Information Security Shake Up: What to Expect in 2013

The Security for Business Innovation Council and RSA forecast developments to watch

Eddie Schwartz
Chief Security Officer, RSA, the Security Division of EMC
Security for Business Innovation Council’s
2013 Trends Report

• Marene Allison, Worldwide Vice President of Information Security, Johnson & Johnson
• Anish Bhimani, Chief Information Risk Officer, JPMorgan Chase
• William Boni, Corporate Information Security Officer (CISO) and Vice President, Enterprise Information Security, T-Mobile USA
• Roland Cloutier, Vice President, Chief Security Officer, Automatic Data Processing, Inc.
• Dr. Martijn Dekker, Senior Vice President, Chief Information Security Officer, ABN Amro
• Jerry Geisler, Office of the Chief Information Security Officer, Walmart Stores Inc.
• Renee Guttmann, Chief Information Security Officer, The Coca-Cola Company
• Malcolm Harkins, Vice President and Chief Information Security Officer, General Manager, Information Risk and Security, Intel
• Kenneth Haertling, Vice President and Chief Security Officer, TELUS
• Petri Kuivala, Chief Information Security Officer, Nokia
• Dave Martin, Vice President and Chief Security Officer, EMC Corporation
• Tim McKnight, Executive Vice President, Enterprise Information Security & Risk, Fidelity Investments
• Felix Mohan, Senior Vice President and Global Chief Information Security Officer, Airtel
• Bob Rodger, Group Head of Infrastructure Security, HSBC Holdings plc.
• Ralph Salomon, Vice President IT Security & Risk Office, SAP AG
• Vishal Salvi, Chief Information Security Officer and Senior Vice President, HDFC Bank Limited
• Simon Strickland, Global Head of Security, AstraZeneca
• Leanne Toliver, Interim Chief Information Security Officer, Global Information Security, eBay
• Denise Wood, Corporate Vice President, Information Security, Chief Information Security Officer, Chief IT Risk Officer, FedEx Corp.
2013: The Shake-up Continues

• The threat landscape continues to become more complex
  – Criminal hackers continue getting better, faster—and more collaborative
  – New nations entering the mix with better cyber weapons and tactics
  – Anonymous, insiders, etc.

• Business imperatives: Cloud, social media and mobile technologies expand enterprise risks

• Security gaps: Support, training, technology, process

• Continued pressure on governments to act on our collective behalf … and continued governmental inaction

• Major security event? Conditions are ripe for something much worse than theft or espionage
2013: Rapid Transformation Required

• Accelerate “Intelligence-driven Security” approaches with big data analytics
  – SOC, GRC, IAM

• Develop consultative role for security within the business
  – What really matters?

• Court middle management to gain full support for security initiatives
  – These people really care!

• Enhance supply chain acuity and awareness
  – Where are you in the supply chain?

• Innovate to close security gaps opened by cloud, mobile and social media
SBIC Guidance: Adapting Security for Cloud Computing

• Make the case to earmark IT funds freed up by moving to cloud computing for information-security oversight
• Plan to increase resources for cloud vendor management and ensure your team has skills to evaluate software controls and to secure virtualized environments
• Segregate controls implementation from controls assurance to ensure impartial oversight
• Investigate the possibility of sharing cloud vendor assessments with a small number of trusted partners to reduce redundancy and costs
• Leverage technologies that can perform automated assurance, continuous monitoring and provide visibility into cloud environments such as GRC solutions
• Investigate next-generation encryption solutions that can be used to protect sensitive data in the cloud
• Align plans for an extended “internal” control system with external auditors at an early stage
SBIC Guidance: Adapting Security for Social Media

- Establish a multidisciplinary team to develop a social media risk management strategy, setting clear policies addressing code of conduct, organizational responsibilities and incident response
- Deliver ongoing end-user awareness training programs, including educating employees on what is appropriate to post on social channels and monitor employees’ social media activities
- Monitor social media for threat intelligence and for public-facing threats such as brand hijacking, malware and misrepresentation
- Conduct crisis management drills and exercises to test and improve responsiveness
- Set up Facebook/Twitter accounts for corporate leaders to pre-empt falsified accounts
SBIC Guidance: Adapting Security for Enterprise Mobility

• Establish mobile governance plan, setting goals and acceptable risk levels
• Create action plan built for change—plan for a 12- to 18-month horizon
• Use encryption, MDMs and remote wipe to secure data on devices, but try not to store data on devices at all (VDI)
• Build security into mobile programs at the forefront, not as an afterthought
• Good luck! 😊
THANK YOU

eddie.schwartz@rsa.com
@eddieschwartz
http://www.linkedin.com/in/eddieschwartz/