Information Security Experts Discuss What's Next

September 15, 2009

eBay – Town Hall
2161 N First Street
San Jose, CA

Agenda

- Introduction
- Privacy concerns
- Compliance
- Identity Management
- Risk management
- Key takeaways
- Q&A

Audience

- Security knowledge level
  - Novice
  - Intermediate
  - Expert
- Interested
  - Personally as a consumer
  - How to implement for your business/company
- Roles
  - Technical
  - Business
- Roles
  - Information security
  - Other business/ operational function
  - Compliance/governance
  - Consumer
  - Other

Expert Panelists

- **Leslie Lambert** – VP Information Technology, Sun Microsystems
- **Claire McDonough** – Security Program Manager, Google
- **Brianna Gamp** – Chief Security Architect, eBay
- **Leanne Toliver** – Distinguished Security Architect, eBay
- **Caroline Wong** – Global Information Chief of Staff, eBay

Agenda

- Introduction
- Privacy concerns – Leslie Lambert, Vice President, Information Technology, Sun Microsystems
- Compliance
- Identity Management
- Risk management
- Key takeaways
- Q&A

Privacy & Security

- Privacy & Security

  - You can have security without privacy, but you cannot have privacy without security.

- Defining Privacy

  - The appropriate use of personal information under the circumstances. What is appropriate will depend on context, law, and the individual's expectations; also, the right of an individual to control the collection, use, and disclosure of personal information.

- Privacy treated differently around the globe!

  - USA vs. EU vs. Asia

Privacy & Security

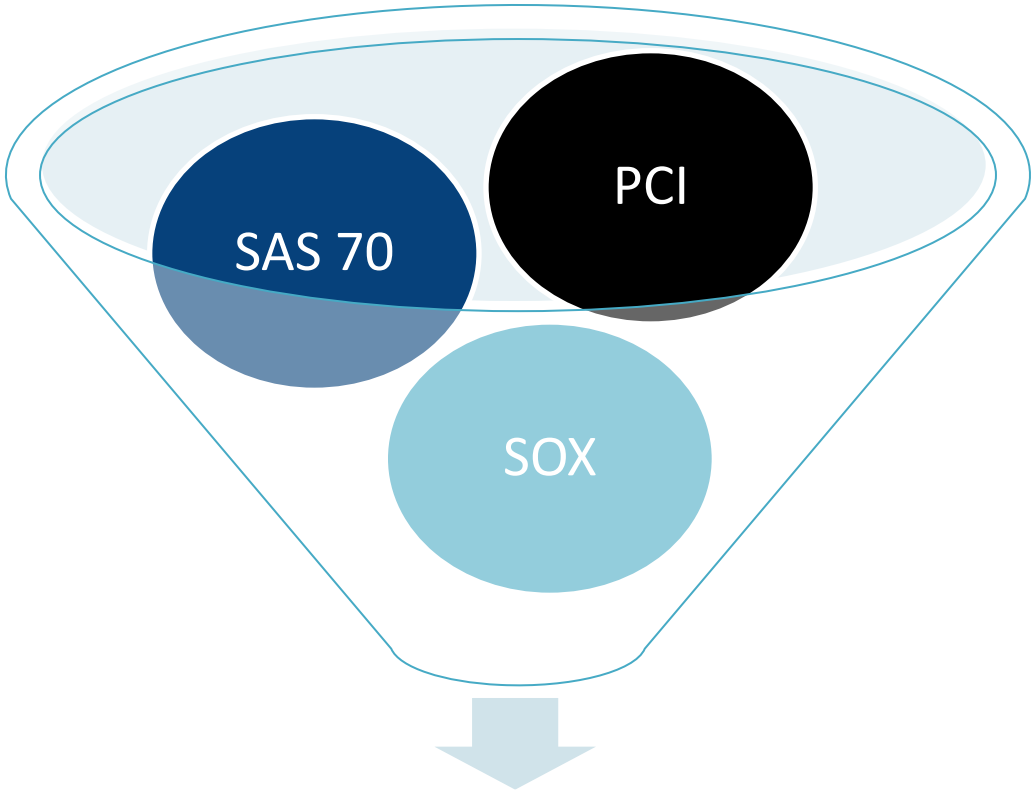
- Why address Privacy in an Information Security panel?
  - Managing and protecting data in the global information economy demands coordination between an organization's privacy and information security teams.
  - With the precipitous rise in reported security incidents, it is paramount that security and privacy work together effectively to deliver comprehensive and compliant programs for your organization.
- A New Language for Security Professionals
  - Notice, opt-in, opt-out, GLBA, HIPAA, Fair Information Practices…….
- Consider expanding your understanding of Privacy!
  - Certification via International Association of Privacy Professionals
  - Certified Information Privacy Professional -- CIPP & CIPP/IT

http://www.privacyassociation.org

Agenda

- Introduction
- Privacy concerns
- Compliance - Claire McDonough, Security Program Manager, Google
- Identity Management
- Risk management
- Key takeaways
- Q&A

Acronym Heaven



Controls to ensure that your information is protected

Build and Maintain a Secure Network	•Example 1: Install and maintain a firewall configuration to protect data •Example 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Data	•Example 3: Protect stored data •Example 4: Encrypt transmission of data across open, public networks
Maintain a Vulnerability Management Program	•Example 5: Use and regularly update anti-virus software •Example 6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures	•Example 7: Restrict access to data by business need-to-know •Example 8: Assign a unique ID to each person with computer access •Example 9: Restrict physical access to data
Regularly Monitor and Test Networks	•Example 10: Track and monitor all access to network resources and data •Example 11: Regularly test security systems and processes
Maintain an Information Security Policy	•Example 12: Maintain a policy that addresses information security

Agenda

- Introduction
- Privacy concerns
- Compliance
- Identity Management - Brianna Gamp, Chief Security Architect, eBay
- Risk management
- Key takeaways
- Q&A

Managing Identity

- Why is identity important?
  - Authentication
  - Authorization
- What can have an identity?
  - Employees
  - Customers
  - Applications
  - Hardware

Managing Identity

- What are the keys to good identity management?
  - Good verification of identity
  - Ability to have one identity that can have multiple assertions
  - Ability to have the customers to control their information

Agenda

- Introduction
- Privacy concerns
- Compliance
- Identity Management
- Risk management - Leanne Toliver, Distinguished Security Architect – Information Risk Management, eBay
- Key takeaways
- Q&A

Information Risk Management

Risk is the possibility of suffering harm or loss. Risk refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence. Risk is composed of an event, a consequence, and uncertainty.

Risk Management is the practice of identifying risks and threats, evaluating the likelihood or probability of exploit, analyzing the effectiveness of controls to mitigate, and determine the overall acceptable level of risk in the environment.

Information Risk Management is identifying and measuring the risks to information and ensuring that the security controls implemented keep those risks at an acceptable level to protect and enable the business.

Key Information Risk Definitions:

Threat – anything (object/person/etc.) that is capable in acting against an asset in a manner that can result in harm.

Vulnerability – weakness that may be exploited by the threat.

Asset – any data, device, or other component of the environment that supports information-related activities which can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen resulting in loss.

Five Steps to Implementation

5 Steps to Implementing a Risk Management Program

- Assess known and emerging threats and determine probability or likelihood of occurrence
- Create or update Information Security policies, standards, or procedures
- Continuously assess and review compliance with policies and standards
- Monitor for threat occurrence and measure results
- Report and communicate results to accountable individuals.

Agenda

- Introduction
- Privacy concerns
- Compliance
- Identity Management
- Risk management
- **Key takeaways - Caroline Wong – Global Information Chief of Staff, eBay**
- Q&A

Markets are down, but Fraud is up!

Phishing in a Down Economy – Company layoffs (spear-phishing), unemployment checks

Timely Social Engineering – Link to Obama's speech (trojan)

Social Messaging – "Look at this!" messages on Facebook re-direct to a fake Facebook profile page requiring log-in with username and password, Twitter "Best Video" link installing malware

Best Practices & Key Take-aways

Phishing and Social Engineering – Be wary of emails that are unexpected and asking for sensitive or financial information. Only distribute information on a need-to-know basis.

Passwords - Use complex passwords with numbers, special characters, and upper and lowercase letters ex. W0men1nTelecom!!!

Anti-Virus, Firewall, and Patching – Install an anti-virus program and always keep it up-to-date. Install a firewall. Keep your software updated by installing patches as soon as they are released by software vendors.

Email and Social Messaging – Only open email, messages, and attachments which are from someone you know, something you expected, and make sense. Don't open anything that sounds too good to be true!

Agenda

- Introduction
- Privacy concerns
- Compliance
- Identity Management
- Risk management
- Key takeaways
- Q&A