Chapter 11 – Information Security Management

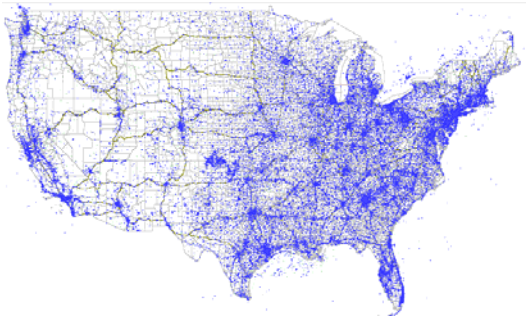
Dr. Hui Xiong
Rutgers University

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

Learning Objectives

- Know the sources of security threats.
- Understand management's role for developing a security program.
- Understand the importance and elements of an organizational security policy.
- Understand the purpose and operation of technical safeguards.
- Understand the purpose and operation of data safeguards.
- Understand the purpose and operation of human safeguards.
- Learn techniques for disaster preparedness.
- Recognize the need for a security incidence-response plan.

220,000 Cell Towers Can Find You



Millions of Wi-Fi Access Points Can Find You

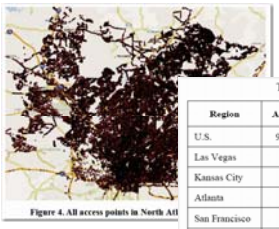
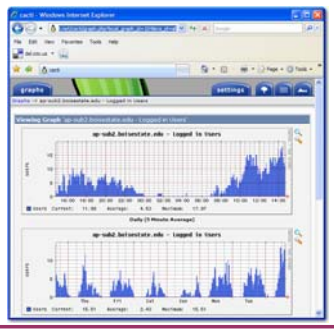


Figure 4. All access points in North Atl

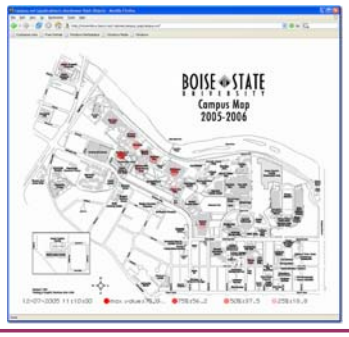
Table 2. Access Point Density

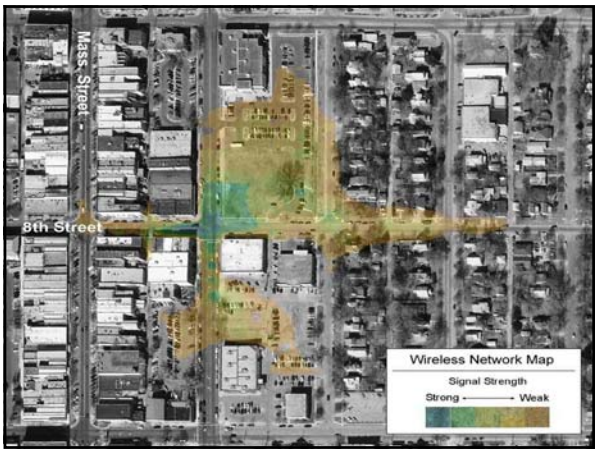
Region	Area (km²)	Access Points	Density (APs/km²)
U.S.	9,166,600	5,615,451	0.6
Las Vegas	240	26,069	109
Kansas City	270	29,438	109
Atlanta	460	65,364	142
San Francisco	213	69,502	326
Seattle	165	64,923	395
Boston	225	164,072	729
Manhattan	105	194,651	1,854

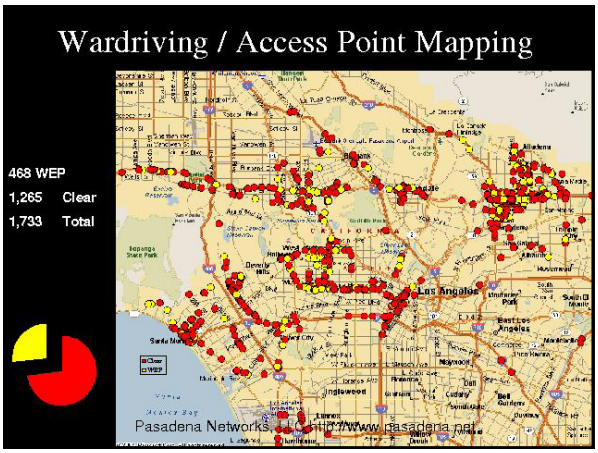
Wireless Usage Volume Over Time



Wireless Usage Locations Over Time







Sources of Threats

- Three sources of security problems are: human error and mistakes, malicious human activity, and natural events and disasters.
- *Human errors and mistakes* include accidental problems caused by both employees and nonemployees.
  - An example is an employee who misunderstands operating procedures and accidentally deletes customer records.
  - This category also includes poorly written application programs and poorly designed procedures.

Sources of Threats (Continued)

- The second source of security problems is *malicious human activity*.
  - This category includes employees and former employees who intentionally destroy data or other systems components.
  - It also includes hackers who break into a system and virus and worm writers who infect computer systems.
  - Malicious human activity also includes outside criminals who break into a system to steal for financial gain; it also includes terrorism.
- *Natural events and disasters* are the third source of security problems.
  - This category includes fires, floods, hurricanes, earthquakes, tsunamis, avalanches, and other acts of nature.
  - Problems in this category include not only the initial loss of capability and service, but also losses stemming from actions to recover from the initial problem.

Location & Privacy Practice

- How many ways have you been located today?
  - When I charged my gas to a credit card.
  - When I walked by the security camera in an secured area.
  - When I carry my cell phone, turned on.
  - When I put my card in the ATM machine.
  - When I drove through a monitored intersection.
  - When I used Google Search.
  - When I signed in to Amazon.com.
  - When I scanned my ID card to enter a room.
  - When I used my laptop computer on campus.
  - When I passed by a Bluetooth-enabled printer.

Problem Types

- Five types of security problems are:
  - Unauthorized data disclosure
  - Incorrect data modification
  - Faulty service
  - Denial of service
  - Loss of infrastructure

Figure 11-1 Security Problems and Sources

		Source		
		Human Error	Malicious Activity	Natural Disasters
Problem	Unauthorized data disclosure	Procedural mistakes	Pretexting Phishing Spoofing Sniffing Computer crime	Disclosure during recovery
	Incorrect data modification	Procedural mistakes Incorrect procedures Ineffective accounting controls System errors	Hacking Computer crime	Incorrect data recovery
	Faulty service	Procedural mistakes Development and installation errors	Computer crime Usurpation	Service improperly restored
	Denial of service	Accidents	DOS attacks	Service interruption
	Loss of infrastructure	Accidents	Theft Terrorist activity	Property loss

Unauthorized Data Disclosure

- *Unauthorized data disclosure* can occur by human error when someone inadvertently releases data in violation of a policy.
  - An example at a university would be a new department administrator who posts student names, numbers, and grades in a public place.
- The popularity and efficacy of search engines has created another source of inadvertent disclosure.
- Employees who place restricted data on Web sites that can be reached by search engines may mistakenly publish proprietary or restricted data over the Web.

Unauthorized Data Disclosure (Continued)

- **Pretexting** occurs when someone deceives by pretending to be someone else.
  - A common scam involves a telephone caller who pretends to be from a credit card company and claims to be checking the validity of credit card numbers.
- **Phishing** is a similar technique for obtaining unauthorized data that uses pretexting via email.
  - The *phisher* pretends to be a legitimate company and sends an email requesting confidential data, such as account numbers, Social Security numbers, account passwords, and so forth.

Unauthorized Data Disclosure (Continued)

- **Spoofing** is another term for someone pretending to be someone else.
  - *If you pretend to be your professor, you are spoofing your professor.*
- **IP spoofing** occurs when an intruder uses another site's IP address as if it were that other site.
- **Email spoofing** is a synonym for phishing.

Unauthorized Data Disclosure (Continued)

- **Sniffing** is a technique for intercepting computer communications.
  - With wired networks, sniffing requires a physical connection to the network.
  - With wireless networks, no such connection is required.
  - **Drive-by sniffers** simply take computers with wireless connections through an area and search for unprotected wireless networks.
  - Even protected wireless networks are vulnerable.
- Other forms of computer crime include breaking into networks to steal data such as customer lists, product inventory data, employee data, and other proprietary and confidential data.

Incorrect Data Modification

- Incorrect data modification can occur through human error when employees follow procedures incorrectly or when procedures have been incorrectly designed.
  - Examples include incorrectly increasing a customer's discount or incorrectly modifying an employee's salary.
- Hacking occurs when a person gains unauthorized access to a computer system.
  - Examples include reducing account balances or causing the shipment of goods to unauthorized locations and customers.

Faulty Service

- *Faulty service* includes problems that result because of incorrect system operation.
- Faulty service could include incorrect data modification, as previously described.
- It also could include systems that work incorrectly, by sending the wrong goods to the customer or the ordered goods to the wrong customer, incorrectly billing customers, or sending the wrong information to employees.
- **Usurpation** occurs when unauthorized programs invade a computer system and replace legitimate programs.
- Faulty service can also result from mistakes made during the recovery from natural disasters.

Denial of Service

- Human error in following procedures or a lack of procedures can result in **denial of service.**
  - For example, humans can inadvertently shut down a Web server or corporate gateway router by starting a computationally intensive application.
- *Denial-of-service attacks* can be launched maliciously.
  - A malicious hacker can flood a Web server, for example, with of millions of bogus services requests that so occupy the server that it cannot service legitimate requests.
  - Natural disasters may cause systems to fail, resulting in denial of service.

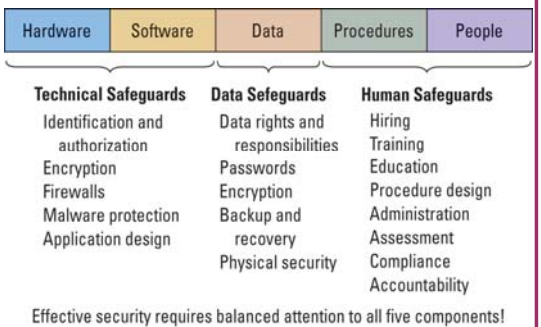
Loss of Infrastructure

- Human accidents can cause *loss of infrastructure.*
  - Examples are a bulldozer cutting a conduit of fiber-optic cables and the floor buffer crashing into a rack of Web servers.
  - Theft and terrorist events also cause loss of infrastructure.
    - A disgruntled, terminated employee can walk off with corporate data servers, routers, or other crucial equipment.
- Natural disasters present the largest risk for infrastructure loss.
  - A fire, flood, earthquake, or similar event can destroy data centers and all they contain.

The Security Program

- A security has three components:
  - Senior management involvement:
    - Senior management must establish the security policy
      - This policy sets the stage for the organization to respond to threats.
    - Senior management must manage risk by balancing the costs and benefits of the security program.
  - Safeguards of various kinds.
    - Safeguards are protections against security threats.
    - Safeguards involve computer hardware and software, data, procedures and people.
  - Incident response
    - A security program consists of the organization's planned response to security incidents.

Figure 11-2 Security Safeguards as They Relate to the Five Components



The NIST Handbook of Security Elements

- When you manage a department, you have the responsibility for information security in that department, even if no one tells you that you do.
- Security can be expensive.
  - Computer security should have an appropriate cost-benefit ratio.
  - Cost can be direct, such as labor costs; and they can be intangible, such as employee or customer frustration
- Managers should assign specific tasks to specific people or specific job functions.
- There is no magic bullet for security.
- Security is a continuing need, and every company must periodically evaluate its security program.
- Social factors put some limits on security programs.

Figure 11-3 Elements of Computer Security

1. Computer security should support the mission of the organization.
2. Computer security is an integral element of sound management.
3. Computer security should be cost-effective.
4. Computer security responsibilities and accountability should be made explicit.
5. System owners have computer security responsibilities outside their own organizations.
6. Computer security requires a comprehensive and integrated approach.
7. Computer security should be periodically reassessed.
8. Computer security is constrained by societal factors.

Security Policy

- A security policy has three elements:
  - A general statement of the organization's **security program.**
    - Management specifies the goals of the security program and the assets to be protected.
    - A department is designated for managing the organization's security program and documents.
  - *Issue-specific policy*
    - For example, management might formulate a policy on personal use of computers at work and email privacy.
  - *System-specific policy* is concerned with specific information systems.
    - For example, what customer data from the order entry system will be sold or shared with other organizations?

Risk Management

- **Risk** is the likelihood of an adverse occurrence.
- Management cannot manage threats directly, but it *can* manage the likelihood that threats will be successful.
- Companies can reduce risks, but always at a cost.
- **Uncertainty** refers to the things we don't know that we don't know.

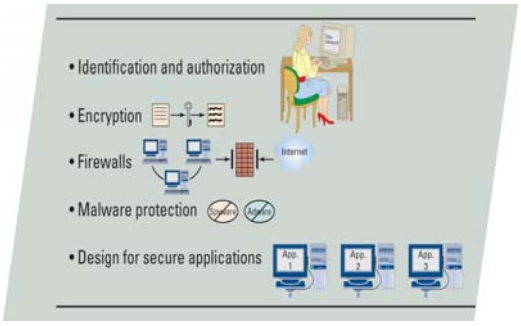
Figure 11-4 Risk Assessment

1. Assets
2. Threats
3. Safeguards
4. Vulnerability
5. Consequences
6. Likelihood
7. Probable loss

Risk-Management Decisions

- After reviewing the risk assessment, senior management must decide what to do.
- Companies can protect some assets by use of inexpensive and easily implemented safeguards.
  - Installing virus protection software is an example.
- Some vulnerability is expensive to eliminate, and management must determine if the costs of the safeguard are worth the benefit of probable loss reduction.

Figure 11-5 Technical Safeguards



Identification and Authentication

- Every information system today should require users to sign in with a user name and password.
- The user name *identifies* the user (the process of **identification**), and the password *authenticates* the user (the process of authentication)

- Smart Cards
  - A **smart card** is a plastic card similar to a credit card, which has a microchip.
  - The microchip is loaded with identifying data.
- Biometric Authentication
  - Biometric authentication uses personal physical characteristics such as fingerprints, facial features, and retinal scans to authenticate users.
  - Biometric authentication provides strong authentication, but the required equipment is expensive.
  - Biometric authentication is in the early stages of adoption.

Single Sign-on for Multiple Systems

- Today's operating systems have the capability to authenticate you to networks and other servers.
- You sign on to your local computer and provide authentication data; from that point on, your operating system authenticates you to another network or server, which can authenticate you to yet another network and server, and so forth.
- A system called **Kerberos** authenticates users without sending their passwords across the computer network.

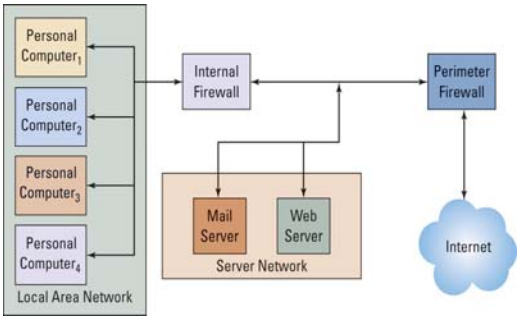
Encryption

- Senders use a key to encrypt a plaintext message and then send the encrypted message to a recipient, who then uses a key to decrypt the message.
- With **symmetric encryption**, both parties use the same key.
- With **asymmetric encryption**, the parties use two keys, one that is public and one that is private.

Digital Signatures

- **Digital signatures** ensure that plaintext messages are received without alterations.

Figure 11-8 Use of Multiple Firewalls



Malware Protection

- The term **malware** has several definitions.
- Our focus will be on the broadest one: *malware* is viruses, worms, Trojan horses, spyware, and adware.

Spyware and Adware

- **Spyware** programs are installed on the user's computer without the user's knowledge.
- Spyware resides in the background and, unknown to the user, observes the user's actions and keystrokes, monitors computer activity, and reports the user's activities to sponsoring organizations.
- Adware is similar to spyware in that it is installed without the user's permission and resides in the background and observes user behavior.
- Most adware is benign in that it does not perform malicious acts or steal data.
- Adware produces pop-up ads and can also change the user's default window or modify search results and switch the user's search engine.

Figure 11-9 Spyware and Adware Symptoms

- Slow system start up
- Sluggish system performance
- Many pop-up advertisements
- Suspicious browser homepage changes
- Suspicious changes to the taskbar and other system interfaces
- Unusual hard-disk activity

Malware Safeguards

- Install antivirus and antispyware programs on your computer.
- Set up your anti-malware programs to scan your computer frequently.
- Update malware definitions.
- Open email attachments only from known sources.
- Promptly install software updates from legitimate sources.
- Browse only in reputable Internet neighborhoods.

Malware Is a Serious Problem

- America Online (AOL) and the National Cyber Security Alliance conducted a malware study using Internet users in 2004.
- They asked the users a series of questions and then, with the users permission, they scanned the users computers to determine how accurately the users understood malware problems on their own computers.

Figure 11-10 Malware Survey Results

Question	User Response	Scan Results
Do you have a virus on your computer?	Yes: 6%	Yes: 19%
	No: 44%	No: 81%
	Don't know: 50%	
Average (maximum) number of viruses on infected computer		2.4 (213)
How often do you update your antivirus software?	Last week: 71%	Last week: 33%
	Last month: 12%	Last month: 34%
	Last 6 months: 5%	Last 6 months: 6%
	Longer than 6 months: 12%	Longer than 6 months: 12%
Do you think you have spyware or adware on your computer?	Yes: 53%	Yes: 80%
	No: 47%	No: 20%
Average (maximum) number of spyware/adware components on computer		93 (1,059)
Did you give permission to someone to install these components on your computer?	Yes: 5% No: 95%	

Data Safeguards

- *Data safeguards* are measures used to protect databases and other organizational data.
- The organization should protect sensitive data by storing it in encrypted form.
  - Such encryption uses one or more keys in ways similar to that described for data communication encryption.
- Backup copies of the database contents should be made periodically.

Data Safeguards (Continued)

- The organization should store at least some of the database backup copies off premises, possibly in a remote location.
- IT personnel should periodically practice recovery, to ensure that the backups are valid and that effective recovery procedures exist.
- The computers that run the DBMS and all devices that store database data should reside in locked, controlled-access facilities.

Figure 11-11 Data Safeguards

Human Safeguards–Position Definitions

- Effective human safeguards begin with definitions of job tasks and responsibilities.
- Given appropriate job descriptions, user accounts should be defined to give users the least possible privilege needed to perform their jobs.
- The security sensitivity should be documented for each position.

Human Safeguards–Hiring and Screening

- Security considerations should be part of the hiring process.
- When hiring for high-sensitive positions, however, extensive screening interviews, references, and high background investigations are appropriate.
  - This also applies to employees who are promoted into sensitive positions.

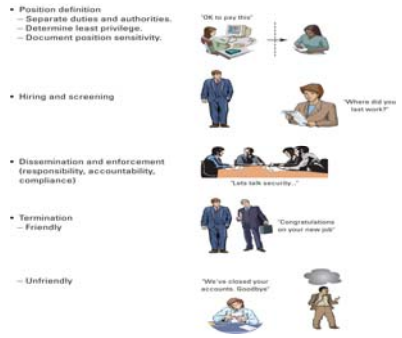
Human Safeguards–Dissemination and Enforcement

- Employees need to be made aware of the security policies, procedures, and responsibilities they will have.
- Employee security training begins during new-employee training with the explanation of general security policies and procedures.
- Enforcement consists of three interdependent factors: responsibility, accountability, and compliance.

Human Safeguards–Termination

- Companies must establish security policies and procedures for the termination of employees.
- Standard human resources policies should ensure that system administrators receive notification in advance of the employee's last day, so that they can remove accounts and passwords.
- The need to recover keys for encrypted data and any other special security requirements should be part of the employee's out-processing.

Figure 11-12 Security Policy for In-House Staff



Human Safeguards for Nonemployee Personnel

- Business requirements may necessitate opening information systems to nonemployee personnel-temporary personnel, vendors, partner personnel (employees of business partners), and the public.
- In the case of temporary, vendor, and partner personnel, the contracts that govern the activity should call for security measures appropriate to the sensitivity of the data and IS resource involved.

Human Safeguards for Nonemployee Personnel (Continued)

- Companies should require vendors and partners to perform appropriate screening and security training.
- The best safeguard from threats from public users is to *harden* the Web site or other facility against attack as much as possible.
- **Hardening** a site means to take extraordinary measures to reduce a system's vulnerability.
- Hardened sites use special versions of the operating system, and they lock down or eliminate operating systems features and functions that are not required by the application.

Account Administration

- The administration of user accounts, passwords, and help-desk policies and procedures are important components of the security system.

Account Management

- Account management concerns the creation of new user accounts, the modification of existing account permissions, and the removal of unneeded accounts.
- Information system administrators perform all of these tasks, but account users have the responsibilities to notify the administrators of the need for these actions.

Password Management

- Passwords are the primary means of authentication.
- Passwords are important not just for access to the user's computer, but also for authentication to other networks and servers to which the user may have access.
- Because of the importance of passwords, NIST recommends that employees be required to sign statements known as account acknowledgement forms.
- Some systems will require a password change every 3 months or perhaps more frequently.

Help-Desk Policies

- Many systems give the help-desk representative a means of authenticating the user.
- Typically, the help-desk information system has answers to questions that only the true user would know such as:
  - User's birthplace
  - Mother's maiden name
  - Last four digits of an important account number

Figure 11-14 System Procedures

	System users	Operations personnel
Normal operation	Use the system to perform job tasks, with security appropriate to sensitivity.	Operate data center equipment, manage networks, run Web servers, and related operational tasks.
Backup	Prepare for loss of system functionality.	Back up Web site resources, databases, administrative data, account and password data, and other data.
Recovery	Accomplish job tasks during failure. Know tasks to do during system recovery.	Recover systems from backed up data. Role of help desk during recovery.

System Procedures

- Procedures exist for both users and operations personnel.
- For each type of user, the company should develop procedures for normal, backup, and recovery operations.
- Normal-use procedures should provide safeguards appropriate to the sensitivity of the information system.

System Procedures (Continued)

- Backup procedures concern the creation of backup data to be used in the event of failure.
- Where as operations personnel have the responsibility for backing up system databases and other systems data, departmental personnel have the need to back up data on their own computers.
- Systems analysts should develop procedures for system recovery.

System Monitoring

- Important monitoring functions are activity log analyses, security testing, and investigating and learning from security incidents.
- Many information system programs produce *activity logs*.
  - Firewalls produce logs of their activities, including lists of all dropped packets, infiltration attempts, and unauthorized access attempts from within the firewall.
  - DBMS products produce logs of successful and failed log-ins.
- Web servers produce voluminous logs of Web activities.
- The operating systems in personal computers can produce logs of log-ins and firewall activities.

System Monitoring (Continued)

- An important security function is to analyze activity logs for threats patterns, successful and unsuccessful attacks, and evidence of security vulnerabilities.
- Companies should test their security programs.
  - Both in-house personnel and outside security consultants should conduct such testing.
- Security incidents need to be investigated.
- New technology changes the security landscape, and new threats arise.
- Security, like quality, is an ongoing process.

Disaster Preparedness

- The best safeguard against disaster is appropriate location.
- If possible, place computing centers, Web farms, and other computer facilities in locations not prone to floods, earthquakes, hurricanes, tornados, or avalanches.
  - Even in these locations, place infrastructure in unobtrusive buildings, basements, backrooms, and similar locations well within the physical perimeter of the organization.
  - Locate computing infrastructure in fire-resistant buildings designed to house expensive and critical equipment.

Disaster Preparedness (Continued)

- Even at a good location, disasters do occur.
- Some businesses prepare backup processing centers in locations geographically removed from the primary processing site.
- Organizations create backups for the critical resources at the remote processing centers.

Disaster Preparedness (Continued)

- **Hot sites** are remote processing centers run by commercial disaster-recovery services.
  - For a monthly fee, they provide all the equipment needed to continue operations following a disaster.
- **Cold sites** provide office space, but customers themselves provide and install the equipment needed to continue operations.
- Preparing a backup facility is very expensive; however, the costs of establishing and maintaining that facility are a form of insurance.

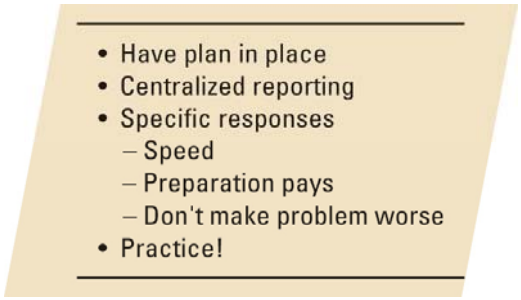
Figure 11-15 Disaster Preparedness

- Locate infrastructure in safe location.
- Identify mission-critical systems.
- Identify resources needed to run those systems.
- Prepare remote backup facilities.
- Train and rehearse.

Incident Response

- Every organization should have an incident-response plan as part of the security program.
- No organization should wait until some asset has been lost or compromised before deciding what to do.
- The plan should include how employees are to respond to security problems:
  - Whom they should contact
  - The reports they should make
  - The steps they can take to reduce further loss
- The plan should provide centralized reporting of all security incidents.
- The incident-response plan should identify critical personnel and their off-hours contact information.

Figure 11-16 Factors in incident Response



Problem Solving Guide–Testing Security

- The combination of bias and dissimilar worldviews means that security systems cannot be tested by the people who build them, or at least not only by the people who built the system.
- Therefore, many companies hire outsiders to test the security of their systems.
- **White hat hackers** are people who break into networks for the purpose of helping the organization that operates the network.

Security Guide–Metasecurity

- Metasecurity is security about security
  - "How do we secure the security system?"
- The accounting profession has dealt with some of these problems for decades and has developed a set of procedures and standards know as **accounting controls.**
  - In general, these controls involve procedures that provide checks and balances, independent reviews of activity logs, control of critical assets, and so forth.
  - Properly designed and implemented, such controls will catch the help-desk representative performing unauthorized account transfers.

Security Guide–Metasecurity (Continued)

- Many computer networks threats are new, proper safeguards are under development, and some threats are not yet known.
  - The safeguards for some problems have unexpected consequences.
- Ironically, the answers for many metasecurity problems lie in openness.
  - Encryption experts generally agree that any encryption algorithm that relies on secrecy is ultimately doomed, because the secret will get out.
- Metasecurity extends to the data, procedures, and people components as well.