MODULE 5

SYSTEMS SECURITY AND CONTROL

OUTLINES

- The business value of security and control
- Organizational and managerial frameworks for security and control
- System vulnerability and abuse
- Preventative maintenance techniques and security controls.
- Disaster recovery planning
- Quality control and quality assurance
- Tools and technologies for safeguarding information resources.

Business value of Security and Control

Companies have very valuable information assets to protect. Systems often house confidential information about individuals' taxes, financial assets, medical records, and job performance reviews. They also can contain information on corporate operations, including trade secrets, new product development plans, and marketing strategies. Government systems may store information on weapons systems, intelligence operations, and military targets. These information assets have tremendous value, and the repercussions can be devastating if they are lost, destroyed, or placed in the wrong hands.

Many firms are reluctant to spend heavily on security because it is not directly related to sales revenue. However, protecting information systems is so critical to the operation of the business that it deserves a second look.

Inadequate security and control may result in serious legal liability. Businesses must protect not only their own information assets but also those of customers, employees, and business partners. Failure to do so may open the firm to costly litigation for data exposure or theft. An organization can be held liable for needless risk and harm created if the organization fails to take appropriate protective action to prevent loss of confidential information, data corruption, or breach of privacy.

Business value of Security and Control… cont

Electronic evidence and computer forensics

Security, control, and electronic records management have become essential for responding to legal actions. Much of the evidence today for stock fraud, embezzlement, theft of company trade secrets, computer crime, and many civil cases is in digital form. In addition to information from printed or typewritten pages, legal cases today increasingly rely on evidence represented as digital data stored on portable floppy disks, CDs, and computer hard disk drives, as well as in e-mail, instant messages, and e-commerce transactions over the Internet. E-mail is currently the most common type of electronic evidence.

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 those 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 now impose severe financial and even criminal penalties for improper destruction of electronic documents.

An effective electronic document retention policy ensures that electronic documents, e-mail, and other records are well organized, accessible, and neither retained too long nor discarded too soon. It also reflects an awareness of how to preserve potential evidence for computer forensics.

Business value of Security and Control… cont

Computer forensics is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law. It deals with the following problems:

- Recovering data from computers while preserving evidential integrity
- Securely storing and handling recovered electronic data
- Finding significant information in a large volume of electronic data
- Presenting the information to a court of law

Electronic evidence may reside on computer storage media in the form of computer files and as *ambient data*, which are not visible to the average user. An example might be a file that has been deleted on a PC hard drive. Data that a computer user may have deleted on computer storage media can be recovered through various techniques. Computer forensics experts try to recover such hidden data for presentation as evidence.

Organizational and Managerial Frameworks for Security and Control

Even with the best security tools, your information systems won't be reliable and secure unless you know how and where to deploy them. You'll need to know where your company is at risk and what controls you must have in place to protect your information systems. You'll also need to develop a security policy and plans for keeping your business running if your information systems aren't operational.

Information Systems Controls

Information systems controls are both manual and automated and consist of both general controls and application controls.

General Controls govern the design, security, and use of computer programs and the security of data files in general throughout the organization's information technology infrastructure.

On the whole, general controls apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment.

Organizational and Managerial Frameworks for Security and Control… cont

General controls include software controls, physical hardware controls, computer operations controls, data security controls, controls over implementation of system processes, and administrative controls.

Application Controls are specific controls unique to each computerized application, such as payroll or order processing. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application.

Application controls can be classified as (1) input controls, (2) processing controls, and (3) output controls.

1. *Input controls* check data for accuracy and completeness when they enter the system. There are specific input controls for input authorization, data conversion, data editing, and error handling.
2. *Processing controls* establish that data are complete and accurate during updating.
3. *Output controls* ensure that the results of computer processing are accurate, complete, and properly distributed.

Organizational and Managerial Frameworks for Security and Control… cont

Risk Assessment

Before your company commits resources to security and information systems controls, it must know which assets require protection and the extent to which these assets are vulnerable. A risk assessment helps answer these questions and determine the most cost-effective set of controls for protecting assets.

A **risk assessment** determines the level of risk to the firm if a specific activity or process is not properly controlled. Not all risks can be anticipated and measured, but most businesses will be able to acquire some understanding of the risks they face. Business managers working with information systems specialists should try to determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage.

Once the risks have been assessed, system builders will concentrate on the control points with the greatest vulnerability and potential for loss.

Organizational and Managerial Frameworks for Security and Control… cont

Security Policy

Once you've identified the main risks to your systems, your company will need to develop a security policy for protecting the company's assets. A **security policy** consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals.

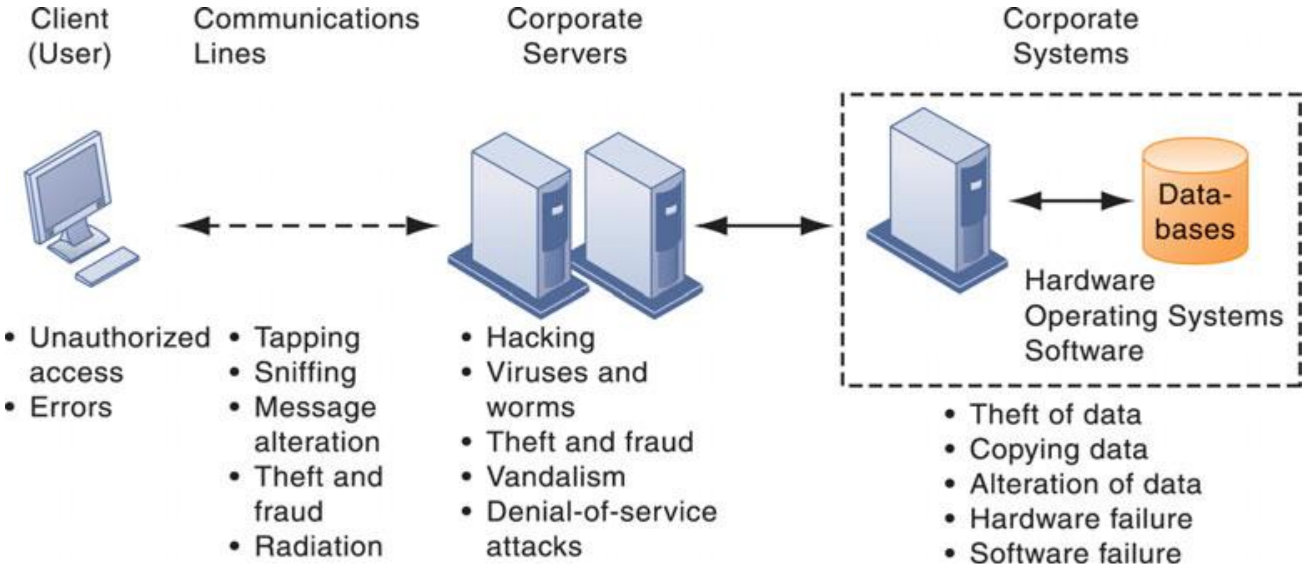
What are the firm's most important information assets? Who generates and controls this information in the firm? What existing security policies are in place to protect the information? What level of risk is management willing to accept for each of these assets? Is it willing, for instance, to lose customer credit data once every 10 years? Or will it build a security system for credit card data that can withstand the once-in-a-hundred-year disaster? Management must estimate how much it will cost to achieve this level of acceptable risk.

System vulnerability and abuse

If you operate a business today, you need to make security and control a top priority. **Security** refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems. **Controls** are methods, policies, and organizational procedures that ensure the safety of the organization's assets; the accuracy and reliability of its records; and operational adherence to management standards.

When large amounts of data are stored in electronic form, they are vulnerable to many more kinds of threats than when they existed in manual form.

Contemporary Security Challenges and Vulnerabilities



System vulnerability and abuse… cont.

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

Malicious software programs are referred to as **malware** and include a variety of threats, such as computer viruses, worms, and Trojan horses. A **computer virus** is a rogue software program that attaches itself to other software programs or data files in order to be executed, usually without user knowledge or permission.

Worms, which are independent computer programs that copy themselves from one computer to other computers over a network. (Unlike viruses, they can operate on their own without attaching to other computer program files and rely less on human behavior in order to spread from computer to computer.

A **Trojan horse** is a software program that appears to be benign but then does something other than expected, such as the Zeus Trojan described in the chapter-opening case. The Trojan horse is not itself a virus because it does not replicate, but it is often a way for viruses or other malicious code to be introduced into a computer system.

Keyloggers record every keystroke made on a computer to steal serial numbers for software, to launch Internet attacks, to gain access to e-mail accounts, to obtain passwords to protected computer systems, or to pick up personal information such as credit card numbers. Other spyware programs reset Web browser home pages, redirect search requests, or slow performance by taking up too much memory.

System vulnerability and abuse… cont.

Computer Crime/Fraud Methods

Computer Crime and Abuse – Computer crime is any illegal act to which a computer is used as the primary tool. Computer abuse is the unethical use of a computer.

Security threats related to computer crime or abuse include:

Impersonation: Gaining access to a system by identifying oneself as another person. Defeating the identification and authentication controls employed by the system, the impersonator enjoys the privileges of a legitimate user.

Trojan horse method: concealing within an authorised program a set of instructions that will cause unauthorised actions.

Logic Bomb: Unauthorised instructions, often introduced with the Trojan Horse technique, which stay dormant until a specific event occurs or time/date (triggers) comes, at which they effect an unauthorised act.

Denial of service: Rendering the system unusable by legitimate users.

Data diddling: Changing data before or during input, often to change the contents of a database.

Salami Technique: Diverting unnoticeable small amounts of money from a large number of accounts maintained by the system into an account the perpetrator can access.

System vulnerability and abuse… cont.

Spoofing: Configuring a computer system to masquerade as another system over the network in order to gain unauthorised access to the resources the system being mimicked is entitled to.

Super zapping: Using a systems program that can bypass regular system controls to perform unauthorised acts.

Scavenging: unauthorised access to information by searching through the residue after a job has been run on a computer. Techniques range from searching waste baskets or dumpsters for printouts to scanning the contents of a computer's memory.

Data leakage: variety of methods for obtaining the data stored in a system. The data may be encoded into an innocuous report in sophisticated ways, e.g. as the number of characters per line.

Wiretapping: Tapping computer telecommunications lines to obtain information.

System vulnerability and abuse… cont.

Software Vulnerability

Software errors pose a constant threat to information systems, causing untold losses in productivity. Growing complexity and size of software programs, coupled with demands for timely delivery to markets, have contributed to an increase in software flaws or vulnerabilities.

A major problem with software is the presence of hidden **bugs** or program code defects. Studies have shown that it is virtually impossible to eliminate all bugs from large programs. The main source of bugs is the complexity of decision-making code. A relatively small program of several hundred lines will contain tens of decisions leading to hundreds or even thousands of different paths.

Important programs within most corporations are usually much larger, containing tens of thousands or even millions of lines of code, each with many times the choices and paths of the smaller programs.

Disaster recovery planning

If you run a business, you need to plan for events, such as power outages, floods, earthquakes, or terrorist attacks that will prevent your information systems and your business from operating. **Disaster recovery planning** devises plans for the restoration of computing and communications services after they have been disrupted. Disaster recovery plans 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.

Quality control and quality assurance

Ensuring Software Quality

In addition to implementing effective security and controls, organizations can improve system quality and reliability by employing software metrics and rigorous software testing. Software metrics are objective assessments of the system in the form of quantified measurements. Ongoing use of metrics allows the information systems department and end users to jointly measure the performance of the system and identify problems as they occur. Examples of software metrics include the number of transactions that can be processed in a specified unit of time, online response time, the number of payroll checks printed per hour, and the number of known bugs per hundred lines of program code. For metrics to be successful, they must be carefully designed, formal, objective, and used consistently.

Early, regular, and thorough testing will contribute significantly to system quality. Many view testing as a way to prove the correctness of work they have done. In fact, we know that all sizable software is riddled with errors, and we must test to uncover these errors.

Good testing begins before a software program is even written by using a *walkthrough*—a review of a specification or design document by a small group of people carefully selected based on the skills needed for the particular objectives being tested.

Tools and Technologies for Safeguarding Information Resources

Businesses have an array of technologies for protecting their information resources. They include tools for managing user identities, preventing unauthorized access to systems and data, ensuring system availability, and ensuring software quality.

Identity Management and Authentication

Large and midsize companies have complex IT infrastructures and many different systems, each with its own set of users. Identity management software automates the process of keeping track of all these users and their system privileges, assigning each user a unique digital identity for accessing each system. It also includes tools for authenticating users, protecting user identities, and controlling access to system resources.

To gain access to a system, a user must be authorized and authenticated. **Authentication** refers to the ability to know that a person is who he or she claims to be. Authentication is often established by using **passwords** known only to authorized users.

New authentication technologies includes tokens, smart cards, and biometric authentications.

Tools and Technologies for Safeguarding Information Resources… cont.

Firewalls, Intrusion Detection Systems, and Antivirus Software

Without protection against malware and intruders, connecting to the Internet would be very dangerous. Firewalls, intrusion detection systems, and antivirus software have become essential business tools.

1. ***Firewalls*** prevent unauthorized users from accessing private networks. A firewall is a combination of hardware and software that controls the flow of incoming and outgoing network traffic. It is generally placed between the organization's private internal networks and distrusted external networks, such as the Internet, although firewalls can also be used to protect one part of a company's network from the rest of the network.
2. ***Intrusion Detection Systems:*** Commercial security vendors now provide intrusion detection tools and services to protect against suspicious network traffic and attempts to access files and databases. Intrusion detection systems feature full-time monitoring tools placed at the most vulnerable points or "hot spots" of corporate networks to detect and deter intruders continually. The system generates an alarm if it finds a suspicious or anomalous event.

Tools and Technologies for Safeguarding Information Resources… cont.

3. Antivirus and Antispyware Software: Defensive technology plans for both individuals and businesses must include antivirus protection for every computer. Antivirus software is designed to check computer systems and drives for the presence of computer viruses. Often the software eliminates the virus from the infected area. However, most antivirus software is effective only against viruses already known when the software was written. To remain effective, the antivirus software must be continually updated. Antivirus products are available for many different types of mobile and handheld devices in addition to servers, workstations, and desktop PCs.

4. Unified Threat Management Systems: To help businesses reduce costs and improve manageability, security vendors have combined into a single appliance various security tools, including firewalls, virtual private networks, intrusion detection systems, and Web content filtering and antispam software. These comprehensive security management products are called **unified threat management (UTM)** systems.

Tools and Technologies for Safeguarding Information Resources… cont.

Encryption and Public Key Infrastructure

Many businesses use encryption to protect digital information that they store, physically transfer, or send over the Internet. **Encryption** is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the intended receiver. Data are encrypted by using a secret numerical code, called an encryption key, that transforms plain data into cipher text. The message must be decrypted by the receiver.

Two methods for encrypting network traffic on the Web are SSL and S-HTTP. **Secure Sockets Layer (SSL)** and its successor Transport Layer Security (TLS) enable client and server computers to manage encryption and decryption activities as they communicate with each other during a secure Web session. **Secure Hypertext Transfer Protocol (S-HTTP)** is another protocol used for encrypting data flowing over the Internet, but it is limited to individual messages, whereas SSL and TLS are designed to establish a secure connection between two computers.

There are two alternative methods of encryption: symmetric key encryption and public key encryption.

Review Questions

1. What is the business value of security and control?
2. How does management know that information systems security and controls are effective?
3. What are the most important tools and technologies for safeguarding information resources?
4. What are the components of an organizational framework for security and control?
5. Why are information systems vulnerable to destruction, error, and abuse?

References

- Laudon, K. C. and Laudon, J. P. (2011) Management Information System: *Managing the Digital Firm*, 12th Edition, Prentice Hall

- Adejola, P. A. (2012): Electronic Accounting & Reporting: Information Technology (IT) Empowerment Tool for Professional Accountants; Rainbow Prints, Abuja- Nigeria.

- Ojuola, O. K. (2014): Corporate Information System (CIS): A Concise Compilation for White Knight Professional Tutors, Abuja
- www.enterpriseresourceplanning.com
- www.studymode.com