Learning Materials for

ITP1232 – INFORMATION ASSURANCE AND SECURITY 1

A compilation of Lectures/Activities

COLLEGE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY
JANUARY 2021

Information Assurance and Security: An Introduction

1

Contents:

Disclaimer

This learning material is used in compliance with the flexible teaching-learning approach espoused by CHED in response to the pandemic that has globally affected education institutions. Authors and publishers of the contents are well acknowledged. As such the College of information and Communications Technology and its faculty do not claim ownership of all sourced information. This learning material will solely be used for instructional purposes not for commercialization.

Key Concepts and Terms:

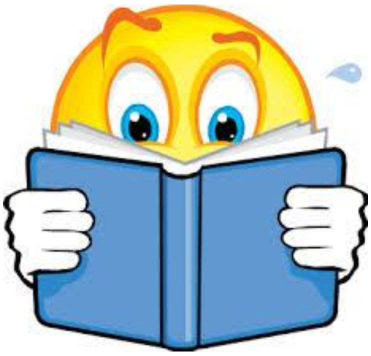
- Authentication
- Authorization
- Availability
- Change Management
- Confidentiality
- Information Assurance
- Information Systems Security
- Integrity
- IT Security
- Policy
- Risk
- Threats
- Vulnerability

Overview:

One of the challenges organizations face is the cost of keeping pace with ever-changing technology. This includes the need to update technology and policies on the proper utilization of technology. Failure to do so could create weakness in the system which results to the vulnerability of information to loss or theft.

Information systems security ensures that information and the systems that stores and process it are protected against the risks of unauthorized access, use, disclosure, disruption, modification or destruction of information. Thus, information needs to be protected in any form and this measure is necessary to business operations. This chapter will provide key terms ad introductory concepts relative to information assurance and security.

Learning Outcomes:



After studying this chapter, the students shall be able to:

1. describe the key terms associated with Information Assurance and Security;
2. gain familiarity with the kinds of information security attacks and the corresponding vulnerabilities;
3. describe the anatomy of an attack and device some security policies for the organization.

1.1. *Key Terms*

In this age of information Technology, the need to ensure the safety of data has become a paramount concern for companies and organizations across the world. Below are some terms associated with Information Assurance and Security.

- **IT Security-** This term is sometimes referred to computer security. Information Technology security is information security applied to technology (most often some form of computer system- starting from non-networked standalone devices to networked mobile computing devices such as smartphones and tablet computers).

- **Information Security –** summary of its definition is stated below:
  - ✓ Preservation of confidentiality, integrity, availability of information. Note: in addition, other properties, such as authenticity, accountability, non-repudiation and reliability could also be involved (ISO/IEC 27000:2009).
  - ✓ The protection of information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity, availability (CNSS, 2010).
  - ✓ Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability) (ISACA, 2008).
  - ✓ Information security is the process of protecting the intellectual property of an organization (Pipkin, 2000).
  - ✓ Information security is a risk management discipline, whose job is to manage the cost of information risk to the business (McDermott and Geer, 2001).
  - ✓ A well-informed sense of assurance that information risks and controls are in balance (Anderson, J., 2003).
  - ✓ Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties (Venter and Eloff, 2003).
  - ✓ Information security is the multi-disciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within or outside organization's perimeter) and consequently, information system, where information is created, processed, stored, transmitted and destroyed free from threats.

  Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. The current relevant security goals may include confidentiality, integrity, availability, privacy, authenticity and trustworthiness, non-repudiation, accountability and auditability.

- **Information Assurance-** This term grew from information systems security (ISS). ISS focuses on protecting the information regardless of form or process. Information Assurance (IA) focuses on protecting information during the process and use.
  Below are five pillars of IA model:

- ✓ **Confidentiality** – goal of ensuring that only authorized individuals are able to access information. A user should be granted access only to specific information necessary to complete his/her job.

In information security, this term is the property that information is not made available or disclosed to unauthorized individuals, entities or properties.

- ✓ **Integrity** – ensures that information has not been improperly changed. in other words, the data owner must approve any change to the data or approve the process by which the data changes.

In information security, this term means maintaining and assuring the accuracy and completeness of data over its entire life cycle. This means that data cannot be modified in an unauthorized or undetected manner.

- ✓ **Availability** – ensures information is available to authorized users and devices.

In information security, this term means that the computing systems used to store and process the information, the security control used to process it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as flood of incoming messages to the target system essentially forcing it to shut down.

- ✓ **Authentication** – is the ability to verify the identity of a user or device.

- ✓ **Nonrepudiation** – is the assurance that an individual cannot deny having digitally signed a document or been party to a transaction. As a legal concept it is the sum total of evidence that proves to the court's satisfaction that only one person could have executed that transaction.

  It is the act of providing trust of the information, that the confidentiality, Integrity, availability (CIA) are not violated. It ensures that data is not lost when critical issues arise. These issues include, but not limited to natural disasters, computer/server malfunctions, physical theft, or any other instance where data has the potential of being lost. A common method of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

- **Information Systems Security-**Is the act of protecting information and systems that store and process it.

- **Risk.** The likelihood or probability of an event and its impact. It is the likelihood that something bad will happen that causes harm to an informational asset.

- **Risk Management** – the process of identifying vulnerabilities and threats to information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.

There are two things in this definition that may need clarification: ***first***, the process of risk management is an ongoing, iterative process. It must be repeated indefinitely. The business environment is constantly changing, and new threats arise every day; ***second***, the choice of countermeasures (control) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasures, and the value of the informational asset being protected.

The most vulnerable point in mist information systems is the human user operator, designer or other human. The following should be examined during risk assessment:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Regulatory compliance

In broad terms, the risk management process consists of:

- Identification of assets and estimating their value. Include people, buildings, hardware, software, data (electronic, print other), supplies.
- Conduct a threat assessment. Include: acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.
- Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
- Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
- Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness and value of the asset.
- Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost-effective protection without discernable loss of productivity.

Selecting proper controls and implementing those will initially help an organization to bring down risk to acceptable levels. Control selection should follow and should be based on the risk assessment. Controls can vary in nature but fundamentally, there are ways of protecting the confidentiality, integrity or availability of information.

Administrative Controls (also called procedural controls) consists of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform the people on how the business is run and how day-to-day operations are to be conducted. Administrative controls form the basis for the selection and implementation of logical, physical controls. Logical and physical controls are manifestations administrative controls.

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. Examples are password, network and host-based firewalls, network intrusion detection systems, access control lists and data encryption.

Physical Controls monitor and control the environment of the workplace and computing facilities. They also monitor and control access to and from such facilities. Examples are doors, locks, heating and air-conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. separating network and workplace into functional areas are also physical controls.

- **Threats.** Threats are human-caused or natural event that could impact the system. It is anything (manmade or act of nature) that has potential to cause harm. Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identify theft, theft of equipment or information, sabotage or information extortion. Example of software attacks are viruses' worms, phishing attacks and trojan horses.

- **Intellectual Property –** ownership of property usually consisting of some form of protection.

- **Identity Theft –** is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information.

- **Sabotage** - consists of destruction of an organization's website in an attempt to cause loss of confidence to its customers.

- **Information Extortion**- consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner.

- **Vulnerability**. A weakness in a system that can be exploited. It is a weakness that could be used to endanger or cause harm to an informational asset

Security Classification for Information:

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information.

The first step in information classification is to identify the member of senior management as the owner of the particular information to be classified. Next, develop a classification policy.

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification.

Access Control

Access to protected information must be restricted to people who are authorized to access the information. Computer programs and the computer that process the information must also be authorized. Likewise, mechanisms should be in place to control the access to protected information.

Access control is generally considered in three steps: Identification, Authentication and Authorization.

Identification

Identification is an assertion of who someone is or what something is. Requiring “username” is one form of identification.

Authentication

Authentication is the act of verifying a claim of identity. There are three different types of information that can be used for authentication:

- Something you know: things such as a PIN, password, or your mother’s maiden name
- Something you have: a driver’s license or magnetic swipe card
- Something you are: biometrics including palm prints, fingerprints, voice prints and retina (eye) scans.

Authorization

Determining what informational resources are permitted to access and what actions will be allowed to perform. Authorization to access information and other computing services begins with administrative policies and procedures. The polices describe what information and computing services can be accessed by whom, and under what condition.

Change Management

Change management is a formal process for directing and controlling alterations to the information processing environment. This includes alterations to desktop computers, the network, servers and software.

The objectives of change management is to reduce risks posed by changes to the information processing environment and improve the stability and radiality of the processing environment as changes are made. Any change to the information processing environment introduces an element of risk.

Change management is usually overseen by a Change Review Board composed of Representatives form key business areas, security, networking, system administrators, database administrators, application development, desktop support and help desk. The tasks of the Change Review Board can be facilitated with the use of automated workflow application.

1.2. Information Security Attacks and Vulnerabilities

Below is the list of types of attacks that hackers may launch against the company's network:

Spamming consists of an identified or unidentified source sending bulk mail to one's site. In the **non-malicious form**, it consists of sending bulk advertising mail to many accounts at one's site consistently even multiple times a day. In the **malicious form**, it consists of the attacker sending bulk mail until your mail server runs out of disk space. This type of attack consumes part of all the communications bandwidth to your site and attempts to deny service to your maul server by keeping it busy and filling up its disk space. When the disk space is full, then the mail server will be unable to receive any additional mail.

Viruses are compact packages of software that require a host in order to replicate and possibly cause damage. Viruses can attack any part of the computer's software such as its bot block, operating system, file allocation (FAT) tables, EXE file, COM files and application program macros. Boot block viruses replace the boot block with virus code and relocate it to another disk location where data may be overwritten at that location. EXE or COM file viruses insert or append the virus code into these files. Some viruses take steps to conceal the addition of the code by modifying the file structure or making sure the Cyclic Redundancy Check (CRC) does not change. Such viruses need to be cleaned up which takes time. Cleaning up viruses requires removing them form the computer and form other systems that exchange data with the infected system.

Denial of Service Attacks disable computer system by eating system resources until the system or applications come to halt. Flooding a system with junk mail or synchronization (SYN) packets are examples of denial of service attacks.

Password Guessing. Most hackers gain illegal entry into remote computer system by guessing passwords. Hackers guessed people's passwords using common names or combination of letters. Also, password generation programs are commonly used that create passwords, usually a dictionary word, to try to gain access. If access is denied, another password is generated, and the process is replaced.

Worms. Once inside the computer, a hacker can place a program called a worm that self-replicates. Worm programs keep growing larger until disk space or memory is filled. These programs seek out unused resources and then consume them.

Backdoor. Once a hacker breaks into a system, code can be inserted somewhere on the system to create secret backdoor that allows unauthorized access the hacker may deposit a program on the system that allows backdoor access at will. Alternatively, the hacker can create his own innocuous looking account that provides access to the system.

Sweeper. Hackers may use the program called sweeper that sweeps all data from the system.

Sniffers. Sniffers are programs that monitor network traffic (i.e. packets) and can gather useful information that can be used in an attack. Hackers use sniffers to capture that first few hundred bytes of ***telnet, ftp an rlogin session*** in order to obtain clear text passwords and other useful packet information. Once a single computer is compromised and a sniffer is installed, then all the remaining machines on the network can be compromised.

Packet Forge Spoofing. This is a form of attack that involves the subtle alteration of data in a packet. A sophisticated hacker may be able to alter the data effectively in order to do damage to the intended target. This usually results in the receipt of wrong information that was modified by the hacker. Form the attacker's point of view it is better to give the recipient the wrong information rather than no information.

IP Spoofing. A SYN flood attack is a form of internet protocol (IP) spoofing that exploits the three-way handshake in the TCP/IP protocol that initiates every IP connection. This form of attack allows a hacker to fake his identity by sending SYN packets with a spoofed source address to a destination host. The destination host sends a SYN-ACK packet to the unsuspecting host with the spoofed address. The destination host waits for an ACK until there is a time-out. The destination machine connection buffer fills with incomplete connections until it stops accepting new connections.

Trojan Horses. Trojan Horses are software codes that enter the computer system through the front door. This type of software is embedded in a program or utility that the user believes to be harmless, such as text editor or useful utility program. These programs are obtained voluntarily by the user to help with some task or problem. When the program is used, it then performs some malicious function such as deleting or copying files to another computer.

1.3. Anatomy of an Attack

The process below would enlighten us on the things hackers do to discover information and gain access to the system and network:

1). The hacker picks a target organization.

2). The hacker attempts to discover the organization's internet connections by issuing "***whois***" queries to Internet Network Information Center (InterNIC) to find the organization's Domain Name Service (DNS) servers.

3). A DNS zone transfer is requested from the organization's DNS server. This is a probe into the organization that may not be blocked by the organization's firewall.

4). The hacker tries to discover the IP addresses of the filtering router, which is the organization's internet gateway, by probing the site with a program that will trace the route packets will travel. The organization's internal router or firewall will be the last hope before packets issued by the probe gets dropped.

5). IP addresses for bastion host machines outside the firewall attempt to be found.

6). The bastion host machine ports are scanned to determine which ports are active and what system services are running that may be exploited.

7). If access can be gained into the machine, then the accounts database or password file is searched for existing usernames.

8). Password cracking programs are used to try to break into the administrative or "super-user" account. If access is gained, then that machine is entirely compromised and the hacker as free rein.

9). Next to compromise other machines on the network, a password decryption program is run to get username passwords. Some of the same passwords that are on bastion hosts may be used on machines inside the firewall. Also addresses and names of the internal machines may be discovered by checking the "hosts" file or other equivalent files residing on the bastion hosts.

10). Armed with the information, access to the internal machines is attempted via the compromised bastion host machine. Misconfigured or poorly configured firewalls are common. These may contain holes that allow access to the internal networks or clever hackers. If entry is achieved by remote login to any of the internal machines, then a sniffer program can be run from the internal machine to discover clear-text password information flowing on the network and thereby enable hacked access into all the internal machines.

11). Once inside, then other points within the internal network such as other firewalls or machines with modems are secured in case the original intrusion point is discovered. Phone numbers to modems may be published internally or in an administrator's directory. Else, a dialer program that scans the phone lines looking for modem carriers can be run. Internal PC's with modems are a perfect backdoor.

12). The attack progresses to compromise as many machines s possible with the ultimate goal to reach an organization’s most mission-critical machines and those with sensitive information.

1.4. Awareness and Management Commitment to Security

Security policy must be created to ensure information security. Security must be considered a part of the organization’s overall business strategy. Security must be translated in the minds of managers to financial loss, either through lost business, reduced productivity, lost data, revealed corporate secrets or compromised integrity. The threat by hackers must be perceived as real.

If management does not agree to establish and enforce a security policy, then the system is at high-risk to threats. The high-risk threats and the cost of mitigating these threats must be presented accurately and fully.

1.5. Security Policy

Establishing a security policy is the starting point in designing a secure computer network. It is essential that a set of minimum-security requirements must be gathered, formalized and included as the basis of the company’s security policy. This security policy must be enforceable by the organization and will create an additional cost to running and monitoring the network. This additional cost/benefit of a security policy must be understood and embraced by the organization’s management in order to enhance and maintain network and system security.

The lack of accepted and well-thought-out security policy and guidelines document is one of the major security vulnerabilities in most companies today.

Below are information security best practices that may be employed in the organization:

#1: Perform a threat analysis for your organization to determine the level of security that must be implemented.

- Identify all the threats to the computers and network.
- Determine threat categories
- Perform risk assessment
- Recommend action

#2: define a security policy for the entire site and use it as a guide for the network security architecture.

- Define a policy that includes section for confidentiality, integrity, availability, accountability, assurance and enforcement.
- The policy should address as much as possible according to risk and affordability.
- Below is the general security policy:

- ***Confidentiality*** – the system must ensure that confidentiality of sensitive information by controlling access to information, services and equipment. Only the personnel who have the proper authorization and need-to-know can have access to system and data. The system must include features and procedures to enforce access control policies for all information, services and equipment compromising the system.
- ***Integrity*** – the system must maintain the integrity (absence of unauthorized an undetected modification) of information and software while these are processed, stored, transferred across a network or publicly accessible transmission media. Each file or data collected in the system must have identifiable source throughout its life cycle. Also, the system must ensure the integrity of its mission-critical equipment. Automated and/or manual safeguards must be used to detect and prevent inadvertent or malicious destruction or modification of data.
- ***Availability***- the system must protect against denial of service threats. Protection must be appropriate to the operational value of the services and the information provided. This protection must include protection against environmental threats such as loss of power and cooling.
- ***Accountability***- the system must support tracing of all security relevant events, including violations and attempted violations of security policy to the individual systems and/or users including external connections. The system must enforce the following rules: (1) personnel and systems connecting to the system must be uniquely identifiable to the system and must have their identities authenticated before being granted access to sensitive information, services or equipment. (2) each subsystem handling sensitive or mission-critical information must maintain an audit trail of security relevant events including attempts by individual users or interfacing subsystems to gain access through interfaces not authorized for that particular purpose. This audit trail must be tamper-resistant and always active.
- ***Assurance***- the criticality and sensitivity of the information handled, equipment and services, and the need-to-know of personnel must be identified in order to determine the applicable security requirements. The security implementations chosen must provide adequate security protection commensurate with the criticality of data, in accordance with the security policy.
- ***Enforcement*** – the security policy must be enforced throughout the life cycle of the system. All implementations of system security functions including those implemented at the subsystem level must be evaluated to ensure that they adequately enforce the requirements derived from the policy. Each platform must be evaluated to ensure that the installed system configuration enforces the stated security policy. As a result of this evaluation, an assessment of the vulnerability can be generated. This assessment must be evaluated by the security manager or system administrator to decide if any modification to the system must be made so that it complies with the security policy. Security best practices must be employed throughout the life cycle of the system to ensure continued compliance with the stated security policy. New system projects must have information security representatives during

the planning and preliminary design stages in order to implement security into the design.

➢

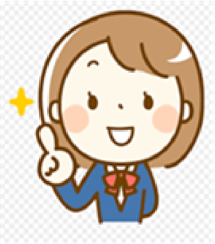
#3: Create a plan for implementing your security policy.

- Once a security policy is established, an implementation plan should be created.
- The implementation plan should include the following steps:
  1). Defining implementation guidelines. These guidelines should specify the personnel to receive the security alarms and what action is to be taken, chains of command for incident escalation and reporting requirements.
  2). Educating staff, customer, etc. about the security policy
  3). Purchasing any needed hardware/software and bring any needed personnel.
  4). Installing and testing equipment/software.

Supplementary Learning Resources:

1. Young, Bill (2015). *CS361C: Information Assurance and Security: Introduction to IA.* PowerPoint Slides.
2. Blyth, A. and Kovacich, G. L. (2001). *Information Assurance: Surviving in the Information Environment*: Springer.
3. Herrmann, D. S. (2007). *Complete Guide to Security and Privacy Metrics*: Auerbach
4. Landoll, D. J. (2006). *The Security Risk Assessment Handbook*: Auerbach, 2006.
5. Whitman, M. E. and Mattord, H. J. (2009). *Principles of Information Security*: Thomson
6. Raggad, B. G. (2010). *Information Security Management*: *Concepts and Practice*: CRC Press, 2010

Self-Assessed Questions 4



1. Briefly describe the following key terms associated with Information Assurance and Security:
   - Information Security
   - Information Assurance
   - Threats
   - Vulnerabilities
   - Risk
   - Risk Assessment

2. Briefly describe the following information security attacks:

   - Virus
   - Worms
   - Sniffer
   - IP Spoofing
   - Backdoor
   - Trojan Horses

3. John works in the accounting department but travels to other company locations. He must present the past quarter's figure to the chief executive officer (CEO) in the morning. He forgot to update the PowerPoint presentation on his desktop computer at the main office. What is at issue here? Justify your answer:
   a) Unauthorized access to the system
   b) Integrity of the data
   c) Availability of the data
   d) Nonrepudiation of the data
   e) Unauthorized use of the system

4. "Implementation and enforcement of policies is a challenge. The biggest hindrance to implementation of the policies is the human factor". Expound these statements.

References:

[1] Carr, Miles (2017). Information Security: Principles and Practices, New York, USA: Larsen and Keller Education.

[2] Johnson, Rob (2015), Security Policies and Implementation Issues. Information Systems Security and Assurance Series. Burlington, Massachusetts, USA: Jones and Barlett Learning, LLC.

[3] Stefanek, George L. (2002), Information Security Best Practices (205 Basic Rules), Woburn, Massachusetts, USA: Butterwoth-Heinemann (Elsevier Science, USA).