# Information Security Fundamentals

**Module Number: 02**

## Module Name: The Need for IT Security

**Version Code: IS1_Updated**
**Released Date:2-Jan-2019**

# The Need for IT Security

## AIM

To familiarize students about the needs for information security and various security attack.

## Objectives

The objectives of this module are to understand:

- The need of security in business.
- Various methods of doing safe operation, protecting data etc.
- Threats related to intellectual property rights.
- Various methods of security attacks.

## Outcome

At the end of this module, you are expected to explain/describe:

- The need of information security for business.
- Technologies and methods for safeguarding the data and the assets.
- The security attacks on network and organization.

# The Need for IT Security

## Content

1. Business Needs
    a. Protecting the functionality
    b. Enabling the safe operations
    c. Protecting the data
    d. Safe guarding the technology assets
2. Threats
    a. Compromises to intellectual property
    b. Deliberate software attacks
    c. Espionage and trespass
    d. Sabotage and vandalism
3. Attacks
    a. Malicious codes
    b. Back doors
    c. Denial of service and distributed denial of service

## IT Security Business Needs

Information security performs four important functions for an organization:

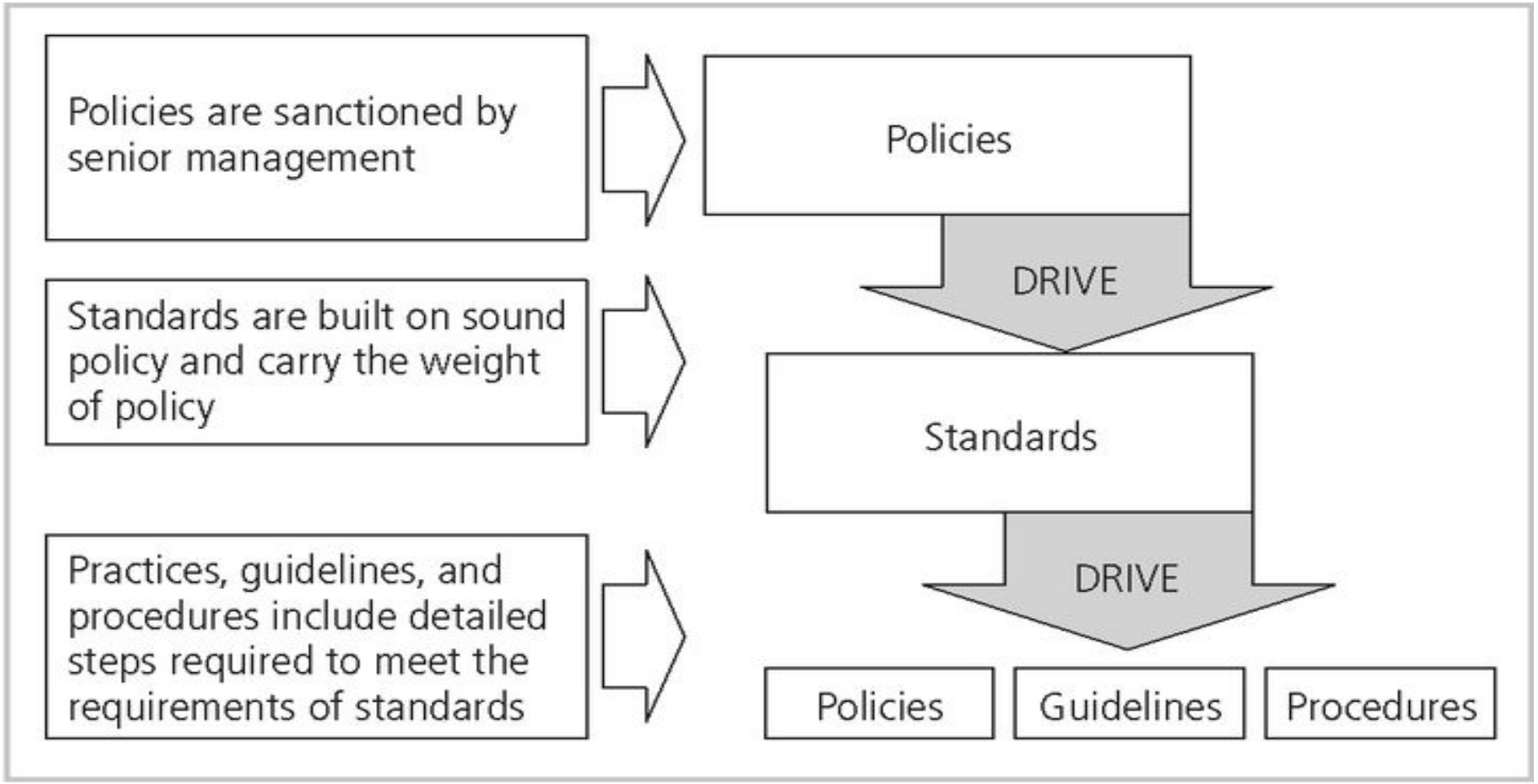
- Protects the organization's ability to function.
- Enables the safe operation of applications implemented on the organization's IT systems.
- Protects the data the organization collects and uses.
- Safeguards the technology assets in use.

- The creation of an information security program begins with an information security blueprint, and before we can discuss the creation and development of a blueprint, it is important to look at management's responsibility in shaping policy.
- It is prudent for information security professionals to know the information security polices and how these policies contribute to the overall objectives of the organization.

## Information Security Policy, Standards and Practices

- Management from all communities of interest must consider policies as the basis for all information security efforts.
- Policies direct how issues should be addressed and technologies used.
- Security policies are the least expensive control to execute, but the most difficult to implement.
- Shaping policy is difficult because:
  - Never conflict with laws.
  - Stand up in court, if challenged.
  - Be properly administered.

## Policies Standards and Practices



## Types of Policy

Management defines three types of security policy:

- General or security program policy
- Issue-specific security policies
- Systems-specific security policies

## Security Program Policy

- A Security Program Policy (SPP) is also known as a general security policy, IT security policy, or information security policy.
- Sets the strategic direction, scope, and tone for all security efforts within the organization.
- An executive-level document, usually drafted by or with, the CIO of the organization and is usually 2 to 10 pages long.

## Issue-Specific Security Policy (ISSP)

As various technologies and processes are implemented, certain guidelines are needed to use them properly.

**The ISSP:**

- Addresses specific areas of technology.
- Requires frequent updates.
- Contains an issue statement on the organization's position on an issue.

**Three approaches:**

- Create a number of independent ISSP documents.
- Create a single comprehensive ISSP document.
- Create a modular ISSP document.

## Systems-Specific Policy

- While issue-specific policies are formalised as written documents, distributed to users, and agreed to in writing, SysSPs are frequently codified as standards and procedures used when configuring or maintaining systems

Systems-specific policies fall into two groups:

- Access Control Lists (ACLs) consists of the access control lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system.
- Configuration Rules comprise the specific configuration codes entered into security systems to guide the execution of the system.

## Information Classification

- The classification of information is an important aspect of policy.
- The same protection scheme created to prevent production data from accidental release to the wrong party should be applied to policies in order to keep them freely available, but only within the organization.
- In today's open office environments, it may be beneficial to implement a clean desk policy.
- A clean desk policy stipulates that at the end of the business day, all classified information must be properly stored and secured.

## Information Security Blueprints

- One approach is to adapt or adopt a published model or framework for information security.
- A framework is the basic skeletal structure within which additional detailed planning of the blueprint can be placed as it is developed of refined.
- Experience teaches us that what works well for one organization may not precisely fit another.

## Security Education

- Everyone in an organization needs to be trained and aware of information security, but not every member of the organization needs a formal degree or certificate in information security.
- When formal education for appropriate individuals in security is needed, an employee can identify curriculum available from local institutions of higher learning or continuing education.
- A number of universities have formal coursework in information security.

  (See for example http://infosec.kennesaw.edu).

## Security Training

- Security training involves providing members of the organization with detailed information and hands-on instruction designed to prepare them to perform their duties securely.
- Management of information security can develop customised in-house training or outsource the training program.

## Security Awareness

- One of the least frequently implemented, but the most beneficial programs is the security awareness program.
- Designed to keep information security at the forefront of the users' minds.
- Need not be complicated or expensive.
- If the program is not actively implemented, employees begin to 'tune out', and the risk of employee accidents and failures increases.

## Self Assessment Question

1. Information security performs four important functions for an organization. Which one of the following function is not among the stated 4 function.

   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. Increasing the sales.

**Answer: Increasing the sales.**

## Self Assessment Question

2. Before we can discuss the creation and development of a blueprint, it is important to look at management's responsibility in shaping policy. State whether True or False.

a. True

b. False

**Answer: True**

## Self Assessment Question

3. Which one of the given options is one of the reasons for Shaping policy to be difficult?

i. Never conflict with laws
ii. Stand up in court, if challenged
iii. Be properly administered

a. Only i
b. Only ii
c. Only i and ii
d. All i, ii and iii

**Answer: All i, ii and iii**

## Self Assessment Question

4. Management defines three types of security policy. Which one of the given options is not a policy?

   a. General or security program policy

   b. Insurance policy

   c. Issue-specific security policies

   d. Systems-specific security policies

**Answer: Insurance policy**

## Self Assessment Question

5. Which one of the given options sets the strategic direction, scope, and tone for all security efforts within the organization?

a. General or security program policy

b. Issue-specific security policies

c. Systems-specific security policies

**Answer: General or security program policy**

## Self Assessment Question

6. Which of the following is not done by Issue-Specific Security Policy (ISSP)?

a. Addresses specific areas of technology.

b. Requires frequent updates.

c. Contains an issue statement on the organization's position on an issue.

d. Configuration rules comprise the specific configuration codes entered into security systems to guide the execution of the system.

**Answer: Configuration rules comprise the specific configuration codes entered into security systems to guide the execution of the system.**

## Protecting the Ability to Function

- Management is responsible
- Information security is
  - A management issue
  - A people issue
- Communities of interest must argue for information security in terms of impact and cost.

## Enabling Safe Operation

- Organisations must create integrated, efficient, and capable applications.
- Organisation need environments that safeguard applications.
- Management must not abdicate to the IT department its responsibility to make choices and enforce decisions.

## Protecting Data

- One of the most valuable assets is data.
- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers.
- An effective information security program is essential for the protection of integrity and value of the organization’s data.

## Safeguarding Technology Assets

- Organizations must have secure infrastructure services based on the size and scope of the enterprise.
- Additional security services may have to be provided.
- More robust solutions may be needed to replace security programs, the organization has outgrown.

# The Need for IT Security

## Threats

- Management must be informed of the various kinds of threats faced by the organization.
- A threat is an object, person, or other entity that represents a constant danger to an asset.
- By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls.

# The Need for IT Security

## Threats

The 2018 CSI/FBI survey founds the following:

- 90% of organizations responding detected computer security breaches within the last year.
- Computer breaches, totaling over $77,134,865 reported in 2018.
- The number of complaints received more that 300,000 and reported a loss of $1.4 billion.

https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718

## Threats to Information Security

| Categories of threat | Examples |
|---|---|
| 1. Acts of human error or failure | Accidents, employee mistakes |
| 2. Compromises to intellectual property | Piracy, copyright infringement |
| 3. Deliberate acts of espionage or trespass | Unauthorized access and/or data collection |
| 4. Deliberate acts of information extortion | Blackmail of information disclosure |
| 5. Deliberate acts of sabotage or vandalism | Destruction of systems or information |
| 6. Deliberate acts of theft | Illegal confiscation of equipment or information |
| 7. Deliberate software attacks | Viruses, worms, macros, denial-of-service |
| 8. Forces of nature | Fire, flood, earthquake, lightning |
| 9. Deviations in quality of service from service providers | Power and WAN service issues |
| 10. Technical hardware failures or errors | Equipment failure |
| 11. Technical software failures or errors | Bugs, code problems, unknown loopholes |
| 12. Technological obsolescence | Antiquated or outdated technologies |

## Acts of Human Error or Failure

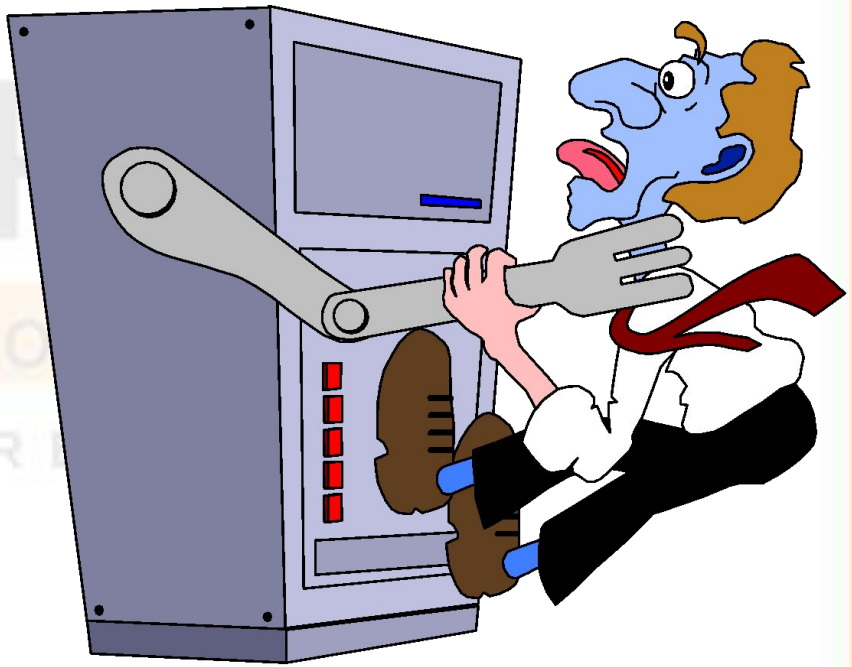
- Includes acts done without malicious intent
- Caused by:
  - Inexperience
  - Improper training
  - Incorrect assumptions
  - Other circumstances
- Employees are greatest threat to information security – They are closest to the organizational data.

## Acts of Human Error or Failure

Employee mistakes can easily lead to the following:

- Revelation of classified data.
- Entry of erroneous data.
- Accidental deletion or modification of data.
- Storage of data in unprotected areas.
- Failure to protect information.

- Many of these threats can be prevented with controls



## Acts of Human Error or Failure

## Deviations in Quality of Service by Service Providers

- Situations of product or services not delivered as expected.
- Information system depends on many inter-dependent support systems.

Three sets of service issues that dramatically affects the availability of information and systems are

- Internet service
- Communications
- Power irregularities

## Internet Service Issues

- Loss of Internet service can lead to considerable loss in the availability of information.
  - Organisations have sales staff and telecommuters working at remote locations.
- When an organization outsources its web servers, the outsourcer assumes responsibility for:
  - All Internet Services.
  - The hardware and operating system software used to operate the website.

## Communications and Other Services

Other utility services have potential impact. Among these are:

- Telephone
- Water and wastewater
- Trash pickup
- Cable television
- Natural or propane gas
- Custodial services

The threat of loss of services can lead to inability to function properly.

## Power Irregularities

Voltage levels can increase, decrease, or cease:

- Spike – momentary increase
- Surge – prolonged increase
- Sag – momentary low voltage
- Brownout – prolonged drop
- Fault – momentary loss of power
- Blackout – prolonged loss

- Electronic equipment is susceptible to fluctuations, controls can be applied to manage power quality.

## Espionage/Trespass

Broad category of activities that breach confidentiality are:

- Unauthorized accessing of information.
- Competitive intelligence vs. espionage.
- Shoulder surfing can occur at any place; a person is accessing confidential information.

- Controls implemented to mark the boundaries of an organization's virtual territory giving notice to trespassers that they are encroaching on the organization's cyberspace.
- Hackers uses skill, guile, or fraud to steal the property of someone else.

## Espionage/Trespass

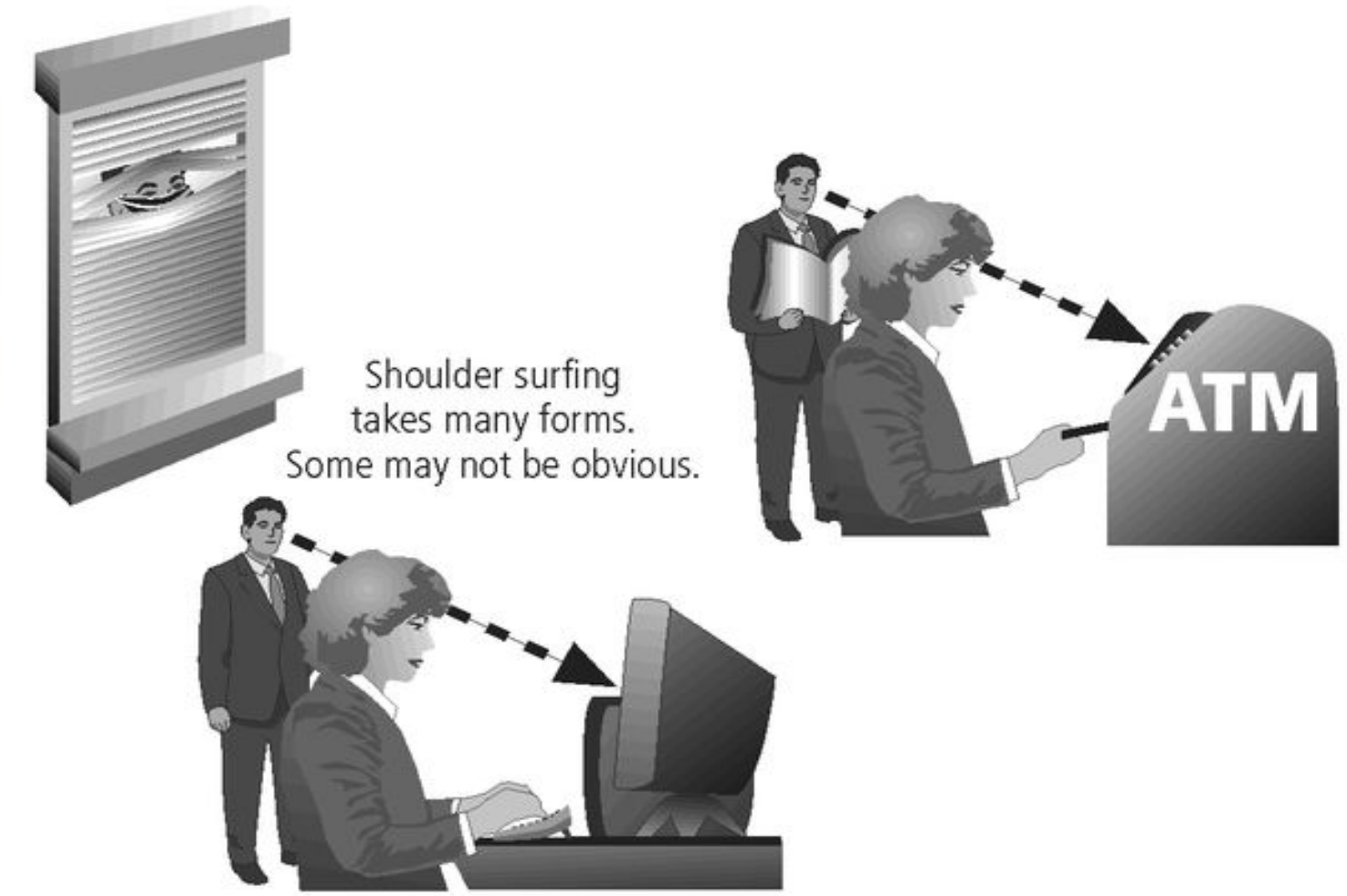
Generally, there are two skill levels among hackers:

- **Expert hacker**
  - Develops software scripts and codes exploits.
  - Usually a master of many skills.
  - Will often create attack software and share with others.
- **Script kiddies**
  - Hackers of limited skill.
  - Use expert-written software to exploit a system.
  - Do not usually fully understand the systems they hack.

Other terms for system rule breakers:

- Cracker - an individual who “cracks” or removes protection designed to prevent unauthorized duplication.
- Phreaker - hacks the public telephone network.

## Shoulder Surfing



## Hacker's Profile

Traditional hacker profile:
Age 13-18, male with limited parental supervision spends all his free time at the computer

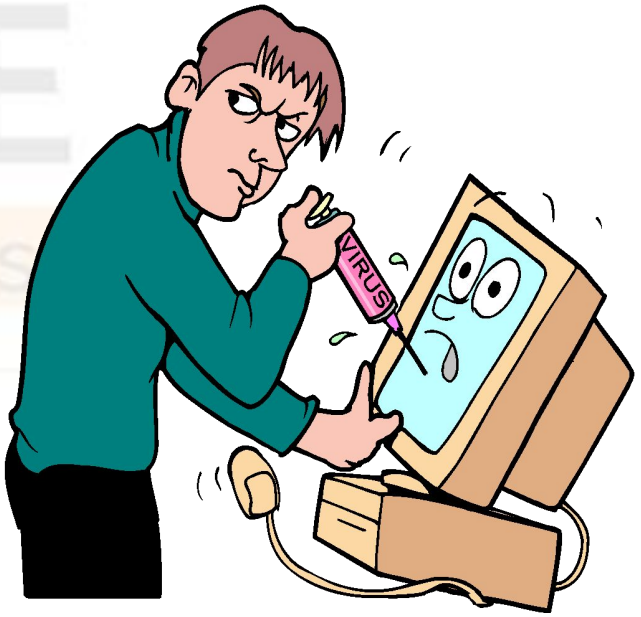
Modern hacker profile:
Age 12-60, male or female, unknown background, with varying technological skill levels; may be internal or external to the organization

## Information Extortion

- Information extortion is an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return or non-use.
- Extortion found in credit card number theft.

## Sabotage or Vandalism

- Individual or group who wants to deliberately sabotage the operations of a computer system or business, or perform acts of vandalism to either destroy an asset or damage the image of the organization.
- These threats can range from petty vandalism to organized sabotage.
- Organizations rely on image, so Web defacing can lead to dropping consumer confidence and sales.
- Rising threat of hacktivist or cyber-activist operations – the most extreme version is cyber-terrorism.



## Deliberate Acts of Theft

- Illegal taking of another's property - physical, electronic, or intellectual.
- The value of information suffers, when it is copied and taken away without the owner's knowledge.
- Physical theft can be controlled - a wide variety of measures used from locked doors to guards or alarm systems.
- Electronic theft is a more complex problem to manage and control - organizations may not even know it has occurred.

## Deliberate Software Attacks

- When an individual or group designs software to attack systems, they create malicious code/software called as malware.
  - Designed to damage, destroy, or deny service to the target systems.

It includes:

- Macro virus
- Boot virus
- Worms
- Trojan horses
- Logic bombs
- Back door or trap door
- Denial-of-service attacks
- Polymorphic
- Hoaxes

## Compromises to Intellectual Property

- Intellectual property is “the ownership of ideas and control over the tangible or virtual representation of those ideas”.

Many organizations are in business to create intellectual property. They are:

- Trade secrets
- Copyrights
- Trademarks
- Patents

## Compromises to Intellectual Property

- Most common IP breaches involve software piracy.
- Watchdog organizations investigate:
  - Software and Information Industry Association (SIIA)
  - Business Software Alliance (BSA)
- Enforcement of copyright has been attempted with technical security mechanisms.

## Forces of Nature

- Forces of nature, force majeure, or acts of God are dangerous because, they are unexpected and can occur with very little warning or no warning.
- Can disrupt not only the lives of individuals, but also the storage, transmission, and use of information.
- Includes fire, flood, earthquake, and lightning as well as volcanic eruption and insect infestation
- Since, it is not possible to avoid many of these threats, management must implement controls to limit damage and also prepare contingency plans for continued operations.

## Technical Hardware Failures or Errors

- Technical hardware failures or errors occur when a manufacturer distributes equipment containing flaws to users.
- These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability.
- Some errors are terminal, in that they result in the unrecoverable loss of the equipment.
- Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated.

## Technical Hardware Failures or Errors

- This category of threats comes from purchasing software with unrevealed faults.
- Large quantities of computer code are written, debugged, published, and sold only to determine that not all bugs were resolved.
- Sometimes, unique combinations of certain software and hardware reveal new bugs.
- Sometimes, these items are not errors, but are purposeful shortcuts left by programmers for honest or dishonest reasons.

## Technological Obsolescence

- When the infrastructure becomes antiquated or outdated, it leads to unreliable and untrustworthy systems.
- Management must recognise that, when technology becomes outdated, there is a risk of loss of data integrity to threats and attacks.
- Ideally, proper planning by management should prevent the risks from technology obsolesce, but when obsolescence is identified, management must take action.

## Attacks

- An attack is the deliberate act that exploits vulnerability.
- It is accomplished by a threat-agent to damage or steal an organization's information or physical asset.
  - An exploit is a technique to compromise a system.
  - A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective.
  - An attack is then the use of an exploit to achieve the compromise of a controlled system.

## Malicious Code

- This kind of 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 in attacking systems in 2002, is the multi-vector worm using up to six attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

## Malicious Code

| Vector | Description |
|---|---|
| IP scan and attack | Infected system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox |
| Web browsing | If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected |
| 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 |
| Shares | Using vulnerabilities in file systems and the way many organizations configure them, it copies the viral component to all locations it can reach |
| Mass mail | By sending e-mail infections to addresses found in the infected system's address book, copies of the infection are sent to many users whose mail-reading programs automatically run the program and infect other systems |
| Simple Network Management Protocol (SNMP) | In early 2002, the SNMP vulnerabilities known to many in the IT industry were brought to the attention of the multi-vector attack community. SNMP buffer overflow and weak community string attacks are expected by the end of 2002 |

## Attack Descriptions

- **IP Scan and Attack** – Compromised system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits.
- **Web Browsing** - If the infected system has write access to any Web pages, it makes all Web content files infectious, so that users who browse to those pages become infected.
- **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.

## Attack Descriptions

- **Unprotected Shares** - using file shares to copy viral component to all reachable locations.
- **Mass Mail** - sending e-mail infections to addresses found in address book.
- **Simple Network Management Protocol** - SNMP vulnerabilities used to compromise and infect.
- **Hoaxes** - A more devious approach to attacking computer systems is the transmission of a virus hoax, with a real virus attached.

## Attack Descriptions

- **Mail-bombing** - another form of e-mail attack that is also a DoS, in which an attacker routes large quantities of e-mail to the target.
- **Sniffers** - a program and/or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network.
- **Social Engineering** - within the context of information security, the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.

## Attack Descriptions

- "People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything."
- "brick attack" – the best configured firewall in the world can't stand up to a well placed brick.

## Attack Descriptions

### Buffer Overflow

- Application error occurs when more data is sent to a buffer than it can handle.
- When the buffer overflows, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure.

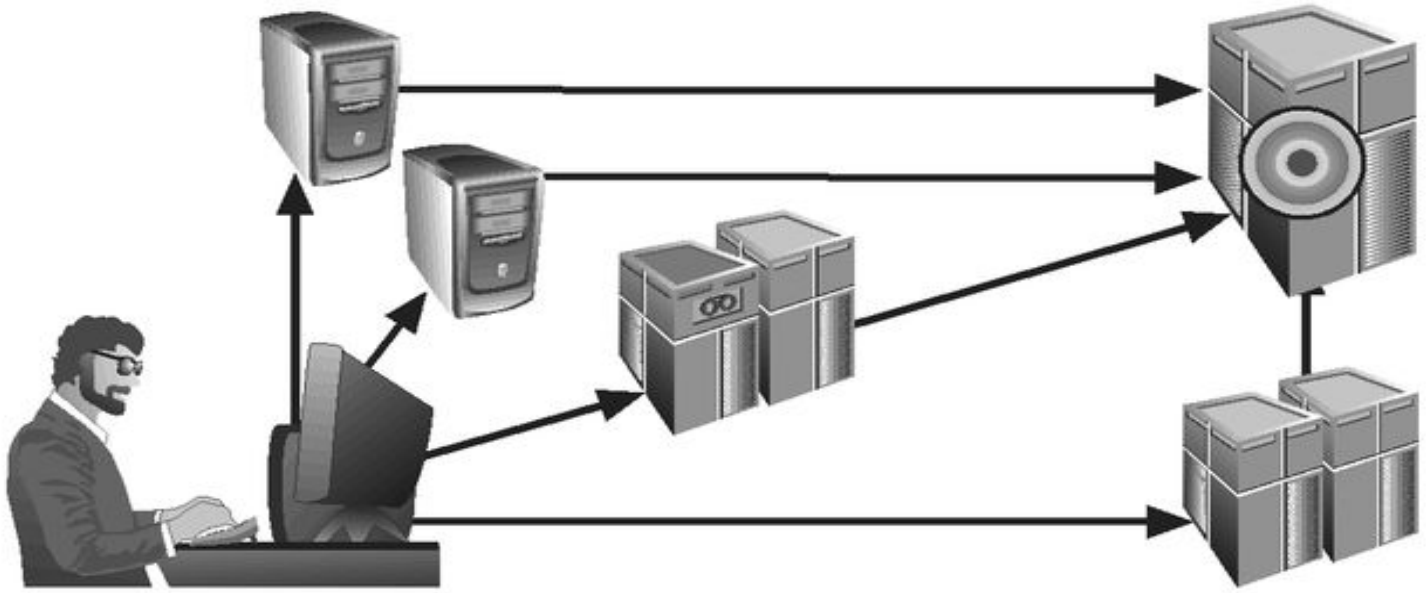
### Timing Attack

- Relatively new.
- Works by exploring the contents of a web browser's cache.
- Can allow collection of information on access to password-protected sites.
- Another attack by the same name involves attempting to intercept cryptographic elements to determine keys and encryption algorithms.

## Denial of Service attack

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.



## Attack Descriptions

- **Back Doors** - Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource.
- **Password Crack** - Attempting to reverse calculate a password.
- **Brute Force** - The application of computing and network resources to try every possible combination of options of a password.
- **Dictionary** - The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guide guesses.

## Attack Descriptions

### Denial-of-service (DoS)

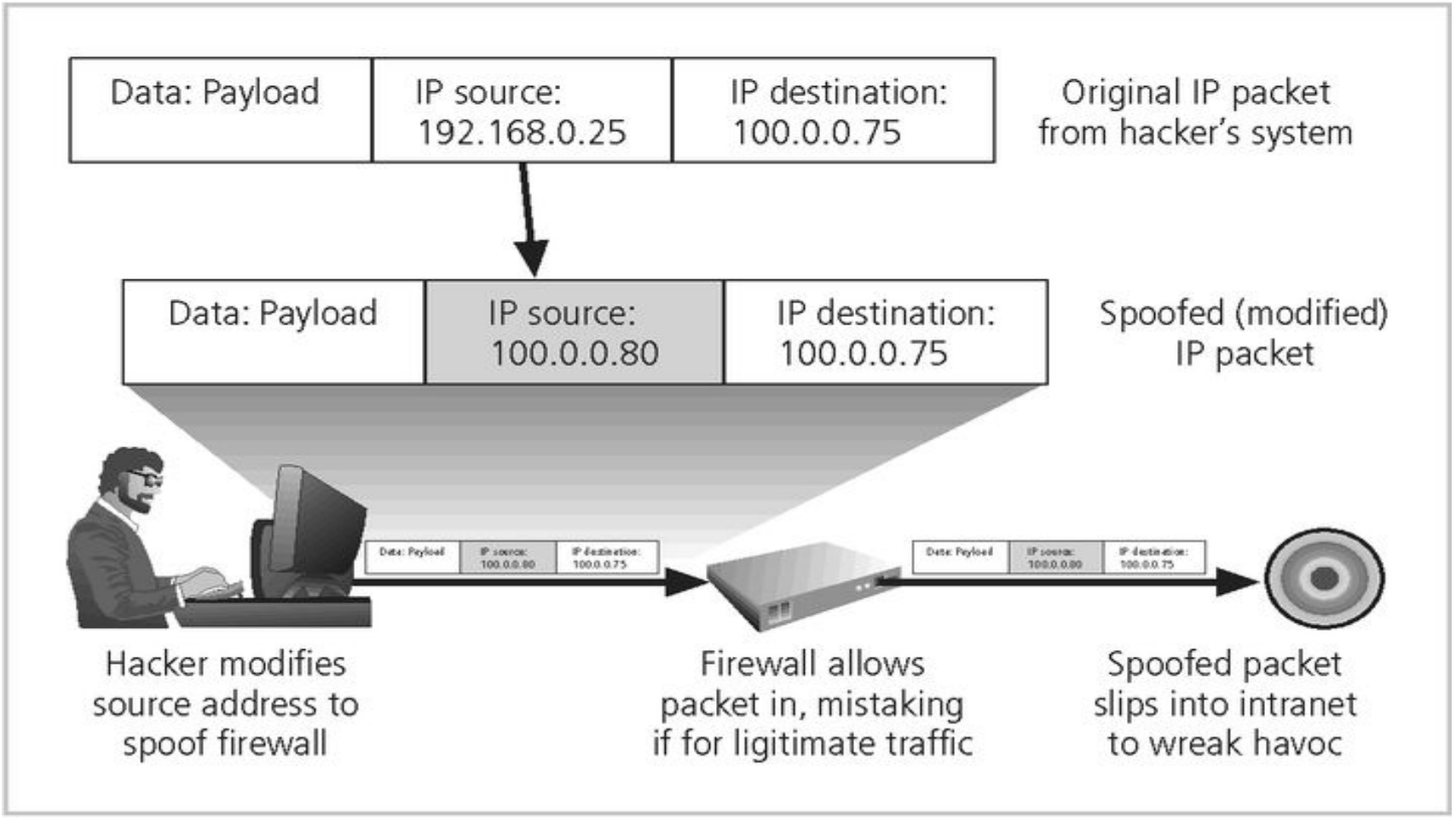
- Attacker sends a large number of connection or information requests to a target.
- So many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service.
- May result in a system crash, or merely an inability to perform ordinary functions.

**Distributed Denial-of-service (DDoS)** - an attack, in which a coordinated stream of requests is launched against a target from many locations at the same time.

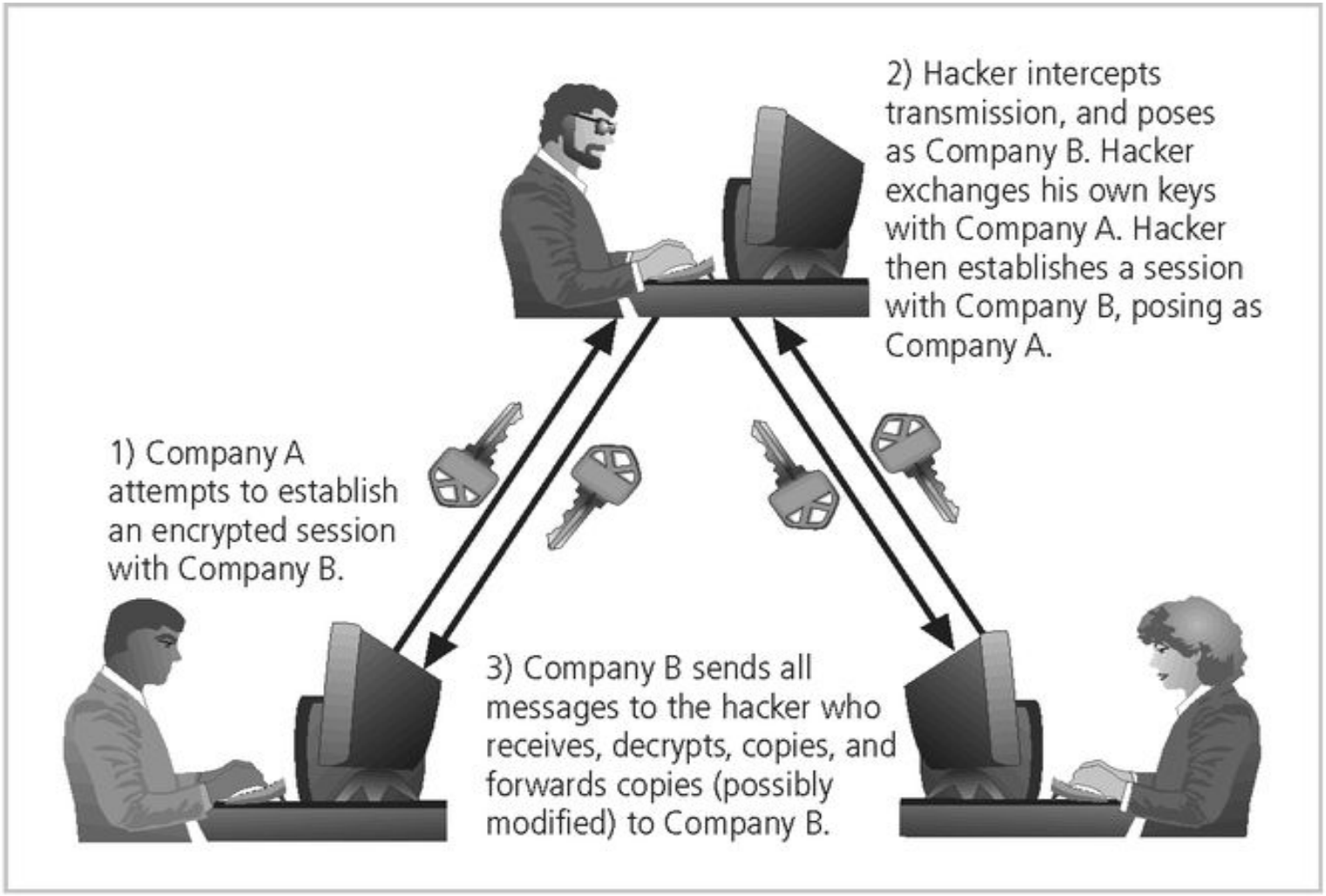
## Attack Descriptions

- **Spoofing** - technique used to gain unauthorised access, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
- **Man-in-the-Middle** - an attacker sniffs packets from the network, modifies them, and inserts them back into the network.
- **Spam** - unsolicited commercial e-mail - while many consider spam a nuisance rather than an attack, it is emerging as a vector for some attacks.

## IP Spoofing


Data: Payload
IP source: 192.168.0.25
IP destination: 100.0.0.75
Original IP packet from hacker's system
Data: Payload
IP source: 100.0.0.80
IP destination: 100.0.0.75
Spoofed (modified) IP packet
Hacker modifies source address to spoof firewall
Firewall allows packet in, mistaking if for ligitimate traffic
Spoofed packet slips into intranet to wreak havoc

## Man In The Middle Attack



## Secure Software Development

- Many information security issues are caused by software elements of system.
- Development of software and systems is often accomplished using methodology such as Systems Development Life Cycle (SDLC).
- Many organizations recognize the need for security objectives in SDLC and have included procedures to create more secure software.
- This software development approach is known as Software Assurance (SA).

## Self Assessment Question

7. Organizations must create integrated application. State whether True or False.

a. True

b. False

**Answer: True**

## Self Assessment Question

8. An effective information security program is essential to the protection of the integrity and value of the organization's data. State whether True or False.

a. True

b. False

**Answer: True**

## Self Assessment Question

9. Size and scope of the enterprise does not affect the organization security services. State whether True or False.

a. True

b. False

**Answer: False**

## Self Assessment Question

10. According to 2002 CSI/FBI survey,____% of organizations responded to detected computer security breaches within the last year.

a. 60

b. 70

c. 80

d. 90

**Answer: 90**

## Self Assessment Question

11. Only ___% of organizations reported their attacks to law enforcement.

a. 30

b. 34

c. 38

d. 35

**Answer: 34**

## Self Assessment Question

12. Employee mistake comes under _____ category of threat.

a. Act of human error or failure

b. Compromise to intellectual property

c. Deliberate act of threat

d. Forces of nature

**Answer: Act of human error or failure**

## Self Assessment Question

13. Fire comes under _____ category of threat.

a. Act of human error or failure

b. Compromise to intellectual property

c. Deliberate act of threat

d. Forces of nature

**Answer: Forces of nature**

## Self Assessment Question

14. Copyright infringement comes under deliberate act of threat category. State True or False.

a. True

b. False

**Answer: False**

## Self Assessment Question

15. Virus and worms are_____ category of threat.

a. Act of human error or failure

b. Deliberate software attack

c. Deliberate act of threat

d. Forces of nature

**Answer: Deliberate software attack**

## Self Assessment Question

16. Which one of the given options is not a cause of an Acts of Human Error or Failure?

a. Inexperience

b. Improper training

c. Incorrect assumptions

d. Failure to protect information

**Answer: Failure to protect information**

## Self Assessment Question

17. Information system do not depend on many inter-dependent support systems. State whether True or False.

a. True

b. False

**Answer: False**

## Self Assessment Question

18. In denial of service attack, an attacker modifies the data on the victim machine.

a. True

b. False

**Answer: False**

## Self Assessment Question

19. Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource is called

a. Back Doors

b. Dictionary attack

c. Brute force attack

d. Password cracking

**Answer: Back Doors**

## Self Assessment Question

20. An attack, in which a coordinated stream of requests is launched against a target from many locations at the same time.

a. DOS

b. DDOS

c. Brute force

d. Dictionary

**Answer: DDOS**

## Self Assessment Question

21. An attacker sniffs packets from the network, modifies them, and inserts them back into the network, is called

a. Spoofing attack

b. Man In The Middle attack

c. DDOS attack

d. Spam attack

**Answer: Man In The Middle attack**

## Self Assessment Question

22. _____ is sending unsolicited commercial e-mail - while many consider spam a nuisance rather than an attack, it is emerging as a vector for some attacks

a. Spoofing attack

b. Man In The Middle attack

c. DDOS attack

d. Spam attack

**Answer: Spam attack**

## Self Assessment Question

23. An attack involves attempting to intercept cryptographic elements to determine keys and encryption algorithms is called

a. Spoofing attack

b. Man In The Middle attack

c. Timing Attack

d. Spam attack DOS

**Answer: Timing Attack**

## Self Assessment Question

24. A program and/or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network is called

a. Spams

b. Virus

c. Worms

d. Sniffers

**Answer: Sniffers**

## Self Assessment Question

25. When technology becomes outdated, there is a risk of loss of data integrity to threats and attacks. State whether true or false

a. True

b. False

**Answer: True**

## Self Assessment Question

26. An exploit

a. is a technique to compromise a system

b. Identifies weakness of a controlled system whose controls are not present or are no longer effective.

c. achieve the compromise of a controlled system

d. none of the above

**Answer: is a technique to compromise a system**

## Assignment

- Explain the security requirement in business
- Describe the process of safeguarding the business process
- Explain the security threat associated with business functionality
- Describe the threats related to intellectual property right
- Discuss attacks that can be performed using software tools
- Describe the term espionage and trespassing
- Discuss sabotage and vandalism
- Explain various security attack process
- What is DOS and DDOS? Explain the attack process
- Explain the steps associated with social engineering attacks

## Summary

- Information security is a “well-informed sense of assurance that the information risks and controls are in balance.”
- Threat: object, person, or other entity representing a constant danger to an asset.
- Management effectively protects its information through policy, education, training, and technology controls
- Attack: a deliberate act that exploits vulnerability.
- Secure systems require secure software.

## Document Links

| Topic | URL's | Description |
|---|---|---|
| Business Needs-Protecting the functionality | https://www.fortinet.com/blog/partners/align-your-customers-business-needs-with-security-functionality.html | Explain the needs of the security in an organization. |
| Protecting the data | https://www.theguardian.com/technology/2013/sep/16/10-ways-keep-personal-data-safe | The link describe the process of securing the information in an organization. |
| Threats-compromises to Intellectual property | https://www.upcounsel.com/compromises-to-intellectual-property | The link explain various threats that exist in an organization. |
| Cyber security attack | https://www.rapid7.com/fundamentals/types-of-attacks/ | The link describe about various security attacks. |

## Video Links

| Topic | URL's | Description |
|---|---|---|
| Protecting the data, safe guarding the technology assets | https://www.youtube.com/watch?v=5b-TlaerQZk | Describe the need and procedure for securing the assets |
| compromises to Intellectual property | https://www.youtube.com/watch?v=EQsZf2G4Sdc | Explain the intellectual property and need to protect it |
| Cybersecurity And attacks | https://www.youtube.com/watch?v=BL0v7KcQH_k | The link explain in details about cyber security |
| Cybersecurity Threats | https://www.youtube.com/watch?v=Dk-ZqQ-bfy4 | The link explain what are common cyber security threats |

## E-Book Links

| Topic | Book Name | | Page |
|---|---|---|---|
| Information security needs | Information Security The Complete reference | http://wiki.informationsecurity.club/lib/exe/fetch.php/%D0%BA%D0%BD%D0%B8%D0%B3%D0%B8:information_security_the_complete_reference_2ed.pdf | 3-23 |
| Threats | | | 25-27 |
| Security Attacks | | | 30-51 |