UNIT-1

Need For Security

The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimizing the impact of security incidents. The Audit Commission Update report (1998) shows that fraud or cases of IT abuse often occur due to the absence of basic controls, with one half of all detected frauds found by accident. An Information Security Management System (ISMS) enables information to be shared, whilst ensuring the protection of information and computing assets.

At the most practical level, securing the information on your computer means:

- ✓ Ensuring that your information remains confidential and only those who *should* access that information, *can*.

.

- ✓ Knowing that no one has been able to change your information, so you can depend on its accuracy (information integrity).

.

- ✓ Making sure that your information is available when you need it (by making back-up copies and, if appropriate, storing the back-up copies off-site).

.

BUSINESS NEEDS FIRST

Information security performs four important functions for an organization:

a. Protects the organization’s ability to function

b. Enables the safe operation of applications implemented on the organization’s IT systems.

c. Protects the data the organization collects and uses.

d. Safeguards the technology assets in use at the organization.

Protecting the functionality of an organization

✓ Decision makers in organizations must set policy and operate their organizations in compliance with the complex, shifting legislation that controls the use of technology.

.

Enabling the safe operation of applications

Organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications

✓ The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly those applications that serve as important elements of the infrastructure of the organization.

.

Protecting data that organizations collect & use

✓ Protecting data in motion

.

✓ Protecting data at rest

.

✓ Both are critical aspects of information security.

✓·The value of data motivates attackers to seal, sabotage, or corrupt it.

It is essential for the protection of integrity and value of the organization’s data

.

Safeguarding Technology assets in organizations

Must add secure infrastructure services based on the size and scope of the enterprise.

Organizational growth could lead to the need for **public key infrastructure,** PKI, an integrated system of software, encryption methodologies.

THREATS

To protect an organization’s information, you must

Know yourself

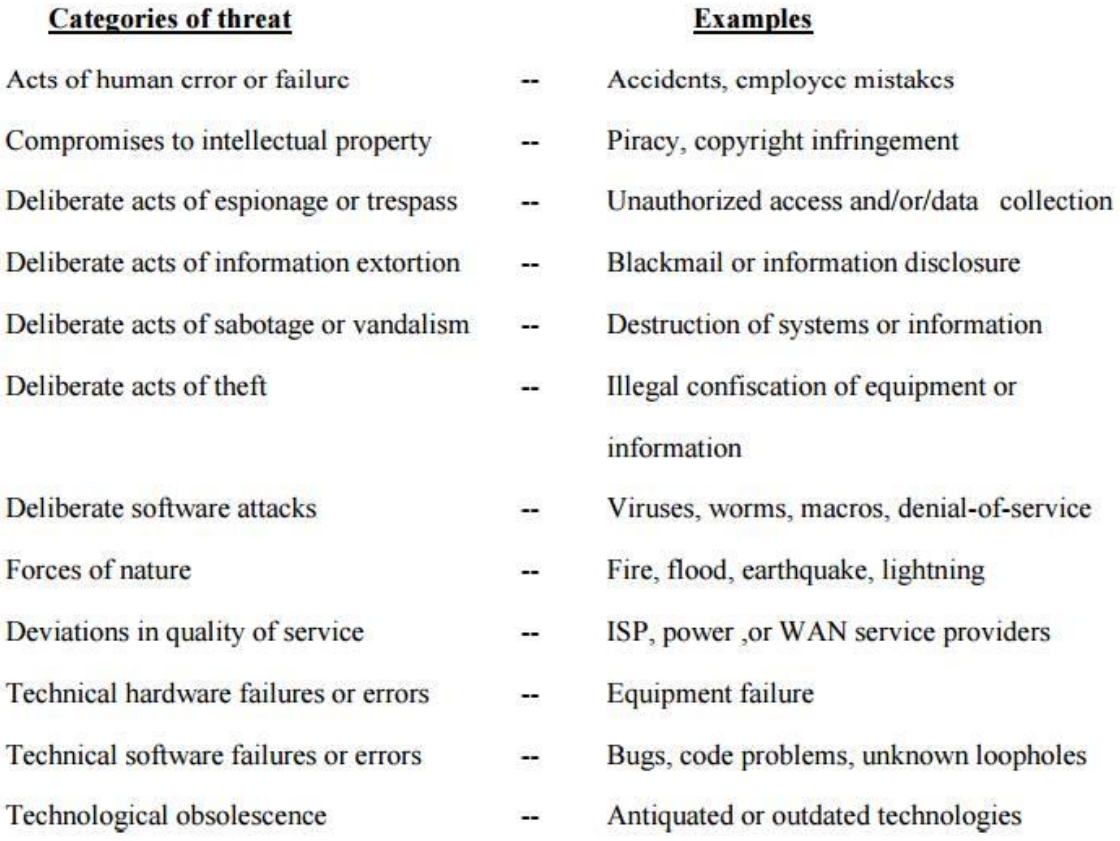
(i.e.) be familiar with the information to be protected, and the systems that store, transport and process it.

2. Know the threats you face

To make sound decisions about information security, management must be informed about the various threats facing the organization, its application, data and information systems.

A threat is an object, person, or other entity, that represents a constant danger to an asset.

1 Threats to Information Security



Categories of threat		Examples
Acts of human crror or failurc	--	Accidcnts, cmployce mistakcs
Compromises to intellectual property	--	Piracy, copyright infringement
Deliberate acts of espionage or trespass	--	Unauthorized access and/or/data collection
Deliberate acts of information extortion	--	Blackmail or information disclosure
Deliberate acts of sabotage or vandalism	--	Destruction of systems or information
Deliberate acts of theft	--	Illegal confiscation of equipment or information
Deliberate software attacks	--	Viruses, worms, macros, denial-of-service
Forces of nature	--	Fire, flood, earthquake, lightning
Deviations in quality of service	--	ISP, power ,or WAN service providers
Technical hardware failures or errors	--	Equipment failure
Technical software failures or errors	--	Bugs, code problems, unknown loopholes
Technological obsolescence	--	Antiquated or outdated technologies

2 Threats

ü **Acts of Human Error or Failure:**

Acts performed without intent or malicious purpose by an authorized user.

.

because of in experience, improper training,

.

Making of incorrect assumptions.

One of the greatest threats to an organization’s information security is the organization’s own employees.

✓ Entry of erroneous data

▪

✓ accidental deletion or modification of data

▪

✓ storage of data in unprotected areas.

✓▪Failure to protect information can be prevented with

Training

Ongoing awareness activities -Verification by a second party

Many military applications have robust, dual- approval controls built in .

Compromises to Intellectual Property

✓ **Intellectual Property** is defined as the ownership of ideas and control over the tangible or virtual representation of those ideas.

✓ Intellectual property includes trade secrets, copyrights, trademarks, and patents.

✓ Once intellectual property has been defined and properly identified, breaches to IP constitute a threat to the security of this information.

✓ Organization purchases or leases the IP of other organizations.

✓ Most Common IP breach is the unlawful use or duplication of software based intellectual property more commonly known as **software Piracy**.

✓ Software Piracy affects the world economy.

✓ U.S provides approximately 80% of world’s software.

In addition to the laws surrounding software piracy, two watch dog organizations

investigate allegations of software abuse.

Software and Information Industry Association (SIIA) (i.e)Software Publishers Association

Business Software Alliance (BSA)

Another effort to combat (take action against) piracy is the online registration process.

□

Deliberate Acts of Espionage or Trespass

✓ Electronic and human activities that can breach the confidentiality of information.

✓ When an unauthorized individual’s gain access to the information an organization is trying to protect is categorized as act of espionage or trespass.

.

✓ Attackers can use many different methods to access the information stored in an information system.

.

Competitive Intelligence[use web browser to get information from market research]

Industrial espionage(spying)

3. Shoulder Surfing(ATM)

Trespass

Can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.

·

Sound principles of authentication & authorization can help organizations protect valuable information and systems.

·

Hackers-> "People who use and create computer software to gain access to information illegally"

·

There are generally two skill levels among hackers.

Expert Hackers-> Masters of several programming languages, networking protocols, and operating systems .

·

Unskilled Hackers

·

ü **Deliberate Acts of information Extortion (obtain by force or threat)**

Possibility of an attacker or trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement not to disclose the information.

·

ü **Deliberate Acts of sabotage or Vandalism**

Destroy an asset or

·

Damage the image of organization

·

Cyber terrorism-Cyber terrorists hack systems to conduct terrorist activities through network or internet pathways.

▪

ü **Deliberate Acts of Theft**

Illegal taking of another’s property-- is a constant problem.

▪

Within an organization, property can be physical, electronic, or intellectual.

▪

Physical theft can be controlled by installation of alarm systems.

▪

Trained security professionals.

▪

Electronic theft control is under research.

▪

ü **Deliberate Software Attacks**

Because of **malicious code** or **malicious software** or sometimes **malware.**

These software components are designed to damage, destroy or deny service to the target system.

▪

More common instances are

▪

Virus, Worms, Trojan horses, Logic bombs, Backdoors.

▪

“The British Internet Service Provider Cloudnine” be the first business “hacked out of existence”

▪

ü **Virus**

Segments of code that performs malicious actions.

▪

Virus transmission is at the opening of Email attachment files.

▪

Macro virus-> Embedded in automatically executing macrocode common in word processors, spreadsheets and database applications.

▪

Boot Virus-> infects the key operating files located in the computer's boot sector.

▪

ü **Worms**

A worm is a malicious program that replicates itself constantly, without requiring another program to provide a safe environment for replication.

▪

Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.

Eg: MS-Blaster, MyDoom, Netsky, are multifaceted attack worms.

▪

Once the worm has infected a computer , it can redistribute itself to all e-mail addresses found on the infected system.

▪

Furthermore, a worm can deposit copies of itself onto all Web servers that the infected systems can reach, so that users who subsequently visit those sites become infected.

▪

ü **Trojan Horses**

Are software programs that hide their true nature and reveal their designed behavior only when activated.

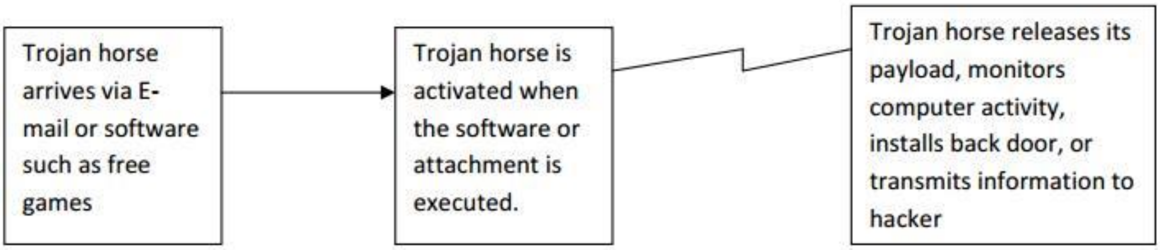

Trojan horse arrives via E-mail or software such as free games
Trojan horse is activated when the software or attachment is executed.
Trojan horse releases its payload, monitors computer activity, installs back door, or transmits information to hacker

Figure 7.3.1 Trojan horse Attack

Back Door or Trap Door

- ✓A Virus or Worm has a payload that installs a backdoor or trapdoor component in a system, which allows the attacker to access the system at will with special privileges.

Eg: Back Orifice

Polymorphism

- ✓A **Polymorphic threat** is one that changes its apparent shape over time, making it undetectable by techniques that look for preconfigured signatures.

.

- ✓These viruses and Worms actually evolve, changing their size, and appearance to elude detection by antivirus software programs.

Virus & Worm Hoaxes

Types of Trojans

🕐 Data Sending Trojans

▪

🕐 Proxy Trojans

▪

🕐 FTP Trojans

▪

🕐 Security software disabler Trojans

▪

🕐 Denial of service attack Trojans(DOS)

Virus

A program or piece of code that be loaded on to your computer, without your knowledge and run against your wishes.

Worm

🗁 A program or algorithm that replicates itself over a computer network and usually performs malicious actions.

Trojan Horse

✓A destructive program that masquerade on beginning application, unlike viruses, Trojan horse do not replicate themselves.

Blended threat

✓Blended threats combine the characteristics of virus, worm, Trojan horses & malicious code with server and Internet Vulnerabilities.

Antivirus Program

A Utility that searches a hard disk for viruses and removes any that found.

▪

ü **Forces of Nature**

Fire: Structural fire that damages the building. Also encompasses smoke damage from a fire or water damage from sprinkles systems.

▪

Flood: Can sometimes be mitigated with flood insurance and/or business interruption Insurance.

▪

Earthquake: Can sometimes be mitigated with specific causality insurance and/or business interruption insurance, but is usually a separate policy.

▪

Lightning: An Abrupt, discontinuous natural electric discharge in the atmosphere.

▪

Landslide/Mudslide: The downward sliding of a mass of earth & rocks directly damaging all parts of the information systems.

▪

Tornado/Severe Windstorm

Huricane/typhoon

Tsunami

Electrostatic Discharge (ESD)

Dust Contamination

Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage.

They must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans, to limit losses in the face of these threats.

ü **Deviations in Quality of Service**

A product or service is not delivered to the organization as expected.

The Organization’s information system depends on the successful operation of many interdependent support systems.

·

It includes power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff & garbage haulers.

This degradation of service is a form of **availability disruption.**

Internet Service Issues

✓ Internet service Provider(ISP) failures can considerably undermine the availability of information.

·

✓ The web hosting services are usually arranged with an agreement providing minimum service levels known as a **Service level Agreement (SLA).**

·

✓ When a Service Provider fails to meet SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.

Communications & Other Service Provider Issues

✓ Other utility services can affect the organizations are telephone, water, waste water, trash pickup, cable television, natural or propane gas, and custodial services.

- ✓The loss of these services can impair the ability of an organization to function.

.

- ✓For an example, if the waste water system fails, an organization might be prevented from allowing employees into the building.
- ✓This would stop normal business operations.

Power Irregularities

- ✓Fluctuations due to power excesses.
- ✓Power shortages &
- ✓Power losses

This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment.

When voltage levels **spike** (experience a momentary increase),or **surge** (experience prolonged increase), the extra voltage can severely damage or destroy equipment.

.

The more expensive uninterruptible power supply (UPS) can protect against spikes and surges.

.

ü **Technical Hardware Failures or Errors**

Resulting in unreliable service or lack of availability

Some errors are terminal, in that they result in unrecoverable loss of equipment.

Some errors are intermittent, in that they resulting in faults that are not easily repeated.

ü **Technical software failures or errors**

This category involves threats that come from purchasing software with unknown, hidden faults.

Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.

These failures range from bugs to untested failure conditions.

ü **Technological obsolescence**

Outdated infrastructure can lead to unreliable and untrustworthy systems.

Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks.

ATTACKS

An attack is an act of or action that takes advantage of a vulnerability to compromise a controlled system.

.

It is accomplished by a **threat agent** that damages or steals an organization's information or physical asset.

Vulnerability is an identified weakness in a controlled system, where controls are not present or are no longer effective.

.

Attacks exist when a specific act or action comes into play and may cause a potential loss.

ü **Malicious code**

The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.

The state –of-the-art malicious code attack is the polymorphic or multivector, worm.

▪

These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

▪

ü **Attack Replication Vectors**

IP scan & attack

Web browsing

Virus

Unprotected shares

Mass mail

Simple Network Management Protocol(SNMP)

ü **IP scan & attack**

The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers.

▪

ü **Web browsing**

If the infected system has write access to any Web pages, it makes all Web content files (.html,.asp,.cgi & others) infectious, so that users who browse to those pages become infected.

·

ü **Virus**

Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.

·

ü **Unprotected shares**

Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.

·

ü **Mass Mail**

By sending E-mail infections to addresses found in the address book, the infected machine infects many users, whose mail -reading programs also automatically run the program & infect other systems.

·

ü **Simple Network Management Protocol (SNMP)**

By using the widely known and common passwords that were employed in early versions of this protocol, the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

Examples

Hoaxes

✓ A more devious approach to attacking the computer systems is the transmission of a virus hoax with a real virus attached.

·

✓ Even though these users are trying to avoid infection, they end up sending the attack on to their co-workers.

Backdoors

✓ Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door.

✓ Sometimes these entries are left behind by system designers or maintenance staff, and thus referred to as trap doors.

🗎🖎🗄🖎🗀 A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

Password Crack

✓ Attempting to reverse calculate a password is often called **cracking.**

▪

✓ A password can be hashed using the same algorithm and compared to the hashed results, If they are same, the password has been cracked.

▪

✓ The (SAM) Security Account Manager file contains the hashed representation of the user’s password.

Brute Force

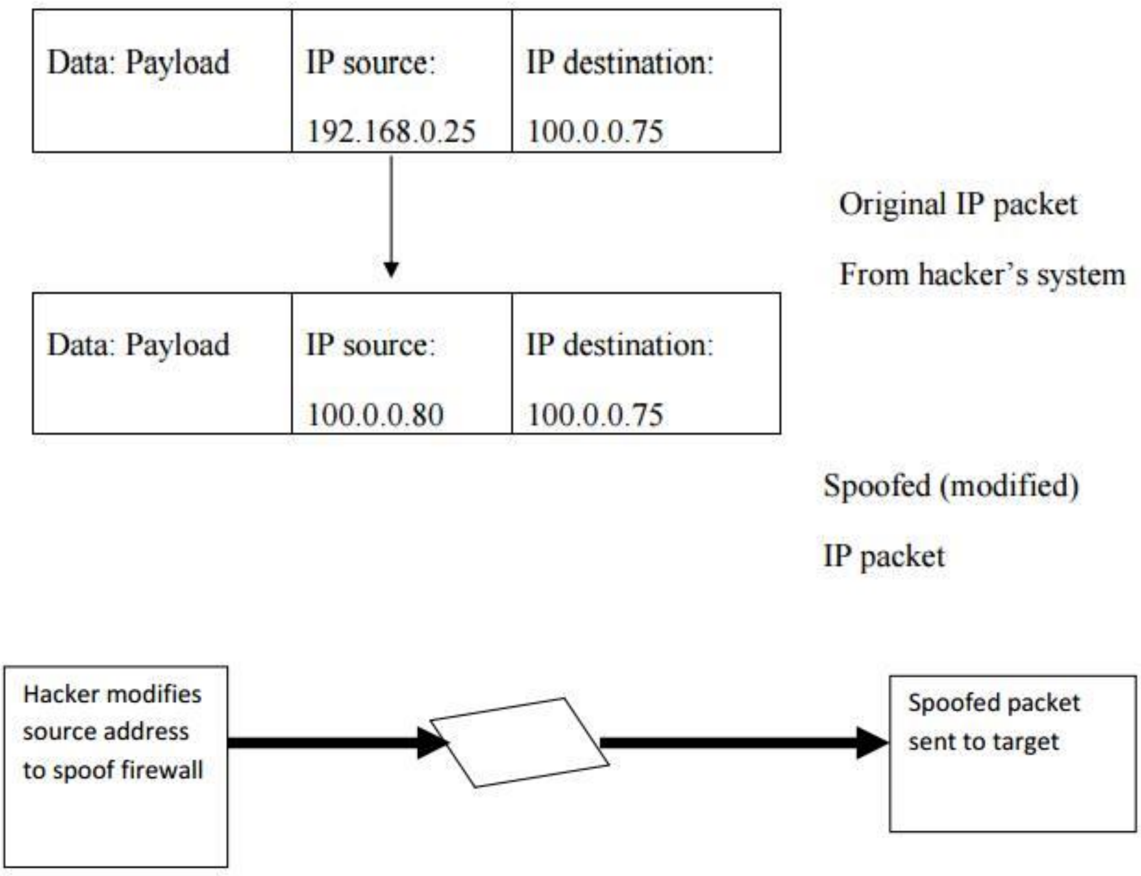
✓ The application of computing & network resources to try every possible combination of options of a password is called a **Brute force attack.**

▪

✓ This is often an attempt to repeatedly guess passwords to commonly used accounts, it is sometimes called a **password attack.**

Spoofing

It is a technique used to gain unauthorized access to computers, where in the intruder sends messages to a computer that has an IP address that indicates that the messages are coming from a trusted host.



Firewall allows packet in, mistaking it for legitimate traffic

Figure 2.4.3.1 IP spoofing

Dictionary

✓ This is another form of the brute force attack noted above for guessing passwords.

✓ The **dictionary attack** narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords instead of random combinations.

Denial –of- Services(DOS) & Distributed Denial –of- Service(DDOS)

✓ The attacker sends a large number of connection or information requests to a target.

.

✓ This may result in the system crashing, or simply becoming unable to perform ordinary functions.

.

✓ DDOS is an attack in which a coordinated stream of requests is launched dagainst a target from many locations at the same.

Man-in-the –Middle

✓ Otherwise called as **TCP hijacking attack**.

.

✓ An attacker monitors packets from the network, modifies them, and inserts them back into the network.

✓ This type of attack uses IP spoofing.

✓ It allows the attacker to change, delete, reroute, add, forge or divert data.

.

✓ TCP hijacking session, the spoofing involves the interception of an encryption key exchange.

SPAM

🕐 Spam is unsolicited commercial E-mail.

🕐 It has been used to make malicious code attacks more effective.

🕐 Spam is considered as a trivial nuisance rather than an attack.

- It is the waste of both computer and human resources it causes by the flow of unwanted E-mail.

Mail Bombing

- ✓ Another form of E-mail attack that is also a DOS called a **mail bomb**.
- ✓ Attacker routes large quantities of e-mail to the target.
- ✓ The target of the attack receives unmanageably large volumes of unsolicited e-mail.

▪

- ✓ By sending large e-mails, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.

▪

- ✓ The target e-mail address is buried under thousands or even millions of unwanted e-mails.

Sniffers

- ✓ A **sniffer** is a program or device that can monitor data traveling over a network.
- ✓ Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere.

▪

- ✓ Sniffer often works on TCP/IP networks, where they are sometimes called **"packet**

▪

Sniffers".

Social Engineering

- It is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.

▪

🗏📨🗄📨🗐 An attacker gets more information by calling others in the company and asserting his/her authority by mentioning chief's name.

Buffer Overflow

✓ A buffer overflow is an application error that occurs when more data is sent to a buffer than it can handle.

✓ Attacker can make the target system execute instructions.

Timing Attack

✓ Works by exploring the contents of a web browser's cache.

▪

✓ These attacks allow a Web designer to create a malicious form of cookie, that is stored on the client's system.

✓ The cookie could allow the designer to collect information on how to access password-protected sites.

Law and Ethics in Information Security

Laws

- Rules that mandate or prohibit certain behaviour
- Drawn from ethics ´ Ethics ´ Define socially acceptable behaviours

Ethics

- Moral values
- Define socially acceptable behaviours

Key difference

- Laws carry the authority of a governing body
- Ethics do not carry the authority of a governing body
- Based on cultural mores

- Fixed moral attitudes or customs
- Some ethics standards are universal

Organizational Liability and the Need for Counsel

Liability

- Legal obligation of organization
- Extends beyond criminal or contract law
- Include legal obligation to restitution
- Employee acting with or without the authorization performs and illegal or unethical act that causes some degree of harm
- Employer can be held financially liable

Due care

- Organization makes sure that every employee knows what is acceptable or unacceptable
- Knows the consequences of illegal or unethical actions

Due diligence

Requires

- Make a valid effort to protect others
- Maintains the effort

Jurisdiction

- Court's right to hear a case if a wrong is committed
- Term – long arm
- Extends across the country or around the world

Policy Versus law

Policies

- Guidelines that describe acceptable and unacceptable employee behaviours
- Functions as organizational laws
- Has penalties, judicial practices, and sanctions

Difference between policy and law

- Ignorance of policy is acceptable
- Ignorance of law is unacceptable

Types of Law

- Civil – govern a nation or state
- Criminal – addresses activities and conduct harmful to public
- Private – encompasses family, commercial, labour, and regulates the relationship between individuals and organizations ´ Public – regulates the structure and administration of government agencies and their relationships with citizens, employees, and other government.

An overview of computer security

1. Computer security, also known as cybersecurity, refers to the protection of computer systems and networks from unauthorized access, theft, damage, or any other form of cyber threats. Computer security involves a range of technologies, practices, and policies designed to safeguard digital information and assets.

2. Some of the key aspects of computer security include:

3. Access control: This involves controlling who can access computer systems and networks, and what level of access they have. Access control measures include passwords, biometric authentication, and access permissions.

4. Encryption: Encryption is the process of converting data into a code or cipher to prevent unauthorized access or theft. Encryption is used to protect sensitive data, such as financial information or personal data, during storage or transmission.

5. Firewalls: Firewalls are hardware or software devices that prevent unauthorized access to computer networks. They act as a barrier between the network and external sources, blocking unauthorized access or cyberattacks.

6. Antivirus and anti-malware software: These programs are designed to detect, prevent, and remove malicious software or malware, including viruses, Trojans, worms, and other types of malicious code.

7. Backup and recovery: Regular backup and recovery procedures are essential to protect data and ensure business continuity in the event of a cyberattack or system failure.

8. Employee training and awareness: Human error is one of the most significant causes of cyber breaches. Therefore, training and awareness programs are essential to educate employees about cybersecurity risks and best practices.

Access control Matrix

An access control matrix is a security model that is used to define and enforce access control policies for computer systems and networks. It is a table that specifies which users or groups of users are allowed to access specific resources or perform specific actions within a system.

The access control matrix is made up of rows and columns. The rows represent the subjects or users that can access the system, while the columns represent the objects or resources that the users can access. Each cell in the matrix contains a set of access permissions that defines the level of access that a particular user or group of users has to a specific resource.

There are two types of access control matrices:

1. Discretionary Access Control Matrix (DAC): In a DAC matrix, the owner of a resource decides who can access that resource and what level of access they have. The owner can grant or revoke access permissions for a resource at any time.

2. Mandatory Access Control Matrix (MAC): In a MAC matrix, access permissions are assigned by a central authority or security administrator. The access permissions are based on the security level or classification of the resource and the security clearance level of the user. Users cannot modify their access permissions in a MAC matrix.

The access control matrix is a useful tool for enforcing access control policies and ensuring the security of computer systems and networks. It is used in a variety of applications, including operating systems, databases, and network security systems.

Policy

Security policy

A security policy is a document that states in writing how a company plans to protect its physical and information technology (IT) assets. Security policies are living documents that are continuously updated and changing as technologies, vulnerabilities and security requirements change.

Why are security policies important?

Security policies are important because they protect an organizations' assets, both physical and digital. They identify all company assets and all threats to those assets.

Physical security policies are aimed at protecting a company's physical assets, such as buildings and equipment, including computers and other IT equipment. Data security policies protect intellectual property from costly events, like data breaches and data leaks.

Physical security policies

Physical security policies protect all physical assets in an organization, including buildings, vehicles, inventory and machines. These assets include IT equipment, such as servers, computers and hard drives.

Protecting IT physical assets is particularly important because the physical devices contain company data. If a physical IT asset is compromised, the information it contains and handles is at risk. In this way, information security policies are dependent on physical security policies to keep company data safe.

Physical security policies include the following information:

- sensitive buildings, rooms and other areas of an organization;
- who is authorized to access, handle and move physical assets;
- procedures and other rules for accessing, monitoring and handling these assets; and
- responsibilities of individuals for the physical assets they access and handle.

Security guards, entry gates, and door and window locks are all used to protect physical assets. Other, more high-tech methods are also used to keep physical assets safe. For example, a biometric verification system can limit access to a server room. Anyone accessing the room would use a fingerprint scanner to verify they are authorized to enter.

Information security policies

These policies provide the following advantages.

Protect valuable assets. These policies help ensure the confidentiality, integrity and availability -- known as the *CIA triad* -- of data. They are often used to protect sensitive customer data and personally identifiable information.

Guard reputations. Data breaches and other information security incidents can negatively affect an organization's reputation.

Ensure compliance with legal and regulatory requirements. Many legal requirements and regulations are aimed at security sensitive information. For example, Payment Card Industry Data Security Standard dictates how organizations handle consumer payment card information. Health Insurance Portability and Accountability Act details how companies handle protected health information. Violating these regulations can be costly.

Dictate the role of employees. Every employee generates information that may pose a security risk. Security policies provide guidance on the conduct required to protect data and intellectual property. **Identify third-party vulnerabilities.** Some vulnerabilities stem from interactions with other organizations that may have different security standards. Security policies help identify these potential security gaps.

Types of security policies

Security policy types can be divided into three types based on the scope and purpose of the policy:

1. **Organizational.** These policies are a master blueprint of the entire organization's security program.
2. **System-specific.** A system-specific policy covers security procedures for an information system or network.
3. **Issue-specific.** These policies target certain aspects of the larger organizational policy. Examples of issue-related security policies include the following:
    - Acceptable use policies define the rules and regulations for employee use of company assets.
    - Access control policies say which employees can access which resources.
    - Change management policies provide procedures for changing IT assets so that adverse effects are minimized.

  - Disaster recovery policies ensure business continuity after a service disruption. These policies typically are enacted after the damage from an incident has occurred.
  - Incident response policies define procedures for responding to a security breach or incident as it is happening.

Key elements in a security policy

Some of the key elements of an organizational information security policy include the following:

- statement of the purpose;
- statement that defines who the policy applies;
- statement of objectives, which usually encompasses the CIA triad;
- authority and access control policy that delineates who has access to which resources;
- data classification statement that divides data into categories of sensitivity -- the data covered can range from public information to information that could cause harm to the business or an individual if disclosed;
- data use statement that lays out how data at any level should be handled -- this includes specifying the data protection regulations, data backup requirements and network security standards for how data should be communicated, with encryption, for example;
- statement of the responsibilities and duties of employees and who will be responsible for overseeing and enforcing policy;
- security awareness training that instructs employees on security best practices -- this includes education on potential security threats, such as phishing, and computer security best practices for using company devices; and
- effectiveness measurements that will be used to assess how well security policies are working and how improvements will be made.

Integrity Policy

Integrity is the protection of system data from intentional or accidental unauthorized changes. The challenges of the security program are to ensure that data is maintained in the state that is expected by the users. Although the security program cannot improve the accuracy of the data that is put into the system by users. It can help ensure that any changes are intended and correctly applied. An additional element of integrity is the need to protect the process or program used to manipulate the data from unauthorized modification. A critical requirement of both commercial and government data processing is to ensure the integrity of data to prevent fraud and errors. It is imperative, therefore, no user be able to modify data in a way that might corrupt or lose assets or financial records or render decision making information unreliable. Examples of *government systems* in which integrity is crucial include air traffic control system, military fire control systems, social security and welfare systems. Examples of *commercial systems* that require a high level of integrity include medical prescription system, credit reporting systems, production control systems and payroll systems.

Protecting against Threats to Integrity: Like confidentiality, integrity can also be arbitrated by hackers, masqueraders, unprotected downloaded files, LANs, unauthorized user activities, and unauthorized programs like Trojan Horse and viruses, because each of these threads can lead to unauthorized changes to data or programs. For example, unauthorized user can corrupt or change data and programs intentionally or accidentally if their activities on the system are not properly controlled. Generally, three basic principles are used to establish integrity controls:

1. **Need-to-know access:** User should be granted access only into those files and programs that they need in order to perform their assigned jobs functions.
2. **Separation of duties:** To ensure that no single employee has control of a transaction from beginning to end, two or more people should be responsible for performing it.
3. **Rotation of duties:** Job assignment should be changed periodically so that it becomes more difficult for the users to collaborate to exercise complete control of a transaction and subvert it for fraudulent purposes.

Integrity Models – Integrity models are used to describe what needs to be done to enforce the information integrity policy. There are three goals of integrity, which the models address in various ways:

1. Preventing unauthorized users from making modifications to data or programs.
2. Preventing authorized users from making improper or unauthorized modifications.

3. Maintaining internal and external consistency of data and programs.

Hybrid Policy

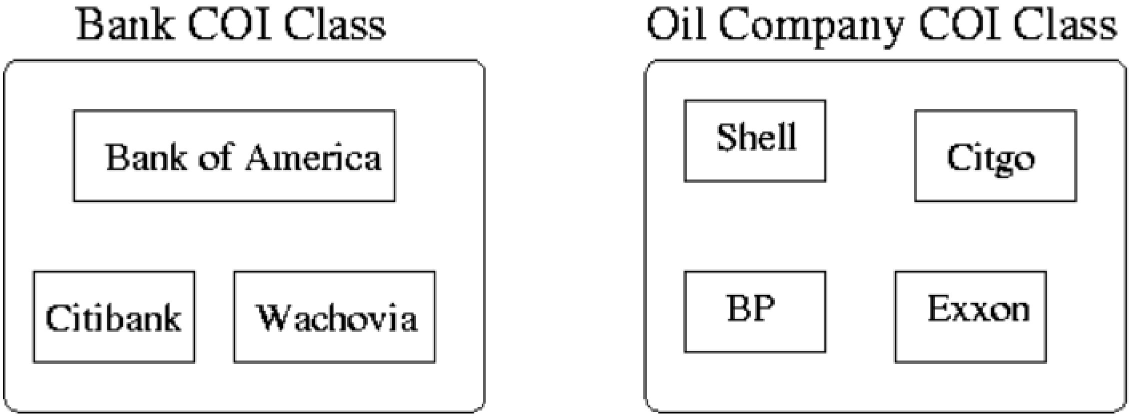
Chinese Wall Model

Security policy that refers equally to confidentiality and integrity Describes policies that involve conflict of interest in business

Def: The objects of the database are items of information related to a company

Def: A Company Dataset (CD) contains objects related to a single company

Def: A Conflict Of Interest (COI) class contains the datasets of companies in competition



CW-Simple Security Condition

S can read O iff either

1. There is an object O such that S has accessed O’ and CD(O’) = CD(O) or

2. For all objects O’, O’ PR(S) COI(O’) COI(O) where PR(S) is the set of previously read objects by S. Subject affects:

a. Once a subject reads any object in a COI class, the only other objects that the subject can read in that class are the same objects, i.e. once one object is read, no other objects in another class can be read.

b. The minimum number of subjects needed to access each object in a class is the number of objects in that class.

Since most companies have information that is available to all subjects, the model distinguishes between sanitized and unsantized data by adding condition 3,

3.O is a sanitized object.

The complete CW-Simple Security Condition is

CW-Simple Security Condition

S can read O iff either

1. There is an object O such that S has accessed O’ and CD(O’) = CD(O)

2. For all objects O’, O’ PR(S) COI(O’) COI(O) where PR(S) is the set of previously read objects by S.

3. O is a sanitized object.

Since two subjects could have access to the same object in one COI and different objects in another COI, we have

CW-*-Property

A subject S may write to an object O if both of the following conditions hold

1. The CW-Simple security conditions permits S to read O

2. Unsantized objects O’, S can read O’ CD(O’) = CD(O)

This prevents one subject from writing sensitive information in the shared common object from an unshared object.