

HEALTHCARE INFO SECURITY®

Course Catalog

Information Security | Risk Management | Compliance | Fraud

ISMG INFORMATION SECURITY MEDIA GROUP

With hundreds of major health data breaches grabbing headlines, healthcare organizations of all types and sizes are ramping up efforts to keep patient information secure and earn public trust.

Tom Field

Faced with the threat of hefty federal penalties for failure to adequately protect sensitive information, hospitals, clinics and health plans are updating their risk assessments and pondering what security technology investments make the most sense.

At Information Security Media Group, we've assembled a broad suite of webinar training programs to give you the latest information you need to make the right risk management and compliance decisions. 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

Course Descriptions

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

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 healthcare organizations: information security, risk management, fraud, and compliance.

As industry trends change, new threats emerge, and regulations expand, so 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 Dept. of Health & Human Services, authorities on risk management from NIST, and c-level information security professionals at healthcare organizations ranging from national to community healthcare providers.

A 130+ 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, Dept. of Health & Human Services HIPAA Audits: How to Prepare, are not a simple overview of the regulation. Expert Mac McMillan provides valuable direct visibility into how these audits are conducted, the expectations of the auditors, the document request requirements and staff preparation for successful interaction with auditors. 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 SAIC, HIMSS, AHIMA, and several top healthcare organizations, 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 healthcare 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 protecting clinical data, secure access to electronic health records, patient privacy, and HIPAA & HITECH 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 healthcare 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 speaks 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 healthcare 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.

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

The HealthcareInfoSecurity Board of Advisers is a unique, active group of industry leaders who guide our coverage of healthcare 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 healthcare organizations of all sizes, to recognized industry thought-leaders from associations and analyst firms, HealthcareInfoSecurity's Board of Advisers is an unparalleled brain trust. Their experience and insight greatly shape our educational offerings.

Dixie Baker, Ph.D.
Former SVP & Technical Fellow, SAIC

Baker has worked in high-assurance computing and information protection for more than 30 years; for the past 16 years, she has applied her skills to health challenges. In 2009, she became a federal adviser for the Health Information Technology Standards Committee and was chair of the Privacy and Security Workgroup of that Committee.

Charles Christian
CIO, Good Samaritan Hospital, Vincennes, Ind.

Charles Christian, CIO of Good Samaritan Hospital in Vincennes, Ind., is the former chairman of the Healthcare Information and Management Systems Society.

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.

Lisa Gallagher
Senior Director, HIMSS

Lisa Gallagher is the senior director, privacy and security, for the Healthcare Information and Management Systems Society, Chicago.

Richard Jankowski
ISO, Memorial Sloan-Kettering Cancer Center, NY

Prior to Sloan-Kettering, Richard was an engineer at Lucent Technologies. Richard served in the U.S. Marine Corps. as an infantry rifleman with responsibilities as a scout and rescue swimmer and has served in combat during Operation Restore Hope in Somalia. He holds a Master of Science in Computer Science from the Stevens Institute of Technology in Hoboken, NJ.

Christopher Paidhrin
IT Security Compliance Officer, PeaceHealth Southwest Medical Center

Paidhrin has worked for many years 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 recognition, nominations and awards for IT service excellence, and he has presented at numerous industry events.

Dan Rode
VP, Policy and Government Relations, American Health Information Management Association, Chicago, IL

Dan Rode, vice president for policy and government relations at the American Health Information Management Association, is a leader in the standards arena. He was among those who drafted the data standards that ultimately were incorporated in the Health Insurance Portability and Accountability Act.

Adam Greene
Partner, Davis Wright Tremaine LLC

Greene was formerly senior health information tech and privacy specialist at the Dept. of Health and Human Services' Office for Civil Rights. He played a significant role in administering and enforcing the HIPAA privacy and security rules as well as the HIPAA breach notification rule and was responsible for determining how HIPAA rules apply to emerging health information technologies.

Webinar Presenters

A who's who of healthcare and security leaders.

We work with actual practitioners at healthcare 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 healthcare 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 healthcare organizations 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 organization. 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, 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

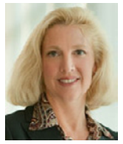
Investigator, New York State Police

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, PeaceHealth Southwest 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

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 Category Matrix

HEALTHCARE INFO SECURITY®

#	Course Title	ID		Breach Notification	Business Associates	Business Continuity	EHRs	Fraud	Governance	HIPAA/ HITECH	Privacy	Technology
1	5 Best Practices for Disaster Recovery and HIPAA Compliance	275				●				●		○
2	6 Tips for Successful EHR Implementation	273		○			●					○
3	Business Continuity for Hospitals	234				●			○			
4	Cloud Computing in Healthcare: Key Security Issues	200					○		○	○	○	●
5	Complying with Healthcare Data Security Mandates & Privacy Laws	240		○			○			●		●
6	Dept. of Health & Human Services HIPAA Audits: How to Prepare	280						○		●		○
7	Dept. of Health & Human Srvcs: Privacy and Security Strategies for Smaller Healthcare Entities	286								●	○	
8	Detecting and Preventing Health Data Breaches	209										●
9	Developing an Effective Security Strategy for Health Data	228							○		○	●
10	Email Security Requirements for Healthcare Providers: HIPAA & Beyond	180		●						○	●	
11	Encryption as Part of a Broader 'Safe Harbor' Strategy	201							○	○	○	●
12	Healthcare Information Security Today: 2011 Survey Executive Summary	254										
13	HIPAA & HITECH Updates: The Vendors' Guide to the Security Essentials	186			○		○		○	●	●	
14	HIPAA and HITECH Enforcement: How to Secure Health Information	174		●						●		
15	HIPAA Modifications & HITECH Rules: A Guide to the Security Essentials	184			○		○		○	●	●	
16	HITECH Tips: Using EHR Security Functions for Protecting Patient Information	202					●				○	●
17	How to Prepare Your Organization for a HIPAA Security Risk Analysis	224		○	●		○			●	○	○
18	Insider Threats in Healthcare: Protecting Your Institution	203		○			○		●			
19	IT Security Risk Analysis for Meaningful Use: What We've Learned	278					●		○	○		
20	Managing Business Associates: Practical Guidance	235		○	●					○		
21	Mobile Devices in Healthcare: Essential Security	198					○				○	●
22	Mobile Technology: How to Mitigate the Risks	256					○			○		●
23	Password Security in the Windows Healthcare Enterprise	197					○					●
24	PCI: What Healthcare Organizations Need to Know	218			○			○	○	●		●
25	Risk Assessment for EHR Meaningful Use: Methodologies and Processes	195			○		●		○	●	●	
26	Risk Assessments: Protecting Your Organization from the Next Major Breach	221		●			○		○	●		
27	Risk Management Framework: Learn from NIST	255		○				●				
28	Social Media in Healthcare: A Guide to Minimizing Your Risk	199							○	○	○	●
29	U.S. Dept. of Justice on Payment Card Fraud Trends & Threats	169					●				●	

● = Primary Category ○ = Secondary Category

THE POWER OF COMMUNITY

Gain access to a range of additional courses from

BANK INFO SECURITY® & GOV INFO SECURITY®

SEE THE COURSES ON THE NEXT PAGE »

Course Category Matrix

BANK INFO SECURITY®

#	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	Assessing Encryption Standards for Financial Institutions	130							○		●	○
6	ATM Skimming Fraud: Banking's Growing Billion Dollar Electronic Crime	258					●				○	
7	Automating Security Controls Within Government Information Systems	160						●	○		●	
8	Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks	87						●		○		
9	Beyond Heartland: How to Prevent Breaches of Security and Trust	129					●			○	○	
10	Beyond Phishing - The Growing Crimeware Threat	29					●			○		
11	Board Responsibilities for IT Risk Management: Building Blocks for a Secure System	11						●				
12	Breach Response: Developing an Effective Communications Strategy	288					●	○		○		
13	Business Continuity Risk Assessment & Resource Allocation	96				●		○	○			
14	Business Impact Analysis — How to Get it Right	95				●		○				
15	BYOD: Manage the Risks and Opportunities	266					○			○	●	
16	Continuous Monitoring: How to Get Past the Complexity	291		○			○		●		●	
17	Creating a Culture of Security - Top 10 Elements of an Information Security Program	150		○				●				
18	Data Protection and Incident Response	162						●		●		
19	Data Protection: The Dirty Little Secret	208							○		●	
20	Defending Against The Insider Threat	67					●	○		○		
21	Developing an Effective Information Security Awareness Training Program - Getting the Word Out	20		○				●				
22	Electronic Evidence & e-Discovery: What You Need to Know & Protect	158		●				○	○			
23	Evolving Threats, Innovative Responses - How to Effectively Combat Spear-Phishing & Data Leaks	293					●				○	
24	Fighting Fraud: Stop Social Engineers in Their Tracks	89		○				●		○		
25	Fraud Prevention: Protect Your Customers and Your Institution from Web Vulnerabilities	177					●	○			●	
26	Hacktivism: How to Respond	287					●	○			○	
27	How to Develop & Maintain Information Security Policies & Procedures	135		○				●	○			
28	How to Prepare for Your First Identity Theft Red Flags Rule Exam	113		●					○	●		
29	How to Prevent Data Leakage from Compromising Your Company's Security	50						●				
30	How to Prevent Security Breaches Through Effective Management and Control of USB Devices	148						○	○		●	
31	How to Use Your Mobile Phone for Free Two-Factor Authentication	58									●	
32	ID Theft Red Flags FAQ's: A Guide to the 'Gotchas' of Compliance	142		●			○			●		
33	Identity Theft: How to Respond to the New National Crisis	155					●			●		

● = Primary Category ○ = Secondary Category

Course Category Matrix

BANK INFO SECURITY®

#	Course Title	ID		Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
34	Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication	81		●						○		○
35	Incident Response: How to React to Payment Card Fraud	144					●			○		○
36	Information Security for Management – What Your Senior Leaders Need to Know	137		○				●				
37	Innovative Authentication Process Provides the Ultimate Security for Online Banking	165		○			○				●	
38	Insider Fraud - Profiling & Prevention	35					●			○		
39	Insider Threat: 3 Faces of Risk	296					●				○	
40	Insider Threat: Defend Your Enterprise	66						●				
41	Insider Threats - Safeguarding Financial Enterprise Information Assets	85					●					
42	Insider Threats in Healthcare: Protecting Your Institution	203		○			○		●			
43	Integrating Risk Management with Business Strategy	176						●				
44	Investigations, Computer Forensics and e-Discovery - A Primer for Every Banking Institution	65		●					○	○		
45	Key Considerations for Business Resiliency	151						●				
46	Legal Considerations About Cloud Computing	159		○				○			●	○
47	Maintaining Compliance with the Gramm-Leach-Bliley Act Section 501b	19		●					○			
48	Malware, Crimeware, and Phishing - An In Depth Look at Threats, Defenses	30					○				●	
49	Malware, Phishing & Mobile Security: Trending Threats	215		●							○	
50	Managing Change: The Must-Have Skills for Security Professionals	283							●	●	○	
51	Managing Shared Passwords for Super-User Accounts	170						○			●	
52	Man-in-the-Browser Attacks: Strategies to Fight the Latest Round in Online Fraud	178					●			○	○	
53	Massachusetts Privacy Law: A Guide to Understanding and Complying with this New Data Protection Standard	132		●						●		○
54	Mobile Banking: Emerging Threats, Vulnerabilities and Counter-Measures	285					○				●	
55	Mobile Technology: How to Mitigate the Risks	256						○			●	
56	Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices	264		○			○	○			●	
57	Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?	72				○		●	○	●		
58	Pandemic Planning & Response Techniques	77		○		●						
59	PCI Compliance: Tips, Tricks & Emerging Technologies	212		●							○	
60	Power Systems: How to Prevent Unauthorized Transactions	190		○					○		●	
61	Practical User Authentication Strategies for Government Agencies	166					○		○		●	
62	Preparing Your Institution for an IT Audit	26							●			
63	Preventing Phone Fraud with Voice Biometric Authentication	36					●				○	
64	Preventing Unauthorized Access To Your Institution's Data	119							○		●	
65	Proactive IT Risk Assessment Strategies	140		○				●				
66	Protect IBM i Data from FTP, ODBC and Remote Command	272									●	

● = Primary Category ○ = Secondary Category

Course Category Matrix

BANK INFO SECURITY®

#	Course Title	ID		Compliance	BSA/AML	BCP	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt.
67	Protecting CUI: Federal Best Practices for Email Security, Archiving and Data Loss Prevention	185		●					○		●	
68	Protecting the Exchange of Sensitive Customer Data with Your Vendors	100								●	○	●
69	Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors	97		●								○
70	Risk Assessment Framework for Online Channel: Learn from an Expert	261		●			○	○				
71	Risk Management: New Strategies for Employee Screening	282		●			○	○				●
72	Risk Management: Third-Party Breach Impact & Preparedness	289										●
73	Securing Your Email Infrastructure	141		○						○	●	
74	Security Risks of Unified Communications: Social Media & Web 2.0	146									●	
75	Social Networking: Is Your Institution Ready for the Risks?	145								○	●	
76	Sound Risk Management Practices: Enterprise-wide Encryption and Key Management	257							○		●	
77	Testing Security Controls at a Banking Institution: Learn from the Experts	56		○					○		●	
78	The Dirty Little Secret About Network Security	204		●				○			●	
79	The Fraud Dilemma: How to Prioritize Anti-Fraud Investments	267					●				○	
80	The Great Application Security Debate: Static vs. Dynamic vs. Manual Penetration Testing	268		○							●	
81	The Identity Enabled Network: The Future of Secure Cyberspace	163						○			●	
82	The Identity Management Challenge for Financial Institutions	48					○			●	●	
83	The Reality of Cyberattacks: Emerging Solutions for Today's Threats	179									●	
84	The State of Print Security 2012	**284**						○		○	●	
85	Threat Detection, Compliance & Incident Response	**181**		●				○				
86	Time: The Hidden Risks - How to Create Compliant Time Practices	**161**		○							●	
87	Top 20 Critical Controls to Ensure Painless FISMA Compliance	167		○				●				
88	Top 5 Reports IT Auditors Request	214		○				○	●			
89	Top IT Compliance Challenges: Who's Touching Your Data and What Are They Doing With It?	73		●						●	○	○
90	Using the NIST HIPAA Security Rule Toolkit for Risk Assessments	262		○				●			○	
91	Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks	98		○					○			●
92	Vendor Management Part II: Assessing Vendors - the Do's and Don'ts of Choosing a Third-Party Service Provider	104		○					○	○		●
93	You & Your Vendors: How to Best Secure Data Exchange	88		○							○	●

● = Primary Category ○ = Secondary Category

Education OnDemand

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

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 organizations, 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.

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.

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

2 Attend

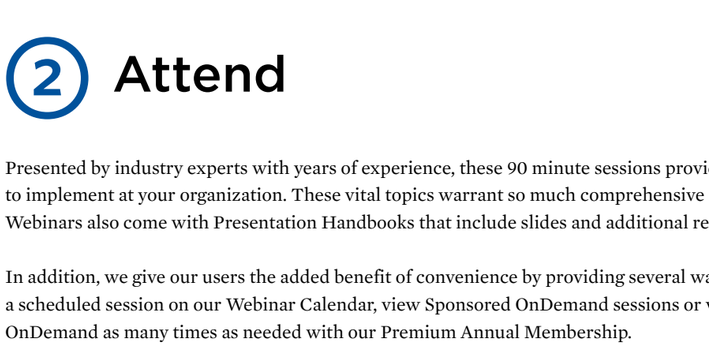
Presented by industry experts with years of experience, these 90 minute sessions provide in-depth actionable advice to implement at your organization. These vital topics warrant so much comprehensive education that our Premium Webinars also come with Presentation Handbooks that include slides and additional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

HIPAA/HITECH Compliance Track

Government regulation is a key motivator in healthcare organizations 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, allowing organizations to confidently address these regulations and take immediate steps towards compliance. Attend webinars in this track to gain the necessary expert insight into exactly what is mandated in the HIPAA and HITECH regulations.

FEATURED

COMP184

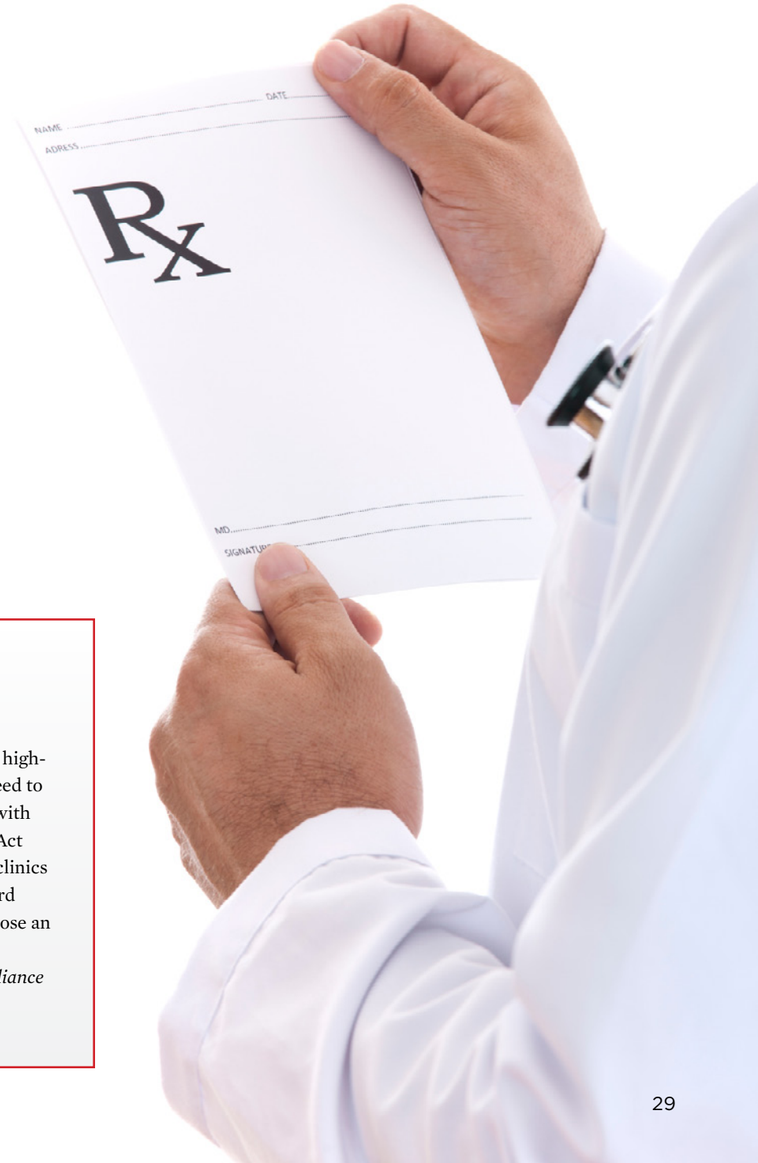
HIPAA Modifications & HITECH Rules: A Guide to the Security Essentials

Sorting through all the complex security details in three new federal regulations is challenging – but essential. Experts will help you set security priorities by pinpointing the key provisions of the HIPAA privacy and security rules.
Presented by Tom Walsh, CISSP and Kate Borten, CISSP, CISM

Course Title	ID
Business Continuity for Hospitals	234
Developing an Effective Security Strategy for Health Data	228
Email Security Requirements for Healthcare Providers: HIPAA & Beyond	180
Encryption as Part of a Broader 'Safe Harbor' Strategy	201
HIPAA and HITECH Enforcement: How to Secure Health Information	174
Healthcare Information Security Today: 2011 Survey Executive Summary	254
HIPAA & HITECH Updates: The Vendors' Guide to the Security Essentials	186
HITECH Tips: Using EHR Security Functions for Protecting Patient Information	202
How to Prepare Your Organization for a HIPAA Security Risk Analysis	224
Insider Threats in Healthcare: Protecting Your Institution	203
Managing Business Associates: Practical Guidance	235
Protecting Electronic Health Records (EHRs): The Benefits Behind Tokenization for Healthcare Organizations	240
Risk Assessments: Protecting Your Organization from the Next Major Breach	221

Course Title	ID
Risk Assessment for EHR Meaningful Use: Methodologies and Processes	195
Risk Management Framework: Learn from NIST	255
HIPAA Modifications & HITECH Rules: A Guide to the Security Essentials	184
Detecting and Preventing Health Data Breaches	209
Social Media in Healthcare: A Guide to Minimizing Your Risk	199

These in-depth sessions prepare you for every aspect of becoming compliant with HIPAA and HITECH, including step-by-step procedures and common missteps.



FEATURED

COMP203

Insider Threats in Healthcare: Protecting Your Institution

The Mayo Clinic recently fired six employees for inappropriately accessing one patient's records. The high-profile announcement helped call attention to the need to address internal threats and set policies for dealing with privacy violations as part of a HIPAA and HITECH Act compliance strategy. Until now, many hospitals and clinics have focused on external threats, taking steps to guard against security breaches. But internal threats may pose an even greater risk.
Presented by Christopher Paidhrin, IT Security Compliance Officer, PeaceHealth Southwest Medical Center

Governance Track

Senior leaders at healthcare organizations 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 organization'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

GOV255

Risk Management Framework: Learn from NIST

From heightened risks to increased regulations, senior leaders at all levels are pressured to improve their organizations' risk management capabilities. 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.

Presented by Ron Ross, Sr. Computer Scientist & Information Security Researcher, NIST

Course Title	ID
Business Continuity for Hospitals	234
Cloud Computing in Healthcare: Key Security Issues	200
Developing an Effective Security Strategy for Health Data	228
Encryption as Part of a Broader 'Safe Harbor' Strategy	201
HIPAA and HITECH Enforcement: How to Secure Health Information	174
Healthcare Information Security Today: 2011 Survey Executive Summary	254
HIPAA & HITECH Updates: The Vendors' Guide to the Security Essentials	186
HIPAA Modifications & HITECH Rules: A Guide to the Security Essentials	184
How to Prepare Your Organization for a HIPAA Security Risk Analysis	224
Insider Threats in Healthcare: Protecting Your Institution	203
Managing Business Associates: Practical Guidance	235
Mobile Devices in Healthcare: Essential Security	198
Mobile Technology: How to Mitigate the Risks	256
Risk Assessments: Protecting Your Organization from the Next Major Breach	221
Information Security for Management – What Your Senior Leaders Need to Know	137
Risk Assessment for EHR Meaningful Use: Methodologies and Processes	195
Detecting and Preventing Health Data Breaches	209
Social Media in Healthcare: A Guide to Minimizing Your Risk	199
Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks	87

Course Title	ID
Board Responsibilities for IT Risk Management: Building Blocks for a Secure System	11
Business Impact Analysis — How to Get it Right	95
Creating a Culture of Security - Top 10 Elements of an Information Security Program	150
Electronic Evidence & e-Discovery: What You Need to Know & Protect	158
Developing an Effective Information Security Awareness Training Program - Getting the Word Out	20
Risk Management Framework: Learn from NIST	255
Insider Fraud - Profiling & Prevention	35
Key Considerations for Business Resiliency	151
Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?	72
Pandemic Planning & Response Techniques	77
Fighting Fraud: Stop Social Engineers in Their Tracks	89

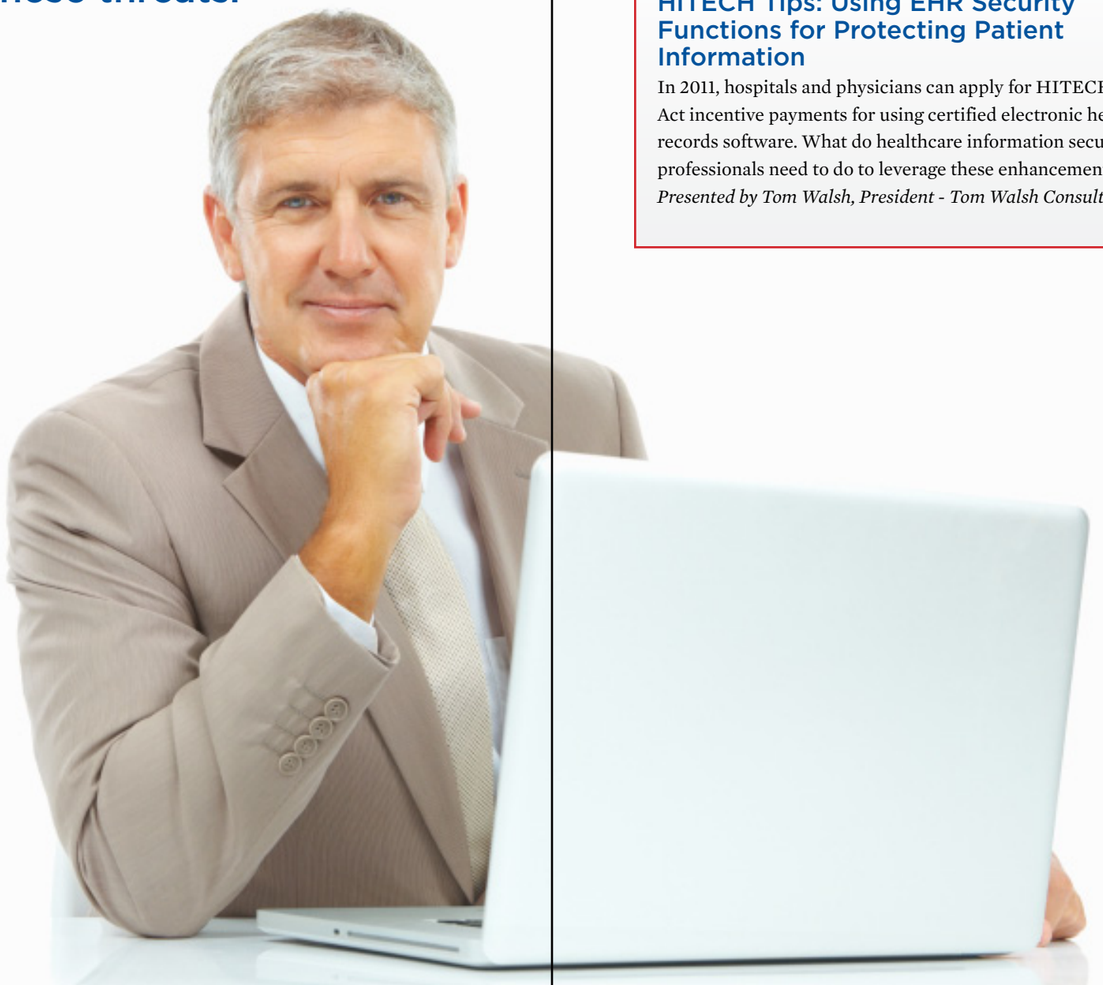
Secure healthcare organizations begin with security-minded leaders.

Breach Prevention & Response Track

In today's threat landscape, having a plan in place for breach prevention and incident response is a necessity. Healthcare organizations must stay ahead of emerging threats and new technology trends and know how to efficiently respond should an incident occur. Planning is a concerted effort involving many teams and departments including C-Suite and operations professionals, IT departments, and even marketing and legal teams. This track is developed to ensure your organization is prepared before it's time to put your plan into action.

Course Title	ID
How to Prevent Security Breaches Through Effective Management and Control of USB Devices	148
Risk Assessments: Protecting Your Organization from the Next Major Breach	221
Beyond Heartland: How to Prevent Breaches of Security and Trust	129
Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication	81
Incident Response: How to React to Payment Card Fraud	144
Pandemic Planning & Response Techniques	77
Threat Detection, Compliance & Incident Response	181
Data Protection and Incident Response	162

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



FEATURED

BR81

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

An Incident Response plan isn't just 'nice to have' for a healthcare organization - it's a must. This webinar outlines the critical components, including:

- The latest regulatory guidance on incident response;
- 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.

Presented by Kate Borten, CISSP, CISM, President - The Marblehead Group

Privacy Track

Patient privacy is a perpetual concern among healthcare organizations. However, with government's aggressive audit program to measure HIPAA and HITECH compliance and increased push for electronic health records, the issue of privacy has been brought to the forefront.

This privacy track focuses on the key factors needed to keep healthcare organizations secure and within the regulation guidelines for compliance.

FEATURED

PR202

HITECH Tips: Using EHR Security Functions for Protecting Patient Information

In 2011, hospitals and physicians can apply for HITECH Act incentive payments for using certified electronic health records software. What do healthcare information security professionals need to do to leverage these enhancements?

Presented by Tom Walsh, President - Tom Walsh Consulting

Course Title	ID
Cloud Computing in Healthcare: Key Security Issues	200
Developing an Effective Security Strategy for Health Data	228
Email Security Requirements for Healthcare Providers: HIPAA & Beyond	180
Encryption as Part of a Broader 'Safe Harbor' Strategy	201
HIPAA & HITECH Updates: The Vendors' Guide to the Security Essentials	186
HIPAA Modifications & HITECH Rules: A Guide to the Security Essentials	184
HITECH Tips: Using EHR Security Functions for Protecting Patient Information	202
How to Prepare Your Organization for a HIPAA Security Risk Analysis	224
Mobile Devices in Healthcare: Essential Security	198
Risk Assessment for EHR Meaningful Use: Methodologies and Processes	195
Social Media in Healthcare: A Guide to Minimizing Your Risk	199
Data Protection: The Dirty Little Secret	208
Electronic Evidence & e-Discovery: What You Need to Know & Protect	158
Massachusetts Privacy Law: A Guide to Understanding and Complying with this New Data Protection Standard	132
Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?	72

Patient privacy is a requisite for any successful compliance initiative.

Business Associates Track

When a healthcare organization utilizes a business associate, that associate's vulnerabilities become the organization's vulnerabilities. To ensure your patients' records are fully protected from threats, an in-depth business associate management program must be established.

Webinars in this track are dedicated to providing you a framework to assess associates, including what questions to ask, what should be included in agreements, and how to best secure sensitive information.

FEATURED

BA235

Managing Business Associates: Practical Guidance

Developing good relationships with business associates is an essential component of an information security strategy. It also helps to ensure compliance with HIPAA and the HITECH Act and to avoid breaches.

Presented by Kate Borten, CISSP, CISM, President - The Marblehead Group

Course Title	ID
HIPAA & HITECH Updates: The Vendors' Guide to the Security Essentials	186
HIPAA Modifications & HITECH Rules: A Guide to the Security Essentials	184
How to Prepare Your Organization for a HIPAA Security Risk Analysis	224
PCI: What Healthcare Organizations Need to Know	218
Managing Business Associates: Practical Guidance	235
How Well Do You Know Your Vendors?	13
Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication	81
Protecting the Exchange of Sensitive Customer Data with Your Vendors	100
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
You & Your Vendors: How to Best Secure Data Exchange	88

Don't allow business associates' security blunders to become your organization's.

Mobile, Payments Security and Emerging Threats Track

In many industries it is customers who push the trends in necessary offerings an organization must provide to remain competitive. With the ubiquitous adoption of smartphones and tablets, now patients are quickly defining a new benchmark for healthcare organizations. This track is custom built for the healthcare industry to ensure the organizations are prepared for specific trends and emerging threats that will affect them.

FEATURED

MOB198

Mobile Devices in Healthcare: Essential Security

A majority of the healthcare information breaches reported to federal authorities so far have involved the theft or loss of mobile devices. To help make sure your organization isn't added to the list, register for this webinar to hear an experienced security officer's Top 10 Tips for securing mobile devices.

Presented by Terrell Herzig, Information Security Officer, UAB, Birmingham, AL

Course Title	ID
Mobile Technology: How to Mitigate the Risks	256
Malware, Phishing & Mobile Security: Trending Threats	215
How to Use Your Mobile Phone for Free Two-Factor Authentication	58
U.S. Dept. of Justice on Payment Card Fraud Trends & Threats	169
Incident Response: How to React to Payment Card Fraud	144
Beyond Heartland: How to Prevent Breaches of Security and Trust	129
Beyond Phishing - The Growing Crimeware Threat	29
Mobile Devices in Healthcare: Essential Security	198
PCI Compliance: Tips, Tricks & Emerging Technologies	212
PCI: What Healthcare Organizations Need to Know	218
Insider Threats in Healthcare: Protecting Your Institution	203
Social Media in Healthcare: A Guide to Minimizing Your Risk	199

Course Descriptions

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

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.healthcareinfosecurity.com/webinars.php?webinarID=174

221

Risk Assessments: Protecting Your Organization from the Next Major Breach

Overview

Organizations were embarrassed by the WikiLeaks episode that resulted in the unauthorized release of more than 250,000 sensitive and classified government and financial documents. This leak - and the threat of others in both the public and private sectors - forces information security leaders to ask: What more can we do to protect access, portability and privacy of critical data?

Join an expert panel for a discussion on:

- Risk assessments, corrective actions and incident response essentials for WikiLeaks-type breaches;
- Strategies to control users' access to private information;
- Tools and techniques for preventing data loss.

Background

Late in 2010, the group known as WikiLeaks released thousands of sensitive government documents obtained by insiders who had too much access to critical data. Around the same time, the group threatened to release even more documents that potentially could embarrass public and private sector entities, including Bank of America.

In this session, you'll hear from a U.S. government CISO, a noted security expert and one of the industry's top security solutions providers, as they discuss:

- The data exposure risks to organizations of all types;
- Lessons learned from WikiLeaks;
- Systems and processes that can help ensure greater security against the new insider threat.

Presented By

Patrick Howard, Chief Information Security Officer, Nuclear Regulatory Commission

Robert Hamilton, Senior Product Marketing Manager - Data Loss Prevention, Symantec

Eric Cole, Security Expert, SANS Institute Faculty Fellow

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=221

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.healthcareinfosecurity.com/webinars.php?webinarID=180

235

Managing Business Associates: Practical Guidance

Overview

Developing good relationships with business associates is an essential component of an information security strategy. It also helps to ensure compliance with HIPAA and the HITECH Act and to avoid breaches. Join us for this webinar, where a leading health information security expert will address such issues as:

- What are the most important questions to ask business associates about their privacy and security practices?
- What provisions are essential to include in business associate agreements?
- How does business associate management differ based on the type of vendor involved?

Background

Developing and maintaining good relationships with business associates is an essential component of successful information security and privacy programs. Although business associates are entrusted with protected health information, patients rely on healthcare organizations, including hospitals, clinics and health plans, to safeguard their data. That's why it's essential that these organizations work closely with their business partners to protect patient information, prevent breaches and ensure compliance with HIPAA and the HITECH Act.

In this exclusive session, a leading security expert will provide strategies for working closely with business associates to reduce the risk of breaches. You will learn:

- Questions to ask prospective and current business associates about their privacy and security practices;
- Tips for all the details to include in business associate agreements - including HIPAA and HITECH compliance - and how and when to update these details;
- How to use different strategies depending on a business associate's size and type;
- Techniques for strengthening communication, and why it's critical;
- Ways to work with business associates to comply with the proposed accounting of disclosures rule, which calls for providing patients with access reports.

Presented By

Kate Borten, CISSP, CISM, President - The Marblehead Group

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=235

224

How to Prepare Your Organization for a HIPAA Security Risk Analysis

Overview

Learn how to prepare your organization for a HIPAA security risk analysis. In this webinar, we'll share pro-active steps that you can take to speed the process, improve the outcome and lower the potential mitigation costs of performing a HIPAA risk analysis. Our objective is to help you achieve meaningful use and, most importantly, safeguard electronic protected health information.

Topics covered:

- What is a HIPAA risk analysis;
- How it fits into your overall information security program;
- Key preparation steps;
- How to avoid potential pitfalls.

Background

The healthcare IT landscape is changing fast. Through government-sponsored incentive payments, the 2009 HITECH Act promotes the adoption and "meaningful use" of healthcare IT. Accelerating the migration to electronic health records (EHR) enables greater access to and sharing of patient health information among providers, patients, payers and employees. With increased access and data sharing comes increased risk.

This webinar will help you understand how a HIPAA security risk analysis is conducted and why it's a mandatory requirement of achieving meaningful use. Then, to better prepare your organization for the assessment, you'll learn a few pro-active steps to help you avoid common pitfalls and maximize the value of your investment. You'll also understand how a HIPAA security risk analysis fits into your overall information security program so that you cannot only achieve compliance but also begin a process of continuous and durable improvements in IT security.

Topics covered include:

- HITECH Act and meaningful use attestation;
- What constitutes a HIPAA security risk analysis;
- Advance preparations: How can I maximize my ROI;
- Avoiding potential pitfalls;
- Beyond compliance to meaningful healthcare IT security.

Presented By

John Abraham, Founder & Chief Security Evangelist, Redspin

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=224

275

5 Best Practices for Disaster Recovery and HIPAA Compliance

Overview

Choosing a disaster recovery solution to support your healthcare organization is a critical step in becoming HIPAA and HITECH compliant. Choose wrong, and you can invite unnecessary downtime and data loss. Choose right, and you can be a hero.

Attend this webinar to learn:

- How HIPAA and HITECH requirements impact the need for DR solution;
- Pros and cons between various DR solution methodologies;
- 5 best practices for a successful DR program.

Background

Fact: 2.5 Million Healthcare facilities must become HIPAA compliant by 2015.

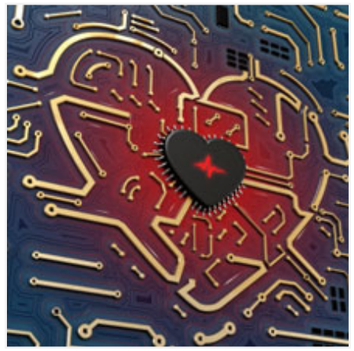
The primary goal of any healthcare provider is providing healthcare on demand to a wide array of patients. An equally important goal is the ability to financially sustain the practice and its employees. Finally, there is the goal of protecting patient's records which is now government mandated by HIPAA regulations.

Chances are, choosing a disaster recovery (DR) solution to support your healthcare organization is a critical step in becoming HIPAA and HITECH compliant, as well as improving business continuity and security. Choose the wrong DR solution can cause unnecessary downtime and dataloss. Choose the right DR solution and you become a hero to your organization...and to your bottom line by reducing your total cost of ownership and putting your HIT dollars to good use.

Join this webinar to help steer you disaster recovery and compliance in the right direction.

HEROware, a leader in business continuity, HIPAA and HITECH compliant appliance-based DR solutions, and Kaseya, the leader in IT service solutions, will discuss details on how to navigate this complex process, including:

- How HIPAA and HITECH requirements impact the need for DR solutions
- Implementing 5 best practices for a successful DR program
- Pros and cons between various DR solution methodologies



You'll also hear from HEROware/Kaseya customer, Dan Gross, as he discusses his real-life DR implementation and steps to success. Don't miss this opportunity to leverage these lessons learned for your healthcare organization!

Presented by

Fred Mayne, Co-Founder & VP - Sales/Marketing, HEROware

Jeff Keyes, Senior Product Marketing Manager, Kaseya

Dan Gross, ServiCorps Systems

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=275

234

Business Continuity for Hospitals

Overview

As the healthcare industry moves from paper to electronic records, it must transition its disaster recovery and emergency operations processes. But what are the essential elements of a comprehensive 21st century business continuity plan for hospitals?

In this webinar, the chief information security officer at a hospital that coped with tornadoes that ravaged Alabama offers insights on such topics as:

- Why it makes sense to use a new approach that relies on co-located real-time operations;
- Lessons learned from the Alabama tornado experience;
- How to test a disaster recovery plan.

Background

Hospitals store massive amounts of information, ranging from diagnostic images to electronic health records, in large racks of file servers and mainframes within their data centers.

Every data center is subject to interruptions of service, both large and small. Such interruptions may involve equipment failures, utility interruptions, power outages, fires, floods or a major disaster that impacts an entire community. And hospitals cannot afford outages or loss of connectivity when patients' lives are at stake.

Organizations that rely on the restoration of large data transfers from tape may find that strategy doesn't work with the high volumes of data generated by electronic health records and other applications. Instead, they should look to continuous operations with replication of data to remotely located sites, a strategy known as "co-location."

In this session, Terrell Herzig, information security officer at UAB Medicine, will provide timely, practical tips. You'll get a:

- Detailed explanation of the "co-location" strategy;
- Description of why every hospital needs a disaster recovery plan that can be activated in the event of a communitywide disaster;
- Review of important lessons learned in coping with the Alabama tornadoes, including the importance of cross-training staff;
- Guide to how to set recovery objectives;
- Explanation of the most important infrastructure considerations;
- Summary of advice on how to test a business continuity plan.

Presented by

Terrell Herzig, CISO, UAB Medicine

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=234

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.healthcareinfosecurity.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.healthcareinfosecurity.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 ensure 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.healthcareinfosecurity.com/webinars.php?webinarID=77

275

5 Best Practices for Disaster Recovery and HIPAA Compliance

Overview

Choosing a disaster recovery solution to support your healthcare organization is a critical step in becoming HIPAA and HITECH compliant. Choose wrong, and you can invite unnecessary downtime and data loss. Choose right, and you can be a hero.

Attend this webinar to learn:

- How HIPAA and HITECH requirements impact the need for DR solutions;
- Pros and cons between various DR solution methodologies;
- 5 best practices for a successful DR program.

Background

Fact: 2.5 million healthcare facilities must become HIPAA compliant by 2015.

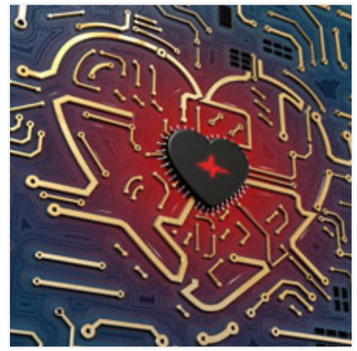
The primary goal of any healthcare provider is providing healthcare on demand to a wide array of patients. An equally important goal is the ability to financially sustain the practice and its employees. Finally, there is the goal of protecting patient's records which is now government mandated by HIPAA regulations.

Chances are, choosing a disaster recovery (DR) solution to support your healthcare organization is a critical step in becoming HIPAA and HITECH compliant, as well as improving business continuity and security. Choosing the wrong DR solution can cause unnecessary downtime and dataloss. Choose the right DR solution and you become a hero to your organization...and to your bottom line by reducing your total cost of ownership and putting your HIT dollars to good use.

Join this webinar to help steer you disaster recovery and compliance in the right direction.

HEROware, a leader in business continuity, HIPAA and HITECH compliant appliance-based DR solutions, and Kaseya, the leader in IT service solutions, will discuss details on how to navigate this complex process, including:

- How HIPAA and HITECH requirements impact the need for DR solutions;
- Implementing 5 best practices for a successful DR program;
- Pros and cons between various DR solution methodologies.



You'll also hear from HEROware/Kaseya customer Dan Gross as he discusses his real-life DR implementation and steps to success. Don't miss this opportunity to leverage these lessons learned for your healthcare organization.

Presented by

Fred Mayne, Co-Founder & VP - Sales/Marketing, HEROware

Jeff Keyes, Senior Product Marketing Manager, Kaseya

Dan Gross, ServiCorps Systems

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=275

240

Complying with Healthcare Data Security Mandates & Privacy Laws

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.healthcareinfosecurity.com/webinars.php?webinarID=240

280

Dept. of Health & Human Services HIPAA Audits: How to Prepare

Overview

A good way to prepare for federal HIPAA compliance audits is to learn from the experiences of the first organizations audited earlier this year.

This webinar will feature timely insights from a consultant who observed first-hand an audit at a hospital that was one of the 20 initial sites audited under the Department of Health and Human Services' Office for Civil Rights' new program. Another 95 sites will be audited by year's end, and most have yet to be notified.

Join us for this exclusive session, when you'll gain a clear understanding of:

- The audit process and protocol and how to prepare for the experience;
- The level of rigor in the audit process and the expectations of the auditors;
- The essential steps to take to prepare staff, including insights on how to successfully interact with the auditors.

Background

The HITECH Act called for HIPAA compliance audits as part of an effort to help ensure compliance with its privacy and security provisions. The HHS Office for Civil Rights has completed the first 20 pilot audits, and it plans to complete another 95 by the end of this year.

Those to be audited will be notified in phases in months ahead. How can you help ensure your organization is well-prepared if it's selected? By learning from the experiences of those who've been through the audit experience.

This webinar will feature timely insights from an experienced consultant who aided a client with its audit, from start to finish.

The protocol for these assessments presents a rigorous audit experience that emphasizes the need for readiness, consultant Mac McMillan stresses.

McMillan's experience advising a client who was audited provided valuable direct visibility into how these audits are conducted, the expectations of the auditors and the process. This session is designed to chronicle that experience and provide insights into how to improve your readiness posture.

In this webinar, you'll learn:

- What the audit process looks like and what to expect;
- How to prepare for the document request requirements;
- How to prepare your staff for successful interaction with the auditors;
- How to prepare all your departments for the audit process;
- How to review your information security program to understand weaknesses;
- How to prepare your response.

Presented By

Mac McMillan, Co-Founder & CEO, CynergisTek Inc.

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=280

286

Dept. of Health & Human Services: Privacy and Security Strategies for Smaller Healthcare Entities

Overview

For small and midsize hospitals, clinics and business associates with limited resources, developing an effective privacy and security strategy can be difficult. Federal regulators recently issued new guidance tailored for these organizations. But putting that guidance into action is challenging.

In this webinar, two security experts will sort through the latest guidance from the Department of Health and Human Services and provide a roadmap for conducting a successful risk assessment and building an effective privacy and security strategy.

Our speakers will:

- Describe how federal guidance on risk assessments has changed - and what that means for your organization;
- Review privacy and security requirements under HIPAA and the HITECH Act electronic health record incentive program;
- Describe how to address the biggest compliance challenges for smaller organizations.

Background

Many small and midsize hospitals and clinics are ramping up their privacy and security efforts as they implement electronic health records. Faced with limited resources and expertise, conducting a risk assessment and building a solid strategy for protecting patient information is challenging.

To help these organizations, the Department of Health and Human Services recently released a "Guide to Privacy and Security of Health Information" that provides comprehensive guidance on a variety of issues. For example, the guide offers insights on conducting risk assessments to comply with the requirements of the HITECH electronic health record incentive program as well as HIPAA.

This 47-page document is both comprehensive and extensively referenced. But extracting relevant information from the guide and putting it to use is a formidable task.

In this webinar, two experienced information security and privacy consultants will sort through the latest advice from HHS and provide insights based on their real-world experience on how

smaller organizations can make the right moves to protect patient information.

In this webinar, you'll get tips on how to:

- Interpret the latest federal guidance on risk assessments;
- Carry out a risk assessment on a tight budget;
- Comply with the privacy and security requirements under HIPAA and the HITECH Act electronic health record incentive program;
- Develop an effective plan for training staff on privacy and security issues;
- Weigh the risks and rewards of attesting to compliance with the HITECH EHR incentive program's "meaningful use" requirements;
- Understand the effects of information security risks on patients and providers alike;
- Learn why a "checklist" approach to privacy and security compliance is inadequate as well as how to guard against following other bad advice.

Presented By

Robert Peterson, CTO, ACR 2 Solutions

Rebecca Herold, CEO, The Privacy Professor

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=286

186

HIPAA & HITECH Updates: The Vendors' Guide to the Security Essentials

Overview

Sorting through all the complex security details in three new federal regulations is challenging - but essential. These rules could help set a healthcare organization's security priorities.

And whether you're a business associate directly impacted by the regulations, or a service vendor helping organizations be compliant - you need to know the newest federal mandates.

Join us for this exclusive session in which noted experts will pinpoint the key provisions of a proposal to modify the HIPAA privacy and security rules, as well as two final rules for the federal electronic health record incentive program.

Our speakers will provide you with:

- An explanation of how the HIPAA modifications would beef up requirements for business associates, hospitals and physicians;
- A detailed description of the security components required for electronic health records software in the incentive program;
- An analysis of what security steps hospitals and physicians must take to qualify for the incentives;
- Answers to the questions that matter most to healthcare/security vendors.

Background

The HITECH Act, part of the massive economic stimulus package, will provide as much as $27 billion in incentives to hospitals and physicians who implement certified EHRs. But qualifying for the incentive payments will be a challenging task that involves meeting tough security requirements.

In addition, the HITECH Act required HIPAA modifications that, among other things, clarify that business associates that serve healthcare organizations must comply with HIPAA.

In this session, you'll learn how to:

- Comply with the meaningful use rule's mandate for risk assessments;
- Interpret the meaningful use rule's requirements for protecting patient information;
- Determine the specific EHR software security components required under the incentive program;

- Understand what business associates must do to ensure they're in compliance with HIPAA;
- Respond to patients' requests for timely access to their electronic records while maintaining security;
- Address many other issues, including how to comply with patients' requests to restrict access to their records.

Presented By

Tom Walsh, CISSP, President - Tom Walsh Consulting

Kate Borten, CISSP, CISM, President - The Marblehead Group

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=186

184

HIPAA Modifications & HITECH Rules: A Guide to the Security Essentials

Overview

Sorting through all the complex security details in three new federal regulations is challenging - but essential. These rules could help set your organization's security priorities.

Join us for this exclusive session in which noted experts will pinpoint the key provisions of a proposal to modify the HIPAA privacy and security rules, as well as two final rules for the federal electronic health record incentive program.

Our speakers will provide you with:

- An explanation of how the HIPAA modifications would beef up requirements for business associates, hospitals and physicians;
- A detailed description of the security components required for electronic health records software in the incentive program;
- An analysis of what security steps hospitals and physicians must take to qualify for the incentives.

Background

The HITECH Act, part of the massive economic stimulus package, will provide as much as $27 billion in incentives to hospitals and physicians who implement certified EHRs. But qualifying for the incentive payments will be a challenging task that involves meeting tough security requirements.

In addition, the HITECH Act required HIPAA modifications that, among other things, clarify that business associates that serve healthcare organizations must comply with HIPAA.

In this session, you'll learn how to:

- Comply with the meaningful use rule's mandate for risk assessments;
- Interpret the meaningful use rule's requirements for protecting patient information;
- Determine the specific EHR software security components required under the incentive program;
- Understand what business associates must do to ensure they're in compliance with HIPAA;
- Respond to patients' requests for timely access to their electronic records while maintaining security;

- Address many other issues, including how to comply with patients' requests to restrict access to their records.

Presented By

Tom Walsh, CISSP, President - Tom Walsh Consulting

Kate Borten, CISSP, CISM, President - The Marblehead Group

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=184

224

How to Prepare Your Organization for a HIPAA Security Risk Analysis

Overview

Learn how to prepare your organization for a HIPAA security risk analysis. In this webinar, we'll share pro-active steps that you can take to speed the process, improve the outcome and lower the potential mitigation costs of performing a HIPAA risk analysis. Our objective is to help you achieve meaningful use and, most importantly, safeguard electronic protected health information.

Topics covered:

- What is a HIPAA risk analysis;
- How it fits into your overall information security program;
- Key preparation steps;
- How to avoid potential pitfalls.

Background

The healthcare IT landscape is changing fast. Through government-sponsored incentive payments, the 2009 HITECH Act promotes the adoption and "meaningful use" of healthcare IT. Accelerating the migration to electronic health records (EHR) enables greater access to and sharing of patient health information among providers, patients, payers and employees. With increased access and data sharing comes increased risk.

This webinar will help you understand how a HIPAA security risk analysis is conducted and why it's a mandatory requirement of achieving meaningful use. You'll also understand how a HIPAA security risk analysis fits into your overall information security program so that you cannot only achieve compliance but also begin a process of continuous and durable improvements in IT security.

Topics covered include:

- HITECH Act and meaningful use attestation;
- What constitutes a HIPAA security risk analysis;
- Advance preparations: How can I maximize my ROI;
- Avoiding potential pitfalls;
- Beyond compliance to meaningful healthcare IT security.

Presented By

John Abraham, Founder & Chief Security Evangelist, Redspin

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=224

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.healthcareinfosecurity.com/webinars.php?webinarID=185

218

PCI: What Healthcare Organizations Need to Know

Overview

The Payment Card Industry Data Security Standard (PCI DSS) was created as a result of a cooperative effort between the major credit card companies, requiring merchants to protect cardholder information. This standard has been around for several years, yet many healthcare organizations still need to complete the required self-assessment.

Join us for this exclusive session, which will offer in-depth guidance including:

- The drivers behind PCI DSS;
- The key security requirements within PCI DSS;
- A high-level action plan for moving toward PCI DSS compliance;
- Insights on how PCI DSS compliance relates to HIPAA security rule compliance.

Background

In 2006, the five major credit card companies worked collaboratively to create a common industry standard for security known as the Payment Card Industry Data Security Standard (PCI DSS). Merchants (any organizations that accept credit and/or debit cards for payments) may be fined, held liable for losses resulting from a compromised card, or lose their merchant status if adequate security controls are lacking.

For the last decade, however, healthcare organizations have been focused heavily on HIPAA's privacy and security rules while sometimes overlooking other industry standards, such as PCI DSS.

Credit card fraud is ever-increasing due primarily to holes in data security controls. As a result, organizations are facing tarnished reputations because of public disclosures of breaches and unbudgeted costs associated with damage control.

Large payment card transaction volume merchants must have independent audits and frequent vulnerability tests; those with smaller payment card transaction levels are required to conduct a self-assessment and complete a self-assessment questionnaire. All merchants are required to complete an attestation of compliance. These self-assessments can be difficult to complete if an organization is unsure about what to do.

In this session, a leading healthcare information security specialist will provide timely, practical tips, including:

- An explanation on the background to the PCI DSS; the 12 requirement areas; merchant attestation levels; penalties and liabilities that can occur from non-compliance; and the four self-assessment questionnaire types;
- A summary of relevant state legislation affecting payment card security, in addition to PCI DSS;
- Examples of major breaches of payment card data security and why they were successful;
- A detailed discussion of the key areas and departments to focus on for a successful PCI DSS self-assessment within healthcare;
- Ideas on who in your organization needs to be included and the key departments for your organization's PCI DSS compliance focus;
- Insights on how PCI DSS compliance relates to HIPAA security rule compliance;
- Sample wording and areas to address in a credit card handling policy;
- Suggestions for employee training;
- Tips for developing a basic project plan;
- References to resources for additional information.

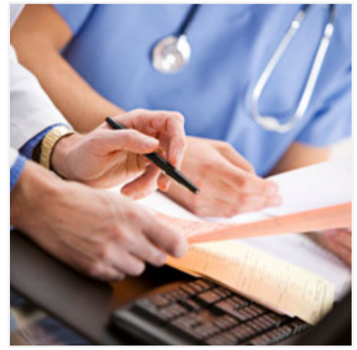
Presented By

Tom Walsh, CISSP, President - Tom Walsh Consulting

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=218

195

Risk Assessment for EHR Meaningful Use: Methodologies and Processes



Overview

The HITECH Act provides substantial financial incentives to hospitals and physician groups that become meaningful users of electronic health records. But to qualify, they must conduct a detailed risk assessment.

Join us for this exclusive session where you'll receive:

- An analysis of what the HITECH risk assessment objective actually means and how it relates to the existing HIPAA security rule;
- A detailed plan for conducting a streamlined risk assessment;
- Advice on prioritizing remediation efforts to achieve the greatest risk-reduction return on investment.
- How to prioritize risk and remediation practices to not only meet the meaningful use requirements but also to reduce the likelihood of experiencing a breach;
- How to manage information security risks and compliance requirements on a continual basis to alleviate patient concerns.

Background

The Health Information Technology for Economic and Clinical Health Act was designed to help transform the U.S. healthcare system to improve the quality, safety and efficiency of care. Among its many components, the HITECH Act provides funding for Medicare and Medicaid incentive payments for the meaningful adoption of certified electronic health record technology. Registration for eligible physicians and hospitals begins in January 2011, and incentive payments will begin in May 2011.

While the technology selected is a major component in meeting the meaningful use requirements, an overlooked and often challenging requirement is the performance of a risk assessment to protect the confidentiality, integrity and availability of protected health information.

So how does an organization realistically establish a plan and actually identify and mitigate its security risks?

In this exclusive session, healthcare organizations of all sizes will learn how to efficiently and effectively perform a risk assessment for meaningful use and correct identified security deficiencies.

You'll learn:

- The top security risks that hospitals, payers and physician practices now face;
- How to conduct a simplified, streamlined risk assessment, focusing on key risk areas and assessing management controls;

Presented By

Christopher Hourihan, Programs & Operations Manager, Health Information Trust Alliance

---

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=195

221

Risk Assessments: Protecting Your Organization from the Next Major Breach

Overview

Organizations were embarrassed by the WikiLeaks episode that resulted in the unauthorized release of more than 250,000 sensitive and classified government and financial documents. This leak - and the threat of others in both the public and private sectors - forces information security leaders to ask: What more can we do to protect access, portability and privacy of critical data?

Join an expert panel for a discussion on:

- Risk assessments, corrective actions and incident response essentials for WikiLeaks-type breaches;
- Strategies to control users' access to private information;
- Tools and techniques for preventing data loss.

Background

Late in 2010, the group known as WikiLeaks released thousands of sensitive government documents obtained by insiders who had too much access to critical data. Around the same time, the group threatened to release even more documents that potentially could embarrass public and private sector entities, including Bank of America.

These incidents raised new questions about security, privacy, ethics and especially access - who are the people who really should have access to your organization's most sensitive data?

Organizations today are more sensitive to the insider threat that could result in WikiLeaks-like revelations. But are they putting in place the correct systems and processes to ensure greater security and privacy?

In this session, you'll hear from a U.S. government CISO, a noted security expert and one of the industry's top security solutions providers, as they discuss:

- The data exposure risks to organizations of all types;
- Lessons learned from WikiLeaks;
- Systems and processes that can help ensure greater security against the new insider threat.

Presented By

Patrick Howard, Chief Information Security Officer, Nuclear Regulatory Commission

Robert Hamilton, Senior Product Marketing Manager - Data Loss Prevention, Symantec

Eric Cole, Security Expert, SANS Institute Faculty Fellow

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=221

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.healthcareinfosecurity.com/webinars.php?webinarID=158

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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.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 costumer 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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=65

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.

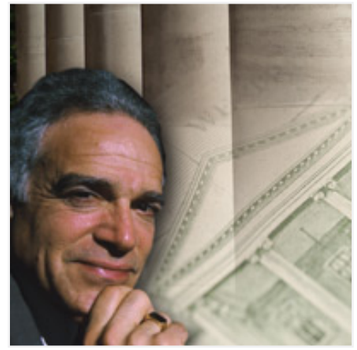
Background

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 theinvolvement 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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=132

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.healthcareinfosecurity.com/webinars.php?webinarID=212

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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=282

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.healthcareinfosecurity.com/webinars.php?webinarID=204

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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=73

273

6 Tips for Successful EHR Implementation

Overview

Total EHR software spending is expected to grow to approximately $3.8 billion in 2015. Yet, despite this large investment, many healthcare providers fail to meet their critical goals.

Attend this session to learn six new tips for EHR success, including how to:

- Align process redesign and technology with the electronic health record implementation;
- Gain visibility into your entire network;
- Improve network security and reduce the risk of human error and non-compliance.

Background

Total EHR software spending by all types of providers was approximately $2 billion in 2009 and is expected to grow to approximately $3.8 billion in 2015.

Still, despite this large investment, many providers fail to achieve the critical goals of implementation and use. Why?

Adding technology to ineffective workflows does not resolve the underlying problems. Successful implementation occurs with the combination of a new technology and process changes simultaneously.

In this session, join Kaseya, the leading global provider of IT systems management software, and Juran Institute, the global source for business process improvement training and consulting, to learn how your healthcare organization can:

- Align process redesign with technology to alleviate the pain of converting to an EHR;
- Increase the likelihood of achieving real financial and operational benefits.

Presented By

Jeff Keyes, Senior Product Marketing Manager, Kaseya

Joseph DeFeo, MBA, President & CEO, Juran Institute, Inc

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=273

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. What steps can you take to avoid being the next payment card fraud victim?

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.

Peretti, 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.healthcareinfosecurity.com/webinars.php?webinarID=169

202

HITECH Tips: Using EHR Security Functions for Protecting Patient Information

Overview

In 2011, hospitals and physicians can apply for HITECH Act incentive payments for using certified electronic health records software.

To be certified as qualifying for the Medicare and Medicaid incentive program, EHR software must have numerous security capabilities that, until now, have often been missing from clinical information systems.

What do healthcare information security professionals need to do to leverage these enhancements?

Join us for this exclusive session, which will offer in-depth guidance including:

- An explanation of all the required security functions for certified EHR software;
- An action plan for the next steps that hospitals and physician group practices should take to leverage these security controls;
- A detailed description of how to conduct a risk assessment to meet the incentive program's meaningful use requirements and prioritize security projects.

Background

The HITECH Act, part of the massive economic stimulus package, will provide as much as $27 billion in incentives to hospitals and physician groups that implement certified electronic health records software and put it to meaningful use.

The meaningful use requirements include conducting a risk assessment and using appropriate security controls to mitigate those risks.

Electronic health records software must include specific security controls to be certified for the incentive program. Until now, these controls have often been missing from clinical information systems. So many organizations applying for EHR incentives have limited experience in adopting these security measures.

How can your organization rapidly develop a plan for making the most of the security controls in certified EHRs? And what's the best way to set your security priorities?

In this session, a leading healthcare information security specialist will provide timely, practical tips. You'll get:

- A detailed explanation of all of the required security functions for certified EHR software;
- An action plan for all the steps to take to leverage the security controls;
- A detailed description of how to conduct a risk assessment on a tight deadline to meet the incentive program's meaningful use requirements and help prioritize security projects;
- Tips on how to assign security responsibilities during and after an EHR rollout;
- Insights on other relevant aspects of the meaningful use requirements, including providing patients with electronic copies of their records.

Presented By

Tom Walsh, CISSP, President - Tom Walsh Consulting

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=202

278

IT Security Risk Analysis for Meaningful Use: What We've Learned

Overview

Safeguarding protected health information (PHI) from data breaches has become a critical risk management issue for all healthcare organizations. Over the past 18 months, Redspin, Inc. an expert IT security firm, has helped more hospitals meet the Security Risk Analysis requirement of the EHR Meaningful Use Incentive Program than any other professional services provider.

In this exclusive webinar, Dan Berger, Redspin's President and CEO, will share his "real world" observations and insights on the security risk analysis process and how it can most benefit your organization.

Attend this webinar to gain answers to the following questions:

- What are the 3 most important steps you can take to safeguard PHI from data breach?
- How can an IT security risk analysis better prepare an organization for OCR audits and avoid enforcement actions?
- What proactive steps can a hospital take in regard to the risk of breach by business associates?
- How do the Stage 2 Meaningful Use security risk analysis requirements differ from Stage 1?

Background

Prompted by the EHR Meaningful Use Incentive Program, many hospitals and eligible providers are taking a fresh look at the HIPAA Security Rule requirement for regular IT security risk analysis (SRA). Nearly 100 hospitals have chosen Redspin to help them conduct their SRA and attest to meaningful use. While engaging an external firm is not mandatory, it enables healthcare providers to more efficiently use their internal resources while leveraging expertise that they may not have in-house.

In this webinar, Dan Berger, Redspin's President and CEO, will share his company's vast experience helping healthcare organizations meet the requirements of the HIPAA Security Rule. See how compliance with regulations is necessary but not sufficient as it relates to safeguarding PHI from data breaches. Learn why even the SRA itself is only a first step - and how reducing IT security risk requires an ongoing process of testing, remediation, validation and re-testing. See how web applications,

business associates, and mobile/BYOD are often overlooked as security risks yet pose significant threats. Gain a deeper understanding for how to make IT security an integral part of your overall risk management program and corporate culture.

Redspin promotes Meaningful Healthcare IT Security ® - a process-driven approach for healthcare firms to achieve continuous and durable improvements in IT security. The program provides a systematic reduction of vulnerabilities over time, even as organizations add new employees, systems, applications and customers.

Attend this webinar to gain answers to the following questions:

- What is the best governance strategy to employ to reduce IT security risk?
- Which 3 common areas of IT security vulnerability are the most prevalent in the healthcare industry?
- How can healthcare providers better prepare themselves as enforcement of HIPAA increases (audits, breach penalties, resolution agreements)?
- Beyond the SRA: How can health organizations deal with new areas of risk such as applications, business associates, mobile and BYOD?
- How can healthcare providers promote a "culture of compliance," or better yet, "a culture of security?"

Presented By

Dan Berger, President & CEO, Redspin

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=278

195

Risk Assessment for EHR Meaningful Use: Methodologies and Processes

Overview

The HITECH Act provides substantial financial incentives to hospitals and physician groups that become meaningful users of electronic health records. But to qualify, they must conduct a detailed risk assessment.

Join us for this exclusive session where you'll receive:

- An analysis of what the HITECH risk assessment objective actually means and how it relates to the existing HIPAA security rule;
- A detailed plan for conducting a streamlined risk assessment;
- Advice on prioritizing remediation efforts to achieve the greatest risk-reduction return on investment.

Background

The Health Information Technology for Economic and Clinical Health Act was designed to help transform the U.S. healthcare system to improve the quality, safety and efficiency of care. Among its many components, the HITECH Act provides funding for Medicare and Medicaid incentive payments for the meaningful adoption of certified electronic health record technology. Registration for eligible physicians and hospitals begins in January 2011, and incentive payments will begin in May 2011.

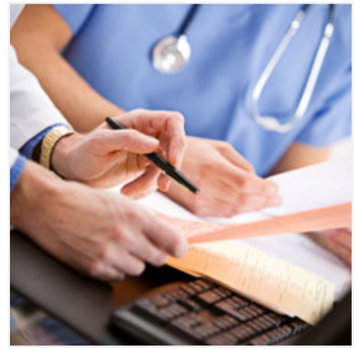
While the technology selected is a major component in meeting the meaningful use requirements, an overlooked and often challenging requirement is the performance of a risk assessment to protect the confidentiality, integrity and availability of protected health information.

So how does an organization realistically establish a plan and actually identify and mitigate its security risks?

In this exclusive session, healthcare organizations of all sizes will learn how to efficiently and effectively perform a risk assessment for meaningful use and correct identified security deficiencies.

You'll learn:

- The top security risks that hospitals, payers and physician practices now face;
- How to conduct a simplified, streamlined risk assessment, focusing on key risk areas and assessing management controls;



- How to prioritize risk and remediation practices to not only meet the meaningful use requirements but also to reduce the likelihood of experiencing a breach;
- How to manage information security risks and compliance requirements on a continual basis to alleviate patient concerns.

Presented By

Christopher Hourihan, Programs & Operations Manager, Health Information Trust Alliance

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=195

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.healthcareinfosecurity.com/webinars.php?webinarID=255

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.healthcareinfosecurity.com/webinars.php?webinarID=258

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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=29

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

---

http://www.healthcareinfosecurity.com/webinars.php?webinarID=67

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 contracted 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.healthcareinfosecurity.com/webinars.php?webinarID=288

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.healthcareinfosecurity.com/webinars.php?webinarID=293

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.healthcareinfosecurity.com/webinars.php?webinarID=177

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.

Hacktivists are 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.healthcareinfosecurity.com/webinars.php?webinarID=287

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.healthcareinfosecurity.com/webinars.php?webinarID=155

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

http://www.healthcareinfosecurity.com/webinars.php?webinarID=85

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.healthcareinfosecurity.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

http://www.healthcareinfosecurity.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 it's 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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=296

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.healthcareinfosecurity.com/webinars.php?webinarID=178

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.healthcareinfosecurity.com/webinars.php?webinarID=270

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.healthcareinfosecurity.com/webinars.php?webinarID=267

203

Insider Threats in Healthcare: Protecting Your Institution

Overview

The Mayo Clinic recently fired six employees for inappropriately accessing one patient's records. The high-profile announcement helped call attention to the need to address internal threats and set policies for dealing with privacy violations as part of a HIPAA and HITECH Act compliance strategy.

Until now, many hospitals and clinics have focused on external threats, taking steps to guard against security breaches. But internal threats may pose an even greater risk.

Join us for this exclusive session, where you'll learn:

- The major internal threats that can put protected health information in jeopardy;
- The roles that specific security technologies can play in addressing these threats, as well as their limitations;
- The essential elements of creating a corporate culture that values privacy and security.

Background

The HITECH Act toughens the penalties for violations of the HIPAA privacy and security rules, making it more important than ever for healthcare organizations to mitigate all security threats.

Healthcare organizations considering strategies for ensuring the privacy and security of protected health information often neglect to address a major area of risk: insider threats.

The actions and behaviors of those trusted to properly use and secure protected health information have the potential to pose a bigger threat than an external attack.

How can you guard against employees snooping at patient records they're not authorized to view? Or staff members taking patient identifiers from records to commit fraud?

In this exclusive session, a hospital security officer who's developed a comprehensive strategy for addressing internal threats will provide timely insights. You'll learn how to:

- Identify the internal risks that can jeopardize the privacy and security of patient information;
- Determine the roles that specific security technologies can play in addressing those threats and understand their limitations;
- Create privacy and security policies and educate staff;

- Determine appropriate sanctions for violations of those policies;
- Create a corporate culture that values privacy and security;
- Monitor workforce activity while maintaining worker privacy.

Presented By

Christopher Paidhrin, IT Security Compliance Officer, PeaceHealth Southwest Medical Center

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=203

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 cybersecurity 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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=50

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 socialed."

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.healthcareinfosecurity.com/webinars.php?webinarID=89

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.healthcareinfosecurity.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.healthcareinfosecurity.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 Moceri, Co-Founder and CEO of Convergint, 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 Moceri, Co-founder and CEO, Convergint

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=66

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.healthcareinfosecurity.com/webinars.php?webinarID=151

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.healthcareinfosecurity.com/webinars.php?webinarID=176

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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=167

262

Using the NIST HIPAA Security Rule Toolkit for Risk Assessments

Overview

A risk analysis, as required under the HIPAA Security Rule, is a critical and foundational component of an effective risk management process that helps covered entities, and their business associates, to perform their mission and protect the health information entrusted to them.

The National Institute of Standards and Technology has developed the HIPAA Security Rule Self-Assessment Toolkit to help organizations with their risk management processes.

In this webinar, a NIST security specialist will:

- Provide a detailed overview of the toolkit;
- Outline practical ways to use the toolkit to support an organization's risk management process; and
- Explain additional NIST information security resources that can help organizations to safeguard health information.

Background

The National Institute of Standards and Technology, a non-regulatory agency of the Department of Commerce, is responsible for providing standards and technology to protect against threats to the confidentiality, integrity and availability of information and information systems. NIST's Computer Security Division is positioned to ensure that new technologies are selected, deployed and operated in a manner that reduces risk.

The Health Insurance Portability and Accountability Act Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used or maintained by a covered entity. Covered entities include hospitals, physician groups, health plans and claims clearinghouses. Soon, the rule also will apply to business associates - business partners that have access to sensitive patient information. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information.

To help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environments, NIST has developed a HIPAA Security Rule Self Assessment Toolkit.

In this session, Kevin Stine, manager of the Security Outreach and Integration Group within NIST's Computer Security Division, will:

- Introduce participants to NIST and its role in information security;
- Provide a detailed overview of the toolkit application;
- Discuss how the toolkit can be used to support an organization's risk management process, help improve security safeguards and aid security assessment and compliance activities; and
- Identify additional NIST information security resources, such as risk assessment and security control guidelines, which can help organizations to manage risk and safeguard health information.

Presented By

Kevin Stine, Acting Manager - Security & Integration Group, National Institute of Standards and Technology (NIST)

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=262

203

Insider Threats in Healthcare: Protecting Your Institution

Overview

The Mayo Clinic recently fired six employees for inappropriately accessing one patient's records. The high-profile announcement helped call attention to the need to address internal threats and set policies for dealing with privacy violations as part of a HIPAA and HITECH Act compliance strategy.

Until now, many hospitals and clinics have focused on external threats, taking steps to guard against security breaches. But internal threats may pose an even greater risk.

Join us for this exclusive session, where you'll learn:

- The major internal threats that can put protected health information in jeopardy;
- The roles that specific security technologies can play in addressing these threats, as well as their limitations;
- The essential elements of creating a corporate culture that values privacy and security.

Background

In this exclusive session, a hospital security officer who's developed a comprehensive strategy for addressing internal threats will provide timely insights. You'll learn how to:

- Identify the internal risks that can jeopardize the privacy and security of patient information;
- Determine the roles that specific security technologies can play in addressing those threats and understand their limitations;
- Create privacy and security policies and educate staff;
- Determine appropriate sanctions for violations of those policies;
- Create a corporate culture that values privacy and security;
- Monitor workforce activity while maintaining worker privacy.

Presented By

Christopher Paidhrin, IT Security Compliance Officer, PeaceHealth Southwest Medical Center

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=203

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.healthcareinfosecurity.com/webinars.php?webinarID=214

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.healthcareinfosecurity.com/webinars.php?webinarID=291

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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=26

186

HIPAA & HITECH Updates: The Vendors' Guide to the Security Essentials

Overview

Sorting through all the complex security details in three new federal regulations is challenging - but essential. These rules could help set a healthcare organization's security priorities.

And whether you're a business associate directly impacted by the regulations, or a service vendor helping organizations be compliant - you need to know the newest federal mandates.

Join us for this exclusive session in which noted experts will pinpoint the key provisions of a proposal to modify the HIPAA privacy and security rules, as well as two final rules for the federal electronic health record incentive program.

Our speakers will provide you with:

- An explanation of how the HIPAA modifications would beef up requirements for business associates, hospitals and physicians;
- A detailed description of the security components required for electronic health records software in the incentive program;
- An analysis of what security steps hospitals and physicians must take to qualify for the incentives;
- Answers to the questions that matter most to healthcare/security vendors.

Background

The HITECH Act, part of the massive economic stimulus package, will provide as much as $27 billion in incentives to hospitals and physicians who implement certified EHRs. But qualifying for the incentive payments will be a challenging task that involves meeting tough security requirements.

In addition, the HITECH Act required HIPAA modifications that, among other things, clarify that business associates that serve healthcare organizations must comply with HIPAA.

In this session, you'll learn how to:

- Comply with the meaningful use rule's mandate for risk assessments;
- Interpret the meaningful use rule's requirements for protecting patient information;
- Determine the specific EHR software security components required under the incentive program;

- Understand what business associates must do to ensure they're in compliance with HIPAA;
- Respond to patients' requests for timely access to their electronic records while maintaining security;
- Address many other issues, including how to comply with patients' requests to restrict access to their records.

Presented By

Tom Walsh, CISSP, President - Tom Walsh Consulting

Kate Borten, CISSP, CISM, President - The Marblehead Group

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=186

184

HIPAA Modifications & HITECH Rules: A Guide to the Security Essentials

Overview

Sorting through all the complex security details in three new federal regulations is challenging - but essential. These rules could help set your organization's security priorities.

Join us for this exclusive session in which noted experts will pinpoint the key provisions of a proposal to modify the HIPAA privacy and security rules, as well as two final rules for the federal electronic health record incentive program. Our speakers will provide you with:

- An explanation of how the HIPAA modifications would beef up requirements for business associates, hospitals and physicians;
- A detailed description of the security components required for electronic health records software in the incentive program;
- An analysis of what security steps hospitals and physicians must take to qualify for the incentives.

Background

The HITECH Act, part of the massive economic stimulus package, will provide as much as $27 billion in incentives to hospitals and physicians who implement certified EHRs. In this session, you'll learn how to:

- Comply with the meaningful use rule's mandate for risk assessments;
- Interpret the meaningful use rule's requirements for protecting patient information;
- Determine the specific EHR software security components required under the incentive program;
- Understand what business associates must do to ensure they're in compliance with HIPAA;
- Respond to patients' requests for timely access to their electronic records while maintaining security.

Presented By

Tom Walsh, CISSP, President - Tom Walsh Consulting

Kate Borten, CISSP, CISM, President - The Marblehead Group

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=184

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. What steps can you take to avoid being the next payment card fraud victim?

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.

"We've gone from card farms to card resellers to international hackers," says Kimberly Peretti, former senior counsel in the department's computer crime section.

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.healthcareinfosecurity.com/webinars.php?webinarID=169

195

Risk Assessment for EHR Meaningful Use: Methodologies and Processes

Overview

The HITECH Act provides substantial financial incentives to hospitals and physician groups that become meaningful users of electronic health records. But to qualify, they must conduct a detailed risk assessment.

Join us for this exclusive session where you'll receive:

- An analysis of what the HITECH risk assessment objective actually means and how it relates to the existing HIPAA security rule;
- A detailed plan for conducting a streamlined risk assessment;
- Advice on prioritizing remediation efforts to achieve the greatest risk-reduction return on investment.

Background

The Health Information Technology for Economic and Clinical Health Act was designed to help transform the U.S. healthcare system to improve the quality, safety and efficiency of care. Among its many components, the HITECH Act provides funding for Medicare and Medicaid incentive payments for the meaningful adoption of certified electronic health record technology. Registration for eligible physicians and hospitals begins in January 2011, and incentive payments will begin in May 2011.

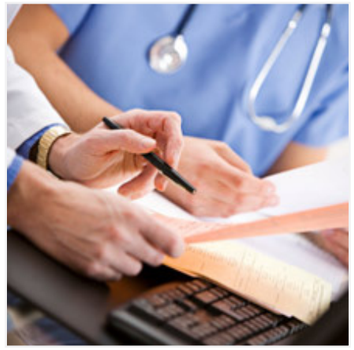
While the technology selected is a major component in meeting the meaningful use requirements, an overlooked and often challenging requirement is the performance of a risk assessment to protect the confidentiality, integrity and availability of protected health information.

So how does an organization realistically establish a plan and actually identify and mitigate its security risks?

In this exclusive session, healthcare organizations of all sizes will learn how to efficiently and effectively perform a risk assessment for meaningful use and correct identified security deficiencies.

You'll learn:

- The top security risks that hospitals, payers and physician practices now face;
- How to conduct a simplified, streamlined risk assessment, focusing on key risk areas and assessing management controls;



- How to prioritize risk and remediation practices to not only meet the meaningful use requirements but also to reduce the likelihood of experiencing a breach;
- How to manage information security risks and compliance requirements on a continual basis to alleviate patient concerns.

Presented By

Christopher Hourihan, Programs & Operations Manager, Health Information Trust Alliance

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=195

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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=180

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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=155

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.healthcareinfosecurity.com/webinars.php?webinarID=48

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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.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, Vice President, Product Management at Ipswitch

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=100

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.healthcareinfosecurity.com/webinars.php?webinarID=73

200

Cloud Computing in Healthcare: Key Security Issues

Overview

Cloud computing has drawn a great deal of attention as a way to reduce IT costs in healthcare. But are the companies that offer cloud computing well-prepared to meet the HIPAA privacy and security requirements?

Join us for this exclusive session, where you'll gain an in-depth understanding of issues relevant to all healthcare organizations, including:

- Working with cloud vendors to address key information security and privacy compliance issues;
- Strategies for satisfying HIPAA privacy and security legal requirements "in the cloud;"
- The impact of the pending modifications to the HIPAA privacy and security rules, in addition to the HITECH Act rules.

Background

As hospitals and clinics alike consider their options for adding new applications in a hurry, on a tight budget or lacking necessary resources, many are considering the cloud computing option.

With the HITECH EHR incentive payment program kicking into high gear, organizations are feeling pressure to devise ways to roll out new systems quickly so they can earn the maximum payments from Medicare and Medicaid.

But cloud computing presents special risks, particularly with respect to privacy and security. And many vendors, unfortunately, do not appear to fully understand the importance of addressing these risks as healthcare organizations work to comply with the updated HIPAA privacy and security rules. One of the requirements for receiving EHR incentive payments is to perform a risk assessment, and then appropriately remediate the identified risks.

Healthcare organizations considering cloud computing need to carefully consider the risks before taking the plunge, and then take the right steps to obtain adequate due diligence protection.

In this session, a healthcare security and privacy compliance expert will offer a clear, detailed explanation of key issues, including:

- Cloud computing safeguards necessary to satisfy HIPAA and other privacy and security requirements, including such strategies as using "private clouds" and restricting data to servers in the United States;
- The impact of the pending modifications to the HIPAA privacy and security rules, in addition to the HITECH Act rules, including new standards for accounting for disclosures, on the decision about using cloud computing;
- The negotiation of a HITECH-compliant business associate agreement with the cloud vendor;
- How to effectively obtain assurance that cloud vendors are in compliance with HIPAA and HITECH;
- Metrics to use to determine that vendors maintain compliance on an ongoing basis;
- Performance issues, including availability of data and services;
- Increased complexity of e-discovery if processes and/or data storage are handled using cloud computing;
- The handling of the transition to another cloud vendor or back to the health care organization without disruption of operations or conflicting claims to the data.

Presented By

Rebecca Herold, CEO, The Privacy Professor

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=200

240

Complying with Healthcare Data Security Mandates & Privacy Laws

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

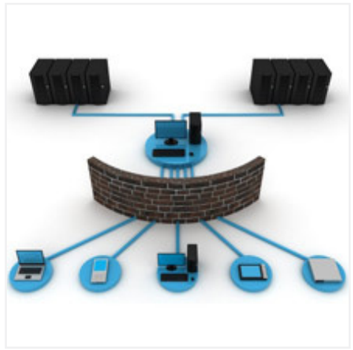
Abir Thakurta, Senior Director - Pre-Sales & Professional Services, Liaison Technologies

---

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=240

209

Detecting and Preventing Health Data Breaches



Overview

Healthcare data breaches and regulatory mandates have combined to create a new standard for data security that relies heavily on system and user activity awareness. To be compliant and avoid costly breaches, organizations must improve their ability to predict and see in near real time where incidents are likely to occur, then proactively address them to avoid risk.

Join us for this exclusive session, where you will learn:

- Why system and user activity awareness is so critical to avoiding risk;
- How to unlock the intelligence captured in your enterprise that's key to creating awareness and mitigating risk;
- How to assess your organization's readiness to deploy or optimize leading-edge technology solutions.

Background

In 2010 there were 18 major breaches, potential compromises of more than 500 individual records containing unprotected patient health information, reported monthly to the Office of Civil Rights (OCR). To be exact, 214 total notifications were made in 2010. As bad as this sounds, it was probably nowhere near the real number. Why? Because most organizations still do not have the level of system or data awareness needed to even know when unauthorized access or disclosure is occurring. This does not even address the higher number of smaller compromises that occur every day in most healthcare organizations. The take away from this ought to be validation that the old practices of relying on barriers to keep the bad guys out and data secure are not sufficient anymore.

In addition, the regulatory landscape continues to have new privacy and security requirements introduced, making compliance all the more challenging. It's not simply HIPAA anymore. Now its HIPAA, HITECH, PCI, FRCP, Red Flags, state laws, business partner requirements, etc. It ought to be obvious, once again, that there's an emerging standard of care in healthcare for data security that requires a more precise level of informational awareness.

Such awareness is enabled by harnessing the intelligence waiting in the log information within the enterprise. But simply collecting the logs and reviewing them reactively, or even periodically, is not enough. Healthcare today needs the right tools and technologies to automate the collection, analysis and reporting, but more importantly the need to be able to correlate multiple log inputs from myriad sources to create a more accurate picture of exactly what happened, who was involved, and the status of the information or system involved.

In this exclusive session, healthcare organizations will learn about:

- Why system and data security awareness is so important and what makes it difficult in healthcare today;
- Basic log management functions and why automation is necessary and critical;
- What's involved in user activity monitoring and what makes this a challenge in healthcare;
- What is SIEM, how it enables proactive or near real time security and compliance, and why its such a powerful tool for transforming user behavior.

Presented By

Brian Singer, Senior Solutions Marketing Manager, Novell

Mac McMillan, Co-Founder & CEO, CynergisTek Inc.

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=209

228

Developing an Effective Security Strategy for Health Data

Overview

Regulations such as HIPAA and HITECH drive healthcare providers and payers to adopt information protection strategies. But adoption of consumer-facing electronic privacy is a mixed bag.

Join us to discuss some of the elements that make a good security strategy for the dissemination of health information, including:

- Key regulations and their impact on how to secure and disseminate data;
- What's required to enable protection of sensitive health information, including key patient requirements;
- How to augment a low-profile portal with pro-active communication with patients - and save money.

Background

The HITECH Act is a terrific step forward in enabling hospitals and physicians as well as the healthcare industry at large to implement electronic health records. Yet most approaches result in poor adoption because they fail to take into account the latest consumer trends in how patients wish to consume information - information which must be protected and only disseminated in a secure fashion. By drawing on examples from the financial services industry where information for consumers has successfully transitioned from passive portals to secure messages and mobile applications, we will explore some examples such as electronic explanation of benefits (EoBs) where securely pushing information to patients can enable dramatic cost savings.

In this session, participants will learn about:

- Key consumer-patient trends as they relate to consumption of information;
- Common techniques for securing information that needs to be sent to patients;
- How to augment the relative poor performance of passive portal-based approaches to sharing information;
- Leveraging the success of secure consumer communication from the financial services industry;
- How to dramatically save costs associated with business processes such as explanation of benefits.

Presented By

Wasim Ahmad, VP - Marketing, Voltage Security

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=228

201

Encryption as Part of a Broader 'Safe Harbor' Strategy

Overview

Because the HITECH Act's breach notification rule includes a safe harbor that exempts the reporting of breaches if the data involved was properly encrypted, many organizations are investigating whether to make wider use of encryption. But healthcare organizations need to develop a better understanding of how encryption fits as just one of many components in a broader security strategy.

Join us for this exclusive session, when you'll learn how to:

- Analyze your environment to identify breach risks;
- Follow a systematic approach to evaluating enterprise security controls and pinpoint encryption needs;
- Address technology, process and people requirements in developing a broader "safe harbor" breach prevention strategy.

Background

The HITECH Act's interim final breach notification rule, published in the fall of 2009, spelled out when major breaches affecting 500 or more individuals must be reported to federal authorities as well as those affected. But the rule contained a significant "safe harbor" provision, exempting the reporting of breaches of data that was encrypted in compliance with specific NIST guidelines.

The HITECH Act, as well as HIPAA and other federal rules, all stop short of mandating encryption. But because a majority of the major breaches reported to federal authorities so far have involved the theft or loss of unencrypted computer devices and media, many organizations are considering making widespread use of encryption.

Approaching breach prevention through encryption alone, however, is not the right approach. Such a strategy is costly and can have an adverse effect on system performance and create a false sense of security.

In this exclusive session, healthcare organizations of all sizes will learn how to:

- Analyze their environment to understand breach risks by taking a lifecycle approach to mapping protected health information in the enterprise;
- Follow a systematic approach to evaluating enterprise security controls as well as encryption needs;

- Address technology, process and people requirements in developing a broader, well-balanced, integrated approach to security, resulting in a "safe harbor" breach prevention strategy;
- Plan for and understand why the use of encryption needs to change over time as the IT environment changes.

Presented By

Mac McMillan, Co-Founder & CEO, CynergisTek Inc.

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=201

202

HITECH Tips: Using EHR Security Functions for Protecting Patient Information

Overview

In 2011, hospitals and physicians can apply for HITECH Act incentive payments for using certified electronic health records software.

To be certified as qualifying for the Medicare and Medicaid incentive program, EHR software must have numerous security capabilities that, until now, have often been missing from clinical information systems.

What do healthcare information security professionals need to do to leverage these enhancements?

Join us for this exclusive session, which will offer in-depth guidance including:

- An explanation of all the required security functions for certified EHR software;
- An action plan for the next steps that hospitals and physician group practices should take to leverage these security controls;
- A detailed description of how to conduct a risk assessment to meet the incentive program's meaningful use requirements and prioritize security projects.

Background

The HITECH Act, part of the massive economic stimulus package, will provide as much as $27 billion in incentives to hospitals and physician groups that implement certified electronic health records software and put it to meaningful use.

The meaningful use requirements include conducting a risk assessment and using appropriate security controls to mitigate those risks.

Electronic health records software must include specific security controls to be certified for the incentive program. Until now, these controls have often been missing from clinical information systems. So many organizations applying for EHR incentives have limited experience in adopting these security measures.

How can your organization rapidly develop a plan for making the most of the security controls in certified EHRs? And what's the best way to set your security priorities?

In this session, a leading healthcare information security specialist will provide timely, practical tips. You'll get:

- A detailed explanation of all of the required security functions for certified EHR software;
- An action plan for all the steps to take to leverage the security controls;
- A detailed description of how to conduct a risk assessment on a tight deadline to meet the incentive program's meaningful use requirements and help prioritize security projects;
- Tips on how to assign security responsibilities during and after an EHR rollout;
- Insights on other relevant aspects of the meaningful use requirements, including providing patients with electronic copies of their records.

Presented By

Tom Walsh, CISSP, President - Tom Walsh Consulting

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=202

198

Mobile Devices in Healthcare: Essential Security

Overview

A majority of the healthcare information breaches reported to federal authorities so far have involved the theft or loss of mobile devices. To help make sure your organization isn't added to the list, register for this webinar to hear an experienced security officer's top 10 tips for securing mobile devices. He describes how to:

- Tackle the tough task of inventorying all devices;
- Develop comprehensive policies for encryption and many other safeguards;
- Educate staff on why security is vital to the reputation of your organization.

Background

Under the HITECH Act, healthcare organizations now must report major breaches to the Health and Human Services' Office for Civil Rights. And a majority of the incidents reported so far have involved the theft or loss of computer devices or media.

What can your organization do to minimize the risk of a breach involving a mobile device?

This session provides tools, tips and techniques to develop a comprehensive portable device security program.

Terrell Herzig, information security officer at UAB Medicine, offers his top 10 tips, including:

- Working with suppliers to ensure encryption standards are met;
- Developing several layers of security controls;
- Restricting use of USB ports.

He explains why a mobile device security policy must go far beyond simply investing in encryption.

Presented By

Terrell Herzig, CISO, UAB Medicine

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=198

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.healthcareinfosecurity.com/webinars.php?webinarID=148

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's 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.healthcareinfosecurity.com/webinars.php?webinarID=256

197

Password Security in the Windows Healthcare Enterprise

Overview

Securing confidential patient health data for compliance with HIPAA and HITECH is now more important than ever. Successful compliance with these standards can involve many tools, IT components and business practices at significant cost to healthcare organizations. Even with all these initiatives in place, the weakest link in the security chain, basic access to data via password control, remains a major risk factor. Implementing strong password policies custom tailored to a user's security risk is one of the simplest and most cost-effective methods of significantly lowering the possibility of a breach of confidential medical information.

View this recorded webinar to learn about:

- How a strong and secure password management infrastructure can aid in meeting HIPAA and HITECH requirements;
- Tools and methods that are routinely used to gain unauthorized access to confidential patient data;
- Why passwords are the weak link in the core security model and what steps can be easily taken to better protect patient data;
- Tools that can be used to implement truly strong passwords.

Background

All employees with access to electronic protected health information (ePHI) need additional security controls in place to ensure confidentiality of this information as directed in the HIPAA and HITECH acts. These employees include IT administrators, help-desk personnel, doctors, nurses and any other employees that access ePHI data.

The HIPAA/HITECH security and privacy rules clearly state that employees that have access to ePHI information must be addressed with higher security measures than those that don't. These users are clearly a higher risk and have access to more sensitive data. The only way to increase the security of these users in comparison to other users on the network is to increase their password complexity requirements. This can be done on a tiered structure, as these users have more access and more risk associated with the ePHI data. An example might be IT having a 20+ character password, doctors and nurses having a 15 character password, and all other employees having an 8 character password.

The new HIPAA/HITECH requirements clearly indicate that users need to be able to reset their own passwords. This is a good security measure and one that all companies should implement. The requirement also indicates that the user must input unique answers to questions that only the user would know.

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.healthcareinfosecurity.com/webinars.php?webinarID=197

218

PCI: What Healthcare Organizations Need to Know

Overview

The Payment Card Industry Data Security Standard (PCI DSS) was created as a result of a cooperative effort between the major credit card companies, requiring merchants to protect cardholder information. This standard has been around for several years, yet many healthcare organizations still need to complete the required self-assessment.

Join us for this exclusive session, which will offer in-depth guidance including:

- The drivers behind PCI DSS;
- The key security requirements within PCI DSS;
- A high-level action plan for moving toward PCI DSS compliance;
- Insights on how PCI DSS compliance relates to HIPAA security rule compliance.

Background

In 2006, the five major credit card companies worked collaboratively to create a common industry standard for security known as the Payment Card Industry Data Security Standard (PCI DSS). Merchants (any organizations that accept credit and/or debit cards for payments) may be fined, held liable for losses resulting from a compromised card, or lose their merchant status if adequate security controls are lacking.

For the last decade, however, healthcare organizations have been focused heavily on HIPAA's privacy and security rules while sometimes overlooking other industry standards, such as PCI DSS.

Credit card fraud is ever-increasing due primarily to holes in data security controls. As a result, organizations are facing tarnished reputations because of public disclosures of breaches and unbudgeted costs associated with damage control.

Large payment card transaction volume merchants must have independent audits and frequent vulnerability tests; those with smaller payment card transaction levels are required to conduct a self-assessment and complete a self-assessment questionnaire. All merchants are required to complete an attestation of compliance. These self-assessments can be difficult to complete if an organization is unsure about what to do.

In this session, a leading healthcare information security specialist will provide timely, practical tips, including:

- An explanation on the background to the PCI DSS; the 12 requirement areas; merchant attestation levels; penalties and liabilities that can occur from non-compliance; and the four self-assessment questionnaire types;
- A summary of relevant state legislation affecting payment card security, in addition to PCI DSS;
- Examples of major breaches of payment card data security and why they were successful;
- A detailed discussion of the key areas and departments to focus on for a successful PCI DSS self-assessment within healthcare;
- Ideas on who in your organization needs to be included and the key departments for your organization's PCI DSS compliance focus;
- Insights on how PCI DSS compliance relates to HIPAA security rule compliance;
- Sample wording and areas to address in a credit card handling policy;
- Suggestions for employee training;
- Tips for developing a basic project plan;
- References to resources for additional information.

Presented By

Tom Walsh, CISSP, President - Tom Walsh Consulting

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=218

199

Social Media in Healthcare: A Guide to Minimizing Your Risk

Overview

Social media provide healthcare organizations with a low-cost way to communicate effectively with consumers. But using this form of communication brings with it many risks.

For example, one California hospital recently fired five employees because they used social media to post personal discussions about patients, violating their privacy.

Hospitals, clinics and others, however, can use proven methods to minimize the risks involved, helping to ensure compliance with the HITECH Act and HIPAA. Join us for this exclusive session where you'll receive:

- An explanation of the important role social media can play in healthcare;
- A detailed description of the security concerns, including reputational harm;
- An analysis of the security steps healthcare organizations must take to minimize their risks and control usage.

Background

A growing number of healthcare organizations are joining the social media revolution, taking advantage of a new, low-cost way of communicating with current and potential patients. And some technology innovators envision a day when social networks could support real-time sharing and collaboration, which could further enhance productivity.

But as is the case with all new technologies, social media bring new risks, including the potential for privacy violations. And the HITECH Act toughened penalties for violations of the HIPAA privacy and security rules, bringing a renewed sense of urgency to privacy protection.

For most healthcare organizations, however, social media is emerging as an indispensible part of their communications efforts. So how can they make the most of the new communication channels while managing the risks they pose? In this session, the lead developer of Adventist Health System's social media policy will provide timely insights about how to:

- Understand the risks that surround social media;
- Evaluate how social media can help your organization meet its communication needs;

- Develop a social media policy and strategy that balances marketing, leadership, legal, human resources, compliance and security issues;
- Develop an education plan for all team members;
- Determine how much control of social media your organization can take onsite and offsite;
- Learn how to balance your organization's rights to protect its assets against individuals' rights to free speech and privacy.

Presented By

Sharon Finney, CISM, CISSP, Corporate Data Security Officer, Adventist Health System

---

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=199

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.healthcareinfosecurity.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.healthcareinfosecurity.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 cybersecurity 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.healthcareinfosecurity.com/webinars.php?webinarID=160

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.
- 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.healthcareinfosecurity.com/webinars.php?webinarID=130

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:

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 Datoo, Chief Product Officer, Zenprise

View the complete outline and register for this webinar at:
http://www.healthcareinfosecurity.com/webinars.php?webinarID=266

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.healthcareinfosecurity.com/webinars.php?webinarID=291

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.healthcareinfosecurity.com/webinars.php?webinarID=208

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.healthcareinfosecurity.com/webinars.php?webinarID=177

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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=165

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

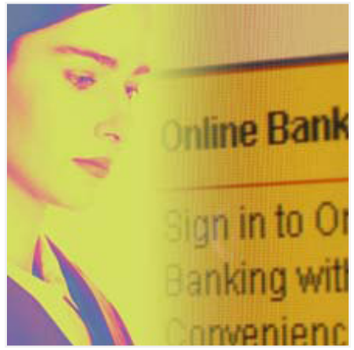
The evolution of malware and crimeware has produced more insidious and harmful intrusions to networks and systems. This webinar will show how these types of intrusions relate to phishing and will help put current attacks into perspective and help organizations anticipate likely trends.

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.healthcareinfosecurity.com/webinars.php?webinarID=30

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 super-user 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 super-user 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.healthcareinfosecurity.com/webinars.php?webinarID=170

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.healthcareinfosecurity.com/webinars.php?webinarID=185

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.healthcareinfosecurity.com/webinars.php?webinarID=148

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.healthcareinfosecurity.com/webinars.php?webinarID=285

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.healthcareinfosecurity.com/webinars.php?webinarID=256

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

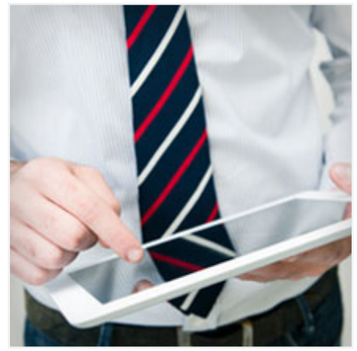
At Intel, the BYOD trend started in 2009, when employees began using their own smart phones, tablets and mobile storage devices on the job. Rather than reject the trend, as many organizations initially attempted, Intel's senior leaders were quick to embrace it as a means to cut costs and improve productivity.

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.healthcareinfosecurity.com/webinars.php?webinarID=264

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.healthcareinfosecurity.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.

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.healthcareinfosecurity.com/webinars.php?webinarID=166

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.healthcareinfosecurity.com/webinars.php?webinarID=272

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.healthcareinfosecurity.com/webinars.php?webinarID=119

141

Securing Your E-mail 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 e-mail message originates from (SOX);
- Ensuring complete access to e-mail 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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=204

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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=163

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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=284

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.healthcareinfosecurity.com/webinars.php?webinarID=161

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.healthcareinfosecurity.com/webinars.php?webinarID=143

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.healthcareinfosecurity.com/webinars.php?webinarID=282

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.healthcareinfosecurity.com/webinars.php?webinarID=289

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?

Presented By

Greg Shields, Microsoft MVP in Terminal Services

Kevin Gillis, Vice President, Product Management at Ipswitch

http://www.healthcareinfosecurity.com/webinars.php?webinarID=100

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.healthcareinfosecurity.com/webinars.php?webinarID=88

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.healthcareinfosecurity.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.healthcareinfosecurity.com/webinars.php?webinarID=104

Premium Membership

Become a Premium Member to stay up to date on the latest information security and risk management topics.

Individual

1 Member

OnDemand Access

CPE Credit Tracking

$1,995/year

Corporate

SAVE 25%

Up to **5** Members

OnDemand Access

CPE Credit Tracking

$7,495/year

Enterprise

Unlimited Members

OnDemand Access

CPE Credit Tracking

Tiered Pricing

Groups: Save up to an additional 25% with a group membership.

Membership Features

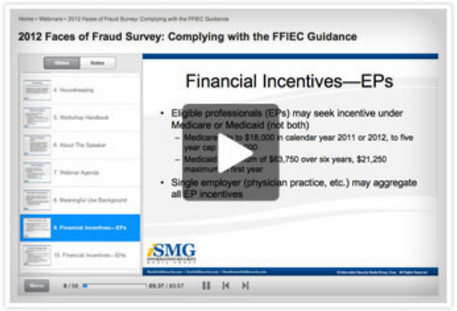
Unlimited Access

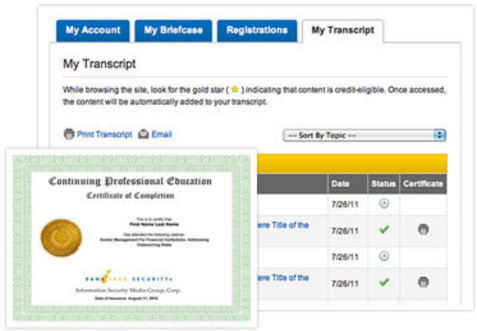
Gain unrestricted access to an expanding curriculum of over 200 courses. No education solution is as comprehensive. Our industry expert practitioners have developed over 300 hours of exclusive courses and, on average, create 15 new courses each quarter.

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.





Continuing Professional Education

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® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY
Prevention. Response. Notification.

4 Independence Way • Princeton, NJ • 08540 • www.ismgcorp.com