The Business of Security

Chapter 4

Lecturer: Pei-yih Ting

Overview

- Building a Business Case
- Business Continuity Planning
- Vulnerability Assessment, Implementing Controls
- Maintaining the BCP
- Disaster Recovery Planning (DRP) and Facilities
- Disaster Recovery Training and Testing
- Maintaining the DRP
- Data classification
- Security Ethics
- Computer Security Laws

Building a Business Case

- A business exists to satisfy business objectives
  - Security programs are there to support this primary goal
  - Business people vs. security people (who just don't understand how to run a business)
- The first step to building a business case is to understand the business's goal and objectives
- Security efforts must be described in relation to organization's mission
- Use quantitative and qualitative analysis to justify security measures

Building a Business Case (cont'd)

- Justify security measures (cont'd), examples,
  - Quantitative: This new spam filter will save us 1,000 man-hours per year. Each man-hour costs $15 on average; therefore, the total savings from the filter will be $15,000. The cost of the filter is only $5,000, so we should implement it.
  - Qualitative: This firewall will help prevent intruders from entering our network and stealing our trade secrets which, if disclosed to our competitors, would cause the failure of our entire business. Therefore we must implement it at any cost. (If there is another choice of similar security measure, it will be a different story.)

Business Continuity Planning

- A business continuity plan (BCP) describes how a business will continue operations in the face of risk (BCP prevents an organization from feeling the impact of a disaster.)
- Initial step: Vulnerability assessment determines which risks merit attention
  - Risk = Threat X Vulnerability
  - Risk exists while threat and vulnerability co-exist.
- A quadrant map is a good tool for vulnerability assessment

Vulnerability Assessment

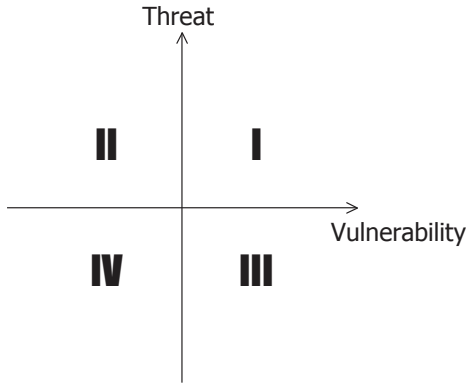

Figure 4.1 Vulnerability assessment quadrant map

Implementing Controls

- Four techniques used to manage risks identified in vulnerability assessment
  - Risk avoidance, risk mitigation, risk acceptance, risk transference
- BCP team must determine exactly how these risk management strategies will be implemented to each of the risks identified
- Not all risks can be handled with technical approaches, some may require education & training or external expertise for example

Maintaining the Plan

- BCP is a living document
- Changes in the environment, the business, and in current technologies will induce new risks
- BCP should be flexible and comprehensive enough to absorb changes
- However, periodic review and updating of the BCP will be required

Disaster Recovery Planning

- Disaster recovery planning is used to prepare for continuing an organization's operations when they are interrupted due to a crisis (when the BCP fails)
- A Disaster Recovery Plan (DRP) is the document describing the recovery plan
- Goals of a DRP
  - Resume operations at an alternate facility as necessary
  - Provide for extended operation at the alternate facility
  - Prepare for transition back to the the primary facility when possible

Selecting the Team

- Who should be on a disaster recovery team?
  - Selection of well-qualified members covering critical departments and missions within the organization
  - Size of the organization dictates size of team
  - In a larger organization, planning and implementation teams can be different. Members in the implementation team actually carry specific DRP roles.
  - DRP responsibilities are usually secondary to the team members' primary roles within the organization

Building the Plan

- The DRP should describe the processes to follow in the event of disaster, in order to transfer operations to and back from a recovery facility
  - Should detail the responsibilities of all individuals involved in the plan
  - Should detail resources needed, including financial, manpower, hardware, and software
- Selection of one or more alternate facility is a primary challenge to the team
  - The greater the required capabilities, the more expensive it will be

Disaster Recover Facilities

- Hot site
  - Contains all hardware, software, and data required. Capable of taking over production *immediately*
- Warm site
  - Contains most hardware and software required, does not maintain live copies of data. Capable of taking over production *within hours or days*
- Cold site
  - Contains basic power, telecommunications, and support systems. Does NOT maintain hardware, software, or data. Capable of taking over production *within weeks or months*

Creative Disaster Recovery

- Nontraditional arrangements for disaster recovery are possible and may be suitable for a particular organization
- Geographically dispersed organizations might consider mobile facilities
  - Trailers, mobile homes, air-transportable units
  - Don't keep them all in one place
- Mutual assistance agreements
  - Share costs with other organizations
  - Care must be taken in maintaining confidentiality of data

Training

- DRP team members need training to prepare for responsibilities under the plan
- Initial training
  - Comprehensive training (on the DRP and the security responsibilities) takes place when individuals are placed on the team
- Refresher training
  - Periodic training to update and refresh team members' skills and readiness
- Length, frequency, and scope of DRP training must be customized according to each individual's responsibilities

Testing

- Checklist review
  - Simplest, least labor-intensive form of testing
  - Each individual has a checklist of responsibilities under the DRP
  - During testing, each individual reviews his/her checklist
  - Can be done as a group or individually (most often)
- Tabletop exercise
  - Test facilitator describes a specific disaster scenario
  - DRP team members verbally walk through their responses to the scenario
  - Scenarios can be disseminated at the test or in advance

Testing (cont'd)

- Soft test (parallel test)
  - DRP team members are given a disaster scenario and respond by activating the recovery facility
  - Recovery facility works in parallel with main facility, does NOT take responsibility for full operation
  - A more comprehensive test, also a more expensive test
- Hard test (full-interruption test)
  - Used only rarely in mission critical situations, too disruptive and extremely expensive
  - Involves full transfer of control to alternative facility and back

Implementing the Plan

- When a plan must be implemented, the situation is going to be chaotic
- Plan must define actions of first responders, whoever they might be
  - All employees should know what to do if they witness an event that might signal a need for disaster recovery
- The authority to declare a disaster situation should be carefully allocated
  - Senior managers and possibly to multiple people

Maintaining the Plan

- The disaster recovery team's membership, procedures, and tools will change over time
- The team should rely heavily on checklists to avoid panic and chaos
  - Checklists must be up-to-date
- The DRP should be continually tested and evaluated with lessons learned debriefings

Data Classification

- Provides users with a way to stratify sensitive information
- Provides a system for applying safeguards appropriate to the level of confidentiality required
- Prerequisites for access to classified data are
  - Security clearance
  - Need to know
- Government and private industry have similar classification systems

Security Clearances

- Obtaining a security clearance depends on the organization
  - It can sometimes involve rigorous background checks, polygraphs, and agreements about nondisclosure of sensitive information
- Security clearances can be granted at various levels that specify the maximum sensitivity level of information a user is authorized to access
- Usually clearance is tied to essential activities of an individual's current task
- Security clearance is normally enforced by a central security office

Need to Know

- Need to know is often required in addition to security clearance in order to access sensitive information
- Security clearance offers access to broad categories of information, need to know restricts access to the actual information required for a specific task
- Need to know is normally enforced in a distributed way by the custodians of the information

Classification Systems

- Normally government classification systems are more restrictive and bureaucratic than industry systems
- U.S. Government Classifications
  - Top Secret, Secret, Confidential, Sensitive but Unclassified (For Official Use Only), and Unclassified
- Common Industry Classifications
  - Trade Secret, Company Confidential/Proprietary, Unclassified
  - Trade secrets are often not protected by patents or copyrights, employees must understand legal obligation to not disclose information

Security Ethics

- Security professionals often have access to highly confidential information
  - Must exhibit high degree of ethical standards
- ISC^2 is a professional organization for security personnel
  - International Information Systems Security Certification Consortium
  - Has developed a four-rule Code of Ethics for information security professionals
    - **Protect society, the common wealth and the infrastructure**
    - **Act honorably, honestly, justly, responsibly, and legally**
    - **Provide diligent and competent service to principals**
    - **Advance and protect the profession**

Monitoring

- Security professionals are often entrusted with monitoring an organization's internal and external activities
  - Security professionals are trusted with a high degree of confidence
  - The ethics of handling information gathered during the process of monitoring requires a high degree of discretion and professionalism
- Who watches the watchers?
  - Ensure that the monitors themselves handle information appropriately

Computer Security Law

- A number of laws have an effect on the security industry including
  - Electronic Communications Privacy Act (ECPA)
    - Interception and monitoring of electronic communications
  - USA Patriot Act
    - Provide government officials additional power in the use of electronic monitoring systems
  - Children's Online Privacy Protection Act (COPPA)
    - Forbid collecting any personally identifying information from children under the age of 13

Computer Security Law (cont'd)

- Health Insurance Portability and Accountability Act (HIPAA)
  - Protect the consumer's privacy from organizations that handle personal medical records
- Gramm-Leach-Bliley Act
  - Firms that possess and manipulate private financial information must disclose their uses of that information to the subjects of the records
- European Union Directive on Data Privacy
  - Restricts the collection and use of personal information and limits the transfer of it across international borders

Summary

- Security professionals must work within the limits of the resources and business objectives of their organization to build a business case for security
- A Business Continuity Plan (BCP) is a document that deals with keeping a organization functioning in the face of risk
- Developing a BCP requires vulnerability assessment, control implementation, and plan maintenance

Summary (cont'd)

- A Disaster Recovery Plan (DRP) deals with keeping a business functioning when some event interrupts the organization's normal operations
- A DRP requires
  - An alternate facility where operations can be moved
  - A team of trained individuals who can facilitate the move
  - An up-to-date plan for accomplishing the transition
  - Ongoing maintenance, training, and testing

Summary (cont'd)

- In organizations with sensitive information, data classification systems are often used
  - Individuals require security clearance and need to know to access classified data
- Security professionals may have access to highly confidential information and must exhibit high ethical behavior
- Information security and privacy is subject to a number of laws and regulations
  - Security professionals must be aware of responsibilities and obligations under these laws

Assignments

- Reading: Chapter 4
- Practice 4.9 Challenge Questions

- Turn in Challenge Exercise 4.1 next week