2011 Course Catalog

Educational Webinars for Financial Institutions

BANK INFO SECURITY®

ISMG INFORMATION SECURITY MEDIA GROUP

Welcome to the University of You


Tom Field

The bad news: Fraud incidents are on the rise. Our "Faces of Fraud" survey indicates that banking institutions are under constant attack by payment card, check, phishing/vishing, ACH/ wire and even internal data leakage.

The good news: Institutions also are investing more time and resources in employee training – not just for information security professionals, either, but for everyone in the organization, ranging from customer-facing personnel to senior business management.

Why the renewed emphasis on training? Mostly, to keep up with the latest threats, as well as new trends and technologies. In some cases, to comply with industry or government regulations. In all cases, continuing education is vital for today's professionals to stay current – and particularly when training counts toward continuing education credits for industry certifications.

At Information Security Media Group, publisher of BankInfoSecurity.com, GovInfoSecurity.com and HealthcareInfoSecurity.com, we've assembled a broad suite of webinar training programs that are relevant to your career needs. These sessions cover the gamut of industry/security topics such as:

- **Regulatory Compliance** – including sessions that walk you through risks assessments, anti-money laundering and vendor management, as well as how to prepare for an ID Theft Red Flags Rule exam.
- **Fraud** – with emphasis on hot topics such as skimming, phishing and how to resist social engineering.
- **Today's Pressing Needs** – how to mitigate risks presented by the insider threat, social media and emerging technologies such as cloud computing.

For our virtual faculty, we draw upon a broad range of presenters. Industry thought-leaders, top consultants, current industry/ security leaders, even federal regulators.

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 course offerings that could most benefit you.

Tom Field
Editorial Director, Information Security Media Group
tfield@ismgcorp.com

BANK INFO SECURITY®

ISMG INFORMATION SECURITY MEDIA GROUP

Contents

Inside the Catalog

Courses by Category

Our courses are constantly updated, and we're continually striving to respond to industry trends and challenges – to give you exactly the hands-on training you need to succeed in your job and career.

The Web Approach

The most effective training for today's workforce

Gone are the days of week-long getaways at exotic locales featuring minimal classroom time and maximum leisure time.

In fact, in-person training in general seems to be giving way to web-based alternatives. During a recent survey administered on BankInfoSecurity.com and CUInfoSecurity.com, 76% of those responding indicated they would be utilizing webinars as a primary form of training, as opposed to just 36% who indicated classroom training.

Live webinars offer the same interaction classroom or in-person training offer but eliminates travel cost and time spent away from the office. With on-demand webinars, the need to retain a subject matter expert for multiple training sessions is eliminated. And because webinars are completely Internet-based, staff members in different locations can easily join together for the same session.

Why are webinars so popular?

- **Virtually no time away from the office**
- **No costs for travel, lodging, or meals**
- **Leisure time is greatly reduced – focus is 100% on training and education**
- **Easily accommodate large groups of people from a single location**

Don't miss out. Join the other **30,000+** webinar attendees from **thousands of organizations** worldwide.

The Importance of Employee Training

Employee training is vital for any organization, especially for the banking industry, and even more so during such a tumultuous time.

Training helps build a stronger, more decisive employee. Educated employees will be better suited to more efficiently handle day-to-day tasks, long-term projects, and make better informed decisions during times of stress.

- **Helps create trust between an institution and its workforce**
- **Keeps staff prepared to make better informed decisions during times of stress**
- **An educated employee is an institution's best asset**

Why Webinar Training?

Training budgets are tight, and every dollar spent must be justified. Following are three reasons to justify your investment in webinar training from ISMG:

1 They're Real

Our webinars aren't taught by theorists; they're led by banking/security practitioners, regulators and thought-leaders that have hands-on experience in the information security and risk management areas that matter most to you.

2 They're Relevant

These sessions are devoted to current and hot topics – regulatory compliance, risk management, fraud, emerging threats – and are continually updated to ensure response to our ever-changing industry.

3 They Deliver ROI

Our webinars allow you to stay in your own office, focused on day-to-day concerns, while leveraging instruction that not only helps you do your job today, but also helps you earn CPE credits to assist you in your career.

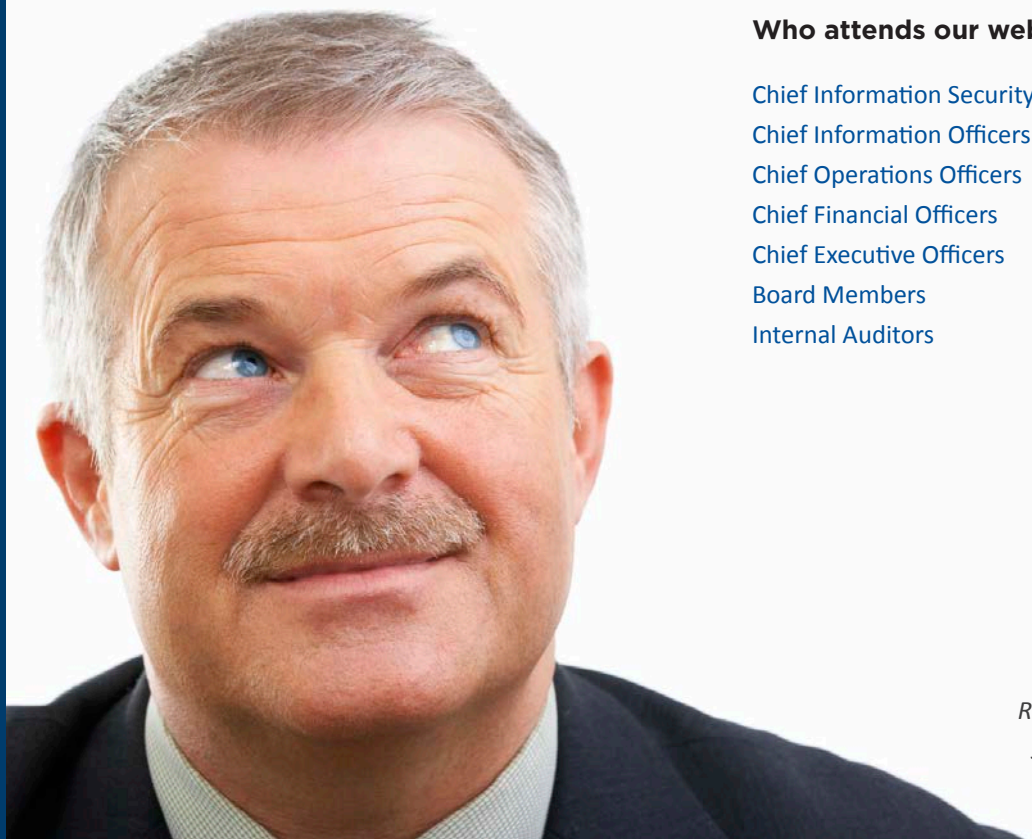
Designed for Decision Makers

Covering the topics your institution cares about

Focus on Information Security and Risk Management

A financial institution's risk management program is arguably the most important component of the institution's overall IT security program. A robust risk management program should ensure the security of not just information technology assets, but any function within the institution that would prevent it from operating and achieving its core mission. Accordingly, risk management and information security should not be seen solely as technical issues, but rather core business objectives.

Business leaders and executives are just as crucial to an institution's risk management and information security practices as are technology leaders. At BankInfoSecurity.com and CUInfoSecurity.com we understand this, and we strive to ensure students from both sides of an institution's operating dichotomy, the technology side and business executive side, are equally satisfied with the content of our training sessions. This is accomplished by utilizing practitioners and subject matter experts who speak from experience, and offer hands-on, actionable advice – focusing on the core objective of the training topic as opposed to what certain employee roles mandate.



Who attends our webinars?

- Chief Information Security Officers
- Chief Information Officers
- Chief Operations Officers
- Chief Financial Officers
- Chief Executive Officers
- Board Members
- Internal Auditors
- Fraud Specialists
- Network Professionals
- Privacy Officers
- Risk Managers
- AML/BSA Officers
- Online Marketing Managers
- HR/Training Managers

Risk management, compliance, fraud, and security training for senior management.

Topics You Care About

When it comes to information security and risk management for financial services organizations continuing education is a must in this ever changing environment. Security is an evolving practice and failure to protect your customers' information will have serious consequences. As a result, everyone — from IT staffers and risk officers to business managers and executives — needs to keep pace.

Our extensive library of education and training webinars covers all facets of risk management and information security for professionals at institutions of all sizes. Whether you deal with strictly compliance initiatives or delve into the intricacies of technology implementation, we have training webinars for you.

Here are some of the topics our training covers:

Authentication
Cloud Computing
Compliance
DR/Business Continuity
Data Loss Prevention
Emerging Technologies
Encryption
Fraud Detection & Prevention
Governance, Risk, & Compliance
Hiring & Background Checks
Identity & Access Management
Identity Theft & Phishing
Incident Response
Insider Fraud
Mobile Banking
Physical Security
Security Policies & Standards
Social Engineering
Training and Education
Vendor Management
Web Application Security

Presented by Industry Experts

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

Training and education are only as effective as the presenter and his/her subject matter expertise. That is why we strive to utilize only the best and brightest in the financial industry to present our training webinars.

Many of our presenters have gone through the same challenges you do, and 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, most importantly, how-to. After attending our webinars you will walk away with definitive steps and actionable advice that you can utilize at your institution. Our presenters go through a considerable vetting process and are monitored throughout the entire webinar production cycle to ensure only the highest quality educational content is conveyed.

Matthew Speare

SVP of Information Technology, M&T Bank

Matthew oversees security for M&T Bank Corporation, the nation's 17th largest bank holding company, based in Buffalo, New York. He is responsible for developing and sustaining an information risk program that effectively protects the personal information of millions of M & T Bank customers.

William Henley

Former Director of IT Risk Management, OTS

William has spent his entire professional career as a financial institution regulator. Henley is the Director of IT Risk Management for the Office of Thrift Supervision. In his role as the Director, Henley serves as the principal advisor regarding the development, implementation and maintenance of policies, procedures and guidelines.

Steven Jones

Director of Information Security, Synovous Financial

As a member of senior management, Steven is responsible for the company's organizational policy, risk management, security awareness, identity management, disaster recovery, and other areas of risk management. He is active in BITS, Information Risk Executive Council, and serves on several advisory boards including SecureWorks and Blue Coat.

Tom Wills

Senior Analyst Risk, Security and Fraud, Javelin Strategy and Research

Tom leads Javelin Strategy & Research'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 strategically navigate the challenges of security. His breadth of expertise enables Javelin to deepen its support of clients.

Paul Smocer

VP Security, BITS

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

Linda Coven

Head of Online Banking Channel Solutions, Silicon Valley Bank

Linda is a 20 year veteran of the banking industry who developed and manages the online banking platform for Silicon Valley Bank. With over 7 years experience at SVB, she serves as strategic advisor to the company's executives and steering committee related to products and services that will help further the commercial bank's strategic objectives.

David Matthews

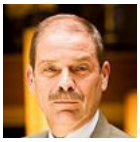
Deputy Chief Information Security Officer for the City of Seattle

David Matthews is currently the Deputy Chief Information Security Officer for the City of Seattle. He has worked in the Information Technology field since 1992. He began working for the City of Seattle as the Technology Manager for the Legislative Department (City Council) in 1998.

Neil Katkov

Celent

Neil is the manager of Celent's Asia Research group. His areas of expertise include the Asian financial services industry, financial services distribution channels, and compliance issues including anti-money laundering and business continuity planning. Dr. Katkov produces Celent's popular reports on IT spending trends in the Asian banking, securities, and insurance industries.



David Dixon

Managing Director of Financial Crime Norkom

David provides leadership for Norkom's development and delivery of industry leading financial crime solutions. He brings more than 20 years' experience providing financial crime and risk management expertise to global financial services firms.

Randy Sabett

Information Security Attorney, SN&R LLP

Randy, CISSP, is a partner in the Washington, D.C. office of Sonnenschein Nath & Rosenthal LLP, where he is a member of the Internet, Communications & Data Protection Practice. He counsels clients on information security, privacy, IT licensing and patents.

E.J. Hilbert

Former FBI Special Agent

E.J. is a former Federal Bureau of Investigation 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. E.J. served as the agent in charge of the investigations into the intrusions of over 300 financial institutions.

Kevin Sullivan

Investigator, New York State Police

Kevin Sullivan is an investigator with the NY State Police and was the state investigations coordinator assigned to the NY HIFCA El Dorado Task Force in Manhattan. He has 20 years of police experience, specializing in anti-money laundering and conducting numerous investigations. Sullivan has a Masters in Economic Crime Management and is a certified anti-money laundering specialist.

Keir Breitenfeld

Sr. Dir. Fraud and Identity Solutions, Experian Decision Analytics

Keir Breitenfeld's responsibilities at Experian include stewardship of their comprehensive suite of consumer and commercial authentication and fraud management products and services. Keir brings with him a diverse set of experiences including fraud operations management, risk management consulting, and project management.

Ori Eisen

Founder, Chairman and Chief Innovation Officer, 41st Parameter

Ori Eisen has spent the last ten years in the information technology industry, his background includes an in-depth application of innovative solutions for preventing business to consumer e-commerce fraud. Prior to launching 41st Parameter, Mr. Eisen served as the Worldwide Fraud Director for American Express.

Reed Taussig

President & CEO, ThreatMetrix

Reed has over 30 years experience in the computer hardware and software fields. Prior to ThreatMetrix, Mr. Taussig was president and CEO of Vormetric, Inc., a leader in data privacy and protection. Under his leadership, Vormetric established itself as a leading provider of encryption solutions for the Payment Card Industry Data Security Standards industry.

Charles Robertson

Sr. Product Manager, Verafin

Dr. Robertson contributes directly to the development of Verafin's advanced anti-fraud solutions and behavior-based analytics, and speaks frequently about money laundering and fraud across North America. Dr. Robertson has an extensive background in R&D related to image processing, pattern recognition and artificial intelligence.

Mike Urban

Sr. Dir. & Fraud Chief , FICO

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

James Christiansen

CEO, Evantix

Prior to joining Evantix, James was Chief Information Security Officer for Experian Solutions. James joined Experian after serving as Chief Information Security Officer for General Motors. Prior to joining GM, James leveraged his years of security experience to provide global leadership to Visa International. James has been featured in the New York Times.

Krista Tedder

VP Debit Solutions - Fraud and Risk Management, MasterCard

Krista is currently responsible for fraud and collections solutions for financial institutions. Krista provides consultation services to financial institutions with a focus on reducing operational expenses and strengthening brand reputation through consistent customer experience and stronger fraud management capabilities.

Dr. Markus Jakobsson

Associate Prof., Indiana University

Markus is Associate Professor at Indiana University's School of Informatics. He is also Associate Director of the Center of Applied Cybersecurity Research, and founder of RavenWhite, Inc. He is an author, as well as the inventor or co-inventor of more than fifty patents.

Bill Sewall

Information Security, Compliance and Risk Management Specialist

Bill is an Information security, compliance and risk management specialist with 30 years experience as a corporate attorney and general counsel, CIO, information security officer, and operational risk manager. Most recently, Sewall spent 10 years as a senior executive information security officer in Citigroup.

Steve Neville

Director of Identity Products, Entrust

Steve joined Entrust in 1999, and has played a consistent leadership role in Entrust's product evolution and innovation. Working closely with customers and key departments such as R&D, sales and marketing, Steve is passionate about ensuring that Entrust fields market-driven, innovative products.

George Tubin

Senior Research Director, TowerGroup, Inc.

George Tubin's areas of expertise include consumer online banking, online fraud and identity theft prevention, information security strategy, and customer authentication, mobile banking and contact center strategies and technologies. Before joining TowerGroup, George was a senior consultant with ADS Financial Services Solutions.

Andy Schmidt

Research Director - Global Payments, TowerGroup, Inc.

Andy Schmidt focuses on trends and developments in the payments, including payments hubs, mobile payments, service-oriented architecture, standards, and anti-money laundering. Andy has 20 years of experience in the financial services industry as both a banker and a consultant.

Shirley Inscoe

Director - Financial Services Solutions, Memento

A 29-year banking veteran, Shirley Inscoe is a recognized expert in helping financial institutions apply innovative technology and strategies to address dynamic and costly fraud challenges. Shirley is a former SVP of Enterprise Payments Strategy at Wachovia, Chair of BITS Fraud Reduction Steering Committee, and Co-Chair of Early Warning Services' Advisory Committee.

Patrick Howard

Chief Information Security Officer, Nuclear Regulatory Commission

Patrick D. Howard serves as the Chief Information Security Officer of the Nuclear Regulatory Commission. He provides vision, leadership and oversight in developing, promulgating and implementing an agency IT security strategy.

Michael Smith

Security Evangelist, Akamai

Michael Smith is the customer-facing ambassador from the Information Security Teamat Akamai, helping customers to understand both the internal security program and the unique security features and capabilities of the Akamai product portfolio and cloud-based solutions. He is also an adjunct professor for Carnegie Mellon University.

Harold Moss

CTO - Cloud Security Strategy, IBM

Harold Moss, as a member of the corporates strategy team, participates in defining technical directions for security technologies and is an active contributor to the IBM Security Technology Institute. Harold is currently working on cloud security for various cloud patterns, as well as correlating workload to specific cloud patterns.

Jeff Lake

VP - Federal Operations, Proofpoint

Jeff Lake directs Proofpoint's strategic growth in the U.S. federal government market. With over 20 years of technology and security experience, Lake has held several leadership positions in technical sales, consulting and operations. Previously, Lake was a commissioned U.S. Army Military Intelligence officer, holds a Top Secret security clearance.

Terry Austin

President & CEO
Guardian Analytics, Inc.

Terry Austin is the CEO at Guardian Analytics and a regular speaker at conferences and seminars on the topic of new strategies for fraud prevention at banks and credit unions.

Evelyn Royer

Vice President, Purdue Employee Federal Credit Union

Evelyn joined Purdue Employees Federal Credit Union in 1994 as the internal auditor and later was promoted to accounting manager. She was chosen to develop the risk management department in 2002, and in 2005 she was named vice president, overseeing collections, compliance, internal audit and servicing for loans, deposits and plastic products.

Tom Walsh

CISSP and Certified Business Continuity Professional

A nationally recognized speaker on a range of information security related topics, including business continuity and disaster recovery. Prior to launching a consulting firm offering information technology risk management services for its clients, Tom was responsible for leading information security efforts for Saint Luke's Health System in Missouri.

Rebecca Herold

Analyst

Rebecca is an information, security, privacy and compliance analyst, author and instructor. Herold is also an adjunct professor for the Norwich University Master of Science in Information Assurance program. She has provided information security, privacy and regulatory services to organizations from a wide range of industries throughout the world.

Course Category Matrix

Webinar Title
5 Critical Data Security Predictions for 2011
Anti-Money Laundering/Fraud Convergence: Why Should I Care?
Anti-Money Laundering: The Practitioner's Guide to the Laws
Anti-Money Laundering: The Investigator's Guide to the Laws
Application Security Testing and OCC Bulletin 2009-16 Compliance
Are You Effectively Protecting Your Customer's Private Data?
Assessing Encryption Standards for Financial Institutions
ATM Fraud: Strategies to Beat the Skimming Scams
Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks
Beyond Compliance: Meeting the New Threat Landscape Head-On
Beyond Heartland: How to Prevent Breaches of Security and Trust
Beyond Phishing - The Growing Crimeware Threat
Board Responsibilities for IT Risk Management: Building Blocks for a Secure System
BSA Compliance: How to Conduct an Anti-Money Laundering Investigation
Business Banking Under Attack: How to Fight Back Against Cybercriminals
Business Continuity Planning Best Practices
Business Continuity Risk Assessment & Resource Allocation
Business Impact Analysis — How to Get it Right
Check Fraud Management 2.0: A New Approach to a Persistent Challenge
Cloud Computing: Regulatory Security & Privacy Challenges
Creating a Culture of Security - Top 10 Elements of an Information Security Program
Data Protection and Incident Response
Debit Fraud: Trends and Typologies
Defending Against The Insider Threat
Developing an Effective Information Security Awareness Training Program - Getting the Word Out
Effective End-to-End Fraud Management: Managing Financial Crime Risks in Today's Banking Climate
Email Security Requirements for Healthcare Providers: HIPAA & Beyond

● Primary Category ○ Secondary Category

BSA/AML	BCP	Compliance	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt
				○		○	●	
●		○	○		○			
●		○			○			
●		○			○			
		○				○	●	○
○					○	●		
					○		●	○
			●				○	
				●		○		
		●					○	
			●			○	○	
			●			○		
				●				
●		○			○			
			●				○	
	●							
	●			○	○			
	●			○				
			●				○	
		●				○	●	●
		○		●				
				●		○		○
			●		○		●	
			●	○		○		
○				●				
			●			○		
		○				○	●	

Webinar Title
Evaluating Security Risks Associated with Banking Vendors
Expert's Guide to Suspicious Activity Reports (SARS): Tips to Avoid Regulatory Pitfalls & Penalties
Fight Back Against Fraud: Strategies on How to Meet the Multi-Channel Challenge
Fighting Fraud Schemes: Education, Response and Defense
Fighting Online Banking Cybercrime with a Holistic Security Strategy
Fraud Detection & Prevention Strategies for Financial Institutions: Emerging Technologies Insights
Fraud Prevention: Protect Your Customers and Your Institution from Web Vulnerabilities
Gaining Control of Compliance Mandates, Security Threats, & Data Leaks
GLBA Privacy Requirements: How to Build an Effective Program That Meets GLBA Compliance and Ensures Customer Privacy
HIPAA Modifications & HITECH Rules: A Guide to the Security Essentials
How Identity Fraud is Evolving and Impacting Customer Trust in Your Financial Institution
How to Develop & Maintain Information Security Policies & Procedures
How to Launch a Secure & Successful Mobile Banking Platform
How to Prepare for Your First Identity Theft Red Flags Rule Exam
How to Prevent Data Leakage from Compromising Your Company's Security
How to Use Your Mobile Phone for Free Two-Factor Authentication
How Well Do You Know Your Vendors?
Identity Theft: How to Respond to the New National Crisis
Incident Response Essentials: Regulatory Compliance, Vendor Management and Customer Communication
Incident Response: How to React to Payment Card Fraud
Information Security for Management – What Your Senior Leaders Need to Know
Information Security Risk Assessments: Understanding the Process
Information Technology Risk Management Program (IT-RMP) Examination Procedures: How to Satisfy Regulatory Demands
Insider Fraud - Profiling & Prevention
Insider Threat: Defend Your Enterprise
Insider Threats - Safeguarding Financial Enterprise Information Assets
Integrating Risk Management with Business Strategy
Investigations, Computer Forensics and e-Discovery - A Primer for Every Banking Institution
Is Your Device Identification Ready for New FFIEC Guidance?

● Primary Category ○ Secondary Category

BSA/AML	BCP	Compliance	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt
						○	○	●
●		○						○
		○	●				●	
			●	○			○	
			●	○			○	
		○	●				○	
			●			○	○	
		●			○			
		●				○		
		●				○		
			●			○	○	
		○		●	○			
							●	
		●			○	○		
				●				
							●	
				○		○		●
			●			○		
		●				○		○
			●			○		○
		○		●				
		○		●	○			
		●					○	
			●			○		
				●				
			●					
				●				
		●			○	○		
		●				○	●	

Webinar Title
Key Considerations for Business Resiliency
Legal Considerations About Cloud Computing
Maintaining Compliance with the Gramm-Leach-Bliley Act Section 501b
Maintaining Secure Government Information Systems
Malware, Crimeware, and Phishing - An In Depth Look at Threats, Defenses
Managing Shared Passwords for Super-User Accounts
Man-in-the-Browser Attacks: Strategies to Fight the Latest Round in Online Fraud
Massachusetts Privacy Law: A Guide to Understanding and Complying with this New Data Protection Standard
Meeting Federal Compliance to Secure Windows Desktops
Money Laundering Update: The Latest Threats to Your Institution
Next-Generation Threats: Understanding, Investigating and Defending Global Attacks Against the Financial Services Industry
Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?
Pandemic Planning & Response Techniques
PCI Compliance: Tips, Tricks & Emerging Technologies
PCI: What Healthcare Organizations Need to Know
Power Systems: How to Prevent Unauthorized Transactions
Preparing for an Information Technology Regulatory Exam
Preparing for Your Next Audit: The Five Habits of Successful Security Programs
Preparing Your Institution for an IT General Controls Audit
Preventing Phone Fraud with Voice Biometric Authentication
Preventing TJX Type Data Breaches
Preventing Unauthorized Access To Your Institution's Data
Proactive IT Risk Assessment Strategies
Protecting CUI: Federal Best Practices for Email Security, Archiving and Data Loss Prevention
Protecting the Exchange of Sensitive Customer Data with Your Vendors
Records Retention: How to Meet the Regulatory Requirements and Manage Risk with Vendors
Responding to a Privacy Breach: Protect Yourself and Your Vendors
Risk Management, Continuity and Compliance - What All Financial Organizations Need to Know
Securing Your Email Infrastructure

● Primary Category ○ Secondary Category

BSA/AML	BCP	Compliance	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt
				●				
		○		○			●	○
		●			○			
				●			○	
			○				●	
				○			●	
			●			○	○	
		●				○		○
		●			○		●	
●			○		○			
			○				●	
	○			●	○	○		
	●	○						
		●					○	
		●					○	
		○			○		●	
		●					○	
		○			●			
					●			
			●				○	
							●	○
					○		●	
		○		●				
		●			○		●	
						○	○	●
		●						○
○						●		○
		●		○				
		○				○	●	

Webinar Title
Security Risks of Unified Communications: Social Media & Web 2.0
Social Engineering: How to Train Your Employees to Spot and Stop the Scams
Social Networking Compliance for FINRA Regulated Organizations
Social Networking: Is Your Institution Ready for the Risks?
Steps to Managing Security Risk from Your Software Vendors
Taking Fraud Out of Online Banking
Testing Security Controls at a Banking Institution: Learn from the Experts
The Dirty Little Secret About Network Security
The Faces of Fraud: How to Counter 2011's Biggest Threats
The Fraud Deficit: Why Deposit Account Fraud Budgets Need to Shrink
The Future of Banking Enterprise Access Management & Authentication - Emerging Technologies Insights
The Identity Enabled Network: The Future of Secure Cyberspace
The Identity Management Challenge for Financial Institutions
The Mobile Environment: Challenges and Opportunities for Secure Banking
The Reality of Cyberattacks: Emerging Solutions for Today’s Threats
Time: The Hidden Risks - How to Create Compliant Time Practices
Top 5 Reports IT Auditors Request
Top 20 Critical Controls to Ensure Painless FISMA Compliance
Top IT Compliance Challenges: Who’s Touching Your Data and What Are They Doing With It?
User Authentication: Best Practices for Managing Risk & Compliance
Vendor Management Part I: FDIC Explains How to Manage Your Outsourcing Risks
Vendor Management Part II: Assessing Vendors - the Do’s and Don’ts of Choosing a Third-Party Service Provider
Vendor Management Part III: Inside the BITS Shared Assessments Program
Voice Over IP -Helping Financial Institutions Learn and Mitigate Security Risks
You & Your Vendors: How to Best Secure Data Exchange
ZeuS and Other Malware Threats Force Authentication to "Step Out" Of Band

● Primary Category ○ Secondary Category

BSA/AML	BCP	Compliance	Fraud	Governance	IT Audit	Privacy	Technology	Vendor Mgmt
							●	
		○		●		○		
		●			○	○	●	
					○	●		
		○						●
			●			○	○	
		○			○		●	
		○		○			●	
			●	○				
			●				●	
							●	
				○			●	
			○			○	●	
					○		●	
							●	
		○					●	
		○		○	●			
		○		●				
		●				○	○	○
		○		○			●	
		○			○			●
		○			○	○		●
					○			●
							●	
		○					○	●
			●				○	

Course Descriptions

Anti-Money Laundering

Anti-money laundering is one of the classic threats to a financial institution, and fighting this threat is a key component of Bank Secrecy Act (BSA) compliance. Learn how to conduct an AML investigation, as well as how to write an effective Suspicious Activity Report (SAR) and spot the latest trends.

AML154

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

Money-laundering is one of the most common and complex financial crimes, and the government regulations can be daunting. Learn first-hand from a former investigator exactly what you need to know about the specific statutes and regulations that govern the crime.

- Key anti-money laundering laws and how they apply;
- Penalties for money-laundering crimes;
- Tips for how to conduct a successful money-laundering investigation.

Presented by Kevin Sullivan, Investigator, NY State Police

AML153

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

Money laundering is a growing crime that affects numerous organizations. As a regulated entity, learn exactly what you need to know to uphold specific statutes and regulations that govern this crime.

- Key anti-money laundering laws and what they mean to your organization;
- Penalties for money-laundering crimes;
- How your organization can best respond to money laundering mandates.

Presented by Kevin Sullivan, Investigator, NY State Police

AML59

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

This session will take a deep dive and uncover key hidden connections in Anti-Money Laundering and Fraud. We will also take a look at the similarities in function, challenges, and technology used to combat this.

- What analytics are similar/different in Anti-Money Laundering and Fraud
- Trends for enterprise-wide case management and the combination of Anti-Money Laundering and Fraud prevention
- What are the integration areas and data requirements issues
- Latest developments in investigations and operations

Presented by Amir Orad, Celent; and Neil Katkov, Manager of Celent's Asia Research group

AML80

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

Money laundering is one of the most frequent crimes against financial institutions, and regulatory compliance with the Bank Secrecy Act (BSA) is one of the prime directives for banking/security professionals.

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

Presented by Kevin Sullivan, Investigator, NY State Police

AML86

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

At the core of any good Anti-Money Laundering (AML) program is the Suspicious Activity Report (SAR), which all financial institutions must file when confronting questionable transactions.

- How to properly complete a SAR;
- How to determine when it's appropriate to file a SAR;
- SAR writing guidelines and etiquette.

Presented by Kevin Sullivan, Investigator, NY State Police

AML116

Money Laundering Update: The Latest Threats to Your Institution

Mobile Payment Systems, Digital Precious Metals, Virtual worlds. These are among the targets of the modern-day money launderer, and it behooves your institution to understand and prepare for them.

- The rise of trade-based money laundering, including trade price manipulation and Internet/mobile payment systems;
- The return of classic crimes - how to spot new attempts at old schemes such as ATM's, shared value cards and micro-structuring.

Presented by Kevin Sullivan, Investigator, NY State Police

See the current scheduled sessions for all courses:
http://www.bankinfosecurity.com/webinarsCalendar.php

Business Continuity

Natural disasters, man-made threats and pandemics – they all threaten financial institutions. Learn the fundamentals of preparedness, including how to conduct a business impact analysis and how to create a pandemic response program to meet regulatory standards.

BCP27

Business Continuity Planning Best Practices

Financial institutions understand the need for effective business continuity planning. But increased threats from natural, man-made and pandemic disasters make this security measure a must.

- Key Components of a Business Continuity Plan;
- Exercising and Testing Business Continuity and Disaster Recovery Plans;
- How to Avoid Common Mistakes.

Presented by Tom Walsh, CISSP, Tom Walsh Consulting

BCP96

Business Continuity Risk Assessment & Resource Allocation

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

Presented by Dana Turner, Crime and Security Expert, Security Education Systems

BCP95

Business Impact Analysis — How to Get it Right

- 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;
- 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.

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

BCP77

Pandemic Planning & Response Techniques

Pandemic planning is a significant regulatory requirement for every financial institution and a key component in your next examination.

- What Examiners Expect From Your Institution's Pandemic Plan;
- How Your Institution Can Prevent Or Mitigate A Pandemic's Effects;
- How to Test Your Pandemic Plan.

Presented by Dana Turner, Security Education Systems

See the current scheduled sessions for all courses: http://www.bankinfosecurity.com/webinarsCalendar.php

Compliance

Financial institutions are driven by regulatory mandates, and these sessions provide the building blocks for complying with major regulations such as GLBA, BSA and the Identity Theft Red Flags Rule.

COMP215

Beyond Compliance: Meeting the New Threat Landscape Head-On

Malware, phishing, 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, learn "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.

Presented by Chenxi Wang, VP, Principal Analyst, Forrester Research and Bernd Leger, Senior Director - Marketing, Rapid7

COMP188

Cloud Computing: Regulatory Security & Privacy Challenges

Cloud computing is the hot, new practice that offers a scalable, centralized resource for data and applications that can be available to anyone, anywhere. But as an emerging trend, cloud computing is also fraught with risk - already we've seen organizations whose data has been compromised. Register for this session to hear the lessons learned about cloud computing from a panel of experts who will discuss:

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

Presented by Matthew Speare, SVP - Information Technology, M & T Bank Corporation; Michael Smith, Security Evangelist, Akamai; Harold Moss, CTO - Cloud Security Strategy, IBM

COMP147

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

Data integrity and confidentiality is critical for financial services - no other industry is more frequently targeted by cyber-crime and cyber-piracy. Learn how to leverage the logs that you are already collecting to achieve regulatory compliance, protect valuable customer information and improve the efficiency of your IT operations team.

- How to easily and cost-effectively automate your

log management;

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

Presented by Sudha Iyer, Director of Product Management, LogLogic

COMP94

GLBA Privacy Requirements: How to Build an Effective Program That Meets GLBA Compliance and Ensures Customer Privacy

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

- How to establish policies, procedures and technical controls to support and maintain privacy;
- How to align vendor contracts to include Privacy-related requirements and outline vendors' responsibilities;
- Industry "best practices" for customer communications for privacy-related notifications.

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

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.

- How HIPAA modifications add to current requirements;
- Security requirements for electronic health records software;

Presented by Tom Walsh, CISSP and Kate Borten, CISSP, CISM

COMP113

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

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.

Presented by Bill Sewall, Information security, compliance and risk management specialist

COMP81

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

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.

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

COMP28

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

Banking regulatory agencies regularly examine banking practices -- including Information Technology -- at the

institutions they oversee. In this presentation, you will hear about the basic tenants behind the Information Technology (IT) examinations conducted by the Federal Deposit Insurance Corporation (FDIC) using Information Technology Risk Management Program (IT-RMP).

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

Presented by Vincent Pisciotta, Former Sales Manager for BankInfoSecurity.com

COMP65

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

This webinar takes a practical approach to the necessity of forensics and e-discovery in financial institutions, offering insight on how to deploy best-practices.

- Federal rules and regulatory requirements that underscore the need for forensics and e-discovery;
- How investigators have used forensics to crack tough cases at financial institutions;
- How to build or enhance a forensics program at your institution.

Presented by Matthew Speare, M&T Bank Corporation; and Warren Kruse, Encore Legal Solutions

COMP217

Is Your Device Identification Ready for New FFIEC Guidance?

Since the FFIEC guidance on "Authentication in an Internet Banking Environment" cybercriminals have evolved, leading the FFIEC to draft new guidance for protecting your business and customers from fraud. Learn about smart device identification technologies banks will need to comply with new FFIEC guidance and meet today's challenges of identity and password theft, botnets, trojans and new risks introduced by smartphones including:

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

Presented by Alisdair Faulkner, Chief Products Officer, ThreatMetrix

COMP19

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

GLBA is one of the fundamental regulations governing the principles of secure banking. Understand your role and responsibilities.

- Determine The Board's role in the creation and oversight of an information security program;
- Evaluate the risk assessment process;
- Assess the measures taken to oversee third-party service providers.

Presented by Susan Orr, of Susan Orr Consulting

COMP132

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

The Massachusetts "Standards for the Protection of Personal Information" may well be the new "gold standard" for privacy legislation. Know its implications.

- The details of the Massachusetts privacy standards;
- How these new standards impact your organization;
- Road map for achieving compliance;
- The potential impact on federal privacy legislation.

Presented by Bill Sewall, Information security, compliance and risk management specialist

COMP189

Meeting Federal Compliance to Secure Windows Desktops

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

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

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

COMP212

PCI Compliance: Tips, Tricks & Emerging Technologies

Version 2.0 of the Payment Card Industry Data Security Standard is in effect, and thought-leaders are reviewing emerging technologies and payment card security trends focusing on how they may impact PCI's future. Merchants, processors and service providers focus is how to stay PCI compliant. This panel will explore:

- 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.

Presented by Tom Field, Editorial Director, ISMG, Corp., Anton Chuvakin, Author & PCI Expert, and André Bakken, Director Product Management, Ipswitch

COMP218

PCI: What Healthcare Organizations Need to Know

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 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.

Presented by Tom Walsh, CISSP, President - Tom Walsh Consulting

COMP18

Preparing for an Information Technology Regulatory Exam

All banking regulatory agencies examine banking practices, including Information Technology, on a periodic basis.

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

Presented by Susan Orr, CISA, CISM, CRP, Susan Orr Consulting

COMP185

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

Email continues to be one of the primary risk vectors of exposure of Controlled Unclassified Information (CUI) and other sensitive data in federal organizations today, but most have yet to deploy technology to help prevent costly breaches. Join this discussion to find out what you need to know about the latest security, data privacy and archiving regulations for government agencies. 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.

Presented by Jeff Lake, VP - Federal Operations, Proofpoint

COMP97

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

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.

- 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.

Presented by Rebecca Herold - CISM, CISSP, CISA, CIPP, FLMI

COMP102

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

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

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

Presented by Rodney Nelsestuen, Research Director, Tower Group; and Bill Hammond, Director of Product Marketing, Vision Solutions

COMP193

Social Networking Compliance for FINRA Regulated Organizations

Now you can maintain FINRA compliance across Facebook, LinkedIn, Twitter and over 1000 social networks. The secrets are shared during this exclusive webinar. Control and compliance is the key to Social Media survival in today's regulated industries. So you need a solution for true compliance. This exclusive webinar will explore the requirements of FINRA with regard to Social Networking - and how Socialite, a new social media compliance solution from FaceTime Communications, helps you meet them.

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

Presented by Sarah Carter, VP - Marketing, FaceTime Communications

COMP73

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

Do you really know who is accessing your critical data? Do you really know where threats to your data security originate? 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.

Presented by Paul Reymann, CEO, The Reymann Group; and Bob Flinton, VP Product Marketing, netForensics

---

See the current scheduled sessions for all courses:
http://www.bankinfosecurity.com/webinarsCalendar.php

Fraud

Bank Fraud is commonly known as a "crime of persuasion," involving efforts to knowingly execute, or attempting to execute, a plan to defraud a financial institution, or to obtain property controlled by a financial institution, by means of false or fraudulent pretenses. Check fraud, wire/ACH fraud, debit card fraud, ATM fraud, phishing and other identity theft attempts all fall under the fraud category.

FR125

ATM Fraud: Strategies to Beat the Skimming Scams

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

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

Presented by P. Kevin Smith, CPP; and Jeff Rinehart, Special Agent, United States Secret Service, Criminal Investigative Division; and Christopher J. Carney, Business Development Manager, Financial & Banking, ADT Security Services, Inc.

FR129

Beyond Heartland: How to Prevent Breaches of Security and Trust

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

- An overview of the Heartland breach and its impact on banking institutions, as portrayed by Tom Field, Editorial Director of ISMG;
- 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.

Presented by Tom Field, Editorial Director of Information Security Media Group; Stephen Wilson, VP of McGehee Bank; Randy Sabett, Privacy Attorney; Kevin Prince, Chief Architect of Perimeter eSecurity

FR29

Beyond Phishing - The Growing Crimeware Threat

Join the industry experts in a one hour presentation discussing the growing threat phishing presents to the banking and finance industry.

- 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 and RSA Security

FR149

Business Banking Under Attack: How to Fight Back Against Cybercriminals

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

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

Presented by Linda Coven, Head of Online Banking Channel Solutions, Silicon Valley Bank; and Terry Austin, President & CEO, Guardian Analytics, Inc.

FR152

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

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

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

Presented by Mike Mulholand, Director, Fraud Solution Strategy - Memento, Inc.; and Tim Brady, Director, Investigation Services - Memento, Inc.

FR194

Debit Fraud: Trends and Typologies

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

- Overview of Debit Fraud;
- Current & Forecasted Trends;
- Typologies & Sample Scenarios;
- Things to look for in a fraud solution.

Presented by Charles Robertson, Verafin

FR67

Defending Against The Insider Threat

The insider threat - it may be the hardest to detect, yet it poses the greatest risk to information security and regulatory compliance.

- How to identify and mitigate insider threats;
- The different types of threats - accidental and malicious;
- Proper procedures and tools to help maintain regulatory compliance and protect against the insider threat.

Presented by Gerald Murphy, Director of Research Operations for Robert Frances Group

FR196

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

Payment card breaches, check fraud and phishing/vishing - these are the most common forms of fraud striking banking institutions today. Yet, what form of fraud do institutions feel most prepared to prevent? Money laundering. This is just one of the sobering results from the new Faces of Fraud: Fighting Back study conducted by BankInfoSecurity.com. 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:

- How to ensure you're prepared to defend against the most common fraud threats;
- Bridging the institutional silos that stand in the way of fighting fraud;
- How to improve employee and customer awareness, ensuring that fraud prevention is a shared responsibility.

Presented by Mike Urban, Senior Director & Fraud Chief, Fraud Product Management, FICO; Matthew Speare, SVP - Information Technology, M & T Bank Corporation; Tom Field, Editorial Director, Information Security Media Group

FR187

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

ACH and wire fraud. ATM skimming. Payment card compromises. Mortgage fraud. Phishing. Financial institutions are besieged by fraud threats today - and not just via one dominant channel, but through all of them. Simultaneously. How can institutions fight back - as well as educate & enlist their consumer and business customers to do their parts, too? Join this panel discussion to hear new insights from industry thought-leaders on:

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

Presented by Reed Taussig, President & CEO, ThreatMetrix; Matthew Speare, SVP - Information Technology, M & T Bank Corporation; Kim Peretti, Director of PricewaterhouseCoopers' U.S. Forensic Technology Solutions Practice; Ori Eisen, Founder, Chairman and Chief Innovation Officer, 41st Parameter; Keir Breitenfeld, Senior Director Fraud and Identity Solutions, Experian Decision Analytics

FR168

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

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

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

Presented by Neil Katkov - Celent; Robert Snider, Financial Industry Solutions Architect with IBM; David Dixon, Norkom's Managing Director of Financial Crime

FR40

Fighting Fraud Schemes: Education, Response and Defense

This webinar will describe many of the current financial scams that are circulating in our society right now, and will offer proactive defenses to prevent consumers and employers from falling victim to these scams, and what rights and resources are available should you become a victim of these type of crimes.

- Learn in detail the current financial scams in circulation from phishing and lottery scams, ATM and credit card skimming, among many others.
- Learn proactive defenses to prevent consumers and employers from falling victim.

Presented by Kirk McGee, AVP, Regional Security Officer at TD Banknorth, N.A.

FR172

Fighting Online Banking Cybercrime with a Holistic Security Strategy

Learn why the dynamic landscape of online banking and payments demands a strategic and holistic security strategy designed for the long haul, one that can withstand the ever-evolving threats against online banking.

- The opportunities for banks and credit unions to use online banking to capture increased wallet share, grow customer loyalty and grow revenue;
- The latest trends in cyber attacks against online banking and where fraudsters have the advantage;
- Why a bank's strategic advantage - deep knowledge of the customer - is the centerpiece of a holistic security strategy and how it can be used to stop new and emerging attacks like Man-in-the-Browser attacks;
- How a layered approach built on behavioral analytics and risk scoring makes other security technologies like MFA, OOB, and secure clients more effective and more valuable and create an environment that can withstand ever-evolving threats against institutions.

Presented by Jerry Silva, Founder, PG Silva Consulting and Terry Austin, President & CEO, Guardian Analytics, Inc.

FR192

The Fraud Deficit: Why Deposit Account Fraud Budgets Need to Shrink

To effectively manage fraud prevention teams, processes and technology, banks and credit unions must establish annual fraud "budgets" to predict, measure and account for losses and other related costs. Explore the impact of thinking of fraud as a budgeted expense which is "under control" as long as the budget is met and how new approaches can shrink fraud budgets and increase bank profits. Join industry experts Andy Schmidt, George Tubin and Shirley Inscoe as they discuss:

- The true cost of deposit account fraud;
- Why many fraud budgets are too high;
- Why check fraud losses continue to go up;
- How to effectively engage senior management.

Presented by George Tubin, Senior Research Director, TowerGroup, Inc.; Andy Schmidt, Research Director - Global Payments, TowerGroup, Inc.; Shirley Inscoe, Director - Financial Services Solutions, Memento

FR120

Fraud Detection & Prevention Strategies for Financial Institutions: Emerging Technologies Insights

The recent Heartland Payment Systems data breach exposed hundreds of banking institutions and thousands of customers to potential credit and debit card fraud. But Heartland is only one example of the many fraud risks that threaten institutions from the inside and out.

- Hear about the top fraud threats facing financial institutions - inside and out -- including examples such as the Heartland Payment Systems breach;
- Learn best-practices for detecting suspicious behavior and high-risk activities;
- Discuss strategies for defending against fraudsters without negatively impacting your systems or the customer experience.

Presented by Tom Wills, Senior Analyst Risk, Security & Fraud, Javelin Strategy & Research and Steve Neville, Director of Identity Products, Entrust

FR177

Fraud Prevention: Protect Your Customers and Your Institution from Web Vulnerabilities

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.

- 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.

Presented by Matthew Speare, SVP of IT, M&T Bank; Patrik Runald, Sr. Manager of Security Research at Websense; and David Navetta, Founding Partner, Information Law Group

FR83

How Identity Fraud is Evolving and Impacting Customer Trust in Your Financial Institution

Learn about the latest findings on the impact of identity fraud on your financial institution and your customers:

- Why banking customers are shying away from the online banking channel
- How stolen identities are used to defraud your customers and damage your brand
- Which banking channels are most vulnerable to identity fraud
- How financial institutions are empowering customers to prevent identity fraud
- The latest phishing trends and tactics to commit identity theft
- The techniques financial institutions use to protect their brands and customers from identity fraud

Presented by John LaCour, CISSP and Rachel Kim

FR155

Identity Theft: How to Respond to the New National Crisis

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 national identity theft crisis.

- 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.

Presented by Neville Pattinson, VP of Government Affairs & Standards, NA., Gemalto information

FR144

Incident Response: How to React to Payment Card Fraud

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.

- How to immediately respond to a payment card breach;
- Lessons learned from Heartland and other incidents;
- Customer protection: What do you say and when?

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

FR35

Insider Fraud - Profiling & Prevention

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.

- Why is insider fraud on the rise now? What are the trends?
- What is the strategy of how to deal with it? Controls, analytics, etc.
- 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.

Presented by Paul Henninger of Actimize and Kirk McGee AVP, Regional Security Officer, TD Banknorth N.A

FR85

Insider Threats - Safeguarding Financial Enterprise Information Assets

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.

- Do you have more employees than active accounts?
- Do you know who is accessing your applications?
- Can you enforce password policy across all users?
- Do you have visibility into all access activities across disparate systems?
- Can you lock down ALL of a user's network and application access?

Presented by Geoff Hogan, Senior Vice President, Business Development & Product Management, Imprivata

FR178

Man-in-the-Browser Attacks: Strategies to Fight the Latest Round in Online Fraud

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 trend and threats. Attend this session to discover:

- 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

FR36

Preventing Phone Fraud with Voice Biometric Authentication

If you are a call center and IVR risk/fraud manager or compliance officer for a financial institution, or involved in cross-channel security, then this webinar is for you!

- Learn 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.

Presented by Dan Faulkner, Director of Product Marketing at Nuance; and Chuck Buffum, Senior Evangelist for Phone Authentication

FR44

Taking Fraud Out of Online Banking

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

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

FR211

ZeuS and Other Malware Threats Force Authentication to "Step Out" Of Band

Malware like ZeuS has rapidly outpaced all other banking security threats and, according to a recent survey, is regarded as the greatest threat to online banking today. Because malware has evolved to defeat most security measures currently in place, out-of-band authentication and transaction verification have taken on a new level of importance for financial institutions and regulators. During this webcast presenters:

- Share Insights From Their Latest Research On Online Banking Security;
- Dissect Current Malware Threats and Present The Latest Best Practices for Mitigating Them;
- Explore The Role Of Out-of-Band Authentication and

Transaction Verification in Preventing Fraud.

Presented by Sarah Fender, VP - Marketing & Product Management, PhoneFactor and Steve Dispensa, CTO & Co-Founder, PhoneFactor

---

See the current scheduled sessions for all courses:
http://www.bankinfosecurity.com/webinarsCalendar.php

Governance & Management

The fundamentals of information security at a banking institution, including how to conduct risk assessments, incident response and security awareness programs for employees and board members.

MGMT87

Avoid Negligent Hiring - Best Practices and Legal Compliance in Background Checks

Financial institutions, as well as all employers, have an obligation to exercise a reasonable duty of care in hiring. Can your institution afford the potential cost of a bad hire?

- How to obtain and utilize criminal record 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.

Presented by Les Rosen, President & CEO, ESR

MGMT11

Board Responsibilities for IT Risk Management: Building Blocks for a Secure System

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.

- 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.

Presented by Bill Sewall, Information security, compliance and risk management specialist

MGMT150

Creating a Culture of Security - Top 10 Elements of an Information Security Program

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.

- Develop the Security Program and Policy
- Manage Security Risks
- Provide User Awareness, Training and Education
- Respond to Incidents

Presented by Patrick Howard, Chief Information Security Officer, Nuclear Regulatory Commission

MGMT162

Data Protection and Incident Response

Get first-hand insight on incident response procedure, as well as roles and responsibilities for information security staff. We will take you inside a real case study from a unique government perspective, Matthews and Glave 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.

Presented by David Matthews, Deputy Chief Information

Security Officer for the City of Seattle and Geoff Glave, Product Manager, Absolute Software

MGMT20

Developing an Effective Information Security Awareness Training Program - Getting the Word Out

From GLBA to the ID Theft Red Flags Rule, information security awareness is a lynch pin of banking regulatory guidance. Register for this webinar to learn:

- The 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.

Presented by Bill Sewall, Information security, compliance and risk management specialist

MGMT135

How to Develop & Maintain Information Security Policies & Procedures

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.

- 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.

Presented by Bill Sewall, Information security, compliance and risk management specialist

MGMT50

How to Prevent Data Leakage from Compromising Your Company's Security

Listen to this webcast on turning your network, messaging and web gateways into security gateways, using strong bidirectional technologies that can ferret out infected computers, prevent data loss and eliminate Internet threats.

- 4 sources of potential abuse and 4 advanced technologies that can eliminate internal data threats
- 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

Presented by Elan Winkler, Director of Messaging Product Marketing, Secure Computing

MGMT137

Information Security for Management – What Your Senior Leaders Need to Know

By law, senior leaders must understand what's at risk, how information is protected and what their organizations are doing to maintain regulatory compliance.

- How to engage senior leaders about their role in enforcing security;
- 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

MGMT75

Information Security Risk Assessments: Understanding the Process

Federal regulators require financial institutions to conduct an information security risk assessment - but nobody shows them how. This session offers hands-on advice and tools you

can use.

- How to build process and strategies to identify and manage risks;
- How to tie risk assessment to your institution's daily business decisions;
- Risk assessment techniques that work - and those that don't.

Presented by Steven Jones - Vice President, Director Information Security, Synovus Financial Corp.

MGMT66

Insider Threat: Defend Your Enterprise

Studies show that nearly 80% of publicized data breaches come from internal sources. View this 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.

Presented by David Ting, Founder and CTO of Imprivata and Dan Moceri, Co-Founder and CEO of Convergent

MGMT176

Integrating Risk Management with Business Strategy

This session will focus on integrating 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) Solution 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 and Clark Abrahams, Chief Financial Architect, SAS

MGMT151

Key Considerations for Business Resiliency

Organizations understand the need for Business Continuity and Disaster Recovery in the face of disaster. But Business Resiliency is the new competency you need to develop.

- How to account for the most overlooked threats to sustaining your organization – and how to then test your plan effectively;
- Combining key components of Business Resiliency a heterogeneous approach;
- How to assemble the Business Resiliency basics;

Presented by John Pironti, President, IP Architects, LLC

MGMT173

Maintaining Secure Government Information Systems

Learn how to effectively support environments that require the highest levels of security, including Common Criteria, STIG, FIPS 140-2 and DCID 6/3. Topics will cover:

- Industry leading protection with SELinux - a mandatory Access Control System based on collaboration with the National Security Agency
- User authentication and access control with industry standard management and identity products
- Ease in automated provisioning, patching, and configuration management
- Flexibility in logging, and monitoring, and auditing

Presented by Rick Ring, Senior Solutions Architect, Red Hat

MGMT72

Offshore Outsourcing: Do You Know Where Your Data is and How it's Managed?

Just because you aren't directly offshoring any of your core systems or processes doesn't mean your third-party service provider isn't.

- The impact of political & cultural realities of overseas outsourcing;
- The differences between direct & indirect outsourcing;
- Responsible outsourcing (maximizing your returns while minimizing risk).

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

MGMT140

Proactive IT Risk Assessment Strategies

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 webcast: "Staying Ahead of Changing Threats."

- 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.

Presented by John Pescatore, VP and research fellow in Gartner Research; and André Gold, information Security Strategist and Business Development Consultant

MGMT89

Social Engineering: How to Train Your Employees to Spot and Stop the Scams

The strongest defenses in the world are worthless if someone leaves the gate open. That "someone" is any one of your well-intentioned employees, and the key to the "gate" is that individual's susceptibility to social engineering

- The latest social engineering scams targeting financial institutions;
- Proactive measures to mitigate the effects of "being socialed";
- How to test your employees preparedness.

Presented by E.J. Hilbert, former FBI Special Agent

MGMT167

Top 20 Critical Controls to Ensure Painless FISMA Compliance

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.

- 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.

Presented by Steve Trebbe, Director, Government Sales at Safend ; Mark P. Williamson, Chief Technology Officer and co-founder of Conquest Security; and Edy Almer, VP Product Management at Safend

---

See the current scheduled sessions for all courses:
http://www.bankinfosecurity.com/webinarsCalendar.php

IT Audits

The process of collecting and evaluating evidence of an Information Technology organization's assets, practices and operations to ensure policy/regulatory compliance. These reviews may be performed in conjunction with a financial statement audit, internal audit or other form of engagement.

ITA26

Preparing Your Institution for an IT General Controls Audit

Getting your institution ready for an IT audit needs preparation, planning and a sharpened knowledge of what systems really are running in your institution. Do you know what IT controls are in place?

- Why IT Audit is needed and what it will achieve;
- Tools to use in preparing for IT Audit;
- How to identify, evaluate and improve IT Controls.

Presented by Adam Losner, Founder, FTC Consulting

ITA219

Preparing for Your Next Audit: The Five Habits of Successful Security Programs

Institutions must enhance their security infrastructure and protect their customers' data in order to keep up with the demands of new and more stringent regulations. But how do you select the right providers for your institution to ensure compliance in your next audit? This webinar will present:

- The Five Habits of Successful Security Programs;
- Know Your Regulators;
- Internal Controls; Why They Are Important.

Presented by Andrew Jaquith, CTO, Perimeter E-Security

ITA214

Top 5 Reports IT Auditors Request

Meeting regulatory compliance is essential for financial institutions, but can be a time consuming process to validate. Knowing what the most common reports requested by Auditors can help to make this process more efficient. In this webinar, we will examine:

- The top 5 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.

Presented by Jagat Shah, CTO & Co-Founder, EventTracker by Prism Microsystems, Inc. and A .N. Ananth, CEO, EventTracker by Prism Microsystems, Inc.

See the current scheduled sessions for all courses:
http://www.bankinfosecurity.com/webinarsCalendar.php

Privacy

The protection of personal or classified data contained within a business information system.

PRIV82

Are You Effectively Protecting Your Customer's Private Data?

Identity theft is one of the fastest growing crimes in the country and concern by the public is growing rapidly with each new data breach exposed. Your customers, clients, partners and employees all trust your organization to take the appropriate steps to ensure the safety of their Personally Identifiable Information (PII).

- Gain an understanding of Personally Identifiable Information and what types of information are most valuable to thieves.
- Learn how many organizations expose PII and end up on the pages of today's newspapers.
- Determine if your organization is properly protecting PII.
- Learn how you can quickly and cost-effectively employ a SaaS solution to reduce the risk of security incidents involving PII and remedy information security weaknesses.

Presented by Jeff Pollard, Technical Sales Engineer for Perimeter eSecurity

PRIV63

Responding to a Privacy Breach: Protect Yourself and Your Vendors

Privacy breaches can have a devastating impact upon organizations if they do not respond to them well - and ensure that their third-party service providers are also

adequately protected.

- How to plan for - and respond to - a privacy breach;
- Steps to take to prevent a similar privacy breach;
- Why organizations must ensure their vendors have plans for security incidents and privacy breaches.

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

PRIV145

Social Networking: Is Your Institution Ready for the Risks?

Are your employees using Facebook, Twitter, and Linked-In safely, within your guidelines (do you even have guidelines?) and without divulging potentially compromising information? And do you have a risk management policy in place?

- How to develop corporate guidelines outlining the use of social networking sites such as Facebook, Twitter and Linked-In;
- How to respond to a social networking incident that compromises security.

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

---

See the current scheduled sessions for all courses:
http://www.bankinfosecurity.com/webinarsCalendar.php

Technology

Information technology is at once the backbone of an effective banking institution – and one of its biggest vulnerabilities. Our experts lead you through sessions ranging from testing your own internal security controls to piloting a mobile banking program.

IST205

5 Critical Data Security Predictions for 2011

There were a number of lessons to learn from the data security mistakes in 2010. The term "data leak prevention" entered common usage among security professionals, while new buzzwords like "advanced persistent threat" presented more to worry about. This webinar highlights:

- Top security stories of 2010;
- Key Incidents and Lessons Learned;
- Predictions for 2011

Presented by Andrew Jaquith, CTO, Perimeter E-Security

IST110

Application Security Testing and OCC Bulletin 2009-16 Compliance

Your IT organization - no matter what the size is learning to do more with less. Yet whether you choose to build applications internally, purchase third party software or outsource your needs, the burden of managing IT security risk—and specifically application security risk—has not reduced.

- Hear about how leading organizations are leveraging Bulletin 2008-16 as a blueprint for securing third party applications;
- Learn about contract language you can use in SLAs to demand secure software from third parties;
- Learn to cost-effectively manage the risk of built, bought or outsourced code without additional hardware, software or personnel investments.

Presented by Mike Puglia, Director of Product Marketing, Veracode

IST130

Assessing Encryption Standards for Financial Institutions

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 email traffic to board communications, remote access and mobile & Internet banking.

- 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.

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

IST188

Cloud Computing: Regulatory Security & Privacy Challenges

Cloud computing is the hot, new practice that offers a scalable, centralized resource for data and applications that can be available to anyone, anywhere. But as an emerging trend, cloud computing is also fraught with risk - already we've seen organizations whose data has been compromised. Register for this session to hear the lessons learned about cloud computing from a panel of experts who will discuss:

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

Presented by Matthew Speare, SVP - Information Technology, M & T Bank Corporation; Michael Smith, Security Evangelist, Akamai; Harold Moss, CTO - Cloud Security Strategy, IBM

IST194

Debit Fraud: Trends and Typologies

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

- Overview of Debit Fraud;
- Current & Forecasted Trends;
- Typologies & Sample Scenarios;
- Things to look for in a fraud solution.

Presented by Charles Robertson, Verafin

IST204

The Dirty Little Secret About Network Security

If you are sending data over a service provider's network, there is a dirty little secret you need to know. 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. Register for this webinar to learn about:

- The importance of data centric security and the latest findings in 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.

Presented by Jim Doherty, Chief Marketing Officer, CipherOptics; Michael Davis, CEO, Savid Technologies

IST180

Email Security Requirements for Healthcare Providers: HIPAA & Beyond

Learn what to look for in a secure email solution for complying with the web of regulations that now apply to so many companies.

- 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 US economic stimulus legislation (ARRA) that expand the scope of HIPAA security rules, and the impact on your organization's email security and compliance strategy;
- New HIPAA violation penalties and the impact of the breach notification requirements enforced by the

FTC;

- Technology requirements for protecting the confidentiality of healthcare information in both outbound and archived email messages.

Presented by Rami Habal, Director of Product Marketing, Proofpoint

IST187

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

ACH and wire fraud. ATM skimming. Payment card compromises. Mortgage fraud. Phishing. Financial institutions are besieged by fraud threats today - and not just via one dominant channel, but through all of them. Simultaneously. How can institutions fight back - as well as educate & enlist their consumer and business customers to do their parts, too? Join this panel discussion to hear new insights from industry thought-leaders on:

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

Presented by Reed Taussig, President & CEO, ThreatMetrix; Matthew Speare, SVP - Information Technology, M & T Bank Corporation; Kim Peretti, Director of PricewaterhouseCoopers' U.S. Forensic Technology Solutions Practice; Ori Eisen, Founder, Chairman and Chief Innovation Officer, 41st Parameter; Keir Breitenfeld, Senior Director Fraud and Identity Solutions, Experian Decision Analytics

IST192

The Fraud Deficit: Why Deposit Account Fraud Budgets Need to Shrink

To effectively manage fraud prevention teams, processes and technology, banks and credit unions must establish annual fraud "budgets" to predict, measure and account for losses and other related costs. Explore the impact of thinking of fraud as a budgeted expense which is "under control" as long as the budget is met and how new approaches can shrink fraud budgets and increase bank profits. Join industry experts Andy Schmidt, George Tubin and Shirley Inscoe as they discuss:

- The true cost of deposit account fraud;
- Why many fraud budgets are too high;
- Why check fraud losses continue to go up;
- How to effectively engage senior management.

Presented by George Tubin, Senior Research Director, TowerGroup, Inc.; Andy Schmidt, Research Director - Global Payments, TowerGroup, Inc.; Shirley Inscoe, Director - Financial Services Solutions, Memento

IST118

The Future of Banking Enterprise Access Management & Authentication - Emerging Technologies Insights

At a time when the banking industry is in flux - institutions are failing and merging, and employee layoffs are widespread - it is imperative that banking institutions improve their enterprise Identity Access and Management (IAM) practices.

- Hear about emerging trends in banking enterprise access management;
- Find out how employee access management and authentication can be improved with emerging technologies and new functionalities;
- Learn how to reduce your vulnerability to employee threats and insider fraud.

Presented by Paul Smocer, VP Security, BITS and Robert Grapes, Chief Technologist - Cloakware and David Dingwall, Senior Solutions Architect - Fox Technologies

IST105

How To Launch a Secure & Successful Mobile Banking Platform

Mobile banking ranks #1 among new services being rolled out by banking institutions of all sizes.

- The pros and cons of popular mobile solutions in the marketplace;

- Whether to build your program with internal or outsourced resources;
- How to create the most secure mobile banking program;
- How to prepare for future regulations/ examinations for mobile banking.

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

IST58

How to Use Your Mobile Phone for Free Two-Factor Authentication

Listen to this webinar to learn more about PhoneFactor and how it simplifies two-factor authentication. You'll learn:

- 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.

Presented by Jason Sloderbeck, VP of Security & Service Delivery, Positive Networks; and Evan Conway, Executive Vice President of Channel Management, Positive Networks

IST163

The Identity Enabled Network: The Future of Secure Cyberspace

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.

- 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.

Presented by Russel Rice, Director of Marketing, Policy Management Business Unit - Cisco; and Dave Klein, Lead Systems Engineer - Cisco Federal Security

IST48

The Identity Management Challenge for Financial Institutions

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?

- 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.

Presented by Gijo Mathew, CA

IST217

Is Your Device Identification Ready for New FFIEC Guidance?

Since the FFIEC guidance on "Authentication in an Internet Banking Environment" cybercriminals have evolved, leading the FFIEC to draft new guidance for protecting your business and customers from fraud. Learn about smart device identification technologies banks will need to comply with new FFIEC guidance and meet today's challenges of identity and password theft, botnets, trojans and new risks introduced by smartphones including:

- What smart identification entails;

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

Presented by Alisdair Faulkner, Chief Products Officer, ThreatMetrix

IST159

Legal Considerations About Cloud Computing

Organizations have jumped to embrace the concept of "cloud computing" - accessing virtualized resources via the Internet. But have they leapt too soon without weighing all the legal considerations? Register for this webinar to hear a government security leader's insights on:

- E-discovery and records retention challenges;
- Responsibilities and risks;
- The future of cloud computing.

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

IST30

Malware, Crimeware, and Phishing - An In Depth Look at Threats, Defenses

The evolution of malware and crimeware has produced more insidious and harmful intrusions to networks and systems at financial institutions. Understand how to mitigate these threats.

- Overview of current attacks and help to anticipate likely trends;
- Traditional and current malware, and different types of phishing;
- The human factor as an increasing factor in phishing solutions.

Presented by Markus Jakobsson, Associate Professor, Indiana University

IST170

Managing Shared Passwords for Super-User Accounts

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 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.

Presented by Dr. Eugene Schultz, CISM, CISSP, Chief Technology Officer at Emagined Security; and David McNeely, Director of Product Management at Centrify Corporation

IST189

Meeting Federal Compliance to Secure Windows Desktops

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

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

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

IST216

The Mobile Environment: Challenges and Opportunities for Secure Banking

Financial institutions are no exception to the pressure of extending their online services to the mobile channel. By

2015 mobile banking could reach one in five adults in the United States. Growth in mobile devices has also driven the incidence of mobile fraud. As banks look to capitalize on the mobile environment they are needing to bolster consumer confidence in online banking, particularly in the face of pending new FFIEC guidelines. This webcast gives insight into:Best Practice tips to ensure your desktop security policies meet Federal mandates;

- Understanding the latest threats to mobile and online banking;
- Why current solutions are ineffective against the latest fraud threats;
- New approaches for strong authentication and transaction verification;
- How mobile devices can strengthen mobile and online security and address pending FFIEC regulatory guidance.

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

IST213

Next-Generation Threats: Understanding, Investigating and Defending Global Attacks Against the Financial Services Industry

In this session, learn current and next-generation methodologies being deployed by global organized crime rings, and effective techniques to analyze and disrupt them. Also gain insights on conducting global due diligence operations on international individuals and companies. To protect your organization, your assets and your customers from fraudsters takes both an understanding of their capabilities and techniques. Topics discussed include:

- Current and emerging methodologies employed by organized crime to defraud financial institutions;
- Structure and methodologies for black market malware distribution and money laundering through physical and virtual money mules ;
- Advanced information on international due diligence and compliance issues that will benefit financial organizations;
- Successful cases of investigation and arrest.

Presented by Ronald Plesco, CEO, National Cyber Forensic Training Alliance, William News, Director - Investigative Resources, NFC Global and Brandt Heatherington, Global Director - Commercial Marketing, i2 Group

IST190

Power Systems: How to Prevent Unauthorized Transactions

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 1500 IBM servers;
- Learn best practices for auditing network access (including FTP), user profiles, and events;
- Determine your organization's true network security status.

Presented by Robin Tatam, Director - Security Technologies, PowerTech; Jill Martin, Product Support Manager, PowerTech

IST33

Preventing TJX Type Data Breaches

In this webinar, attendees will hear from industry veterans - Susan Orr, a former federal regulator, and William Henley, Director of IT Risk Management at the OTS. During the course of the presentation the speakers will outline the state of affairs that financial institutions face when it comes to the regulations and compliance guidance that cover data protection. Attendees will also hear best practices in data protection from a regulator and a banker including "lessons learned" from previous data breaches that attendees can use to improve data protection at their institution.

- Lessons learned from TJX and previous data breaches to improve data protection;
- Outline data protection regulations financial

institutions face;

- What regulators expect financial institutions to have in place for data protection;
- Best practices in data protection from a regulator, banker and processor.

Presented by Susan Orr, of Susan Orr Consulting; William Henley, Director of IT Risk Management at the OTS

IST119

Preventing Unauthorized Access To Your Institution's Data

In this webinar - the third installment of Information Security Media Group's Emerging Technologies Insights series - 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 & internal threats via cloud/client security model, securing email, and data leak prevention.

Presented by Tom Wills, Senior Analyst Risk, Security & Fraud, Javelin Strategy & Research; and Victor Lee, Director, Data Protection Marketing, Trend Micro, Inc.; and Tom Field, Editorial Director, ISMG

IST185

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

Email continues to be one of the primary risk vectors of exposure of Controlled Unclassified Information (CUI) and other sensitive data in federal organizations today, but most have yet to deploy technology to help prevent costly breaches. Join this discussion to find out what you need to know about the latest security, data privacy and archiving regulations for government agencies. 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.

Presented by Jeff Lake, VP - Federal Operations, Proofpoint

IST179

The Reality of Cyberattacks: Emerging Solutions for Today's Threats

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.

- 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; and Robert Rodriguez, Chairman & Founder - Security Innovation Network; and Mark Bower, Vice President Product Management - Voltage Security

IST141

Securing Your Email Infrastructure

One compromised e-mail can damage your corporate brand, compromise intellectual property or put you in non-compliance with the law.

- Factors that drive the need for secure communication;
- How to deploy email encryption;

- Key technology considerations for securing your e-mail.

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

IST146

Security Risks of Unified Communications: Social Media & Web 2.0

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.

- 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.

Presented by Eric Young, Senior Director of Field Services, FaceTime Communications; and John Vigilante, Unified Communications Specialist, Microsoft and Michael Osterman, President, Osterman Research

IST193

Social Networking Compliance for FINRA Regulated Organizations

Now you can maintain FINRA compliance across Facebook, LinkedIn, Twitter and over 1000 social networks. The secrets are shared during this exclusive webinar. Control and compliance is the key to Social Media survival in today's regulated industries. So you need a solution for true compliance. This exclusive webinar will explore the requirements of FINRA with regard to Social Networking - and how Socialite, a new social media compliance solution from FaceTime Communications, helps you meet them.

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

Presented by Sarah Carter, VP - Marketing, FaceTime Communications

IST56

Testing Security Controls at a Banking Institution: Learn from the Experts

Banking regulations require financial services organizations to conduct independent testing of their computing and networking environment at regular intervals.

- 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.

Presented by James Kist, CISSP

IST161

Time: The Hidden Risks - How to Create Compliant Time Practices

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. 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.

Presented by Bill Sewall, Information security, compliance and risk management specialist

IST166

User Authentication: Best Practices for Managing Risk & Compliance

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. The 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.

- 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.

Presented by Sarah Fender, Vice President of Marketing & Product Management, PhoneFactor; and Steve Dispensa, Chief Technology Officer, PhoneFactor

IST39

Voice Over IP - Helping Organizations Learn and Mitigate Security Risks

Voice over IP or "VoIP", is becoming an attractive alternative to conventional phone networks. VoIP services are becoming more widely deployed in today's enterprise markets as an effective measure for cost savings and increased feature sets. Organizations must realize VoIP introduces fundamental changes to Internet Protocol (IP) architectures and creates new endpoints for attack. These new endpoints create new methods for hackers to find new methods for intrusion, extortion and pretexting.

- Understand what Voice over IP offers and the trade-offs between cost savings and security.
- Learn VoIP technical terminology, technology used to set up VoIP networks.
- Learn the attack methods used to break into VoIP networks and what to do to mitigate the security risks posed.

Presented by Juan Deaton, Cellular Systems Engineer at the Idaho National Lab's Next Generation Wireless Test Bed

---

See the current scheduled sessions for all courses:
http://www.bankinfosecurity.com/webinarsCalendar.php

Vendor Management

Each of the major regulatory agencies is now stressing the need for financial institutions to improve vendor management. In this new series of webinars, learn the vendor management basics, how to assess your vendors, and then the latest improvements to the BITS Shared Assessments Program.

VM188

Cloud Computing: Regulatory Security & Privacy Challenges

Cloud computing is the hot, new practice that offers a scalable, centralized resource for data and applications that can be available to anyone, anywhere. But as an emerging trend, cloud computing is also fraught with risk - already we've seen organizations whose data has been compromised. Register for this session to hear the lessons learned about cloud computing from a panel of experts who will discuss:

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

Presented by Matthew Speare, SVP - Information Technology, M & T Bank Corporation; Michael Smith, Security Evangelist, Akamai; Harold Moss, CTO - Cloud Security Strategy, IBM

VM127

Evaluating Security Risks Associated with Banking Vendors

A new approach is needed to secure, make compliance easier, and enhance the operating efficiency for critical financial data centers and those processing sensitive cardholder information or personally identifiable information (PII).

- Facilitate PCI compliance and go beyond to provide demonstrable security for critical financial data centers
- Decrease the burden of proof and yet provide the verification of operational controls in a new way that will increase confidence for vendor management due diligence
- Reduce your risk and secure your infrastructure against emerging threats to ensure that only authorized changes are allowed

Presented by Kim Singletary, Director of OEM & Compliance Solutions, Solidcore Systems and Ken Harris, Vice President, MTXEPS Inc. and Preetham Gowda, CIO, SecureNet Payment Solutions

VM13

How Well Do You Know Your Vendors?

In this workshop, we will be looking at third-party oversight from the moment a project is initiated through production implementation and beyond. What does "third party oversight" really mean? What does it entail? Who is responsible for doing it, and what happens when the results do not turn out as expected? We will be looking at this topic from two vantage points – a security practitioner who developed and implemented a plan for a Fortune 500 bank, and a former FDIC regulator who would have evaluated the approach and reviewed the results.

- A look at why financial institutions want third party relationships;
- What do the regulators see as risks?
- Assessing a new product/service and its vendor;
- Planning an exit strategy.

Presented by Susan Orr, Founder of Susan Orr Consulting; and Anne Terwilliger

VM100

Protecting the Exchange of Sensitive Customer Data with Your Vendors

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.

- 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, email or IM?

Presented by Greg Shields, Microsoft MVP in Terminal Services; and Kevin Gillis, Vice President, Product Management at Ipswitch

VM143

Steps to Managing Security Risk from Your Software Vendors

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.

- 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 to cost-effectively manage the risk of built, bought or outsourced code without additional hardware, software or personnel investments.

Presented by Sam King, Vice President of Service Delivery, Veracode

VM98

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

The FDIC's Donald Saxinger details exactly what federal regulators are looking for when it comes to managing third-party service provider relationships

- Clarify Vendor Management guidance;
- Outline the four main elements of an effective third-party risk management process.

Presented by James Christiansen, CEO, Evantix & Donald Saxinger, Senior Examination Specialist, FDIC

VM104

Vendor Management Part II: Assessing Vendors - the Do's and Don'ts of Choosing a Third-Party Service Provider

- 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.

Presented by James Christiansen, CEO, Evantix

VM117

Vendor Management Part III: Inside the BITS Shared Assessments Program

The BITS Shared Assessments Program allows institutions to evaluate the security controls of key IT service providers and meet regulatory compliance.

- The latest version enhancements;
- How to integrate the program's two key components - the Standardized Information Gathering questionnaire (SIG) and Agreed-Upon Procedures (AUP) into your existing framework.

Presented by Jim Routh, CISM, Chief Information Security Officer, The Depository Trust & Clearing Corporation; Eddie Holt, PartnerKPMG LLP; Michele Edson, Senior Vice President, The Santa Fe Group; Niall Browne, CISO, LiveOps; Scott Brown, Program Manager, Financial Services, Iron Mountain; Andrew Hout, Citi

VM88

You & Your Vendors: How to Best Secure Data Exchange

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.

- 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

Presented by Greg Pridgen, Director of Operations Support for TSYS and William McKinney, Global Product Marketing Director, Sterling Commerce

---

See the current scheduled sessions for all courses:
http://www.bankinfosecurity.com/webinarsCalendar.php

Start Training Today

Take advantage of our easy attendance options

A la Carte

The easiest way to attend a webinar. If you're looking for an introduction to what our training offers, attending a webinar a la carte is the best entry-point.

- One webinar at a time
- Single attendee or Corporate Pass (Up to 5 attendees)

Get Started

Vouchers

Purchase seats to a determined number of webinars up-front, and use them for whichever sessions you please, for yourself or for anyone at your institution.

- Multiple webinars, available in packs of 4, 10, and 20
- Flexible schedule

Get Started

Annual Membership

Register once, attend as many webinars as you'd like for an entire year. If you plan to attend multiple webinars, this is the option for you.

- Unlimited webinars for 1 year
- Coporate and Enterprise memberships available
- Transcript tracking interface
- Certificates which may be used towards CPE credits
- OnDemand access to our entire catalog, 24/7

Get Started

Membership: A Sound Business Case

For one flat annual fee – either as an individual or as a corporate member – you and your team can attend any or all of our unique webinars over the course of your subscription. These are sessions that normally cost hundreds of dollars each, but all are open to you as part of your membership.

Individual Membership

One person gains access to our entire library of webinars for one year. Included is a transcript-tracking page which organizes all of the classes the member attends along with the ability to print proof of attendance certificates on-demand, which may be used towards securing CPE credits.

Learn More

Corporate Membership

Ideal for your institution's information risk management and security team - up to 5 people from the institution can attend as many webinars as they'd like for an entire year. Each member can pick-and-choose their own webinars to attend, and have their own transcript-tracking page where they can print proof of attendance certificates, which may be used towards securing CPE credits.

Learn More

Enterprise Membership

Your entire organization gains unlimited access to our training portfolio for the entire year. Each division may access the webinars that are appropriate based on their information security and risk management responsibilities. Transcript tracking pages are available to prove attendance, which may be used towards securing CPE credits.

Learn More

Registration Form

Customer Information

First Name _____ Last Name _____

Title _____

Email Address _____

Company Name _____ Industry _____

Address _____

City _____ State _____ Zip _____

Telephone _____ Fax _____

Webinar Title (optional)

1. _____

2. _____

3. _____

Payment Method

☐ Check enclosed (Payable to "Information Security Media Group, Corp.")

☐ Visa ☐ Mastercard ☐ AMEX ☐ Discover ☐ Company P.O.

Card Number _____ Exp. Date _____

Billing Address _____

City _____ State _____ Zip _____

Signature _____ **Date** _____

Webinar Benefits

- **Earn CPE credits**
- **Save time & money — no travel required**
- **Further your education on information security, fraud, compliance, and risk management topics**

Select Attendance Method

Multiple Sessions

☐ Vouchers (4 pack)	$1,095
☐ Vouchers (10 pack)	$2,795
☐ Vouchers (20 pack)	$5,295

Unlimited Sessions (1 year)

☐ Indvidual Membership	$1,895
☐ Corporate Membership (Up to 5 individuals)	$6,995
☐ Enterprise Membership (Unlimited individuals)	CALL

Print and mail this form to:
Information Security Media Group
4 Independence Way, Suite 130
Princeton, NJ 08540
or fax: (732) 875-1065

Register Online

The easiest way to register! Visit BankInfoSecurity.com/training

Register Now

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

Employee training is a necessity for individuals in the banking industry. Our training webinars are taught by industry experts, devoted to current topics and offer the ability to earn CPE credits. Learn to solve the information security and risk management challenges of today with ISMG training.

Contact

Contact a representative for information on membership options:

ISMG Membership Team
(800) 944-0401
memberships@ismgcorp.com

BANK INFO SECURITY®

ISMG
INFORMATION SECURITY
MEDIA GROUP

ISMG
INFORMATION SECURITY
MEDIA GROUP

4 Independence Way | Princeton, NJ 08540
ISMGCorp.com