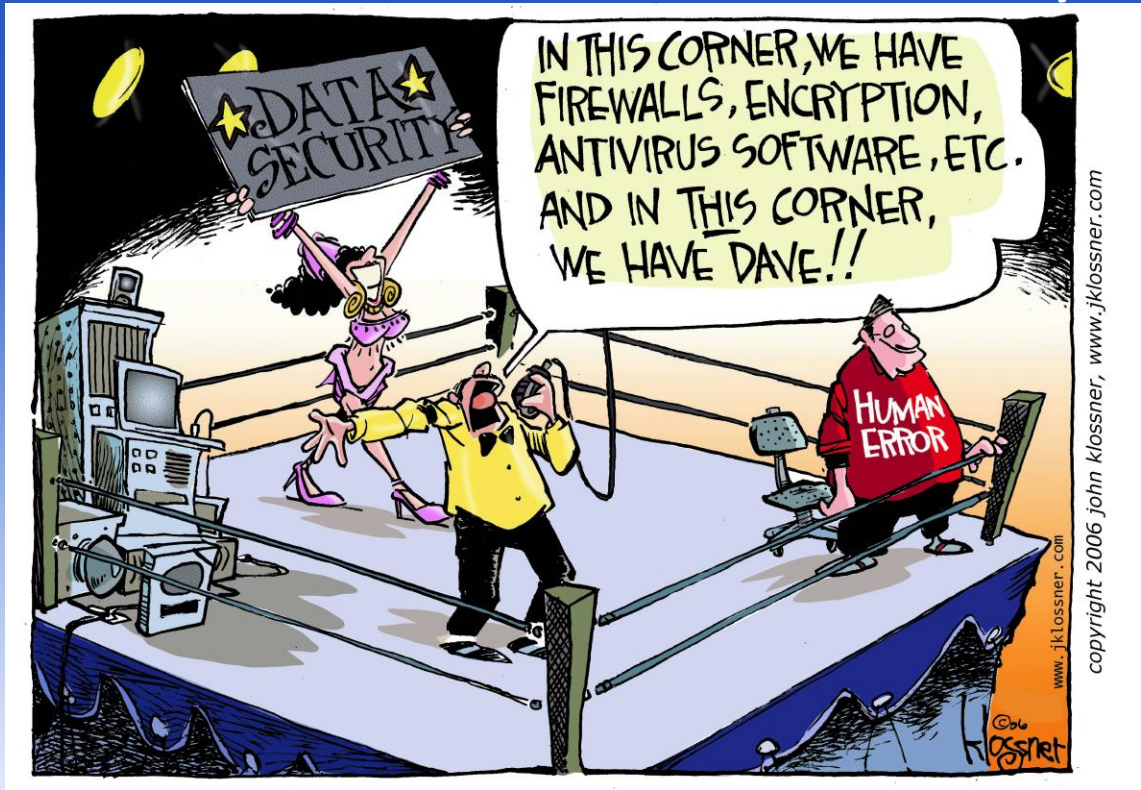
CS 493
Secure Software Systems

Ch 12-13 - Personnel Training

- A Culture of Security



Dr. Williams Central Connecticut State University

Objectives

- Identifying the target audience of an organization's security policy
- Establishment of an information and security awareness training program
- Methods for constructing and utilizing personnel training in security
- Sources and solutions for external personnel training and certifications in security
- What constitutes cybercrime, and legal issues regarding security policies
- The interaction with law enforcement in response to a violation of computer security

Goals

- Identify components of an information and security awareness training program.
- Map the security goals of your organization to construct a plan for personnel training and education.
- Identify metrics that can be used for establishing and upholding a security policy.
- Determine how and when law enforcement needs to become involved in an organization’s security matter.
- Understand what to document during and after an attack.

Social testing

- "New employee"
  - Check physical security to systems
  - Information that can be obtained from staff
    - Ports, ips, passwords, etc
  - Access via aide

The Information Security Audience

A security curriculum for your organization must be developed that covers the following four groups of personnel:

- The senior executive team
- Information technology managers
- Information technology personnel
- Information technology users

Information and security awareness

- Information and security awareness program
  - Requires buy in and enforcement to be successful
  - Information security policy
    - Written guidance and rules to protect IT assessts
    - Usually originates with Chief Information Security Officer (CISO)
  - CISO
    - Responsible for policy
    - Responsible for promoting security culture
    - Security standards

Incident Response Plan

There is no set format for an Incident Response Plan, but the following elements should be evaluated in its construction:

- Monitoring duties for the software in live operation
- A definition for incidents
- A contact for incidents
- An emergency contact for priority incidents
- A clear chain of escalation
- Procedures for shutting down the software or components of the software
- Procedures for specified exploits or attacks
- Security documentation or references for external code or hardware used in the software system

Organizational Culture

Based on security incidents, several key questions arise:

- What is needed to effectively implement an information-assurance-and-security training program?
- How does an organization's culture impede or promote information security?
- Did the organization have an effective information security plan?
- How should information security breaches be investigated?

Information Assurance Curriculum Content

- NIST Special Publication 800-16 titled *Information Technology Security Training Requirements: A Role and Performance-Based Model* provides a method that can be used to develop an awareness and training program.
  - **Awareness** is presenting the existing threats to the organization's personnel or infrastructure.
  - **Training** is defined as the effort "to produce relevant and needed security skills and competency by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing)."
  - **Education** is the increase in awareness and knowledge of personnel with respect to security and how it affects their daily routines and performance.

How would content differ?

- Same content elements
  - Awareness
  - Training
  - Education
- Key audiences
  - The senior executive team
  - Information technology managers
  - Information technology personnel
  - Information technology users

Pre-decide Policies

- It is imperative that you decide as an organization what security policies are most essential and what security goals the organization has.
- A policy should not try to cover everything about security all at once.
- Center your communication on what personnel can put in practice.
- Define simple and digestible goals for your personnel; goals may differ depending on roles and responsibilities.
- It is better to have three goals in practice than 50 that are ignored.

Security Training Delivery Methods

- Outsourcing is always an option that can provide excellent training but can be expensive.
- Online training, computer-based training, or webinars are available from a variety of sources.
- You can produce your own training as well or create a mixed (hybridized) solution.

Security workshops

- Often personnel and users see security awareness/training as not their issue, but rather “higher ups”
- More effective approach often training for personal information security
  - What’s in it for me syndrome
  - Show how security issues affect them personally more likely to appreciate need

Implementing a Training Solution

Step 1: Identify the program scope, goals, and objectives

Step 2: Identify training staff

Step 3: Identify target audience

Step 4: Motivate management and employees

Step 5: Administer the program

Step 6: Maintain the program

Step 7: Evaluate the program

Essentials to assist and react to computer incident

- Preserve state of computer at time of incident
  - Backup copies of logs
  - Damaged or altered files
  - Files created by intruder
- If incident in progress
  - Activate additional audit monitoring
  - Consider keystroke monitoring if internal system
- Document losses
  - Time, $ temp help, $ damaged equip., data value, customer incentives to retain, lost revenue, trade secrets
- Contact law enforcement

Enforcing Computer Policy and Computer Crime Investigations

- According to CERT, a **Computer Security Incident Response Team (CSIRT)** is a "service organization [..] responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency."
- If the FBI is involved, investigators will gather information in four ways:
  - Request for voluntary disclosure of information
  - Court order
  - Federal grand jury subpoena
  - Search warrant

Summary

- Personnel are the greatest assets to an organization and they need to be prevented from becoming the greatest weaknesses.
- There are three components to a successful security focus in an organization: awareness, training, and education.
- Whether you develop your training and education programs in-house or outsource them, it is essential that personnel are provided with opportunity and practice at putting these in place.
- Understanding how to document an attack and knowing the legal limits in security are also essential in formulating a response policy.

Chapter 13
A culture of security

Objectives

- Managing risk in the development process
- Legal guidelines affecting the development of secure applications
- Privacy and data in an organization
- The concepts of confidentiality, integrity, and availability as they apply to the software developer
- Security and legal guidelines that support a successful software development process

Goals

- Identify the concepts of confidentiality, integrity, and availability as they relate to secure coding.
- Identify basic risk management concepts.
- Build the team component needed to develop a secure development culture component.
- Define and describe current legal guidelines affecting privacy that could affect your development process.
- Identify compliance laws that affect information systems initiatives.
- Determine how governance should be applied in the organization.
- Describe the differences between policies and procedures.

Confidentiality, Integrity, and Availability

- Threats in the information security arena center around three areas in the application development process: the familiar confidentiality, integrity, and availability.
  - **Confidentiality** is the act of protecting data and information from unauthorized disclosure.
  - **Integrity** ensures that the data in your information systems is not modified or damaged in any way.
  - **Availability** is the ability to ensure that information and data services are available when requested.

Handling Risk

Successfully dealing with risk requires the following three separate functions, outlined by NIST publication 800-30:

- **Risk assessment:** the process of identifying existing risks to the information systems infrastructure.
- **Risk mitigation:** the implementation of the mitigation suggestions from the risk assessment process; this also includes the process for maintaining the mitigations in place.
- **Risk evaluation:** the process of continually evaluating to identify potential new risks and maintaining assurance that current strategies in place are working properly.

Risk Assessment Methodology

The nine step risk assessment methodology:

1. **System characterization:** This is used to assess the scope of the project and the types of systems involved.
2. **Threat identification:** Identify all potential threats to the new information system.
3. **Vulnerability identification:** Identify all of the vulnerabilities within the new system.
4. **Control analysis:** Determine how well a security control is working to deal with vulnerability.
5. **Likelihood determination:** Determine how likely it is for a threat to materialize into an actual attack on your system or application, based on the controls already in place.

Risk Assessment Methodology (Continued)

6. **Impact analysis:** Determine how the organization will be affected where a vulnerability materializes into an actual threat realization.
7. **Risk determination:** Examine the adequacy of the controls that are in place to protect the assets in question.
8. **Control recommendations:** Ensure that you are applying enough controls to reduce loss to the organization.
9. **Results documentation:** Document all of your findings that include threat and vulnerability identification and mitigation strategies used.

Secure Software Design—Legal Environment

Role based attitudes:

- Senior management
  - Typically most CXX are primarily focused on business risks not appreciating information risk as related to this – CIO responsible for this understanding
- IT professionals
  - Lock down system not appreciate business impact
- Information assurance professionals
- System users

Secure Software Design—Legal Environment

There are several laws governing information use. These relate to various personal information standards for private companies and government, such as:

- Health Insurance Portability and Accountability Act (HIPAA)
  - **Storage of data**
  - **Use of data**
  - **Transmission of data**
- Federal Information Security Management Act (FISMA)
- Sarbanes-Oxley Act (SOX)
- Family Educational Rights and Privacy Act (FERPA)
- Children's Internet Protection Act (CIPA)

Security in the Organization

- In a SANS report dated 2010 it was found that most security breaches are caused by human factors.
- The report's findings indicate that most incidents resulted from the following causes:
  - Lack of employee security awareness and training
  - Lack of employee motivation
  - Although aware of security threats, employees' bad decisions
  - Some employees exposing the organization to risk

Documents related to security policy

- IT standards
  - Proven methodologies to implement a process
- IT procedures
  - Specific steps used to manage a process
- IT security policies
  - Ex. how data flows through the organization and outside
- IT guidelines
  - Set of constraints used towards implementing a process

Enforcing Security Policy

- Technical enforcements when possible
- Nontechnical controls
  - HR carry out disciplinary procedures
- It is imperative that you decide as an organization what security policies are most essential and what security goals the organization has.
- A policy should not try to cover everything about security all at once.
- Center your communication on what personnel can put in practice.
- Define simple and digestible goals for your personnel; goals may differ depending on roles and responsibilities.
- It is better to have three goals in practice than 50 that are ignored.

Summary

- Security policies focused on risk management are likely to be the most successful.
- There is a great deal of data and information available either through NIST or through nongovernment organizations that offer assistance and documentation to implement a risk management process.
- An organization should be to implement a culture that is security aware and accepting of risk management and secure computing practices.
- The best way to acquire buy-in is to attain senior management support; appoint a champion to lead the change and focus on development of a security-conscious culture.

In class research

- Legal environment
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- Sarbanes-Oxley Act (SOX)
- Family Educational Rights and Privacy Act (FERPA)
- Children's Internet Protection Act (CIPA)