network Security, the exit point monitoring and access control software that can help you secure your system.

Presented By

Robin Tatam, Director - Security Technologies, PowerTech Group

Paul Culin, Senior Security Associate, PowerTech Group



View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=272>

220

Protecting Government Agency Assets Through Improved Software Security

Overview

Government agencies continue to see growing cybersecurity challenges. Software Security Assurance (SSA) is a new approach entities are taking to improve security measures in their organizations. A critical component of SSA are threat assessments, which involve accurately identifying and characterizing potential attacks upon an organization's software in order to better understand the risks and facilitate risk management. By starting with simple threat models and building to more detailed methods of threat analysis, an organization improves over time.

Attend this session to:

- Learn about the current threats and attack vectors;
- Understand the basics of threat modeling software applications;
- Learn best practices for securing your software.

Background

To face the growing cybersecurity challenges, government entities are turning to a new approach to application security: Software Security Assurance (SSA). SSA is a comprehensive discipline that provides a systematic way to secure your software at every phase in the application life cycle. As organizations look to implement software security assurance, open frameworks are used to help formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. One such framework is called The Software Assurance Maturity Model (SAMM).

A critical component of SAMM, threat assessment, involves accurately identifying and characterizing potential attacks upon an organization's software in order to better understand the risks and facilitate risk management. By starting with simple threat models and building to more detailed methods of threat analysis, an organization improves over time.

Fortify invites you to view a webinar on Software Threat Modeling. This webinar will provide you with the knowledge to better understand how to conduct threat modeling within your agency. Join us and learn:

- The basics of threat modeling software applications;
- The meaning of threats, attack vectors, and trust zones;



- Secure design concepts and ambiguity analysis;
- Best practices for securing software architecture.

Also, attend this webinar and receive a complimentary copy of "Software Assurance Maturity - A Guide to Building Security into Software Development."

Presented By

Shakeel Tufail, Federal Practice Manager, HP - Fortify Security Solutions

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=220>

198

Register Now: Visit www.bankinfosecurity.com or Call (800) 944-0401

229

Red Hat Enterprise Linux 6 Common Criteria

Overview

Red Hat takes the needs of government seriously, especially when it comes to security. That's why Red Hat Enterprise Linux 5 and 6 are now in evaluation for the 14th (and 15th) time under the internationally recognized Common Criteria process.

In this session, we'll discuss:

- What's new with the RHEL Common Criteria configuration;
- Easy, repeatable Common Criteria-certified builds;
- Certified, secure multi-tenant virtualization with the new sVirt system.

Background

Red Hat is committed to providing secure and stable software that can be easily used in security-sensitive environments. We work closely with U.S. government customers and security specialists to ensure that Red Hat products are certified for government use, and are easily accredited by the appropriate authorities.

Red Hat Enterprise Linux, for instance, is the most certified operating system available today. Through its history, Red Hat Enterprise Linux has passed the Common Criteria process 13 times on four different hardware platforms. Red Hat Enterprise Linux 5 has even received Common Criteria certification at Enterprise Assurance Level 4 (EAL 4+) under the Controlled Access Protection Profile (CAPP), Label Security Protection Profile (LSPP) and the Role-Based Access Control Protection Profile (RBACPP), providing a level of security and a feature set that was previously unheard-of from a mainstream operating system.

Our JBoss Enterprise Middleware solutions include support for common middleware security standards, and both the JBoss Enterprise Application Platform and MetaMatrix Data Services Platform are Common Criteria certified at EAL 2+.

Presented By

Gunnar Hellekson, Chief Technology Strategist, Red Hat

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=229>

Register Now: Visit www.bankinfosecurity.com or Call (800) 944-0401

193

Social Networking Compliance for FINRA Regulated Organizations

Overview

Now you can maintain FINRA compliance across Facebook, LinkedIn, Twitter and over 1000 social networks. The secrets are shared during this exclusive webinar.

Control and compliance are key to social media survival in today's regulated industries. So you need a solution for true compliance.

This exclusive webinar will explore the requirements of FINRA with regard to social networking - and how Socialite, a new social media compliance solution from FaceTime Communications, helps you meet them.

- Content and activity archiving;
- Content moderation controls;
- Granular control of features and content;
- Display context of messages posted;
- On-premise, SaaS, or hybrid deployment options.

Enable social media without compromising regulatory compliance. The first step is Socialite - the new solution for social networking management in the enterprise.

Background

View this specifically designed webinar for FINRA-regulated organizations. You'll get details on how to securely use social networks, while maintaining FINRA compliance and IT best practices.

- Apply granular controls to Facebook, LinkedIn and Twitter, based on the employee's role in your company;
- Use social networking to engage prospects and build relationships, while maintaining a professional code of ethics;
- Monitor employee social media activity in real time, and block unwanted messages from being posted.

This webcast is critical for financial services companies interested in leveraging social media, while maintaining compliance with regulations like FINRA.

Presented By

Sarah Carter, VP - Marketing, FaceTime Communications

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=193>

199

141

Securing Your Email Infrastructure

Overview

Electronic communication is at the heart of every organization, but one compromised e-mail can damage your corporate brand, compromise intellectual property or put you in non-compliance with laws and industry regulations. Privacy concerns, regulatory compliance and corporate guidelines all need to be factored into your decision-making process when it comes to e-mail security management.

GLBA and SOX both have an impact on your e-mail security strategy as your institution is responsible for:

- Preventing the leakage of personally identifiable information via e-mail (GLBA);
- Maintaining an audit trail of where an email message originates from (SOX);
- Ensuring complete access to email messages when needed (SOX);
- Preventing unauthorized access to stored messages (GLBA).

Register for this webinar to learn:

- How industry regulations affect your institution's e-mail archiving strategy;
- Key technology considerations for securing your e-mail;
- An example of how to deploy e-mail encryption.

Background

Trust is the foundation of the banking industry, and there's no surer way to squander that trust than by failing to protect the integrity of your institution's electronic communication.

Think for a moment of the amount of sensitive data your employees exchange daily with colleagues, partners and even customers. Now, consider the ramifications if this information were to fall into the hands of competitors or criminals.

The Federal Bureau of Investigation estimates that corporations lose \$100 billion each year due to "industrial espionage," much of this through insecure e-mail.

As a result of this risk, many banking institutions now recognize the need to automatically secure and encrypt sensitive e-mail communication that exits their infrastructure boundary. Policies alone won't do the job; true security requires technology, too.

Does your messaging solution protect your sensitive information? Register for this webinar to learn more about:



- The specific internal and external threats to e-mail communication;
- The basics of e-mail encryption;
- Technology questions you must answer before deploying the solution that's right for your institution.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=141>

146

Security Risks of Unified Communications: Social Media & Web 2.0

Overview

Today, smart institutions are looking for new ways to stand above the competition. And there's no better way to achieve that edge than by empowering employees with the tools they need to collaborate and communicate more effectively. The rise of social media websites and innovative communications technologies represent a great opportunity for any business. But with that opportunity comes security risks and compliance challenges for IT.

This webinar for business and information security professionals explores the security risks of employees traversing social media websites to building a highly available network and enforcing security policy. Tune in for these key discussions:

- Osterman Research offers insight into the rise in social media and its impact - good and bad - on the financial community;
- Microsoft explains what it takes to integrate Outlook, instant messaging, conferencing and other technologies for more effective communication; and
- FaceTime presents an effective approach to monitoring employees as they use social media websites.

Background

Today's Internet is dominated by connectivity and collaboration. Financial services firms are faced with the challenge of managing and securing the converging worlds of enterprise communications and collaboration tools such as Microsoft Office Communications Server on the one hand, with publicly available social networks, instant messaging clients and Web 2.0 applications on the other.

- Hear about the growing risk of non-compliance; how regulations that govern rules for Unified Communications and instant messaging are interpreting use of social networking and Web 2.0;
- Find out about the productivity, cost savings and competitive advantage to be gained from Microsoft Office Communications Server;
- Learn to reduce your risk and meet the management, security and compliance requirements of UC and Web 2.0 while ensuring an efficient, scalable architecture.



As the communications landscape becomes more complex, so does managing the risk. Real-time communications and Web 2.0 tools are designed to bypass traditional security solutions introducing new compliance and policy challenges. For instance, financial services organizations already using IM now also use Twitter and other channels to communicate with customers; yet regulatory bodies such as FINRA require that these communications be subject to standard sales and marketing message approvals, monitored and archived.

Join Osterman Research, Microsoft and FaceTime for guidance on reaping the productivity and cost savings benefits of UC tools such as Microsoft Office Communications Server while ensuring an efficient and scalable architecture that addresses security and compliance for IM and other modalities, as well as the growing use of social networking and Web 2.0 technologies.

Learn about the converging worlds of enterprise platforms and Web 2.0 - how to control risk and meet increasing regulatory compliance requirements while enabling employees with the tools they need to maintain the very collaboration that makes your business competitive.

Presented By

Eric Young, Senior Director of Field Services, FaceTime Communications

John Vigilante, Unified Communications Specialist, Microsoft

Michael Osterman, President, Osterman Research

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=146>

145

Social Networking: Is Your Institution Ready for the Risks?

Overview

Social networking isn't coming to banking; it's here. Your core processors have Facebook-ready applications to deploy, and you likely already are marketing your services via Twitter and LinkedIn, or will be soon. But take a step back: Are your employees adhering to your social networking policy? Do you even have a formal policy? Are there risk management procedures in place to protect your customers' privacy and your institution's reputation?

Register for this session to see how one organization has approached social networking, including:

- Corporate use of social networking sites such as Facebook, Twitter and LinkedIn;
- The differences between internal and external social networking sites;
- How to create policy that decides: What is acceptable for my organization?
- How to respond to a social networking incident that compromises security.

Background

From MySpace to Facebook, LinkedIn to Twitter, social networking sites have captured the attention of Internet users of all ages and background, and they are quickly proving themselves as an effective medium for organizations looking to forge stronger relationships with their core customers.

Whether it's a company creating an affinity group on LinkedIn, a marketing executive issuing company news on Twitter or an employee discussing business on Facebook, social networks have quickly become the hottest venue for public discourse.

And they represent a huge vulnerability if you don't create and enforce policy about proper social networking. Risk management includes answering key questions such as:

- How should employees identify and conduct themselves when social networking?
- What are the types of business information that should not be discussed in those venues?
- What are the differences between internal and external social networking sites, and how should employees be expected to conduct themselves upon them?



In this exclusive session, Matthew Speare, a banking/security leader at a major U.S. institution, will share his experience in social networking, focusing on:

- Vulnerabilities - What are your organization's biggest risks in social networking?
- Policy - How do you create rules governing social networking on internal and external sites?
- Monitoring - Once policy is in place, how do you enforce the rules on an ongoing basis, constantly evaluating new sites and practices, assessing whether they are acceptable for your enterprise?
- Response - If there is a security breach via a social networking site, what personnel and practices do you have in place to mitigate the damage?

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=145>

257

Defenses Against Major Threats Targeting Large Financial Institutions

Overview

Malware. External hackers. Rogue employees. Banking institutions are subject to each of these risks, and so to protect customer trust, these institutions today must invest in enterprise-wide system encryption and key management technologies.

Learn from a top-four U.S. bank as to how you can:

- Secure thousands of distributed servers with diverse business requirements;
- Achieve ease of deployment without a performance impact;
- Encrypt both structured and unstructured data;
- Provide protection beyond physical theft;
- Ensure compliance with policies and industry regulations.

Background

Securing data from unauthorized access has emerged as a critical business issue for all industries. Regulations, compliance initiatives and customer loyalty all depend on protecting data. Vormetric's customers have rapidly deployed their comprehensive data security solution to protect critical information across applications, databases, file systems and storage architectures.

By attending this webinar, you will discover:

- The necessity behind enterprise system encryption and key management for physical, virtual and cloud environments;
- How enterprise system encryption can defend against rogue users, malware, physical theft and unintended user access;
- The importance of enforcing a security policy enterprise wide.

Presented By

Todd Thiemann, Senior Director - Product Marketing, Vormetric

Jason N. Buck, Technology Manager and VP for Data Encryption, Top 4 Bank

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=257>

48

The Identity Management Challenge for Financial Institutions

Overview

This webcast will describe ways banks can mature and simplify user provisioning and identity life-cycle management:

- Integrated compliance support and the larger governance picture;
- Integrated identity administration and user provisioning across platforms, applications and user-groups;
- Delegated administration of user identities;
- Automation and enforcement of user administration processes;
- User provisioning and self-service of profiles and passwords.

The result: reduced costs and increased productivity, improved security, enhanced regulatory compliance and governance, increased user satisfaction.

Background

How to Manage the Life-Cycle of User Identities across All Applications, Platforms and User-Communities

You know the challenge: manual or ad hoc administration of user identities, accounts and entitlements to applications, systems and resources. The result: increased costs, increased security and regulatory compliance risks, and end-users who complain when they get slow or no access to resources they request. The problem is made worse when you consider all the applications (home-grown and purchased) platforms (from mainframes to mobile devices), and user-groups (employees, contractors et. al.) that you need to cover. And don't forget access from inside and outside the firewall. What's to be done?

This webcast will describe ways financial institutions can mature and simplify user provisioning and identity life-cycle management.

Presented By

Gijo Mathew, Global Practice Vice President, Security Management, CA

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=48>

56

Testing Security Controls at a Banking Institution: Learn from the Experts

Overview

Federal regulations require many organizations to conduct independent testing of their computing and networking environment at regular intervals. Many organizations comply with this requirement by conducting penetration testing and vulnerability analyses. These tests offer a snapshot of an organization's security posture during a given point in time and are valuable in maintaining the overall security architecture of the organization by identifying vulnerabilities.

The management of an organization seeking to conduct an evaluation of the current environment must clearly understand the scope, methodology and the process for conducting penetration tests and vulnerability analyses. During this presentation, James Kist, a veteran of the information security industry, will describe the merits and short-comings of many different approaches employed by security practitioners today. He will discuss some of the key regulatory requirements as well as industry best practices for conducting these types of assessments.

Register for this webinar to listen to proven strategies for:

- Evaluating the testing scope and parameters for penetration testing and vulnerability analysis;
- Testing strategies for all elements of the distributed computing environment;
- Understanding the regulatory as well as technical drivers;
- Defining the test parameters;
- Attack profiles;
- Engagement approach;
- Rules of engagement;
- Reporting of findings and recommendations;
- Making use of the results.

Background

Penetration testing and vulnerability analysis is security testing in which a security analyst attempts to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing or vulnerability analysis is to identify methods of gaining access to a system by using common tools and techniques developed by



“hackers.” This testing is highly recommended for complex or critical systems (e.g., most organizations' networks).

Penetration testing can be an invaluable technique to an organization's IT security program. But, it's a very labor-intensive activity and requires great expertise to minimize the risk. By attending this webinar, attendees will be prepared to get the most from their next penetration tests and vulnerability analyses. The attendees will walk away with real-world solutions to the growing challenges of maintaining the information security posture for their organizations. An organization's security posture includes consideration of personnel, processes and technologies. Definition, periodic testing and continuous maintenance of appropriate information security standards and practices - all vital components of the security architecture of an organization - will be discussed within the context of penetration testing and vulnerability analysis.

Organizations perform penetration testing under several different conditions. The goal is to expose not only vulnerabilities that can be leveraged by outside intruders who have no link to information on the organization, but also vulnerabilities that can be potentially exploited by insiders who possess some knowledge and access to the systems.

Attendees will hear strategies for gaining the most return from their investments while conducting penetration testing and vulnerability analyses.

Presented By

James Kist, CISSP

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=56>

204

The Dirty Little Secret About Network Security

Overview

If you are sending data over a service provider's network, there is a dirty little secret you need to know about. Despite your provider's claims that your data is secure, current Wide Area Network (WAN) technologies including MPLS and Metro-Ethernet offer no inherent data protection. It's time for you to take matters into your own hands to ensure your data is secure.

View this FREE webinar to learn about:

- The importance of data-centric security and the latest findings on how/where data is stolen;
- The truth about the lack of security with MPLS and other WAN technologies;
- A groundbreaking data protection method that secures data without impacting network or application performance.

Background

Many network and security executives believe data is secure as it traverses the Wide Area Network (WAN). This myth is often perpetuated by service providers who claim their networks are “private” - insinuating that your data is safe from attack, theft or redirection as it traverses over network backbone.

The truth is that your data may be more vulnerable on the MPLS/ Metro-E backbone than anywhere else. Since your data is most often sent in clear text (unencrypted), your data can be viewed, replicated, modified or redirected without detection. To make matters worse, there are readily available video instructions on the Internet on how to tap data lines for data replication.

And if your data is breached, it's your company that bears the financial and legal burden. Nearly all standard service level agreements (SLA) specify only availability rather than data security and integrity (another little truth the providers are not keen on sharing).

The good news is that with recent technological advancements, it is now possible to protect data in motion over the WAN, without the complexity, cost and performance issues of IPsec tunnels. With this latest breakthrough in data protection, your information can be secured quickly and easily while maintaining high availability, disaster recovery and any-to-any connectivity - all with performance that meets the standards for voice, video and other high speed applications.



Among the topics to be discussed are:

- How threats to networks and data have changed over the past 15 years;
- The difference between “virtual privacy” and actual security;
- A revealing look at the lack of security within wide area networks;
- Network encryption case studies - how several companies are protecting their data without using performance killing IPsec tunnels.

Presented By

Jim Doherty, Chief Marketing Officer (CMO), Certes Networks

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=204>

192

The Fraud Deficit: Why Deposit Account Fraud Budgets Need to Shrink

Overview

To effectively manage fraud prevention teams, processes and technology, banks and credit unions must establish annual fraud “budgets” to predict, measure and account for losses and other related costs. Explore the impact of thinking of fraud as a budgeted expense which is “under control” as long as the budget is met and how new approaches can shrink fraud budgets and increase bank profits.

Join industry experts Andy Schmidt, George Tubin and Shirley Inscoe as they discuss:

- The true cost of deposit account fraud;
- Why many fraud budgets are too high;
- Why check fraud losses continue to go up;
- How to effectively engage senior management.

Background

The most recent American Bankers Association Survey reports >\$1B in deposit account fraud losses at banks in North America and nearly \$12B in attempts. The amount is significant, as are the considerable resources dedicated to containing the problem. What’s surprising is the fact that many institutions consider deposit account fraud - specifically check fraud - a “covered” problem or a “budgeted expense,” when reducing these costs could have a material impact on profitability and free up resources to strengthen defenses against other fraud threats.

Join TowerGroup analysts Andy Schmidt and George Tubin, and industry veteran Shirley Inscoe, as they explore how many banks are rethinking deposit account fraud and making it a focal point of their cross-channel fraud management strategy. Hear early results from a TowerGroup survey regarding current perspectives towards fraud management. Learn about the tools and techniques required to reduce fraud budgets with confidence and to secure executive support in the effort to rethink fraud.

Register for this webinar to learn:

- Why the decline in check volume will not lead to a decline in check fraud losses or attempts;
- Why deposit account fraud defenses are a critical component of a cross channel fraud management strategy;



- How new approaches to check, deposit and kiting fraud enable loss prevention teams to catch more fraud, more accurately and more efficiently;
- What steps can be taken to help senior management “rethink fraud.”

Presented By

George Tubin, Banking and Security Analyst

Andy Schmidt, Research Director - Global Payments, TowerGroup

Shirley Inscoe, Director - Financial Services Solutions, Memento

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=192>

118

The Future of Banking Enterprise Access Management & Authentication - Emerging Technologies Insights

Overview

Second in a Series of New Roundtable Events Showcasing Emerging Technologies.

- Hear about emerging trends in banking enterprise access management;
- Find out how employee access management and authentication can be improved with emerging technologies and new functionalities;
- Learn how to reduce your vulnerability to employee threats and insider fraud.

At a time when the banking industry is in flux - institutions are failing and merging, and employee layoffs are widespread - it is imperative that banking institutions improve their enterprise Identity Access and Management (IAM) practices.

Background

It’s never been a more challenging time for Identity and Access Management (IAM).

Banking institutions themselves are ever more complex, what with extended networks of remote employees, contractors and vendors, as well as the number of critical business applications - and private data - they’re accessing via these networks.

And then there are the challenging times we’re experiencing. Banking institutions are failing and merging; thousands of employees are being laid off - with the remaining workers subject to new levels of stress - and economic conditions have only heightened security threats from inside and outside the institution.

It’s time to check and re-check IAM methods, and in this webinar you will hear from industry thought-leaders who will discuss trends and technologies related to all aspects of IAM, including:

- Enrollment/Identification - Assigning a “persona” to employees;
- Authentication - Validating the employee is legitimate;
- Provisioning - Assigning and rescinding “rights” to an employee;



- Review/Monitoring - Ongoing and periodic validation of users and their rights.

Presented by

Paul Smocer, VP Security, BITS

Robert Grapes, Chief Technologist - Cloakware

David Dingwall, Senior Solutions Architect - Fox Technologies

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=118>

268

The Great Application Security Debate: Static vs. Dynamic vs. Manual Penetration Testing

Overview

When it comes to application security, which approach is best? Is static application security testing better than dynamic testing? Or is manual penetration testing best of all? Or can I forego testing all together and rely on my web application firewall? The answers to these questions seem to vary depending on who you're talking to; but there's one thing all security professionals agree on - we MUST secure our software now. Maintaining secure software is essential to ensure business processes remain functional and that the data they rely on is not compromised. This webinar will explore the alternative testing methods and approaches available to IT professionals and security practitioners looking to implement a software security program.

After attending this webinar you will:

- Understand why application security testing is a critical component of any enterprise security program;
- Understand the differences between static testing, dynamic testing and manual penetration testing;
- Be able to determine which testing approach is best suited to your organization.

Background

Software applications are an integral part of 21st century business processes. The majority of software is still installed in-house, either as specially developed custom applications or commercially acquired packages. However, the proportion of software procured as a service is on the rise, as is the use of mobile apps and open-source components. In addition, more and more in-house applications are being web-enabled and exposed to the outside world.

Regardless of its origin, the vast majority of software will contain flaws which can constitute a security risk, especially for those applications that are web-enabled. The cost of fixing a flaw increases the later that they are found in the development, acquisition and deployment life-cycle. There are a number of measures that can be taken to mitigate the problem and reduce the overall cost of managing software whilst ensuring better security. Increasingly, businesses are recognizing the benefits of



outsourcing at least some of the effort through the use of on-demand software testing services.

This webinar explores how businesses are deploying software and what measures are in place for checking the security of applications. This webinar will present new research conducted amongst US and UK enterprises from a range of industries and assesses the scale of the software security problem, the ways in which it can be mitigated, the extent to which this is being achieved, the costs involved and how these can be minimized.

- 2011 was the Year of the Breach. Some of the world's best companies and brands were attacked, making securing your enterprise applications a key information security imperative.
- As applications become more mission critical to the enterprise, so too does the need to secure them.
- Learn how enterprises can leverage the various application testing approaches in their application security programs.

Presented By

Chris Wysopal, CTO/CISO, Veracode

Bob Tarzey, Research Analyst, Quocirca

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=268>

163

The Identity Enabled Network: The Future of Secure Cyberspace

Overview

As we have seen from recent domestic and global threats, the federal IT enterprise is under constant attack. Today's network access technologies are a starting point for securing federal agency networks, but they are not enough. Today's secure network requires pervasive security measures that leverage existing infrastructure to meet tomorrow's needs - and are rooted in users' fundamental security asset: their identities.

Register for this session to learn:

- How to safeguard against data leakage in support of regulatory requirements;
- Tactics and tools to simplify identity policy management;
- A strategy to enable role-based identity and controlled access to critical applications and resources.

Background

The traditional network and physical perimeter is no longer the only borderline to defend information security. Collaboration, mobility and new computing technologies are driving productivity gains while presenting renewed security requirements. There is greater pressure on IT to meet the demands of a dynamic government workforce - both in terms of service delivery and security challenges. New solutions are needed to protect borderless networks and to help further improve mission efficiencies in the mean time.

Federal IT leaders are faced with solving the following challenges:

- How to simultaneously continue to expand our networks and access to them while restricting access to IT assets;
- The ability to dynamically access and services for users and devices to support a dynamic workforce;
- How to secure access to the network and resources, whether wired, wireless, or remote access, and ensure that endpoint devices are authorized and compliant with policy;
- How to know who's coming to the agency's network, what they are doing on the network, and what type of resources they are allowed to access for the sake of controls, auditing, and reporting in an effort to meet compliance requirements.

Access to IT assets will increasingly become role-based, meaning that an employee's role or job function dictates his/her access to information, be it citizen data, patient record data, intelligence



data, etc. There are more people coming into an agency's network via a wide variety of means, be it wired or wireless, and on different end-point devices. NAC does a good job of controlling "admission" and device posture but once a user is in, he/she can access any IT resource. To comply with federal legislation such as FISMA and standards such as NIST 800-53 while supporting an ever-increasing network diameter, federal IT leaders need to start thinking about access to IT resources based upon the role of the user and his/her identity.

The greatest challenge to implementing role-based networking lies in the fact that layering auditable compliance requirements on top of an ever increasing massively distributed and connected workforce is a daunting task with existing network security solutions. In short it can't be done in scale. Government needs a network security architecture that delivers granularity of access, ease of administration and does not slow down business process.

Presented By

Russel Rice, Director of Marketing, Policy Management Business Unit - Cisco

Dave Klein, Lead Systems Engineer - Cisco Federal Security

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=163>

216

The Mobile Environment: Challenges and Opportunities for Secure Banking

Overview

Mobile devices have forced a radical shift in the way organizations service their customers. Financial institutions are no exception to the pressure of extending their online services to the mobile channel. By 2015 mobile banking could reach one in five adults in the United States. But the growth in mobile devices has also driven the incidence of mobile fraud, and improved security will be a prerequisite to recognize the exponential growth expected in mobile banking. As banks look to capitalize on the mobile environment they are also challenged by the need to bolster consumer confidence in online banking, particularly in the face of pending new FFIEC guidelines.

Against this backdrop, this webcast will look at how banks can leverage the mobile device itself to strengthen both online and mobile security, including:

- Understanding the latest threats to mobile and online banking;
- Why current solutions are ineffective against the latest fraud threats;
- New approaches for strong authentication and transaction verification;
- How mobile devices can strengthen mobile and online security and address pending FFIEC regulatory guidance.

Background

A recent study by Forrester in January 2011 predicts that by 2015 mobile banking will reach one in five adults in the United States, and for many customers, mobile banking will become the preferred channel for basic banking transactions. In Europe, mobile banking trends are similar to those in the United States - as many as 12% of European Net users take advantage of some mobile banking.

But the growth in mobile devices has also driven the incidence of fraud targeting these devices. Whether simple rogue text messages, fictitious billing scams or more malicious attacks using malware installed on the device, the number of attacks are now increasing alarmingly - by one account mobile malware increased by more than 45% in 2010. And with less education about mobile threats, users seem more inclined to fall victim to them.



But as banks look to address these issues and capitalize on the opportunities of the mobile environment, they're also challenged by the need to bolster consumer confidence in online banking, particularly in the face of pending FFIEC guidance. Online banking users, both consumers and commercial users, continue to be the target of sophisticated attacks. The U.S. now has the highest concentration of websites that host the Zeus crimeware package. And the merger of the Zeus crimeware toolkit and its one-time rival SpyEye, has not only brought together two crimeware toolkits, but also two different bot networks.

Yet the proliferation of mobile devices offers financial institutions an opportunity to leverage the device itself to strengthen both online and mobile security, while addressing customer demand for extended mobile banking services.

This webcast will look at the following:

- Some of the latest threats to mobile and online banking;
- Why many solutions currently deployed in financial institutions cannot address the latest fraud threats;
- How mobile devices can be used to enhance online and mobile security and address upcoming guidance from the FFIEC;
- New proven approaches to provide stronger online and mobile authentication, transaction verification and embedded security for mobile banking applications.

Presented By

Mike Byrnes, Director - Customer Authentication & Fraud Detection Solutions, Entrust

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=216>

179

The Reality of Cyberattacks: Emerging Solutions for Today's Threats

Overview

Recent research shows clearly that our critical infrastructure is under repeated cyberattack often from high-level adversaries like foreign nation-states. In fact the estimated cost from downtime, caused by major attacks, exceeds \$6M per day. It's now confirmed: Our critical infrastructure is under repeated cyberattack from high-level adversaries.

Register for this webinar to learn:

- The top cyber risks to public and private sector organizations;
- How to harden operational environments to ensure sensitive data is always protected;
- How these risks can be mitigated with end-to-end data encryption and tokenization.

Background

Last July 4, key federal government websites were disrupted by a series of distributed denial-of-service attacks.

In January, Google and 30 other major companies revealed they'd been the targets of another sophisticated cyberattack.

These incidents confirm what we all have long believed: our critical infrastructure is under constant attack, and the potential cost of a successful attack is staggering.

In fact, the estimated cost from downtime caused by major attacks exceeds \$6M per day. In a recent survey of federal agencies, the top security concern was the inability to protect sensitive and confidential data.

Some eye-opening facts:

- Nearly one-third of IT executives surveyed said their own sector was either "not at all prepared" or "not very prepared" to deal with attacks or infiltration by high-level adversaries;
- 50% of IT and security executives also identified the United States as one of the three countries "most vulnerable to critical infrastructure cyberattack."

The solution? Increasingly, organizations turn to end-to-end encryption and tokenization coupled with hardened cryptographic



operations to ensure that no matter where data goes, it is always protected.

This webinar will examine these solutions in detail, using the nation's payment system as an example to illustrate how data can be protected from cyberattack.

Thales and Voltage Security have teamed to make protecting data end-to-end easier. In this webinar, you'll learn about:

- End-to-end data protection via encryption and tokenization;
- Hardened operational environments that ensure sensitive data is always protected;
- How key management and a secure environment for encryption provide complete protection.

Presented By

Bryta Schulz, Vice President Product Marketing - Thales Information Systems Security

Robert Rodriguez, Chairman & Founder - Security Innovation Network

Mark Bower, VP - Product Management, Voltage Security

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=179>

284

The State of Print Security 2012

Overview

How well do government agencies secure printing and imaging assets?

A new survey by Information Security Media Group and HP shows a significant disconnect between what agencies say about print security ... and what they are actually doing to ensure it.

To learn more about the state of print security at U.S. government agencies, please register for this exclusive webinar in which a panel of ISMG and HP experts will present the survey results and analysis, discussing:

- The most common threats to printing and imaging assets;
- How well agencies are prepared to face these threats;
- What government/security leaders can do to improve printing and imaging security.

Background

Government entities are focused increasingly on external threats to security and privacy. But how prepared are they for internal threats - specifically, those that manifest through their own printing and imaging devices?

According to the new 2012 Print Security Survey conducted by ISMG and HP, agencies are aware of risks to printing and imaging assets, but are doing little to ensure their protection.

Asked, on a scale of 1-5, how important print/imaging security is to their organization, 86 percent of respondents say "Important" or "Very Important."

But then in subsequent responses, these same respondents reveal:

- Only 45 percent include print and imaging as part of their IT security plan;
- Only 44 percent have a policy or guidelines for managing and maintaining printers and imaging devices;
- Only 9 percent have a solution for detecting tampering or alteration of printed documents.

A growing threat vector, printing and imaging fleets are often overlooked in risk management plans. To determine how well agencies are securing their printing assets, ISMG and HP launched this study, aimed at security leaders within U.S. government agencies of all sizes, to:



- Determine the most common types of breaches against printing and imaging assets;
- Gauge how well agencies are prepared to prevent and detect these breaches;
- Identify the specific steps government/security leaders can take to improve printing and imaging security.

Register now for this webinar to learn more about the 2012 state of print security.

Presented By

Alan Saxton, Market Development Consultant - Imaging and Printing Group, Hewlett-Packard Company

Michael Howard, World Wide Security Practice Lead - Printing and Personal Systems, Hewlett-Packard Company

Tom Field, Vice President, Editorial, Information Security Media Group

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=284>

237

The Role of Out-of-Wallet Questions in Meeting the Updated FFIEC Guidelines

Overview

The updated FFIEC Guidance on Authentication in an Internet Banking Environment, released in June, set a new standard for online banking security. The guidance calls for a layered security approach and stronger, more effective authentication techniques, including replacing challenge questions based on shared secrets with a more sophisticated solution called out-of-wallet challenge questions.

This webinar explores out-of-wallet challenge questions where you'll learn:

- The difference between authentication techniques and how you can establish trust;
- The dangers associated with current authentication technologies like Shared Secrets;
- Where and when to use out-of-wallet questions;
- How you can generate out-of-wallet questions with your own proprietary customer data;
- The different types of out-of-wallet question providers and how to choose the right solution for your bank;
- Recommended approach for being in compliance by January 2012.

Background

Out-of-wallet questions, sometimes referred to as dynamic knowledge-based authentication, are considered a higher level of identity verification to help banks establish trust with any consumer-not-present. Out-of-wallet questions are very different from the more commonly known challenge questions of "what's your mother's maiden name" or "name of your favorite sports team" and can be used in a variety of situations where you need to be sure someone is who they say they are.

This webinar examines both the security and customer service issues associated with challenge questions in place at financial institutions today and why the FFIEC is guiding banks to switch to out-of-wallet challenge questions. You'll hear from an identity verification expert on how other financial institutions are stopping fraud using out-of-wallet questions as well as recommendations for making the switch within your own organization.



Sign up for this webinar if you want to walk away with a clear understanding of the differences between these technologies and the risks your company faces by not switching to this more sophisticated method of authentication.

Presented By

Jodi Florence, VP - Marketing, Idology

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=237>

161

Time: The Hidden Risks - How to Create Compliant Time Practices

Overview

Is your organization vulnerable to a security breach or regulatory action because of its inaccurate time-setting practices?

Too often we take time for granted. Yet, it's critical to securing our operations and validating the integrity of our data - especially in the event of a security breach or a legal action. Register for this session to learn:

- The greatest regulatory and legal risks re: time;
- Where to find your greatest exposures;
- How to establish a compliant, accurate time-setting practice.

Background

Your organization's time-keeping practices are essential for the creation and maintenance of accurate, compliant and provable electronic data. If the timestamps in your data records are not reliable:

- Your transaction processing applications will fail;
- Forensics and audit log management will become a nightmare;
- You may run afoul of regulatory and industry requirements; and
- Courts may reject your electronic data as inadmissible.

Time is a major component in complying with the Payment Card Industry Data Security Standard ("PCI DSS") as well as the Financial Industry Regulatory Authority Order Trail Audit System ("FINRA OATS").

Time also plays a major role in addressing the FFIEC's objectives for the integrity of data and accountability ("FFIEC Information Security Examination Handbook," p.6).

Yet for all time's importance, we understand little of how our systems actually generate and maintain time and the significant deficiencies in most time practices.

For example, as a compliance officer, would you accept a critical business process that was supported by a third party that refused to be audited or enter into a service level agreement?

- What if there was no way to even verify the identity of the third party that provided the critical support?
- What if one of your critical systems accepted input from several company locations and external partners across multiple time



- zones and it was practically impossible to determine the actual time of day on the various time stamps?
- What if one of your systems was dependent on a single source for critical data and no automatic failover process or backup strategy existed?

Most people would be surprised to learn that these problems are common in the vast majority of businesses with respect to how they manage time.

This webinar provides an introduction to how digital time is communicated and maintained in electronic commerce, the various sources for time and the significant vulnerabilities in the existing time practices used in most companies. The presentation will give you detailed recommendations for how to address these vulnerabilities and the basic components for a compliant time-keeping practice.

Presented By

Bill Sewall, Information Security, Compliance, Risk Management Specialist

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=161>

169

U.S. Dept. of Justice on Payment Card Fraud Trends & Threats

Overview

From ATM skimming to the Zeus malware, credit and debit cards are under increased attack by fraudsters, and organizations need to step up their efforts to protect their customers - and themselves.

Join Kimberly Peretti, former senior counsel with the U.S. Dept. of Justice, for her insider's tips on:

- Trends in debit and other payment card thefts;
- Lessons learned from the TJX, Hannaford and Heartland breaches;
- What you can do to avoid being the next victim.

Background

Ten years ago, the Department of Justice was prosecuting mischief-makers for defacing web pages. Today, federal prosecutors are targeting international crime rings behind such high-profile hacks as Heartland Payment Systems, which exposed an estimated 130 million consumer accounts.

Kimberly Peretti, former senior counsel in the department's computer crime section, who played a prominent role in prosecutions against notorious international hackers such as Albert Gonzalez, offers an insider's view of financial data breaches. In this session, she will cover:

- Background on carding: discussion on the current "carding scene," carding forums and carding activity (online, in-store, gift cards, PIN cashing);
- Evolution of prosecutions: From carding forums in 2004 to major resellers in 2006, and now the new, international hacking rings - including the Gonzalez case;
- What we know: Lessons learned from the breaches and the criminals, as well as emerging methods - and victims;
- How we can respond: Emerging technologies and steps organizations can take today to minimize their exposure to financial data breaches.

Presented By

Kim Peretti, J.D., LL.M., CISSP, PricewaterhouseCoopers

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=169>

41

User Authentication: Best Practices for Managing Risk & Compliance

Overview

- Outline the steps for integrating a multi-factor authentication solution;
- Discussion of the FFIEC Multi-Factor Authentication Guidance and what it means for your authentication solution;
- Discuss various multi-factor authentication technologies.

Background

The FFIEC (Federal Financial Institutions Examination Council) has issued updated guidance that essentially states single-factor authentication is inadequate for high-risk transactions. This means financial institutions should be doing risk assessments and subsequently implementing additional authentication controls when appropriate (by year end 2006).

This webinar will briefly discuss the FFIEC regulatory guidance, discuss multi-factor authentication technologies and assess approaches and options for integrating multi-factor authentication technology into web applications.

This session should be of interest to anyone who needs to understand the FFIEC regulatory guidelines, or who is looking for best practices around integrating multi-factor authentication with heterogeneous web applications.

Encode, Inc. is a systems integration company that leverages partnerships with software leaders like IBM and SecurIT to deliver security and directory solutions for identity and access management.

Presented By

Daniel R. TumSuden, CISSP, Encode, Inc.

Susan Orr, CISA, CISM, CRP

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=41>

239

Understand How Financial Institutions Can Benefit from Utilizing Tokenization

Overview

Tokenization is a rising data security model that is gaining traction with CISOs for reducing risk and complying with industry data security mandates and privacy laws in extended heterogeneous IT environments.

This presentation will introduce tokenization to IT and security professionals using some practical, real-life case studies and detail lessons learned from implementing tokenization within large enterprises - both in an on-premise and cloud-based model.

This presentation will also dive into:

- Understanding business benefits behind tokenization, centralized key management and centralized data vaults;
- Providing some specific approaches for implementing tokenization in the enterprise;
- Revealing lessons learned from past implementations.

Background

Most data security practitioners and information security groups within organizations are aware of the value and benefits derived from using tokenization - both on-premise and cloud-based - including its effectiveness for protecting credit card numbers, personally identifiable information (PII) and electronic health records (EHR). However, many organizations face challenges while implementing tokenization. This presentation will introduce some practical approaches to implementing tokenization which are proven, time-tested and sound.

This presentation will detail the business and security benefits of tokenization and will explain what tokenization is, why it's important for companies that need to protect credit cards, PII and EHR, what types of enterprises will benefit the most from it, the technology behind it, the differences between on-premise and cloud-based tokenization solutions, and what IT professionals need to consider in terms of infrastructure requirements when implementing it. The presentation will also detail approaches to implementing tokenization including using integration architecture to tokenize disparate systems, dealing with data quality challenges and initial tokenization and migration methodology. The presentation will be augmented with real-world



examples of implementation challenges that were successfully mitigated, along with lessons learned in the process.

- Understand business benefits behind tokenization, centralized key management and centralized data vaults;
- Discuss how to apply a format-preserving token methodology to reduce risk across the extended enterprise without modifying applications, databases or business processes;
- Distinguish what types of organizations and business processes benefit from tokenization and the differences between on-premise solutions and cloud-based tokenization services;
- Provide some specific approaches for implementing tokenization in the enterprise;
- Reveal lessons learned from past implementations.

Presented By

Abir Thakurta, Senior Director - Pre-Sales & Professional Services, Liaison Technologies

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=239>

39

Voice Over IP - Helping Financial Institutions Learn and Mitigate Security Risks

Overview

- Understand what Voice over IP offers and the tradeoffs between cost savings and security;
- Learn VoIP technical terminology, technology used to set up VoIP networks;
- Learn the attack methods used to break into VoIP networks and what to do to mitigate the security risks posed.

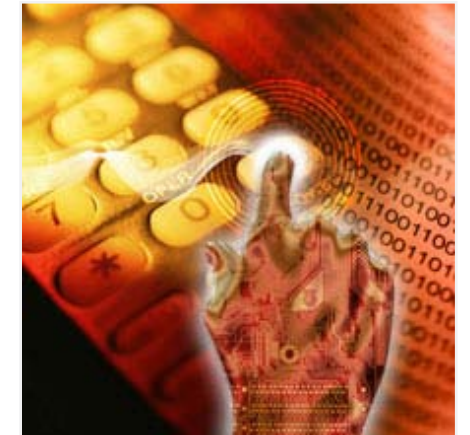
Background

Voice over IP or "VoIP", is becoming an attractive alternative to conventional phone networks. VoIP services are becoming more widely deployed in today's enterprise markets as an effective measure for cost savings and increased feature sets. Organizations must realize VoIP introduces fundamental changes to Internet Protocol (IP) architectures and creates new endpoints for attack. These new endpoints create new methods for hackers to find new methods for intrusion, extortion and pretexting.

In order to understand and prepare to mitigate these network vulnerabilities, technology and information security terms surrounding VoIP must be learned and fully understood. This new vocabulary, along with a firm understanding of how VoIP technology is integrated into existing networks, will allow the IT professional to better understand and mitigate attacks or exploits to VoIP networks.

Federal regulations require many organizations to assess and insure that customer information is safe and secure. With the implementation of VoIP, organizations need to identify internal and external threats to these new or converged networks. Using data networks to transmit VoIP could result in unauthorized disclosure or compromised information systems. Organizations should identify risk exposure and rank information assets to develop mitigation plans, testing of vendor equipment and estimate potential damages from implementing VoIP networks.

In this webinar, non-technical attendees will learn the basic technology terms surrounding VoIP technology. The presenter will give easy-to-understand explanations, how each tie in to the information security needs of existing data networks. IT pros will also benefit from the "inside view" of the presenter, who has



implemented several large VoIP projects for government and large businesses.

VoIP offers significant cost savings from combining devices and networks as well as increased feature set for end users. Using one network or device to offer data and voice is an attractive alternative due to reduction in operational maintenance and devices. From this presentation attendees will learn what the security costs are, the basic terminology and what areas of network and information security must be reviewed prior to implementing a VoIP system.

Presented By

Juan Deaton, Cellular Systems Engineer, Idaho National Lab's Next Generation Wireless Test Bed

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=39>

143

5 Steps to Managing Security Risk from Your Software Vendors

Overview

Application vulnerabilities are real and hackers are targeting industries that offer the best avenues for illicit monetary gains. At the same time, economic, competitive and time-to-market pressures are driving enterprises to use third-party commercial off-the-shelf (COTS), open source, outsourced code and crowd-sourcing as part of their application development and acquisition process - and therefore exposing these enterprises to unacceptable levels of unbounded corporate risk.

This webinar will help you to:

- Understand the major security implications to your application portfolio that come from third-parties like COTS vendors, outsourcers, crowd-sourcers, and open-source applications;
- Learn 5 best practices to help you manage the security of your application portfolio and the sources of your risk;
- Learn how you can cost-effectively manage the risk of built, bought or outsourced code without additional hardware, software or personnel investments.

This webinar will discuss a cost-effective five-step process that enterprises can apply to their third-party application portfolio to gain visibility into their security state, meet regulatory requirements, and establish a third-party governance framework to protect their critical assets.

Background

Application Security is rising to the top of the agenda for Security and Engineering executives. According to the Computer Emergency Response Team (CERT), 75% of new attacks target the application layer. The 2009 Verizon Data Breach report states that “financial services firms were singled out and fell victim to some very determined, very sophisticated and - unfortunately - very successful attacks in 2008. This industry accounted for 93% of the over 285 million records compromised.”

One thing is clear - Application vulnerabilities are real and hackers are targeting industries that offer the best avenues for illicit monetary gains. At the same time, economic, competitive and time-to-market pressures are driving enterprises to use third-party commercial off-the-shelf (COTS), open source and outsourced code as part of their application development process.



While this mixed code base of unknown security quality may be an acceptable artifact of modern application development and acquisition, it pushes liability onto the enterprise, resulting in an unacceptable level of unbounded corporate risk.

This webinar will discuss five cost-effective steps you can take to comprehensively assess your entire portfolio of software applications (whether bought, built internally, outsourced or crowd-sourced) while also meeting your governance, risk and compliance (GRC) requirements.

Special guest presenter, Sam King, VP of Product Marketing at Veracode, will provide insights as to the best practices that financial institutions are implementing to ensure the integrity of their application security posture while meeting GRC requirements.

Presented By

Sam King, Vice President of Service Delivery, Veracode

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=143>

188

Cloud Computing: Regulatory Security & Privacy Challenges

Overview

Cloud computing is the hot, new practice that offers a scalable, centralized resource for data and applications that can be available to anyone, anywhere.

As an emerging trend, the cloud is also fraught with risk - already we've seen organizations whose data has been compromised.

Register for this session to learn:

- Advantages and disadvantages of storing data or running applications online, as opposed to in-house;
- Current regulatory trends toward better security and privacy standards - and how they impact cloud computing;
- Legal, privacy, records management and ethical challenges that have been identified by cloud pioneers - and strategies to avoid those pitfalls.

Background

Attend any industry event this year, and the term you'll hear most frequently is “Cloud Computing.”

But like the old cliché about the weather, one is left to ask: “Everyone is talking about Cloud - but what are they actually doing about it?”

The answer: More than you might think. Banking institutions for years now have practiced cloud computing without using the term, outsourcing core processing to third-party service providers.

Matt Speare, veteran tech leader from M&T Bank, will lead our cloud discussion - setting the stage with a presentation depicting an institution's approach to the cloud. He'll then interact with industry experts, including Jim Reavis of the Cloud Security Alliance, to discuss the theory of cloud and the real business benefits that pioneer banking institutions are realizing today.

Presented By

Matthew Speare, Senior Vice President of Information Technology, M&T Bank

Michael Smith, Security Evangelist, Akamai

Harold Moss, CTO - Cloud Security Strategy, IBM

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=188>

88

You & Your Vendors: How to Best Secure Data Exchange

Overview

Data security breaches add millions of dollars to bottom line expenses, but there is also the immeasurable cost of security breaches on your brand that affect future revenue and growth. Virtually every financial institution today exchanges large amounts of information both inside and outside the organization. Financial data, product plans, and customer records are all at risk.

Register today to learn firsthand from industry leader Greg Pridgen, Director of Operations Support for TSYS, about ways to reduce the risk of lost or compromised data by:

- Increasing security to protect your network;
- Scaling for growth to enhance revenue opportunities;
- Improving visibility to monitor data movement;
- Complying with new rules and regulations;
- Managing cost to increase your bottom line.

Background

The headlines can be chilling. Financial institutions last year accounted for nearly 10% of all reported security breaches in North America and the risks are growing. Virtually every financial institution today does at least some amount of work globally, entrusting critical business information and processes to international partners, customers and third-party service providers.

All of these practices require institutions to exchange large amounts of information - including financial data, product plans, and customer records. Information that is routinely shared in megabyte, gigabyte and even terabyte files with their business partners around the world using protocols like FTP, HTTP, S-HTTP, SFTP and FTPS could be putting them at risk if this information should fall into the wrong hands via an unsecured network.

Presented By

Greg Pridgen, Director of Operations Support for TSYS

William McKinney, Global Product Marketing Director, Sterling Commerce

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=88>

127

Evaluating Security Risks Associated with Banking Vendors

Overview

Regulatory change is coming - fueled by the ever present news of breaches within the credit card payment networks degrading the faith in today's financial institutions. A new approach is needed to secure, make compliance easier, and enhance the operating efficiency for critical financial datacenters and those processing sensitive cardholder information or personally identifiable information (PII).

Attend this webinar to learn to:

- Facilitate PCI compliance and go beyond to provide demonstrable security for critical financial datacenters;
- Decrease the burden of proof and yet provide the verification of operational controls in a new way that will increase confidence for vendor management due diligence;
- Reduce your risk and secure your infrastructure against emerging threats to ensure that only authorized changes are allowed.

Background

Regulatory change is coming - fueled by the ever present news of breaches within the credit card payment networks degrading the faith in today's financial institutions. PCI-DSS is a step in the right direction toward thwarting 'smash and grab' attacks but is weak against zero day attacks and low 'n slow attacks that are designed to persist under the radar of common controls. A new approach is needed to secure, make compliance easier, and enhance the operating efficiency for critical financial datacenters and those processing sensitive cardholder information or personally identifiable information (PII).

As the industry continues to outsource to vendors and rely on multiple parties, those who evaluate risk need better visibility and reporting of the operational controls of these contracted entities as mandated by the regulations and standards of FFIEC and PCI-DSS. Due diligence today encompasses stronger contracts, data center visits and keeping up-to-date on vendor performance. How does a vendor keep up with these requests and provide demonstrable measures of how they secure not only IT infrastructure but applications and critical data? How can vendor management be easier for enterprises beyond submitting lengthy assessments that they can only trust reflect the true operations of the vendor? Being able to provide protection from



device to datacenter systems provides the deep visibility, control enforcement and system integrity needed to go beyond today's standards and be prepared for addressing future regulation changes.

In this webinar, hear about how:

- SecureNet Payment Systems, a leader in supplying cutting-edge payment processing technologies, plans to demonstrate and verify operational controls to ease the due diligence process of vendor management requests and compliance with Solidcore.
- MTXEPS, leader in electronic payments software and solutions, provides end-to-end protection of card holder data going above and beyond today's Data Security Standards (PCI-DSS) from device to datacenter through branded Connected Payments for Retailix retail solutions secured with S3 Control from Solidcore Systems.

Presented By

Kim Singletary, Director of OEM & Compliance Solutions, Solidcore Systems

Ken Harris, Vice President, MTXEPS Inc.

Preetham Gowda, CIO, SecureNet Payment Solutions

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=127>

242

FFIEC Authentication Guidance: Essential Questions You Need to Ask Your Vendors

Overview

Banking regulators, make no bones about it: Your third-party service providers aren't responsible for ensuring that you attain conformance with the FFIEC Authentication Guidance. You are. How do you ensure their ability to aid your efforts towards compliance? Learn the secrets of a vendor management expert, who will share with you the probing questions to ask your vendors, including:

- When and how does your vendor perform external audits checking the security of its products?
- Which authentication controls are built into your vendor's current online banking products - do they conform to the FFIEC Authentication Guidance 2011 update?
- What is your vendor's tactical plan for the remainder of 2011 to ensure its products and services conform to the new guidance in time for 2012?

Background

In a recent interview with BankInfoSecurity, Jeff Kopchik of the FDIC made clear the expectations for banks re: third-party service providers and compliance with the new FFIEC Authentication Guidance.

"The agencies have said many times - and authentication is no different - that it's the financial institution that's ultimately responsible for bringing itself into conformance with the guidance," says Kopchik, one of the principal authors of the guidance. "The buck stops at the financial institution's desk."

For several of the larger banking vendors, the federal regulators conduct their own examinations to ensure compliance. But for the majority of service providers, the responsibility is the banking institution's to ensure that products and services all align with regulatory expectations. This due diligence requires institutions to:

- Sit down with core vendors and ensure mutual understanding of the FFIEC Authentication Guidance;
- Gap analysis to determine which products/services do not currently bring the institution into conformance;
- Creation of a strategic plan with milestones to ensure conformance prior to 2012 regulatory exams.



But two challenges that institutions frequently encounter are:

- What are the specific questions I need to ask my vendors re: FFIEC Authentication Guidance?
- What information will my vendors not offer up unless I know to ask?

To assist you with this due diligence, Philip Alexander, an information security officer at a major U.S. financial institution, will share with you the vendor management tricks he's learned in years of overseeing such relationships for one of the nation's largest banking institutions.

In this exclusive two-part series, Alexander will tackle several key vendor management topics, including:

- Security reviews;
- Vendor's own regulatory compliance;
- Vendor's financial stability;
- Use of 4th-party service providers;
- Liabilities in the event of a breach.

Presented By

Philip Alexander, CISSP - ISSMP, MCSE - MCT, MPA

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=242>

243

FFIEC Authentication Guidance: What Your Vendors Won't Tell You (Unless You Ask)



Overview

So, you've met with your key vendors and conducted a gap analysis of areas that need to be addressed prior to January 2012 to conform to the FFIEC Authentication Guidance. But how do you know if a specific vendor is sharing with you a complete picture of preparedness? Some vendors are upfront on their capabilities and limitations. However, many simply lack the expertise to understand the challenges that come with working with financial institutions. It's important to go into vendor relationships fully informed, even with the data they might not want to tell you freely. Join our vendor management expert, who will share these 'dirty little secrets,' including:

- Does your vendor outsource the work they're doing for you to a fourth-party service provider - particularly overseas?
- Does the vendor employ fulltime employees only, or does it also hire temporary workers, (contractors) who may be allowed to work remotely?
- Is the potential loss resulting from a data breach greater than the vendor's contractual liability plus the vendor's total net worth?

Background

In a recent interview with BankInfoSecurity, Jeff Kopchik of the FDIC made clear the expectations for banks re: third-party service providers and compliance with the new FFIEC Authentication Guidance.

"The agencies have said many times - and authentication is no different - that it's the financial institution that's ultimately responsible for bringing itself into conformance with the guidance," says Kopchik, one of the principal authors of the guidance. "The buck stops at the financial institution's desk."

For several of the larger banking vendors, the federal regulators conduct their own examinations to assess compliance with the regulatory requirements. But for a range of other product/service vendors, that's not the case. Nonetheless, it's the banking institution's responsibility to ensure that products and services used by the institution align with regulatory expectations. This due diligence requires institutions to:

- Work with core products and services vendors and ensure mutual understanding of the FFIEC Authentication Guidance;
- Conduct gap analysis to determine which products/services do not currently bring the institution into conformance;
- Creation of a strategic plan with milestones to ensure conformance prior to 2012 regulatory exams.

But two challenges that institutions frequently encounter are:

- What are the specific questions I need to ask my vendors re: FFIEC Authentication Guidance?
- What information will my vendors not offer up unless I know to ask?

To assist you with this due diligence, Philip Alexander, an information security officer at a major U.S. financial institution, will share with you the vendor management tricks he's learned in years of overseeing such relationships for one of the nation's largest banking institutions.

In this exclusive two-part series, Alexander will tackle several key vendor management topics, including:

- Security reviews;
- Vendor's own regulatory compliance;
- Vendor's financial stability;
- Use of fourth-party service providers;
- Liabilities in the event of a breach.

Presented By

Philip Alexander, CISSP - ISSMP, MCSE - MCT, MPA

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=243>

274

Hackers, Botnets and More: Top Security Trends and Threats from the HP Enterprise Security 2011 Cyber Risk Report



Overview

Enterprise organizations have been under security attacks for the past decade, but security events in 2011 have created a ripple effect that will be felt for years to come and will actually start to shift the way we view security. In the 2011 Cyber Security Risks Report, HP Enterprise Security provides a broad view of the vulnerability threat landscape, as well as in-depth research and analysis on security attacks and trends. This webcast will highlight the latest threat trends and risks that enterprise organizations face today - and to help prioritize mitigation strategies.

Join us for this informative webcast and you will learn:

- Why a decline in vulnerabilities disclosed may lead to a false sense of security;
- How changing attack motivations are increasing security risks;
- What the biggest risks to the enterprise were in 2011.

Background

Organizations have been under security attacks for the past decade, but the security events in 2011 have created a ripple effect that will be felt for years to come and will actually start to shift the way enterprise organizations view security. For example, 2011 saw a significant increase in activity from "hacker" groups Anonymous and Lulz Security (LulzSec). The motivation for these groups' organized, systematic attacks on businesses or individuals - retaliation for perceived wrongdoing - brings new visibility to a security threat that has been looming for years and highlights a new era of security risk that must be addressed. In addition, highly publicized attacks on major corporations such as Sony, RSA and the United States Postal Service demonstrated the significant financial loss that can result from a vulnerable system.

In the 2011 top cybersecurity risks report, HP Enterprise Security provides a broad view of the vulnerability threat landscape, as well as in-depth research and analysis on security attacks and trends. The aim of this report is to highlight the biggest risks that enterprise organizations face today and to help prioritize mitigation strategies. Key findings from this report include the following:

- Continued decline of new, disclosed vulnerabilities in commercial applications - The report notes the decline in commercial vulnerability reporting, and it discusses the key trends in the vulnerability disclosure market that may be hiding a deeper issue. The report also highlights the growing market for private sharing of vulnerabilities, the increased expertise required to uncover complex vulnerabilities and the price these can fetch in various markets. Data from HP Fortify will also highlight the increasing number of vulnerabilities that are being discovered in custom applications - vulnerabilities that can be devastating to the security posture of an organization.
- Increase in the number of attacks against a "smaller" set of known vulnerabilities in commercial applications, the report will use real data - pulled from the HP TippingPoint Intrusion Prevention System (IPS) and HP Fortify - to highlight an increase in severe attacks against both client/server and Web applications. The data is broken down by attacks, vulnerability category, source information and severity to provide a snapshot of the attack landscape. This section also features an actual case study of the web application risks at one large corporation.

Presented By

John W. Pirc, Author, CEH, IAM, Director - Product Management, Hewlett-Packard Company

Jake Kouns, Co-Founder & CEO, Open Security Foundation

View the complete outline and register for this webinar at:

<http://www.bankinfosecurity.com/webinars.php?webinarID=274>

282

Risk Management: New Strategies for Employee Screening

Overview

As part of your risk management strategy, your organization likely conducts pre-employment background checks. But what are your screening strategies after you have made your hires? How would you know, for instance, if:

- An employee's personal finances have crumbled, and that individual is now at risk to embezzle;
- New evidence reveals a senior executive has blatantly falsified academic credentials;
- You uncover a past criminal offense by a current employee - do you have policies to deal with the situation?

Like risk management itself, background screening must be ongoing. In this session, attorney Lester Rosen, renowned expert in employment screening, presents post-hire screening strategies, including:

- How to conduct continual screening of key employees;
- What to do about newly-acquired employees in a merger or acquisition;
- How to proceed when you do uncover past criminal offenses or falsified credentials of current employees.

Additionally, Rosen will offer updates on the latest guidance on use of arrest and conviction records, as well as the do's and don'ts of social media in background screening.

Background

All employers, as part of their risk management strategy, have an obligation to exercise a reasonable duty of care in hiring. In addition, many organizations have a legal duty to not employ individuals with certain enumerated criminal records. There are a number of steps that employers can take in the hiring process to reduce their risk when hiring. But what about after hiring? What role does background screening play in an organization's ongoing risk management framework?

Recently, a prominent online organization made embarrassing headlines with news that its CEO had misrepresented his academic credentials on his resume. Elsewhere, a major U.S. bank fired a longtime employee after a background check revealed two 40-year-old shoplifting arrests.

Incidents such as these - and today's heightened sensitivity to the risks of the insider threat - force organizations to redefine their



screening strategies as part of their risk management approach. No longer is the focus solely on pre-hire background screening. Increasingly, organizations are engaging in continual screening to catch anomalous activity that could be a precursor to actionable behavior. And they also are embracing policies and procedures to handle damaging data when it comes to light about current or acquired employees.

Topics to be discussed in this session include:

- A brief overview of the latest screening trends, including the EEOC's new guidance on the use of arrest and conviction records;
- How to conduct continual screening;
- What to do when you learn about past criminal offenses or falsified credentials of a current employee;
- Proper screening procedures for newly-acquired employees in a merger or acquisition;
- Social media - its proper role in a screening strategy.

Presented By

Lester Rosen, Attorney & President - Employment Screening Resources

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=282>

224

Register Now: Visit www.bankinfosecurity.com or Call (800) 944-0401

289

Risk Management: Third-Party Breach Impact & Preparedness

Overview

Michaels craft stores. TRICARE. Global Payments Inc. These are among the most recent and prominent examples of third-party data breaches that adversely impacted financial institutions, healthcare providers and other affiliated entities.

How prepared is your organization to respond to a third-party breach - not just the hard costs of breach notification, account monitoring or regulatory penalties, but also litigation and reputational loss?

Customers don't care about your partners; they will hold you responsible when you notify them of a breach. You have to be prepared not just to respond to such incidents, but to help prevent them.

Join James Christiansen, a vendor management specialist, for expert advice on how to manage third-party risks, including:

- Prevention: Steps you can take to measure the areas and parties at greatest risk;
- Detection: How to detect a third-party breach, and why some breaches go undiscovered for months;
- Response: Gauging the impact of a third-party breach and addressing breach disclosure. Who needs to be involved, and how quickly should an organization react and mobilize?

Background

In Sept. 2011, the U.S. Defense Department's TRICARE health program notified 4.9 million beneficiaries of a data breach caused when backup tapes were stolen from the car of an employee of Science Applications International Corp., one of TRICARE's business associates.

In the spring of 2012, financial institutions began monitoring accounts and replacing payment cards after news that Global Payments Inc., a payments processor, had been breached, exposing an estimated 1.5 million accounts. Just three years earlier, Heartland Payment Systems, another processor, was breached, impacting 130 million cards.

The common factor among each of these incidents: They occurred at third-party entities, yet adversely affected the healthcare providers and financial institutions that relied on them for services.



James Christiansen, Chief Information Risk Officer at third-party risk-score provider Evantix, has spent more than two decades in the trenches of breach recovery and response. During this session, Christiansen will review recent third-party breaches, highlighting what affected organizations did right and what they could have done better in the wake of those breaches.

Some highlights Christiansen will cover:

- Why the simplest breach-prevention solutions are often the best, and how organizations can rely on best practices to minimize exposure;
- Balancing regulatory and industry security requirements;
- Maximizing human resources and budgetary limitations to ensure due diligence.

The probability that your organization will suffer a third-party breach can be significantly reduced by following these basic strategies, which Christiansen will detail:

- How to assess the potential impact of a third-party breach: The cost drivers, including direct costs, regulatory/industry fines, legal suits and reputational damage.
- Leveraging information: Reviewing PCI certifications and SSAE16 to gauge security and breach risks.
- Reducing risk: The role well-worded contracts play in reducing the probability of a third-party breach, and how to limit financial and reputational damage when a breach does occur.

Presented By

James Christiansen, CEO and Founder, Evantix

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=289>

Register Now: Visit www.bankinfosecurity.com or Call (800) 944-0401

225

100

Protecting the Exchange of Sensitive Customer Data with Your Vendors

Overview

For financial institutions, data security is both an operational and regulatory imperative. A bank or financial services provider that fails to protect a customer's financial data faces the threat of losing customers, tarnishing their reputation and eventually losing competitive advantage.

Register for this exclusive webinar to answer:

- How does regulatory compliance, like GLBA, affect the way your data needs to be handled and audited?
- Who has access to your sensitive files?
- What would the impact be if these files, including sensitive customer data, were compromised?
- Where and when is this data being sent?
- Why would you let employees/partners share your files over insecure FTP, e-mail or IM?

Background

For financial institutions, data security is both an operational and regulatory imperative. A bank or financial services provider that fails to protect a customer's financial data faces the threat of losing customers, tarnishing their reputation and eventually losing competitive advantage. There are some key questions you should think about when it comes to securing your customers' important financial data, including:

- How does regulatory compliance, like GLBA, affect the way your data needs to be handled & audited?
- Who has access to your sensitive files?
- What would the impact be if these files, including sensitive customer data, were compromised?
- Where and when is this data being sent?
- Why would you let employees/partners share your files over insecure FTP, e-mail or IM?

Questions still linger on how to meet compliance regulations that affect financial institutions, like GLBA, PCI and SOX.

With increased government regulation and oversight in the form of mandates such as GLBA, PCI, etc., no organization that deals with financial information can afford to ignore the very real challenge of ensuring data security, integrity and privacy.



Learn more about how your organization can meet these compliance challenges as it relates to financial data security as well as how to manage your partners to ensure that they are also following acceptable data sharing practices. And hear how other financial institutions are tackling these very important data security issues.

Presented By

Greg Shields, Microsoft MVP in Terminal Services

Kevin Gillis, Vice President, Product Management at Ipswitch

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=100>

98

Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks

Overview

Management of third-party service provider relationships has been a regulatory issue as far back as the FDIC's Bank Service Company Act. But top security breaches of Heartland Payment Systems, TJX Companies and Hannaford Brothers have brought vendor management to the fore, and banking regulators continue to issue bulletins re-emphasizing best-practices.

Register for this webinar to:

- Hear directly from Donald Saxinger of the FDIC, who will clarify vendor management guidance, including the four main elements of an effective third-party risk management process;
- Receive from James Christiansen, a noted banking and security professional, a step-by-step guide on how to create an effective vendor management program.

Background

A financial institution can outsource a service, but it cannot cede responsibility for the potential risks.

This is the clear message from banking regulatory agencies to member institutions, hammered home by recent bulletins from the Federal Deposit Insurance Corp. and Office of the Comptroller of the Currency, which combined oversee roughly three-quarters of U.S. banks. Their guidance comes on the heels of the National Credit Union Administration's earlier announcement that vendor management is now a top examination topic for U.S. credit unions.

Selection, contract structuring and ongoing management of third-party service providers are the consistent themes from the agencies. The most frequently used term: "Due diligence."

While management of third-party service providers has been a regulatory issue as far back as the FDIC's Bank Service Company Act, outsourcing has been a major examination focus since 2001, with the establishment of interagency guidelines in support of Section 501(b) of the Gramm-Leach-Bliley Act, which calls for banking institutions to:

- Exercise due diligence in selecting service providers;
- Require service providers to implement appropriate security measures;



- Monitor service providers via audits, test results, etc. to confirm that they have satisfied their security obligations.

Well-publicized security breaches, as well as new guidance such as the ID Theft Red Flags Rule, have brought vendor management to the forefront, and banking regulators in 2008 issued bulletins re-emphasizing best-practices.

Hear from Donald Saxinger of the FDIC, who will clarify vendor management guidance, including the four main elements of an effective third-party risk management process:

- Risk assessment;
- Due diligence in selecting third party;
- Contract structuring and review;
- Oversight.

Beyond the guidance, hear too from David Schneier, a noted banking/security consultant, who will leverage his field experience to share insights on how to:

- Establish the right 'tone at the top' for vendor management;
- Create a vendor management program appropriate for the size of your institution;
- Put the plan into action;
- Avoid common pitfalls that can derail vendor management initiatives.

Presented By

Donald Saxinger, Senior Examination Specialist

James Christiansen, CEO, Evantix

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=98>

104

Vendor Management Part II: Assessing Vendors - the Do's and Don'ts of Choosing a Third-Party Service Provider

Overview

Banking regulators have turned up the heat on institutions to conduct better due diligence when selecting third-party service providers to manage sensitive data. But how does one determine if a vendor's security practices are truly up to snuff? Register for this webinar to learn through case studies and insights from an industry veteran:

- How to conduct vendor audits and assessments that meet regulatory requirements;
- Which vendors to assess and what to look for when assessing vendors for security and privacy practices;
- A proven process for managing vendor risk.

Background

Since the start of 2008, the banking regulatory agencies have been hammering home the importance of due diligence, relationship management and risk assessment when selecting and contracting with third-party service providers. The National Credit Union Administration was first with its announcement that vendor management would be a top examination topic for U.S. credit unions in 2008. Then came recent bulletins from the Federal Deposit Insurance Corp. (FDIC) and Office of the Comptroller of the Currency (OCC) which combined oversee roughly three-quarters of U.S. banks.

The common message: A financial institution can outsource a service, but it cannot cede responsibility for the potential risks to itself and its customers.

In Part I of our multi-part series, we reviewed banking regulations and the various components that go into crafting an effective vendor management program. In this session, we tackle the question: How does one truly assess a vendor's operations for security and privacy practices?

Register for this webinar to learn the do's and don'ts of vendor security assessment first-hand from James Christiansen, the former CISO of Experian, General Motors and Visa.



Currently the CEO of Evantix LLC, a provider of eBusiness Risk and Compliance Management solutions, Christiansen has keen insight on what does and does not work in vendor management.

Since the 1990s, banking institutions have rushed to jump on the band wagon of outsourcing. Just since 2001, the outsourcing market has grown from \$127B to an estimated \$310B in 2008, representing over 40% growth. Unfortunately, risk management practices have not evolved to meet the new demands.

Losses from the breach of sensitive data related to third-party business relationships have reached epidemic proportions. These losses and the inherent risk of eBusiness relationships are the driving force behind the wave of new legislation and enforcement that present a material cost to banking institutions.

In this webinar, Christiansen will rely on case studies and his own field experience to answer these key questions:

- What are the regulatory requirements for assessing vendors?
- Assessing vendors is expensive. Which vendors should I assess?
- I outsourced my sensitive information to a vendor, so now it's their problem, right?
- OK, so if I have to manage all these vendors - how do I start?
- What are the best practices in managing vendor risk?
- What should I look for when I do an assessment?

Presented By

James Christiansen, CEO, Evantix

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=104>

117

Vendor Management Part III: Inside the BITS Shared Assessments Program

Overview

Banking regulators continue to put pressure on financial institutions to improve vendor management. The BITS Shared Assessments Program allows these institutions to evaluate the security controls of key IT service providers and meet regulatory compliance. Learn about the latest version enhancements, as well as how to integrate the program's two key components - the Standardized Information Gathering questionnaire and Agreed-Upon Procedures into your existing vendor management framework.

Background

Management of third-party service provider relationships is a longstanding regulatory issue within the FDIC's Bank Service Company Act. Well-publicized security breaches, such as TJX and Hannaford Brothers, further increased regulatory attention on Vendor Management practices. This year, banking industry regulators issued bulletins re-emphasizing best-practices.

This webinar takes an in-depth look at the BITS Shared Assessments Program.

Originally named the Financial Institution Shared Assessments Program, Shared Assessments is a comprehensive process for financial institutions to evaluate the security controls of their IT service providers. Launched in February 2006, Shared Assessments has more than 60 member companies.

Shared Assessments offer a standardized approach to collecting all of the data necessary to complete a thorough evaluation of a service provider's information security program.

- Financial institutions receive a trusted, comprehensive source of information about prospective vendors;
- Service providers perform one complete security review for all, versus responding to scores of individual audits from each client or potential client;
- All parties rely on a single, efficient process that saves time and expense, and helps financial institutions meet industry regulatory requirements.

In response to member feedback, BITS has just released version 4 of the program's two core elements:



- The Agreed Upon Procedures (AUP) document, which provides an objective and consistent set of procedures to evaluate key controls of third-party service providers;
- The Standardized Information Gathering Questionnaire (SIG), which allows a third-party service provider to complete one questionnaire using a standard set of questions that can be shared across multiple clients.

In this webinar, we will review the key elements and revisions to the Shared Assessments Program with insights from:

- The Santa Fe Group/BITS, on recent member feedback and updates to the program;
- The Depository Trust & Clearing Corporation on how Shared Assessments supports financial institutions' Vendor Management initiatives;
- Iron Mountain on benefits to third-party service providers; and
- Citi, KPMG and LiveOps on the latest efforts to improve and streamline the AUP and the SIG.

Presented By

Jim Routh, CISM, Chief Information Security Officer, The Depository Trust & Clearing Corporation

Andrew Hout, Citi

Eddie Holt, Partner, KPMG LLP

Michele Edson, Senior Vice President, The Santa Fe Group




Niall Browne, Chief Information Security Officer, LiveOps

Scott Brown, Program Manager, Financial Services, Iron Mountain

View the complete outline and register for this webinar at:
<http://www.bankinfosecurity.com/webinars.php?webinarID=117>

Premium Membership

Become a Premium Member to stay up to date on the latest information security and risk management topics.

<h3>Individual</h3>  <p>1 Member OnDemand Access CPE Credit Tracking <i>\$1,995/year</i></p>	<div style="position: relative;"> SAVE 25% <h3>Corporate</h3>  <p>Up to 5 Members OnDemand Access CPE Credit Tracking <i>\$7,495/year</i></p> </div>	<h3>Enterprise</h3>  <p>Unlimited Members OnDemand Access CPE Credit Tracking <i>Tiered Pricing</i></p>
---	--	--

Groups: Save up to an additional 25% with a group membership.

Membership Features

Unlimited Access

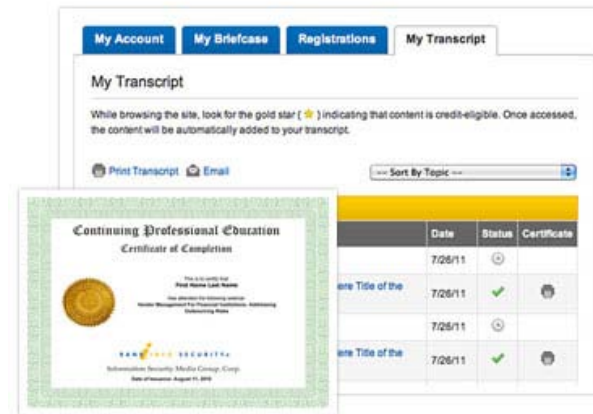
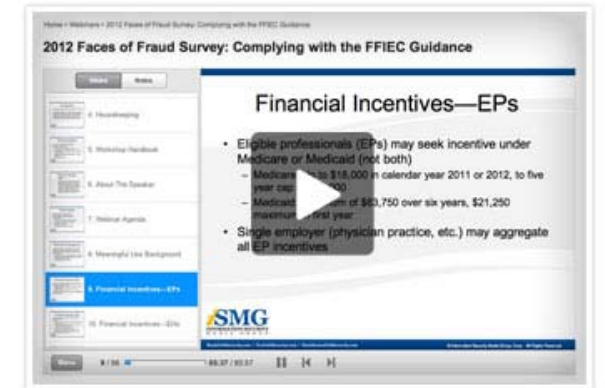
Gain unrestricted access to an expanding curriculum of over 200 courses. No education solution is as comprehensive. Our industry expert practitioners have developed over 300 hours of exclusive courses and, on average, create 15 new courses each quarter.

This continually growing resource ensures you have the latest information available as you need it.



OnDemand Viewing

Convenience is essential when it comes to your professional education. OnDemand capabilities allow you to access the education around your availability, not ours. Whether it's 15 minutes before a meeting, 30 minutes on your lunch break, or even during your daily commute, our education is always at your fingertips.



CPE Credit Tracking

Responding to regulators, senior management and certifying associations can become a hassle. Our Transcript Tracking feature lists date, title and hours of all credit-eligible webinars, articles, interviews, handbooks and other content accessed.

This transcript can be broken down by topic and attendance certificates can be e-mailed or printed directly from our system, making it easy to keep track and report on your continued education.

Presentation Materials

Each Premium Webinar comes with a course handbook developed by the expert presenter. This not only includes all slide materials, but also additional research and reading that couldn't be conveyed during the 90-minute session.

We strive to keep our webinars engaging and packed with actionable advice that can be put to use immediately. These handbooks help us provide further detailed information while keeping the presentation fresh.



Questions & Answers

What is a membership?

A Premium Membership enables OnDemand access and transcript tracking for all 200+ educational webinars in our expansive curriculum. One-month members gain access to three webinars, while all other levels of membership grant unlimited access. New features also include mobile webinar access and a membership community discussion forum.

Is membership individual-based or for the entire organization?

Many institutions provide this access enterprise-wide to meet their information security, risk management, compliance and fraud teams' needs. However, due to our transcript tracking feature, membership must be associated to each specific user.

What else is included besides the ability to attend unlimited webinars?

In addition to webinar access, members also have an exclusive transcript-tracking feature that monitors all educational webinars, articles, interviews and handbooks accessed. Transcripts and proof-of-attendance certificates can be printed or e-mailed directly from this system. Members also get exclusive features, such as mobile device webinar access and a membership community discussion forum, which can be used to directly communicate with peers and expert presenters.

Do I earn Continuing Professional Education (CPE) credits for the webinars I attend?

Yes. Members utilize their transcript to submit proof-of-attendance certificates to certifying associations and senior management. These certificates indicate session title, date, member name and hours earned. This easy-to-use transcript interface also allows for an organization, by category, to help drill down for each specific certification's requirements.

Can I sign up my entire group as part of the membership?

Absolutely. We have a custom offering for teams of all sizes. An increasing number of organizations are relying on us to supplement their information security, risk management, compliance and fraud educational needs. In fact, the larger the team, the more cost-effective membership becomes. Group rates are available for teams as small as two.

Can I as a manager see a report on who has attended which webinars?

Yes. Each member has the capability to e-mail their transcript to managers at any time during their membership. This easy-to-use transcript interface also allows you to organize by category to help drill down for each specific business group's requirements.

Unsure which membership option is best for you?

Contact our sales team by calling (800) 944-0401

Webinar Registration Form

Members can attend unlimited webinars for 1 year.

Attendance Method

Single Session

- Single Attendee \$295
- Multiple Attendees (Up to 5) \$695

Multiple Sessions

- Vouchers (4 pack) \$1,095
- Vouchers (8 pack) \$2,795
- Vouchers (20 pack) \$5,295

Premium Membership

- Individual \$1,995/year
- Corporate \$7,495/year
- Enterprise Call

Save up to **25%** with a group membership.
Call (800) 944-0401 to learn more.

Print and mail this form to:

Information Security Media Group
4 Independence Way, Suite 130
Princeton, NJ 08540

or fax to: (732) 875-1065.

Register Online

The fastest way to register for webinars!

ORDER TOTAL \$ _____

Customer Information

NAME _____

TITLE _____

COMPANY _____

ADDRESS _____

CITY _____ STATE _____ ZIP _____

E-MAIL _____

PHONE _____ FAX _____

Webinars to Attend (Optional)

1. _____

2. _____

3. _____

4. _____

5. _____

Payment Method

Check Enclosed (Payable to "Information Security Media Group, Corp.")

Visa AMEX MasterCard Discover Company P.O.

CARD NUMBER

EXP. (MM/YY)

SIGNATURE _____

 BANK INFO SECURITY®  Just for Credit Unions CU INFO SECURITY®  GOV INFO SECURITY®  HEALTHCARE INFO SECURITY®

 infoRisk
TODAY

 CAREERS INFO SECURITY®

 Data Breach
Prevention, Response, Notification. TODAY

 iSMG
INFORMATION SECURITY
MEDIA GROUP

4 Independence Way • Princeton, NJ • 08540 • www.ismgcorp.com