The Business of Security

Chapter 5

Building a Business Case

- A business exists to satisfy business objectives
  - Security programs are there to support this primary goal
- The first step to building a case is to understand the business objectives
- Security efforts must be described in relation to organization's mission
- Use quantitative and qualitative analysis to justify security measures

Business Continuity Planning

- A business continuity plan (BCP) describes how a business will continue operations in the face of risk
- Vulnerability assessment determines which risks merit attention
  - Risk = Threat x Vulnerability
- A quadrant map is a good tool for vulnerability assessment

Vulnerability Assessment

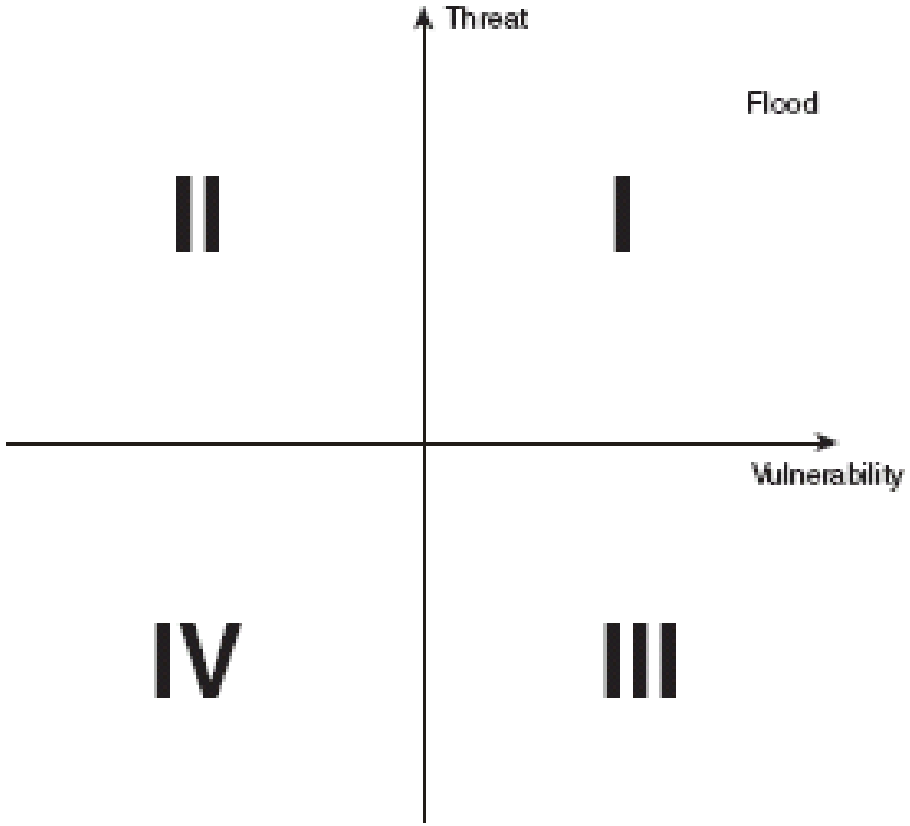

Figure 4.1
Vulnerability assessment quadrant map

Implementing Controls

- Four techniques used to manage risks identified in vulnerability assessment
  - Risk avoidance, mitigation, acceptance, transference (from Chapter 1)
- BCP team must determine exactly how these strategies will be applied 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
- 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?
  - Important to cover critical departments and missions within the organization
  - Size of the organization will dictate size of team
  - In a larger organization, planning and implementation teams can be different
  - 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
  - Should detail the responsibilities of all individuals involved in the plan
  - Should detail resources needed, including financial, manpower, hardware, and software
- Selection of at least one alternate facility is a primary challenge
  - 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, and 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 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 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
- Tabletop exercise
  - Test facilitator describe 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 (continued)

- 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 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
  - 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 level and the organization
  - It can sometimes involve rigorous background checks, polygraphs, and agreements about disclosure of sensitive information
- Security clearances can be granted at various levels
- Usually clearance is tied to essential activities of an individual's current job

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
- Security clearance is normally enforced by a central security office
- Need to know is normally enforced 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 Code of Ethics for information security professionals
  - Four very general canons

Monitoring

- Security professionals are often entrusted with monitoring an organization's internal and external activity
- 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)
  - USA Patriot Act
  - Children's Online Privacy Protection Act (COPPA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Gramm-Leach-Bliley Act
  - European Union Directive on Data Privacy

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

- 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

- 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 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