CISO View: Top 4 Major Imperatives for Enterprise Defense

James Christiansen

Chief Information Security Officer

Evantix, Inc.

Gary Terrell CIPP

Chief Information Security Officer

Adobe

Session ID: Star 403

Session Classification: Intermediate

RSA CONFERENCE 2012

InfoSec Major Imperatives

- How do you focus your limited resources to keep up with the ever changing threat landscape?
- How can a CISO keep up?
- This session focuses on the 4 major imperatives for enterprise defense:
  - evolving security beyond “Outside/In” defenses
  - increasing regulatory focus on data protection
  - extending security controls into the Cloud
  - mobilization of enterprise

Objectives

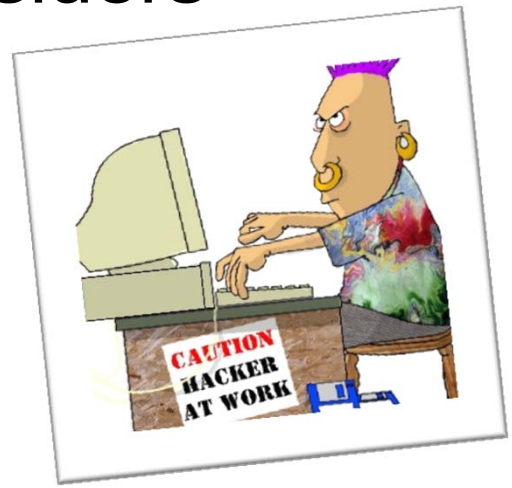
- Learn from current cyber events why these 4 imperatives are so important
- See how to establish your own strategy to meet the demand of modern threats and make it relevant to your environment
- Discuss practical advice for creating a tactical plan for protecting your company from people that have the experience to tackle these issues
- Understand how to build an action plan so you can be ready and quickly react to new threats

Key Leadership Questions

- Given the actual threats encountered in 2011 what do threats look like in 2012?
- How do you think about threats and how do you communicate them to executive teams?
- What 4 imperatives help you deal with threats to separate real threats from background noise?

#1-Beyond ‘Outside / In’ to ‘Inside / Out’ Defense

- “Outside / In” focuses on external threats
  - Mature tools in place have helped control threats
  - Many years experience dealing with these threats has resulted in well established procedures
  - Disaster Recovery and Business Continuity initiatives have elevated awareness of this class of threats
- “Inside / Out” focuses on malicious insiders
  - Fewer tools to monitor data leakage and threats posed by insiders – employees, business partners, temporary workers and contractors



Beyond ‘Outside / In’ to ‘Inside / Out’ Defense

- Data Leakage sources
  - Unintentional employee errors
  - Outsiders: malware, spam, spyware, and hackers
  - Data stolen by employee or Third Party
  - Insider sabotage

- Monitor internal environment
  - FTP, Email and Instant Messaging
  - Media Room
  - Media Disposal

#2-Increased Focus on Data Protection

- Federal Government
  - GLBA
  - HIPAA-HITECH
  - FCRA – Red Flags
- State Privacy Acts
  - Massachusetts
  - Nevada
- International Regulations
  - UK Data Protection Directive
  - Malaysia Data Protection Act
  - French Data Protection Authority

Impact of Data Breaches Growing

- Organized, planned and coordinated attacks generally target specific data/information
  - Breaches impact involve short and long term financial losses
  - Breaches may involve reputation impact when reported
- Hactivism attacks generally target customer information and related data
  - Breaches involve short term financial loss
  - Breaches often involve long term reputation impact

#3-Extend Security Controls to the Cloud

- Before Engagement:
  - Risk vary depending on the cloud category and service model
- During Negotiations:
  - Address the risk requirements, ongoing due diligence and exit strategy
- During Relationship:
  - At least an annual review of security practices. Use a best practice risk methodology to manage the risk
- Exiting Relationship:
  - Plan and continually revise your exit strategy. During exit make sure all information is destroyed

Pro: Security is Core to Cloud Services

- Cloud Computing Companies offer benefits of scale
  - Core product of company provides focus on infrastructure
  - Staffing dedicated to infrastructure and security
  - Reduced overall cost of physical security
- Scale and Agility
  - Cloud computing companies depend on their ability to be agile in delivery and scale quickly to meet client demands
  - Ability to reroute application/network traffic to thwart DOS attacks

Con: Controlling Data is Challenging

- Loss of Direct Control
  - The security controls are in the hands of the cloud providers
  - Malicious Insiders
- Data Protection
  - A shared environment can offer more avenues for data access
  - Movement of data between clouds
  - Complete Data destruction is very difficult in shared cloud
- Legal Risks
  - Electronic Discovery
  - Electronic Forensics

Con: Controlling Data is Challenging

- Compliance Risk
  - State, Local, Federal and International Regulations
  - Industry specific requirements (e.g. PCI)
  - Providing evidence of compliance
- Exit Strategy
  - Being able to move your service in-house or other provider

Cloud Computing Security Management Tools

- Audience interactive discussion:
  - How to handle event logs?
  - How do we manage malware?
  - How do we manage data integrity
  - Tools that are missing in market?
  - What experiences have you had that worked and didn't work?

#4-Mobilization of the Enterprise

- Mobil Device Growth
  - According to a survey by Good Technology, the number of consumer devices entering the workplace has doubled in six months

- Mobile Device Breaches
  - Mobile devices used to commit data breaches increased significantly in cases closed in 2010
  - Leading the way were compromised POS terminals, pay-at-the-pump terminals, and ATMs

#4-Mobilization of the Enterprise

- Security Strategy
  - Traditional practices for securing data on servers does not protect data cached on mobile devices
- Mobile Security Agent
  - An agent on the mobile device is required to establish security controls to encrypt, pins and pw and selective wipes of business data

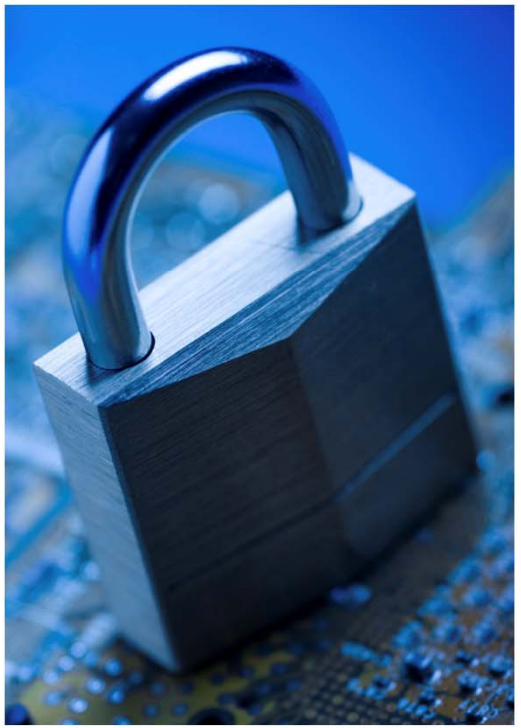
Applying Limited Resources to Changing Threats

- Applying Technology Investments
  - Balance investments in traditional security technology and some cloud centric technologies
  - Examples and benefits of technology investments
- Applying Human Investments
  - Retrain/redeploy human resource to higher value risk activities
  - Examples and benefits of human resource investments

Attacks are trending up sharply year over year

How to Apply What You Have Learned

- Within three months, you should:
  - Assess the impact of organization's use of mobile devices and cloud applications on data loss
  - Assess the rate of deployment to Cloud based applications and mobile services
  - Seek funding for the top 4 imperatives based on the risk of data loss



Conclusion

- We have covered:
  - How to focus your limited resources to keep up with the ever changing threat landscape
  - How a CISO can keep up with new innovations?
  - Top 4 major imperatives for cyber security defenses:
    - evolving security beyond “Outside/In” defenses
    - increasing regulatory focus on data protection
    - extending security controls to the Cloud
    - mobilization of enterprise

Q&A

- Questions?
- Presenter Contact Information:
  - James Christiansen
    - james.christiansen@evantix.com
    - (949) 614-7076
    - http://www.linkedin.com/in/EvantixJames
  - Gary Terrell
    - gary.terrell@adobe.com
    - (408) 536-4311
    - http://www.linkedin.com/in/garyterrell
- Thank You!