Securing Information Systems

System Vulnerability and Abuse

- **Security:**
  - Policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems
- **Controls:**
  - Methods, policies, and organizational procedures that ensure safety of organization’s assets; accuracy and reliability of its accounting records; and operational adherence to management standards

System Vulnerability and Abuse

- **Why systems are vulnerable**
  - **Hardware problems**
    - Breakdowns, configuration errors, damage from improper use or crime
  - **Software problems**
    - Programming errors, installation errors, unauthorized changes)
  - **Disasters**
    - Power failures, flood, fires, etc.
  - **Use of networks and computers outside of firm’s control -** . When data are available over a network, there are even more vulnerabilities
    - E.g., with domestic or offshore outsourcing vendors

System Vulnerability and Abuse

- **Internet vulnerabilities -** Internet is so huge that when abuses do occur, they can have an enormously widespread impact. And when the Internet becomes part of the corporate network, the organization’s information systems are even more vulnerable to actions from outsiders
  - **Network open to anyone**
  - **Size of Internet means abuses can have wide impact**
  - **Use of fixed Internet addresses with permanent connections to Internet eases identification by hackers**
  - **E-mail attachments**
  - **E-mail used for transmitting trade secrets**
  - **IM messages lack security, can be easily intercepted**

Compromising Web Sites

- **SQL injection technique** exploits sloppy programming practices that do not validate user input
  - input SQL statements in a web form to get a badly designed website to dump the database content to the attacker
  - IBM identifies SQL injection as the fastest growing security threat, with over half a million attack attempts recorded each day.
  - Firms have to check the integrity of their Web sites for vulnerabilities

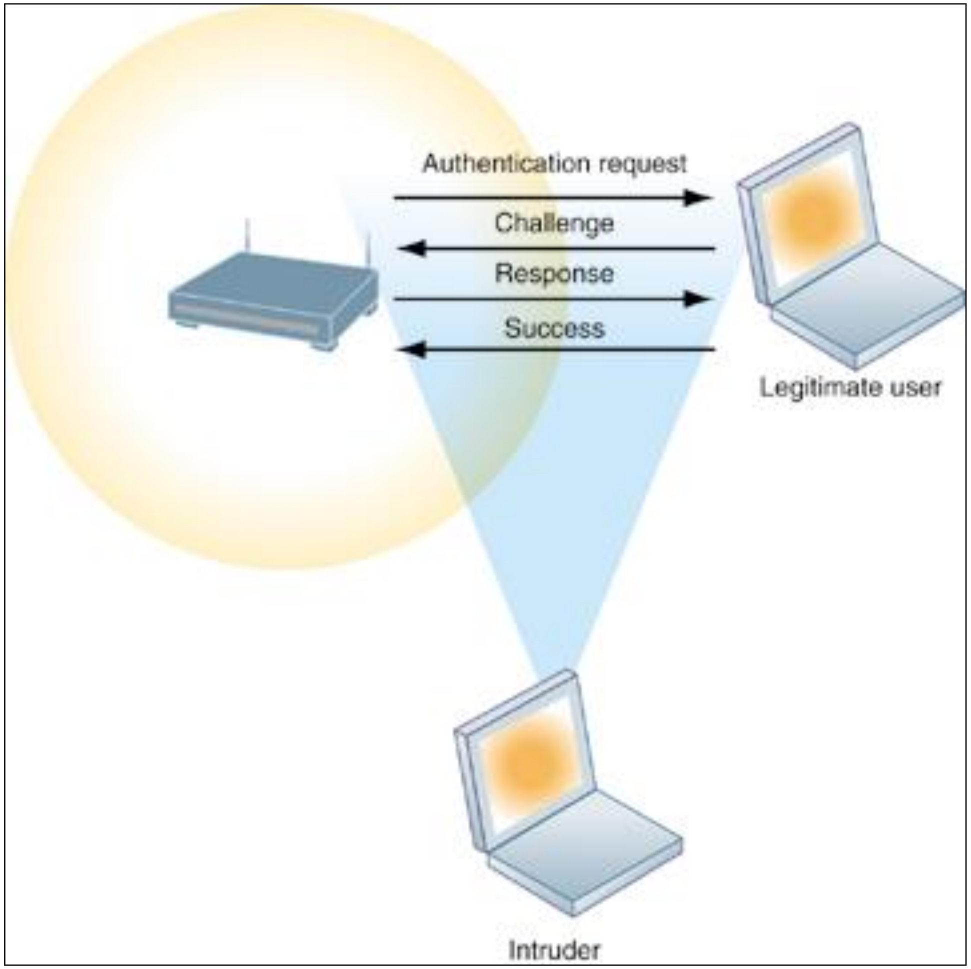
Securing Wireless Networks - Challenges

- Radio frequency bands easy to scan
- SSIDs (service set identifiers)
  - Identify access points.
  - Broadcast multiple times.
- War driving
  - Eavesdroppers drive by buildings and try to intercept network traffic
  - When hacker gains access to SSID, has access to network's resources
- WEP (Wired Equivalent Privacy)
  - Security standard for 802.11 – easy to penetrate by hackers
  - The WEP specification calls for an access point and its users to share the same 40-bit encrypted password.
  - Basic specification uses shared password for both users and access point
  - Users often fail to use security features
  - Assigning unique name to network's SSID
  - TJX fiasco - they should have used WPA
- Wi-Fi Alliance finalized WAP2 specification, replacing WEP with stronger standards
  - Continually changing keys
  - Encrypted authentication system with central server

The service set identifiers (SSIDs) identifying the access points in a Wi-Fi network are broadcast multiple times (as illustrated by the orange sphere) and can be picked up fairly easily by intruders' sniffer programs

Many Wi-Fi networks can be penetrated easily by intruders using sniffer programs to obtain an address to access the resources of a network without authorization.

Wi-Fi Security Challenges



The Worst Data Theft Ever?

- List and describe the security control weaknesses at TJX Companies
- What management, organization, and technology factors contributed to these weaknesses?
- What was the business impact of TJX’s data loss on TJX, consumers, and banks?
- How effectively did TJX deal with these problems?
- Who should be held liable for the losses caused by the use of fraudulent credit cards in this case? The banks issuing the cards or the consumers? Justify your answer.
- What solutions would you suggest to prevent the problems?

The TJX Breach

- Business establishments are increasingly under risk of information security threats
  - Network in TJX retail store was infiltrated via an insecure Wi-Fi base station
  - 45.7 million credit and debit card numbers were stolen
  - Driver’s licenses and other private information pilfered from 450,000 customers
  - TJX suffered under settlement costs and court-imposed punitive action to the tune of $150 million
  - **Even without lawsuit liabilities, Forrester Research estimates that the cost to TJX for the data breach could surpass $1 billion over five years.**

The TJX Breach

- Factors that amplified severity of TJX security breach are:
  - Personnel betrayal: An alleged FBI informant used insider information to mastermind the attacks
  - **Management** gaffe: Executives made conscious **decisions not to upgrade legacy systems that were vulnerable to security compromises**
  - **Technology** lapse: TJX *used WEP, a insecure wireless security technology*
    - failed to follow the **most basic security measures** like installing **antivirus software, upgrading wireless security, encrypting data, and creating and using access controls, and establishing information system controls** (general and application).
  - **Procedural** gaffes: TJX had received an *extension on the rollout of mechanisms that might have discovered and plugged the hole* before the hackers got in
    - **Also willfully violated the Payment Card Industry (PCI) Data Security Standard by holding onto data for years**

Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

- **Malware**
  - **Viruses (email, IM, video, data files downloaded etc)**
    - **Rogue software program that attaches itself to other software programs or data files in order to be executed**
    - Most antivirus software is effective against only those viruses already known when the software is written.
  - **Worms**
    - **Independent computer programs that copy themselves from one computer to other computers over a network**
  - **Trojan horses**
    - **Software program that appears to be benign but then does something other than expected.**
    - In 2004, users were enticed by a sales message from a *supposed* anti-virus vendor.
    - On the vendor's site, a small program called Mitglieder was downloaded to the user's machine. The program enabled outsiders to infiltrate the user's machine.

Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

- **Malware (cont.)**
  - **Spyware**
    - Small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising
  - **Key loggers**
    - Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks

Cookies

- ***Cookie*** – a small file that contains information about you and your Web activities, which a Web site places on your computer
- Handle cookies by using
  - Web browser cookie management option
  - Buy a program that manages cookies
- Not executable, cannot deliver a virus or other malicious code
- Only web server that delivered it can read it
- Your computer can store cookies from many web sites
- May be a security risk if it is implemented poorly on site that you have shared personal information with and rely on cookies to access it
  - Anyone who can access the cookie on your hard drive can now access that personal information
  - Most reputable sites to not rely on cookies for authentication alone.

Hackers and Computer Crime

- **Computer crime**
  - Defined as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution”
  - **Computer may be target of crime:**
  - **Computer may be instrument of crime:**

- According to CSI Computer Crime and Security Survey of nearly 500 companies, participant companies' average annual loss from computer crime and security attacks was $350,424 in 2009 (certainly more in 2013)
- However, many companies are reluctant to report computer crimes. Why?
- What are the most economically damaging types of computer crime?
  - DoS,
  - introducing viruses,
  - theft of services,
  - disruption of computer systems.

Examples of Computer Crime

Computers as Targets of Crime

- Breaching confidentiality of protected computerized data
- Accessing a computer system without authority
- Knowingly accessing a protected computer to commit fraud
- Intentionally accessing a protected computer and causing damage, negligently or knowingly
- Knowingly transmitting program, program code, or command that intentionally cause damage to a protected computer
- Threatening to cause damage to a protected system

Examples of Computer Crime

Computers as Instruments of Crime

- Theft of trade secrets
- Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and video
- Schemes to defraud
- Using e-mail for threats or harassment
- Intentionally attempting to intercept electronic communication
- Illegally accessing stored electronic communication, including e-mail and voice mail
- Transmitting or possessing child pornography

- **Hackers and computer crime**
  - **Hackers vs. crackers (hacker with criminal intent)**
  - **White hat hacker – hackers hired by companies to reveal security weaknesses within the firm’s systems**
  - **Activities include**
    - **System intrusion**
    - **Theft of goods and information**
    - **System damage**
    - **Cybervandalism**
      - Intentional disruption, defacement, destruction of Web site or corporate information system

Hackers and Computer Crime

- **Spoofing**
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Redirecting Web link to address different from intended one, with site masquerading as intended destination
- **Sniffer / Packet sniffer**
  - Eavesdropping program that monitors information traveling over network
  - Enables hackers to steal proprietary information such as e-mail, company files, and so on
    - use your debit card information to purchase items illegally.
    - steal your logon and passwords for various accounts.
    - assume your identity.

Hackers and Computer Crime

- **Denial-of-service attacks (DoS)**
  - Flooding server with thousands of false requests to crash the network.
- **Distributed denial-of-service attacks (DDoS)**
  - Use of numerous computers to launch a DoS
  - **Botnets**
    - Networks of “zombie” PCs infiltrated by bot malware
    - Zombie PCs used to initiate DDoS attacks
    - Extortionists might leverage botnets or hacked data to demand payment to avoid retribution

System Vulnerability and Abuse

- **Computer crime**
  - Defined as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution”
  - **Computer may be target of crime, e.g.:**
    - Breaching confidentiality of protected computerized data
    - Accessing a computer system without authority
  - **Computer may be instrument of crime, e.g.:**
    - Theft of trade secrets
    - Using e-mail for threats or harassment
  - According to CSI Computer Crime and Security Survey of nearly 500 companies, companies’ average annual loss from computer crime and security attacks was $350,424
  - many companies are reluctant to report computer crimes. Why?
  - What are the most economically damaging types of computer crime? (DoS, introducing viruses, theft of services, disruption of computer systems.)

System Vulnerability and Abuse

- **Identity theft:** Theft of personal Information (social security id, driver’s license or credit card numbers) to impersonate someone else
- **Phishing:** Setting up fake Web sites or sending e-mail messages that look like legitimate businesses to ask users for confidential personal data.
- **Evil twins:** Wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet
- **Pharming:** Redirects users to a bogus Web page, even when individual types correct Web page address into his or her browser

System Vulnerability and Abuse

- **Click fraud**
  - Individual or computer program clicks online ad without any intention of learning more or making a purchase
- **Link farming**
  - a type of online advertising fraud where fraudsters attempt to increase a page's results in organic search by creating a series of bogus Web sites linking back to it
- **Global threats - Cyberterrorism and cyberwarfare**
  - Concern that Internet vulnerabilities and other networks make digital networks easy targets for digital attacks by terrorists, foreign intelligence services, or other groups

System Vulnerability and Abuse

- **Internal threats – Employees**
  - **Security threats often originate inside an organization**
    - **Inside knowledge**
    - **Sloppy security procedures**
      - User lack of knowledge
      - Must have separation of duties and controls
    - **Social engineering:**
      - Tricking employees into revealing their passwords by pretending to be legitimate members of the company in need of information

        - **San Francisco Hack: Where Was the Oversight?**

Security Testing

- You may be aware that there are professional security firms that organizations can hire to break into their own networks to test security. BABank (pseudonym) was about to launch a new online banking application, so it hired such a firm to test its security before the launch. The bank's system failed the security test – badly.
- The security team began by mapping the bank's network. It used network security analysis software to test password security, and dialing software to test for dial-in phone numbers. This process found many accounts with default passwords (i.e. passwords set by the manufacturer that are supposed to be changed when the systems are first set up).
- The team then tricked several high-profile users into revealing their passwords to gain access to several high-privilege accounts. Once into these computers, the team used password-cracking software to find passwords on these computers and ultimately gain the administrator passwords on several servers.
- At this point, the team transferred $1000 into their test account. They could have transferred much more, but the security point was made.

System Vulnerability and Abuse

- **Software vulnerability**
  - **Commercial software contains flaws that create security vulnerabilities**
    - Hidden bugs (program code defects)
      - Zero defects cannot be achieved because complete testing is not possible with large programs
    - Flaws can open networks to intruders
  - **Patches**
    - Vendors release small pieces of software to repair flaws
    - However, amount of software in use can mean exploits created faster than patches be released and implemented

The cost to the U.S. economy from software flaws runs to nearly $60 billion each year.

Business Value of Security and Control

- **Legal and regulatory requirements for electronic records management**
  - Firms face new legal obligations for the retention and storage of electronic records as well as for privacy protection
  - **HIPAA:** Medical security and privacy rules and procedures
  - **Gramm-Leach-Bliley Act:** Requires financial institutions to ensure the security and confidentiality of customer data
  - **Sarbanes-Oxley Act:** Imposes responsibility on companies and their management to safeguard the accuracy and integrity of financial information that is used internally and released externally

Business Value of Security and Control

- **Sarbanes-Oxley Act:** designed to protect investors after the scandals at Enron, WorldCom, and other public companies. Sarbanes-Oxley is fundamentally about ensuring that internal controls are in place to govern the creation and documentation of information in

- Financial statements. Because managing this data involves information systems, **information systems must implement controls to make sure this information is accurate and to enforce integrity, confidentiality, and accuracy.**

Business Value of Security and Control

- **Electronic evidence**
  - **Evidence for white collar crimes often found in digital form**
  - Data stored on computer devices, e-mail, instant messages, e-commerce transactions
- **Proper control of data can save time, money when responding to legal discovery request**
- **Computer forensics:**
  - Scientific collection, examination, authentication, preservation, and analysis of data from computer storage media for use as evidence in court of law
  - Includes recovery of **ambien**t and hidden data
  - Ambient data is information that lies in areas not generally accessible to the user: file slack, unallocated clusters, virtual memory files and other areas not allocated to active files. This is a forensic term that describes, in general terms, data stored in non-traditional computer storage areas and formats.

Legal Action

- In a legal action, a firm is obligated to respond to a discovery request for access to information that may be used as evidence,
- and the company is required by law to produce this data.
- The cost of responding to a discovery request can be enormous if the company has trouble assembling the required data or the data have been corrupted or destroyed.
- Courts impose severe financial and even criminal penalties for improper destruction of electronic documents.

Establishing a Framework for Security and Control

- **Application controls**
  - Specific controls unique to each computerized application, such as payroll or order processing
  - Include both automated and manual procedures
  - Ensure that only authorized data are completely and accurately processed by that application
  - Types of application controls:
    - **Input controls -** input authorization, data conversion, data editing, and error handling
    - **Processing controls -** establish that data are complete and accurate during updating
    - **Output controls -** ensure that the results of computer processing are accurate, complete, and properly distributed

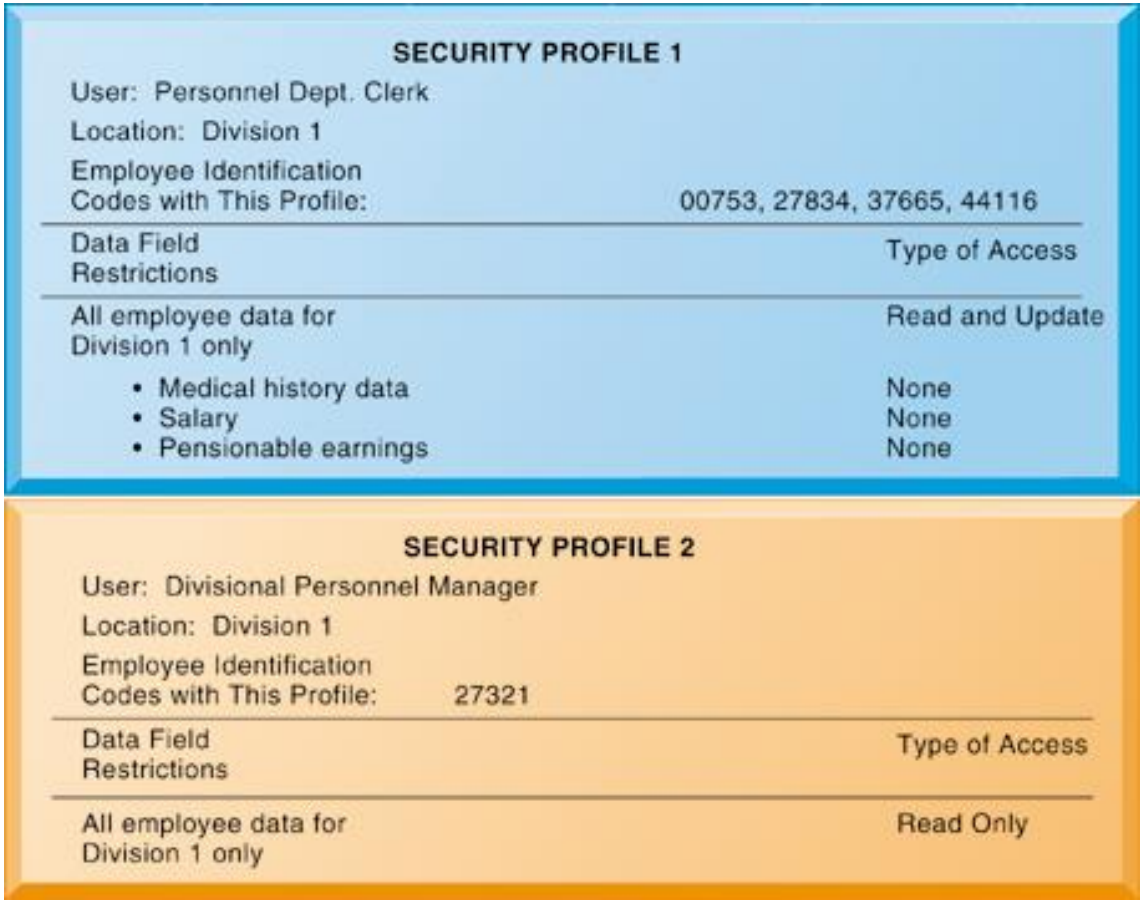
Establishing a Framework for Security and Control

- **Security policy**
  - Ranks information risks, identifies acceptable security goals, and identifies mechanisms for achieving these goals
  - Drives other policies
    - **Acceptable use policy (AUP):** Defines acceptable uses of firm's information resources and computing equipment
    - **Authorization policies:** Determine differing levels of user access to information assets
- **Authorization management systems**
  - Allow each user access only to those portions of system that person is permitted to enter, based on information established by set of access rules, profile

Establishing a Framework for Security and Control

Security Profiles for a Personnel System

These two examples represent two security profiles or data security patterns that might be found in a personnel system. Depending on the security profile, a user would have certain restrictions on access to various systems, locations, or data in an organization.



SECURITY PROFILE 1

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

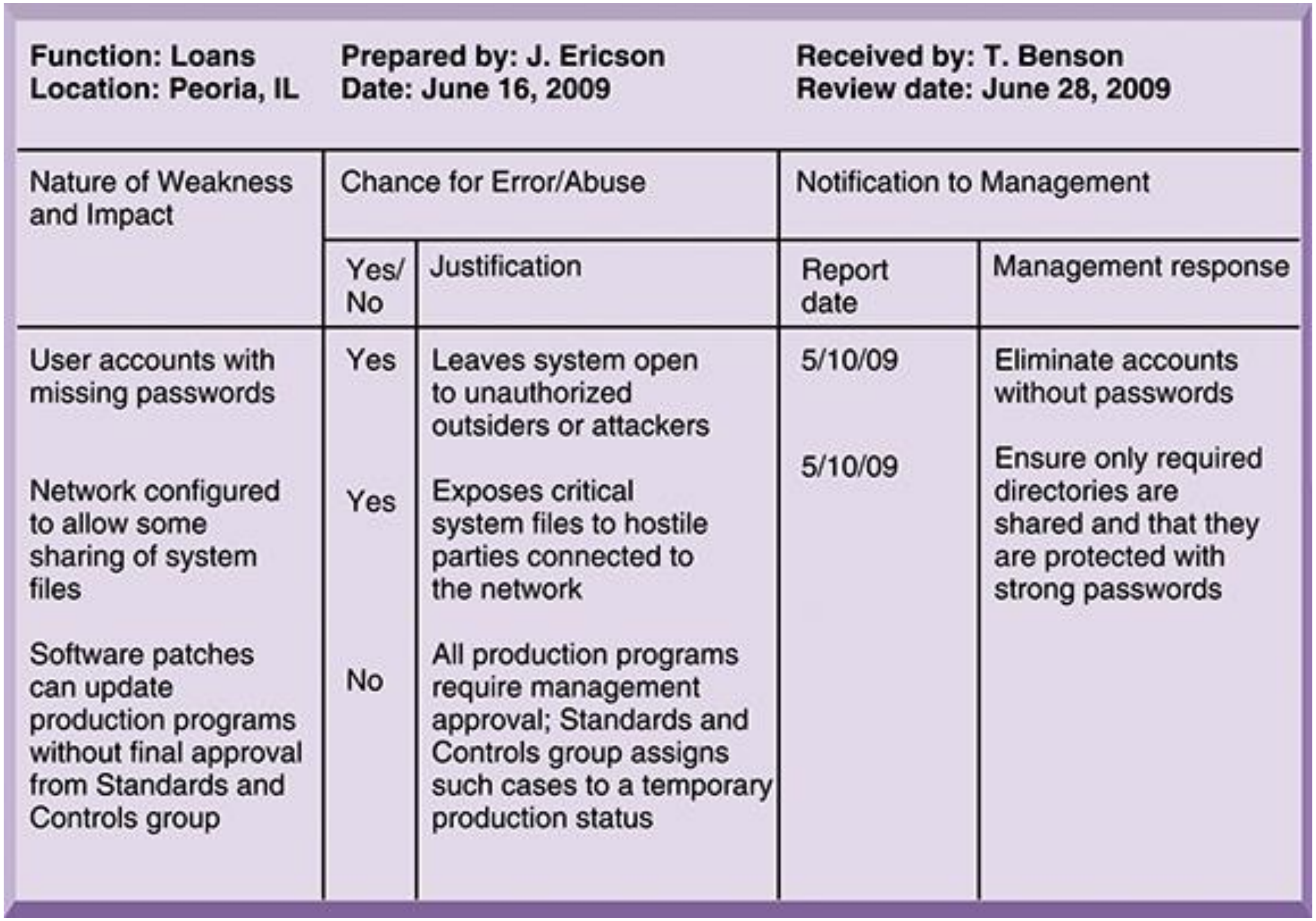
- **Disaster recovery planning:** Devises plans for restoration of disrupted services
    - focus primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services
    - MasterCard, maintains a duplicate computer center in Kansas City, Missouri, to serve as an emergency backup to its primary computer center in St. Louis.
- **Business continuity planning:** Focuses on restoring business operations after disaster
- Both types of plans needed to identify firm’s most critical systems and business processes
    - Business impact analysis to determine impact of an outage
    - Management must determine
        - Maximum time systems can be down
        - Which systems must be restored first

The Role of Auditing

- **MIS audit -** determines if existing security measures and controls are effective
  - Examines firm's overall security environment as well as controls governing individual information systems
  - Reviews technologies, procedures, documentation, training, and personnel
  - May even simulate disaster to test response of technology, IS staff, other employees
  - Lists and ranks all control weaknesses and estimates probability of their occurrence
  - Assesses financial and organizational impact of each threat

Sample Auditor’s List of Control Weaknesses

This chart is a sample page from a list of control weaknesses that an auditor might find in a loan system in a local commercial bank. This form helps auditors record and evaluate control weaknesses and shows the results of discussing those weaknesses with management, as well as any corrective actions taken by management.



Function: Loans **Location: Peoria, IL**	**Prepared by: J. Ericson** **Date: June 16, 2009**		**Received by: T. Benson** **Review date: June 28, 2009**	
Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management	
	Yes/ No	Justification	Report date	Management response
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/09	Eliminate accounts without passwords
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/09	Ensure only required directories are shared and that they are protected with strong passwords
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status		

Technologies and Tools for Security

- **Firewall:** Hardware and/or software to prevent unauthorized access to private networks
- Must maintain detailed internal rules identifying the people, applications, or addresses that are allowed or rejected.
- Firewalls can deter, but not completely prevent, network penetration by outsiders and should be viewed as one element in an overall security plan

- **Intrusion detection systems:** Monitor vulnerable points on networks to detect and deter intruders
  - Examines events as they are happening to discover attacks in progress
  - Scans network to find patterns indicative of attacks
  - Scans for known problems such as Bad passwords, removal of important files etc.

Technologies and Tools for Security

- **Ensuring system availability**
    - **Online transaction processing requires 100% availability, no downtime.**
    - **There is a huge $$ loss in downtime**
    - **Fault-tolerant computer systems**
        - For continuous availability e.g. stock mk’t, airline reservation
        - Contain redundant hardware, software, and power supply components to provide continuous, uninterrupted service
    - **High-availability computing**
        - Helps recover quickly from crash
        - Minimizes, does not eliminate downtime
- Firms with heavy **e-commerce processing or for firms that depend on digital networks for their internal operations** require high-availability computing, using tools such as **backup servers, distribution of processing across multiple servers, high-capacity storage**, and good disaster recovery and business continuity plans

Hot Site

- A hot site is a commercial disaster recovery service that allows a business to continue computer and network operations in the event of a computer or equipment disaster.
- If an firm's data center becomes inoperable it can move all data processing operations to a hot site.
- A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data.
  - The site has all the equipment needed for the enterprise to continue operation, including office space and furniture, telephone jacks and computer equipment.
- Real time synchronization between the two sites may be used to completely mirror the data environment of the original site.
- Following a disruption to the original site, the hot site exists so that the organization can relocate with minimal losses to normal operations.
- Ideally, a hot site will be up and running within a matter of hours or even less.
- Example – Hurricane Katrina - oil company hot sites

Cold Site

- A cold site is the most inexpensive type of backup site for an organization to operate.
- Does not include backed up copies of data and information from the original location of the organization,
- Does not include hardware already set up.
  - The lack of hardware contributes to the minimal startup costs of the cold site,
  - Requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.
- Typically, a business has an annual contract with a company that offers hot and cold site services with a monthly service charge.
- Some disaster recovery services offer backup services so that all company data is available regardless of whether a hot site or cold site is used.