Breaches in the News

- ***Check out Privacy Association site for latest news in PII data breaches to see the latest in the news…***

  – ***www.privacyassociation.org***
- While there consider signing up for having the Daily Dash board emailed to you (published a couple times a week).

Cyber Security Policy and Ethics

Present to ASQ 509 May 26th, 2015

Kelly Yamaguchi, MSIS, CISSP, PhD(abd)

Lawsuits Escalating cont.

- Organizations must comply with federal regulations and state mandates for protecting and maintaining sensitive personal information and remain aware of new regulations. Failing to comply could result in expensive penalties, fines, and attorney fees for you and your organization.

Grama, J. L. (2011) Legal Issues in Information Security. Jones and Bartlett

Ferrera, Lichtenstein, Reder, Bird, and Schiano (2004), 2nd Ed. Thomson-S.W.

Lawsuits Escalating

- As regulations become more complex and the lines of responsibilities between customers, organizations, vendors, etc. blur, the number of lawsuits continue to rise.
- According to the 2012 US Cost of a Data Breach Report, the current avg organizational cost of a data breach stands at about $5.5 million. In addition to expensive individual losses, organizations face the threat of lawsuits from employees or customers whose personal information is mishandled or stolen.

Grama, J. L. (2011) Legal Issues in Information Security. Jones and Bartlett

Ferrera, Lichtenstein, Reder, Bird, and Schiano (2004), 2nd Ed. Thomson-S.W

Lawsuits Escalating Cont.

- Customers are continuing to sue financial organizations, for instance, who fail to protect their information. As breaches continue to escalate, lawsuits will increase and it will be necessary for organizations, banks, etc. to show they have educated their employees and their customers, and provided them with the awareness they need to protect sensitive information.

Grama, J. L. (2010). Legal Issues in Information Security. Jones and Bartlett

Ferrera, Lichtenstein, Reder, Bird, and Schiano (2004), 2nd Ed. Thomson-S.W

FISMA Updated

- http://www.natlawreview.com/article/fisma-updated-and-modernized-federal-information-security-management-act

PCI Updated

- https://www.pcisecuritystandards.org/
  - Take a look at the updates to PCI DSS (two pdf downloads)

The relationship between Risk and Security Policy

- Risk
  - Concept at the heart of information security
- Multifaceted approach to information security
  - Control risk through different management techniques
  - Develop a security policy
  - User awareness and training

Controlling Risk

- Threat
  - Type of action that has potential to cause harm
- Threat agent
  - Person or element with power to carry out a threat
- Vulnerability
  - Flaw or weakness that allows threat agent to bypass security
- Risk
  - Likelihood threat agent will exploit the vulnerability

Risk category	Description	Example
Strategic	Action that affects the long-term goals of the organization	Theft of intellectual property, not pursuing a new opportunity, loss of a major account, competitor entering the market
Compliance	Following a regulation or standard	Breach of contract, not responding to the introduction of new laws
Financial	Impact of financial decisions or market factors	Increase in interest rates, global financial crisis
Operational	Events that impact the daily business of the organization	Fire, hazardous chemical spill, power blackout
Environmental	Actions related to the surroundings	Tornado, flood, hurricane
Technical	Events that affect information technology systems	Denial of service attack, SQL injection attack, virus
Managerial	Actions that are related to the management of the organization	Long-term illness of company president, key employee resigning

Table 14-1 Risk classifications

Controlling Risk (cont'd.)

- Privilege
  - Subject's access level over an object, such as a file
- Privilege management
  - Process of assigning and revoking privileges to objects
- Privilege auditing
  - Periodically reviewing a subject's privileges over an object
  - Objective: determine if subject has the correct privileges

Controlling Risk (cont'd.)

- Change management
  - Methodology for making modifications and keeping track of changes
  - Ensures proper documentation of changes so future changes have less chance of creating a vulnerability
  - Involves all types of changes to information systems
- Two major types of changes that need proper documentation
  - Changes to system architecture
  - Changes to file or document classification

Controlling Risk (cont'd.)

- Change management team (CMT)
  - Body responsible for overseeing the changes
  - Composed of representatives from all areas of IT, network security, and upper management
  - Proposed changes must first be approved by CMT
- CMT duties
  - Review proposed changes
  - Ensure risk and impact of planned change are understood

Controlling Risk (cont'd.)

- CMT duties (cont'd.)
  - Recommend approval, disapproval, deferral, or withdrawal of a requested change
  - Communicate proposed and approved changes to coworkers
- Incident management
  - Response to an unauthorized incident
  - Components required to identify, analyze, and contain an incident

Controlling Risk (cont'd.)

- Incident handling
  - Planning, coordination, communications, and planning functions needed to resolve incident
- Incident management objective
  - Restore normal operations as quickly as possible with least impact to business or users

What Is a Security Policy?

- Document that outlines protections to ensure organization's assets face minimal risks
- Higher level definition
  - Set of management statements that define organization's philosophy of how to safeguard information
- Lower level definition
  - Rules for computer access and how the rules are carried out

What Is a Security Policy? (cont'd.)

- Security policy functions
  - Documents management's overall intention and direction
  - Details specific risks and how to address them
  - Provides controls to direct employee behavior
  - Helps create a security-aware organizational culture
  - Helps ensure employee behavior is directed and monitored

Balancing Trust and Control

- Three approaches to trust
  - Trust everyone all of the time
  - Trust no one at any time
  - Trust some people some of the time
- Security policy attempts to provide right amount of trust
  - Trust some people some of the time
  - Builds trust over time
- Level of control must also be balanced
  - Influenced by security needs and organization's culture

Designing a Security Policy

- Standard
  - Collection of requirements specific to system or procedure that must be met by everyone
- Guideline
  - Collection of suggestions that should be implemented
- Policy
  - Document that outlines specific requirements that must be met

Designing a Security Policy (cont'd.)

- Characteristics of a policy
  - Communicates a consensus of judgment
  - Defines appropriate user behavior
  - Identifies needed tools and procedures
  - Provides directives for Human Resource action in response to inappropriate behavior
  - Helps if necessary to prosecute violators

Designing a Security Policy (cont'd.)

- Three phases of the security policy cycle
  - Vulnerability assessment
    - Asset identification
    - Threat identification
    - Vulnerability appraisal
    - Risk assessment
    - Risk mitigation
  - Create the policy using information from risk management study
  - Review the policy for compliance

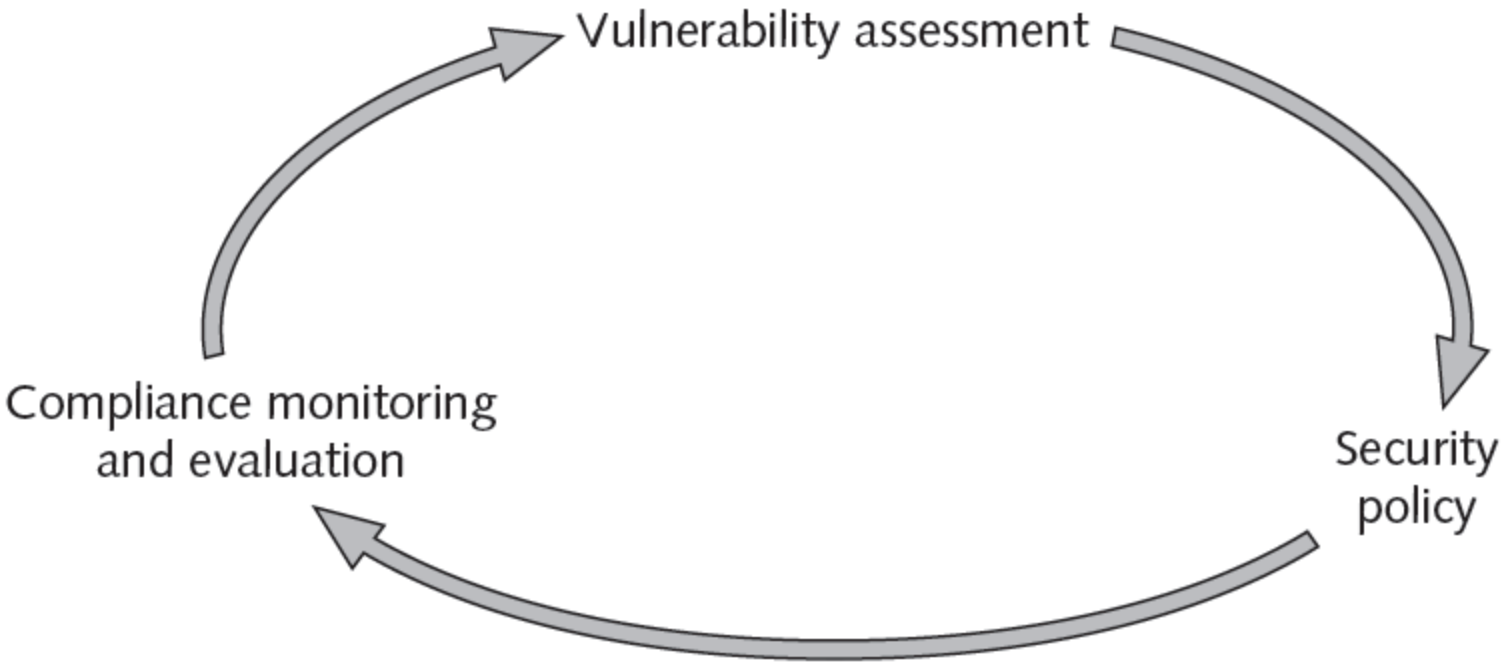

Figure 14-2 Security policy cycle

Security policy must	Security policy should
Be implementable and enforceable	State reasons the policy is necessary
Be concise and easy to understand	Describe what is covered by the policy
Balance protection with productivity	Outline how violations will be handled

Table 14-2 Security policy must and should statements

Designing a Security Policy (cont'd.)

- Security policy design should be the work of a team
- Development team representatives
  - Senior level administrator
  - Member of management who can enforce the policy
  - Member of the legal staff
  - Representative from the user community
- Team should first decide on policy goals and scope
  - Also how specific the policy should be

Designing a Security Policy (cont'd.)

- Due care
  - Obligations imposed on owners and operators of assets
  - Owners must exercise reasonable care of assets and take precautions to protect them
- Examples of due care policy statements
  - Employees should exercise due care in opening attachments received from unknown sources
  - Students will exercise due care when using computers in a crowded lab setting

Designing a Security Policy (cont'd.)

- Policy development guidelines
  - Notify users in advance of development of and reasons for a new security policy
  - Provide affected users an opportunity to review and comment on policy prior to deployment
  - Give users with responsibility the authority to carry out their responsibilities

Types of Security Policies

- Security policies often broken down into subpolicies
  - Acceptable use policy
  - Privacy policy
  - Security-related human resource policy
  - Password management and complexity policy
  - Disposal and destruction policy
  - Classification of information policy
  - Ethics policy

Table 14-3
Types of security policies

Name of security policy	Description
Acceptable encryption policy	Defines requirements for using cryptography
Anti-virus policy	Establishes guidelines for effectively reducing the threat of computer viruses on the organization's network and computers
Audit vulnerability scanning policy	Outlines the requirements and provides the authority for an information security team to conduct audits and risk assessments, investigate incidents, to ensure conformance to security policies, or to monitor user activity
Automatically forwarded e-mail policy	Prescribes that no e-mail will be automatically forwarded to an external destination without prior approval from the appropriate manager or director
Database credentials coding policy	Defines requirements for storing and retrieving database usernames and passwords
Demilitarized zone security policy	Defines standards for all networks and equipment located in the DMZ
E-mail policy	Creates standards for using corporate e-mail
E-mail retention policy	Helps employees determine what information sent or received by e-mail should be retained and for how long
Extranet policy	Defines the requirements for third-party organizations to access the organization's networks
Information sensitivity policy	Establishes criteria for classifying and securing the organization's information in a manner appropriate to its level of security
Router security policy	Outlines standards for minimal security configuration for routers and switches
Server security policy	Creates standards for minimal security configuration for servers
VPN security policy	Establishes requirements for Remote Access IPSec Virtual Private Network (VPN) connections to the organization's network
Wireless communication policy	Defines standards for wireless systems used to connect to the organization's networks

Types of Security Policies (cont'd.)

- Acceptable use policy
  - Policy that defines actions users may perform while accessing systems
  - Users include employees, vendors, contractors, and visitors
  - Typically covers all computer use
  - Generally considered most important information security policy

Types of Security Policies (cont'd.)

- Privacy policy
  - Also called personally identifiable information policy
  - Outlines how organization uses personal information it collects
- Security-related human resource policy
  - Includes statements about how an employee's information technology resources will be addressed
  - Typically presented at employee orientation session after employee is hired

Types of Security Policies (cont'd.)

- Security-related human resource policy (cont'd.)
  - May include statements regarding due process and/or due diligence
  - May include statements regarding actions to be taken when employee is terminated
- Password management and complexity policy
  - Addresses how passwords are created and managed
  - Reminds users of differences between strong and weak passwords

Types of Security Policies (cont'd.)

- Disposal and destruction policy
  - Addresses disposal of confidential resources
  - Describes how to dispose of equipment, records, and data
- Classification of information policy
  - Designed to produce standardized framework for classifying information assets
  - Generally involves creating classification categories
    - Example: high, medium, low

Types of Security Policies (cont'd.)

- Defining ethics can be difficult
- Values
  - A person's fundamental beliefs and principles
- Morals
  - Values attributed to a belief system that helps individuals distinguish right from wrong
- Ethics
  - Study of what a group of people understand to be good and right behavior

Types of Security Policies (cont'd.)

- An organization does not set an employee's values
  - Does set ethical behavior standards
- Ethics policy
  - Written code of conduct
  - Guides employees in decision making
  - Serves as a communication tool to reflect organization's commitments

Awareness and Training

- Providing users with security awareness training
  - Key defense in information security
- Awareness and training topics
  - Compliance
  - Secure user practices
  - Awareness of threats

Compliance

- Users should be informed regarding:
  - Security policy training and procedures
  - Personally identifiable information
  - Information classification
  - Data labeling, handling, and disposal
  - Compliance with laws, best practices, and standards

The Importance of User Practices. Some examples…

Category	Instruction
Password behaviors	Creating strong passwords that are unique for each account and properly protecting them serve as a first line of defense that all employees must practice
Data handling	No sensitive data may leave the premises without prior authorization; all data that is temporarily stored on a laptop computer must be encrypted
Clean desk policies	Employees are required to clear their workspace of all papers at the end of each business day
Prevent tailgating	Never allow another person to enter a secure area along with you without displaying their ID card
Personally owned devices	No personally owned devices, such as USB flash drives or portable hard drives, may be connected to any corporate equipment or network

Table 14-4 User practices

The Importance of Threat Awareness

- For example, Peer-to-peer (P2P) networks
  - Similar to instant messaging
  - Users connect directly to each other
  - Typically used for sharing audio, video, data files
  - Tempting targets for attackers
  - Viruses, worms, Trojans, and spyware can be sent using P2P
- Most organizations prohibit use of P2P
  - High risk of infection
  - Legal consequences

Summary

- A risk is the likelihood that a threat agent will exploit a vulnerability
- Privilege management and change management are risk management approaches
- A security policy states how an organization plans to protect its information technology assets
- Development and maintenance of a security policy follows a three-phase cycle

Summary (cont'd.)

- Security policies are often broken into subpolicies
  - Acceptable use policy
  - Privacy policy
  - Password management and complexity policy
  - Disposal and destruction policy
  - Classification of information policy
- Ongoing awareness training provides users with knowledge and skills necessary to support information security

Ethics 101

"Ethics is the study of the general nature of morals and of the specific moral choices individuals make."

"Ethical behavior is not the same as illegal behavior."

"Ethical issues often involve subtle distinctions, such as the difference between fairness and equity."

(p. 206-208)

If polling different people about their ethical decision making, we would find differences among the participants as it pertains to their thought process rationalizing what behavior they consider to be ethical.

Evans, Martin, and Poatsy (2014) Technology in Action, Complete, 10th Ed.

Major Ethical Systems

- Five Major Systems of Ethical Conduct:
  - Relativism
  - Utilitarianism
  - Divine command Theory
  - Virtue Ethics*
  - Deontology (duty based)

Evans, Martin, and Poatsy (2014) Technology in Action, Complete, 10th Ed.

Which System is Best

- No universal agreement on which is the best system of Ethics”
- “Most societies use a blend of different systems.”
- In spite of the ethical system most prevalent and in use by those in your group, personal ethics also can be expected to play a role in decisions made regarding ethical conduct.

Evans, Martin, and Poatsy (2014) Technology in Action, Complete, 10th Ed.

Personal Ethics cont..

- Your personal ethics likely developed and were influenced by :
  - your family's beliefs, any religious affiliation, and life experiences.

- …plus, overtime, your life experiences may have influenced you to adopt different tenants for what constitutes as ethical behavior as well as how and when to apply them. 208-209

- Having greater awareness of what matters most to you and knowing your values, your own personal ethics, may reduce stress and anger. The field of positive psychology provides support for this.

- Positive psychologist have focused on the relationship between living and working ethically and a person's perception of happiness (Dr. Martin Seligman of the University of Penn. is attributed as having pioneered the field of positive psychology). 209

- Evans, Martin, and Poatsy (2014) Technology in Action, Complete, 10th Ed.

Ethics and Technology

- "Because technology moves faster than rules can be formulated to govern it, how technology is used is often left up to the individual and the guidance of personal ethics". Of course at work, you are expected to follow the appropriate rules of conduct.
- However, how often are ethical considerations clear-cut? Ethical considerations are likely to be complex, such that "reasonable people can have different but equally valid views", including at work. p 211
- Evans, Martin, and Poatsy (2014) Technology in Action, Complete, 10th Ed.

Professional Ethics

- The importance of an organization adopting code of Ethics.
- 10
- The importance of Virtue Ethics and IEEE Ethics code for Software Engineers
- For for cyber-security professionals see also acm.org, issa.org, isc2.org, SANs…

3 general reactions to alruistic whistleblowing

- WB causes harm
- WB as moral obligation
- WB as institutional failure
- Examples of different WB Codes