SECURITY OF INFORMATION SYSTEMS

A. MUASYA

CONTROL AND SECURITY OF INFORMATION SYSTEMS

OBJECTIVES OF INFORMATION SECURITY

- **Confidentiality** -“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Disclosure of trade secrets is a breach on confidentiality.
- **Integrity**-“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Fabrication and alteration of files is a breach on integrity
- **Availability**-“Ensuring timely and reliable access to and use of information. Theft of a component e.g. hard disk or link failure is a breach to availability

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Difficulties in protecting information resources

- Hundreds of potential threats exist.
- Computing resources may be situated in many locations.
- Many individuals control information assets.
- Computer networks can be outside the organization and difficult to protect.
- Rapid technological changes make some controls obsolete as soon as they are installed.
- Many computer crimes are undetected for a long period of time, so it is difficult to learn from experience.
- People tend to violate security procedures because the procedures are inconvenient.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

- Many computer criminals who get caught go unpunished, so there is no deterrent effect.
- The amount of computer knowledge necessary to commit computer crimes is usually minimal. Computer users can learn hacking, for free, on the Internet.
- The cost of preventing hazards can be very high. Therefore, most organizations simply cannot afford to protect against all possible hazards.
- It is difficult to conduct a cost-benefit justification for controls before an attack occurs since it is difficult to assess the value of a hypothetical attack.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

THREATS

- This is any potential danger to information or systems. A threat is a possibility that someone (person, s/w) would identify and exploit the vulnerability.

Unintentional Threats

- *Human errors* can occur in the design of the hardware and/or information system.
- Also can occur in programming, testing, data collection, data entry, authorization and procedures.
- Contribute to more than 50% of control and security-related problems in organizations.
- *Environmental hazards* include earthquakes, severe storms, floods, power failures or strong fluctuations, fires (most common hazard), explosions, ...etc.
- *Computer system failures* can occur as the result of poor manufacturing or defective materials.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Intentional Threats

- Typically criminal in nature
- **Cybercrimes** are fraudulent activities committed using computers and communications networks, particularly the Internet.
- Average cybercrime involves about $600,000 according to FBI.
- **Cyberstalking**- defined as the use of the Internet, e-mail, and other electronic communication media to harass or threaten a person repeatedly.
- **Information warfare** as the use of information technologies to corrupt or destroy an enemy's information and industrial infrastructure
- Disgruntled Employees- probably 80% of all data loss comes from company insiders like disgruntled employees.
- **Salami attack-** a process where small amounts of money are taken from many accounts and diverted elsewhere.
- **Data diddling** - an illegal or unauthorized data alteration

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Intentional Threats cont'd

- **Hacker-** This is an outsider who has penetrated a computer system, usually with no criminal intent. Computer hobbyists for whom breaking into a system is an intellectual game, they rarely steal or damage assets. They subscribe to an unwritten code of conduct called the hacker ethic that forbids the destruction of data.
- **Cracker-** This is a malicious hacker. Their attacks are sophisticated and cause major headaches for system administrators.
- **Social engineering-** Computer criminals or corporate spies get around security systems by building an inappropriate trust relationship with insiders.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Espionage or Trespass

- The act of gaining access to the information an organization is trying to protect by an unauthorized individual.
- *Industrial espionage* occurs in areas where researching information about the competition goes beyond the legal limits.
- *Shoulder surfing* is looking at a computer monitor or ATM screen over another person’s shoulder

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Software Attacks

- Malicious software (malware) designed to damage, destroy, or deny service to the targeted systems.
- Most common types of software attacks are viruses, worms, Trojan horses, logic bombs, back doors, denial-of-service, alien software, phishing and pharming.
- Viruses. Segments of computer code that performs unintended actions ranging from merely annoying to destructive.
- Worms. Destructive programs that replicate themselves without requiring another program to provide a safe environment for replication.
- Trojan horses. Software progams that hide in other computer programs and reveal their designed behavior only when they are activated.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Software Attacks cont'd

- **Logic bombs.** Designed to activate and perform a destructive action at a certain time.
- **Back doors or trap doors.** Typically a password, known only to the attacker, that allows access to the system without having to go through any security.
- **Denial-of-service.** An attacker sends so many information requests to a target system that the target cannot handle them successfully and can crash the entire system.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Alien Software

- **Adware-** Designed to help popup advertisements appear on your screen.
- **Spyware-** Software that gathers user information through the user's Internet connection without their knowledge (i.e. keylogger, password capture).
- **Spamware-** Designed to use your computer as a launch pad for spammers**.**
- **Spam-** Unsolicited e-mail, usually for purposes of advertising.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Alien Software cont'd

- **Cookies-** Small amount of information that Web sites store on your computer, temporarily or more-or-less permanently.
- **Phishing-** Uses deception to fraudulently acquire sensitive personal information such as account numbers and passwords disguised as an official-looking e-mail.
- **Pharming-** Fraudulently acquires the Domain Name for a company's Web site and when people type in the Web site url they are redirected to a fake Web site.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Security Controls

- **Information system controls** are the procedures, devices, or software aimed at preventing a compromise to the system
- **General controls.** Established to protect the system regardless of their application.
- **Physical controls.** Physical protection of computer facilities and resources.
- **Access controls.** Restriction of unauthorized user access to computer resources; use **biometrics** and **passwords** controls for user identification.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

- **Communications (networks) controls.** To protect the movement of data across networks and include border security controls, authentication and authorization.
- **Firewalls.** System that enforces access-control policy between two networks. **It is** a hardware and/or software that permit an organization’s internal computer users to access the external Internet, while placing severe limits on the ability of outsiders to access internal data.
- **Encryption.** Process of converting an original message into a form that cannot be read by anyone except the intended receiver.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

- **Virtual Private Networking.** Uses the Internet to carry information within a company and among business partners but with increased security by uses of encryption, authentication and access control.
- **Application controls.** Controls that protect specific applications and include: input, processing and output controls.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

AUDITING INFORMATION SYSTEMS

- Controls are established to ensure that information systems work properly. Controls can be installed in the original system, or they can be added once a system is in operation. Installing controls is necessary but not sufficient.
- It is also necessary to answer questions such as the following: Are controls installed as intended? Are they effective? Did any breach of security occur? If so, what actions are required to prevent reoccurrence?
- These questions need to be answered by independent and unbiased observers. Such observers perform the information system *auditing* task.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

- An **audit** is an important part of any control system. In an organizational setting, it is usually referred to as a periodical *examination and check* of financial and accounting records and procedures. Specially trained professionals execute an audit.
- In the information system environment, auditing can be viewed as an additional layer of controls or safeguards. Auditing is considered as a deterrent to criminal actions especially for insiders.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

- **The *information systems (IS) audit*** is the process of collecting and evaluating evidence to determine whether;
  - A computer safeguards assets;
  - Maintains data integrity;
  - Allows organizational goals to be achieved effectively;
  - Uses resources efficiently.
- The IS auditor is expected to follow the defined audit process, establish audit criteria, gather meaningful evidence, and render an independent opinion about internal controls.
- The audit involves applying various techniques for collecting meaningful evidence, and then performing a comparison of the audit evidence against the standard for reference.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Steps involved in IS audit

- Plan: understanding the system: operations, facilities, control systems, security objectives, organization structure, stake holders, human procedures, system applications.
- Collection of evidence: auditor collects documentation, input, output, interviews people.
- Evaluation: auditor ranks weaknesses, and probability of event occurrences.
- Audit report: auditor lists the financial and organizational impacts of each threat. Management should devise a plan to address weaknesses.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

- Communication of audit results is very important to the auditor and the management of the firm being audited. Why is it important and how should the results be communicated?
- It gives an opportunity for the auditor to meet the management and discuss issues in the findings before presenting the final results.
- After agreement with management, then the auditor can present the conclusions and recommendations in form of a report
- Executive summary: The Audit report should communicate the results in form of a clearly written report, which will avoid technical jargon and well understood. It should also be presented using power point slides with graphics to illustrate in a better way

CONTROL AND SECURITY OF INFORMATION SYSTEMS

TYPES OF AUDITORS AND AUDITS

- There are two types of auditors (and audits): internal and external.
- An *internal auditor* is usually a corporate employee who is not a member of the ISD.
- An *external auditor* is a corporate outsider. This type of auditor reviews the findings of the internal audit and the inputs, processing, and outputs of information systems. The external audit of information systems is frequently a part of the overall external auditing performed by a certified public accounting (CPA) firm.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

- IT auditing can be very broad, so only its essentials are presented here. Auditing looks at all potential hazards and controls in information systems.
- It focuses attention on topics such as new systems development, operations and maintenance, data integrity, software application, security and privacy, disaster planning and recovery, purchasing, budgets and expenditures, charge-backs, vendor management, documentation, insurance and bonding, training, cost control, and productivity.

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Auditors attempt to answer questions such as these:

- Are there sufficient controls in the system? Which areas are not covered by controls?
- Which controls are not necessary?
- Are the controls implemented properly?
- Are the controls effective; that is, do they check the output of the system?
- Is there a clear separation of duties of employees?
- Are there procedures to ensure compliance with the controls?
- Are there procedures to ensure reporting and corrective actions in case of violations of controls?

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Other items that IT auditors may check include:

- Data security policies plans
- The business continuity plan
- The availability of a strategic information plan
- What the company is doing to ensure compliance with security rules
- The responsibilities of IT security
- The measurement of success of the organization IT security scheme
- The existence of security awareness program
- The security incidents reporting system

CONTROL AND SECURITY OF INFORMATION SYSTEMS

Two types of audits are used to answer these questions.

- The *operational audit* determines whether the ISD is working properly.
- The *compliance audit* determines whether controls have been implemented properly and are adequate.