Chapter 11

Managing the Security Function

Panko, Corporate Computer and Network Security
Copyright 2004 Prentice-Hall

Figure 11-1: Organizational Issues

- Top Management Support
  - Top-Management security awareness briefing
    (emphasis on brief)
  - Corporate security policy statement: Vision, not details
  - Follow-through when security must be upheld in conflicts
  - Business champions to give support and business advice

- Should You Place Security Within IT?
  - Pros
    - Compatible technical skills
    - Making the CIO responsible for security breaches gives accountability
  - Cons
    - Difficult to blow the whistle on the IT staff
    - Vendor preference differences with networking staff (e.g., Cisco vs Check Point)

- Security and Auditing
  - IT Auditing has the skills to determine whether IT rules are enforced, but IT auditing does not set policy
  - Internal Auditing also can audit IT-related procedures, but it does not make policy

- Managed Security Service Providers (Figure 11-2)
  - On-site logging, off-site analysis
  - Practice-based expertise
    - Get plenty of experience on a daily basis—like fire departments
  - Separation of responsibilities: Can blow whistle on IT, even the CIO
Managed Security Service Providers (MSSPs) are expanding.

- Typically, intrusion detection and vulnerability assessment.
- Rarely policy and other control practices.
- Not commonly antivirus protection and other aspects of security, but MSSPs are expanding.

Evaluating the MSSP:
- Diligence: Is it really reading the logs? (Contracts often are vague)
- Skills and background of testers

Security and Business Staffs:
- Cannot Just Lob Policies Over the Wall

Security and Business Partners:
- Your Business Partner’s Security Affects You

Uniformed Security Personnel:
- They are often called first by suspicious users
- They support investigations

Staffing and Training:
- Background checks should be done on the security staff
- All workers involved in IT should have background checks, including the maintenance staff, consultants, and contractors

Certifications are good but vary in what they require and do not make up for lack of experience.
Figure 11-1: Organizational Issues

- Staffing and Training
  - Should you hire a hacker?
    - They are likely to have the knowledge you need
    - But would you be afraid to fire or lay off one?

Figure 11-3: Risk Analysis

- Financially Sensible Protections
  - Risk analysis: Balance risks and countermeasure costs

- Enumeration of Assets
  - Assets: Things to be protected (hosts, data, etc.)
  - Up-to-date asset lists must be created first (can be very difficult)
  - Asset responsibilities: Each asset should have someone accountable for it

- Asset Classification
  - Business continuity asset classifications
    - Scope and degree of disruption: How many things, how bad the damage
    - Financial impacts of a slowdown or shutdown
  - Cost of repairs asset classification

- Threat Assessment
  - Threat likelihood
    - Difficulty of estimation

- Responding to Risk
  - Risk reduction: Implement countermeasures
  - Risk acceptance: Do nothing; suitable for low-threat risks and expensive countermeasures
  - Risk transference: Get insurance. Good for low-probability risks

- Risk Analysis Calculations
  - Threat severity analysis (expected loss)
    - Cost of attack if it succeeds times the probability that the attack will succeed
    - Expressed in terms of some timer period, such as a year
Figure 11-3: Risk Analysis Calculations

- **Value of Protection**
  - Reduction in threat severity (benefit) minus the cost of the countermeasure
  - Invest in a countermeasure only if the value of protection is positive

Figure 11-3: Risk Analysis Calculations

- **Priority**
  - Invest in countermeasures with the greatest value of protection first

Figure 11-3: Risk Analysis Calculations

- **Return on investment (ROI) analysis**
  - For a single-year countermeasure, value of protection divided by the cost of the countermeasure
  - For multiple-year investments, discounted cash flow analysis of multi-year values of protection and countermeasure investments
    - ROI allows investments of different sizes to be compared directly
    - There usually is a hurdle rate of 15% to 25%, and investments that fall below the hurdle rate will not be accepted

Figure 11-3: Qualitative Risk Analysis

- **Danger of business termination**: Can’t be put entirely into dollar terms
- **Loss of reputation**: Difficult to quantify but very important

Figure 11-4: Corporate Security Architecture

- **Security Architectures**
  - Technical security architecture: Countermeasures and their organization into a system
  - Architectural decisions: Plan broadly before installing specific systems
  - Start in the design phase if possible: The earlier the better
  - Deal with legacy security technologies
Five Principles
- Defense in depth
  - Attacker must break through several defenses to succeed
  - Safe even if a vulnerability is discovered in one line of defense. Can fix the vulnerability without break-ins

Five Principles
- Single points of vulnerability
  - The dangers of single points of vulnerability
  - The need for central security management consoles may require accepting a single point of vulnerability (taking over the management system)

Five Principles
- Diversity of Vendors
  - Security effectiveness: Each product will miss some things; jointly will miss less
  - Product vulnerabilities: Each will have some; jointly will have fewer
  - Vendor Survival: If one vendor fails, others will continue

Elements of a Security Architecture
- Border management: Border firewalls, etc.
- Internal site management: To protect against internal threats

Elements of a Security Architecture
- Management of remote connections: Remote users and outsiders are difficult
- Interorganizational systems: Linking the computer systems of two organizations
- Centralized management: Control from a single place where information is gathered
Figure 11-5: Control Principles

- **Policies**
  - Brief vision statements
  - Cannot give details because the environment and technology keep changing

- **Standards**
  - Mandatory actions that MUST be followed

- **Baselines**
  - The application of standards to specific products
  - For example, steps to harden a LINUX server

- **Guidelines**
  - Voluntary recommended action
  - Although voluntary, must consider in making decisions
  - Good when the situation is too complex or uncertain for standards
  - Unfortunately, sometimes should be standards but lack of political power prevents this

- **Employee Behavior Policies**
  - For general corporate employees
  - Theft, sexual harassment, racial harassment, pornography, personal use of office equipment, revealing of trade secrets, etc.

- **Procedures**
  - Sets of action taken by people
  - Steps to do background checks on employees
  - Steps to add user on a server

- **Best Practices and Recommended Practices**
  - Best practices are descriptive of what the best firms do
  - Recommended practices are prescriptions for what the firm should do
  - Both allow a firm to know, at a broad level, if it is doing what it should be doing

- **Operations**
  - The day-to-day work of the IT department and other departments
  - Systems administration (server administration) especially
  - Entering data, upgrading programs, adding users, assigning access permissions, etc.
**Principles**
- Clear roles
  - Who should do what in each step
  - Assign tasks to roles, then assign individuals to roles as needed
- Separation of duties and mandatory vacations to prevent people from maintaining deceptions
- Prospects for collusion: Reduce them
  - Check family and personal relationships assigning people to duties

**Accountability**
- Accountability and roles
  - Owner: Responsible for the asset
  - Custodian: Delegated responsibility
- Auditable protections and controls for specific assets
  - If not auditable, can you tell if they work?
- Exception handling with documentation and audit of who took what actions

**Managing Development and Change for Production Servers**
- Tiers of Servers
  - Development Server: Server on which software is developed and changed
    - Developers need extensive permissions
  - Staging (Testing) Server: Server on which changes are tested and vetted for security
    - Testers should have access permissions; developers should not
  - Production Servers: Servers that run high-volume production operations
    - Neither developers nor testers should have access permissions
Managing Development and Change for Production Servers
- Change Management Control
  - Limit who can request changes
  - Implement procedures for controlling changes
  - Have security examine all candidate changes for potential problems (bad encryption, lack of authentication, etc.)

Auditing Development for individual programs
- Do detailed line-by-line code inspection for security issues

Security Awareness
- Accountability Training
  - Self-Defense Training
    - Social engineering threats and correct responses
    - Make users early warning scouts who know whom to inform if breach suspected
    - In general, mobilize as partners

Authorization
- Nontechnical Problems in Providing Access Permissions
  - Who may submit people for usernames and passwords? Limit it
  - Human resources know when people are hired and fired

Terminating Authentication Credentials
- People often do not have their permissions terminated when they no longer need them
- Person who requests their permissions should have to periodically review them for continuation
Figure 11-8: Vulnerability Testing

- **Vulnerability Testing Technology**
  - Using Attacker Technology
    - Designed to do damage
  - Using Commercial Vulnerability Testing Tools
    - Not as up-to-date as attacker tools
    - Less likely to do damage as side effect
    - Focus on reporting

Figure 11-8: Vulnerability Testing

- **Vulnerability Testing Technology**
  - Reporting and Follow-Up Tools
    - Reports should clearly list vulnerabilities and suggested fixes
    - Follow-up report should document which vulnerabilities fixed, not fixed

Figure 11-8: Vulnerability Testing

- **Vulnerability Testing Contracts**
  - Need a contract before the testing begins to cover everyone involved
  - What Will Be Tested: Specifics
  - How It Will Be Tested: Specifics
  - Hold Blameless for Side Effects

Figure 11-8: Vulnerability Testing

- **Reducing False Positives with Tuning**
  - Avoid meaningless tests, for instance, Apache threat on Microsoft Windows Server

Figure 11-8: Vulnerability Testing

- **Who Should Do Vulnerability Testing?**
  - Outside Firms
    - Expertise
    - Use of reformed hackers?
  - The IT or Security Department
    - Has good knowledge of internal systems
    - If IT staff is the attacker, can hide wrongdoing

Figure 11-8: Vulnerability Testing

- **Who Should Do Vulnerability Testing?**
  - IT Auditing Departments
    - Trained to audit whether standards and procedures are being followed
    - Have to upgrade their specific vulnerability testing skills
**Topics Covered**

- Need for top management support
- Should security be inside or outside IT?
  - Inside provides greater integration and IT accountability
  - Outside brings freedom to criticize IT
- Managed Security Service Providers
  - Have expertise and experience
  - How to ensure quality?
  - Can blow whistle on anyone in the firm

---

**Topics Covered**

- Relationships that must be managed
  - Security and business staffs
  - Security and business partners
  - IT Security and the uniformed security staff
- Staffing and Training
  - Need to train because few have skills
  - Background checks are necessary
  - Hire reformed hackers?

---

**Topics Covered**

- Risk Analysis
  - Risk analysis: Balance risks and countermeasure costs
  - Enumeration of Assets
    - Up-to-date asset lists must be created first
    - Each asset should have someone accountable for it

---

**Topics Covered**

- Risk Analysis
  - Asset Classification
    - Business continuity asset classifications
      - Scope, degree, and financial impact of disruption
    - Cost of repairs asset classification
  - Threat Assessment
    - Threat likelihood

---

**Topics Covered**

- Risk Analysis
  - Responding to Risk
    - Risk reduction: Implement countermeasures
    - Risk acceptance: Do nothing
    - Risk transference: Get insurance

---

**Topics Covered**

- Risk Analysis Calculations
  - Threat Severity Analysis (expected loss)
    - Cost of successful x probability of success
  - Value of Protection
    - Reduction in threat severity (benefit) minus the cost of the countermeasure
    - Invest in a countermeasure only if the value is positive
  - Priority
    - Invest in countermeasures with the greatest value of protection first
Topics Covered

- Risk Analysis Calculations
  - ROI
  - Qualitative Analysis

Topics Covered

- Security Architecture
  - Guides individual decisions
  - Principles
    - Defense in depth
    - Dangers of single points of vulnerability
    - Diversity of vendors
    - Minimizing security burdens on functional departments
    - Implementing planning, protecting, and responding phases well

Topics Covered

- Elements of a Security Architecture
  - Border management: Border firewalls, etc.
  - Internal site management: To protect against internal threats
  - Management of remote connections: Remote users and outsiders are difficult
  - Interorganizational systems: Linking the computer systems of two organizations
  - Centralized management: Control from a single place where information is gathered

Topics Covered

- Policies: Brief vision statements
- Standards: Mandatory actions that MUST be followed
- Guidelines: Voluntary recommended action
- Baselines: The application of standards to specific products
- Procedures: Actions by people

Topics Covered

- Employee Behavior Policies
  - For general corporate employees
  - Theft, sexual harassment, racial harassment, pornography, personal use of office equipment, revealing of trade secrets, etc.
- Best Practices and Recommended Practices

Topics Covered

- Operations Security
  - Operations
  - Principles
    - Clear roles
    - Separation of duties and mandatory vacations
    - Reduce prospects for collusion
**Topics Covered**

- Accountability
  - Accountability and roles
    - Owner: Responsible for the asset
    - Custodian: Delegated responsibility
  - Auditable protections and controls for specific assets
  - Exception handling with documentation and audit of who took what actions

**Topics Covered**

- Permissions and Servers
  - Development server
  - Testing server
  - Production server

**Topics Covered**

- User Training
  - Security Awareness
  - Accountability Training
  - Self-Defence Training
    - In general, mobilize as partners

**Topics Covered**

- Authentication
  - Non-technical Problems in Providing Access Permissions
    - Control who can nominate someone
    - Removal when no longer appropriate

**Topics Covered**

- Vulnerability Testing Technology
  - Using Attacker Technology
  - Using Commercial Vulnerability Testing Tools
  - Reporting and Follow-Up
  - Vulnerability Testing Contracts
  - Reducing False Positives with Tuning
  - Should vulnerability testing be done by outside firms, IT, security, or IT or operations auditing?