STADIO

Information Security for IS Practitioners
ISP152

Note

It is important to note that this study guide must be read in conjunction with the study material contained on the module course site accessed via your Learning Management System (LMS), Canvas.

Please consult Canvas to confirm whether a prescribed textbook must be purchased. Where necessary we will refer to specific pages or chapters.

There may also be reference to additional recommended reading material available for free or at a cost. This will be optional reading intended to enhance your understanding of the material.

The content of the STADIO study guides and teaching documents are not intended to be sold or used for commercial purposes. Such content is, in essence, part of tuition and constitutes an integral part of the learning experience, regardless of the mode.

Links to websites and videos were active and functioning at the time of publication. We apologise in advance if there are instances where the owners of the sites or videos have terminated them. Please contact us in such cases.

A Glossary of terms may be provided at the end of this study guide.

Any reference to gender includes all genders. Similarly, singular may refer to plural and vice versa.

Where AI tools were used to present and organise content for optimal accessibility to students, rigorous quality assurance processes were adhered to.

All figures, tables and other visuals included in this study guide were specifically created for STADIO by commissioned authors, unless otherwise indicated.

It is your responsibility to regularly access Canvas to make sure that you always refer to the latest and most updated material for this module.

We encourage students to make use of the available resources on the STADIO Online Library available on Canvas.

Table of contents

Heading Page number

Module purpose and outcomes

The purpose of this module is to equip you with the knowledge and skills you need to be able to identify and address risks that could undermine the security of organisational information. You will be introduced to computer networking concepts and technologies that underpin organisational information systems; and you will develop an understanding of preventative measures that can be used to counteract information security threats targeting human users as well as organisational networks, software and databases. The module concludes with an overview of principles, tools and methods typically used to conduct a vulnerability assessment.

Upon successful completion of this module, you will be able to:

1. Demonstrate an understanding of the Open Systems Interconnection (OSI) model and common network architectures.
2. Identify the key hardware and software components found in computer networks.
3. Participate in the implementation of the basic principles that underpin the protection of information assets (identification, authentication, etc).
4. Identify the different stages of the operations security process, and the activities that occur within each stage.
5. Identify common threats affecting information security at the human level, the physical level, the network level and the application level; and outline preventative measures that can be used to eliminate or manage these threats.

Prescribed textbooks

The following textbooks are prescribed for this module:

Topic 1:

Dauti, B. 2018. CCENT/CCNA: ICND1 100-105 certification guide. [Chapters 1 and 2 only]. Birmingham, UK: Packt Publishing Ltd. Available via Proquest.

Topics 2 to 5:

Andress, J. 2019. Foundations of information security: A straightforward introduction. San Francisco, CA: No starch press.

Topic 1
Network Fundamentals

1.1 INTRODUCTION

This topic relates to the following module outcomes:

1. Demonstrate an understanding of the Open Systems Interconnection (OSI) model and common network architectures.
2. Identify the key hardware and software components found in computer networks.

Note

The prescribed textbook, *Foundations of Information Security* by Andress (2019), defines and discusses a variety of security practices that can and should be implemented to protect an organisation's information assets. However, it does not include a description of basic network structures and communication methods. This topic is intended to fill that gap.

Networks play a vital role in business operations. They transmit and store organisational data, connect employees within and across business units, and support communication with external stakeholders such as suppliers, customers and statutory bodies. To deal with the broad field of information security, you will need a basic understanding of network structures and principles – which are the focus of this topic.

The physical architecture of a network (also known as its physical topology) describes the physical arrangement of the various hardware components that are connected to the underlying transmission media. Within local area networks (LANs), a network interface card (NIC) connects each individual computer to the network, allowing it to transmit and receive data. For networks that serve a larger area, transmission media may include a combination of wired Ethernet, optical fibre, digital cellular technology and microwave communication. A repeater may be used to retransmit the signal over long distances; and a bridge or router can be used to connect two LANs. Firewalls play an important role in network security by enforcing access rules that block unauthorised sources from the network.

The logical topology of a network describes the flow of data within the physical network infrastructure. The Open Systems Interconnection model (OSI model) is a theoretical model that was developed in the 1980s, which partitions the transmission of data within a network across seven separate layers. However, in practice, the four-layer TCP/IP protocol has been adopted as the standard for networking by most vendors and network administrators.

Network hardware controls the transmission of data within a computer network. Ethernet adapters are a standard component of most computer systems, while wireless networking is available for mobile devices. Data centres contain file and database servers, as well as additional devices such as protocol converters, bridges and routers, proxy servers and firewalls. Shared printers and intranets are accessible to authorised users. Network operating systems (NOS) provide network services such as access control; file, data and application sharing; and sharing of hardware devices such as printers.

In this topic, you will gain knowledge in the following areas:
1. Network topologies, hardware and software.
2. The functions performed by different types of servers on a network.
3. The OSI model and the IEEE 802 standards.

Prescribed reading

For additional information about network topologies and data transmission, refer to Chapters 1 and 2 in the prescribed textbook: Dauti, B. 2018. CCENT/CCNA: ICND1 100-105 Certification Guide. Packt Publishing Ltd, Birmingham, UK. (Available via Proquest).

1.2 NETWORK TOPOLOGIES, HARDWARE AND SOFTWARE

1.2.1 Network topologies

A computer network connects a variety of computing devices such as laptops, smartphones and printers, in order to support the sharing of resources such as information, software applications and services between individuals, groups and institutions. Networks are categorised as follows, based on their range and complexity:

- **Personal area networks** (PANs) are generally limited to home use.
- **Local area networks** (LANs) usually serve an organisation or business.
- **Metropolitan area networks** (MANs) use multiple interconnected LANs to provide shared access to resources within a city or metro.
- **Wide area networks** (WANs) connect multiple PANs, LANs and MANs across a wide geographical area. The Internet is an example of a WAN.
- An **intranet** is an organisational network used for internal communication with and between employees.
- An **extranet** supports external communication with business partners, suppliers and customers.

Activity

Watch the following video:
Title: Network Types: LAN, WAN, PAN, CAN, MAN, SAN, WLAN.
Link: https://www.youtube.com/watch?v=4_zSIXb7tLQ
Time allocation: 04:55

The term 'network topology' refers to how the different physical components within a computer network are arranged and connected.

- A **bus topology** is based on a single 'backbone' (usually of coaxial cable), to which computers, printers and other network devices are connected in series.
- In a **ring topology**, the network cable forms a closed circle to which computers, printers and other network devices are connected.
- In a **star topology**, computers, printers and other network devices are each connected independently to a central server. An extended star topology uses a bus connection to link the servers of two or more star topologies.
- A **hierarchical topology** uses a combination of twisted pair cables and optical fibre to combine multiple star and bus topologies encompassing at least three hierarchical levels.
- In a **mesh topology**, each computer is connected to every other computer that forms the network. A mesh topology usually interconnects multiple LANs to create a WAN.

The **logical topology** of a network reflects the logical paths that carry signals from one computer to another, or from one network node to another. Elements of the logical topology include computer names, network equipment, IP addresses and network communication technology.

Activity

Watch the following video:
Title: Network Topologies (Star, Bus, Ring, Mesh, Ad hoc, Infrastructure, & Wireless Mesh Topology).
Link: https://www.youtube.com/watch?v=zbqrNg4C98U&t=4s
Discuss this with your fellow students and lecturer.
Time allocation: 08:57

1.2.2 Network hardware

Within a computer network, client devices may request access to shared resources that are managed by the server. For example, a PC and a laptop may both request access to the same shared printer; this access will be provided by the network server.

- A **host** is a device with an IP address that requests or provides networking resources to any other host or node on the network.
- A **node** is a device that does not have an IP address but can generate, receive and transmit networking resources on the computer network.
- A **network interface** is a hardware component that allows clients, servers, peripheral devices and other equipment to communicate across a network.
- **Peripheral devices** are printers, scanners and other devices that provide resources to clients across a network.
- **Hubs and switches** enable interconnection and communication between clients, servers and peripheral devices; **routers** direct data packets from a LAN to the Internet and vice versa.
- A **firewall** monitors and controls incoming and outgoing network traffic, based on pre-configured security rules.
- A **wireless access point** is a network device that enables access to the wired network for e.g. mobile devices.

Activity

Study the following:
Descriptions of common network devices and their functions.
Link: https://blog.netwrix.com/2019/01/08/network-devices-explained/
Time allocation: 15 minutes

The most common network transmission media are:

- **Twisted pair cable**: used primarily in LANs.
- **Coaxial cable**: popular for transferring data and video.
- **Fibre optic cable**: used mainly in WANs, MANs, and for provision of fibre to the home (FTTH).
- **Infrared and Bluetooth**: support wireless data transmission over short distances.
- **Radio waves**: used by WANs to cover large areas.
- **Satellite transmission**: utilises a wide spectrum of wavelengths and frequencies to support global telecommunication.

1.2.3 Network software

The network operating system (NOS) provides basic network services such as file and print sharing. More advanced services provided by the NOS support the configuration of directory services, web servers, mail servers, databases servers, and more. Popular NOSs include Windows Server, Linux Server and macOS X server. Network surveillance programs monitor internet traffic to identify potential hacking attempts or other illegal activities. Commonly used network applications include email, video conferencing and anti-virus software.

Note

Refer to Chapter 1 of Dauti (2018) for additional information and illustrations.

1.3 THE FUNCTIONS PERFORMED BY DIFFERENT TYPES OF SERVERS ON A NETWORK

1.3.1 What is a server?

A server is a computer (or a group of computers) that provides resources, data, services or application programs to other computers (known as clients) over a network. Client computers submit requests to a server, for example to transmit an email or to print a document. If the request is valid then the server will perform the required action.

1.3.2 The functions performed by different types of servers

- **File servers** store files and share them with authorised users.
- **Print servers** send files to specified printers and monitor the status of print jobs.
- **Application servers** provide authorised users with access to centrally installed software applications.
- **Domain Name System (DNS) servers** translate server names that are readable by humans into machine-readable IP addresses.
- **Mail servers** send outgoing email messages originating from client computers, and forward incoming email messages to the specified users.
- **Web servers** host applications and data that can be accessed by users via an intranet or over the Internet.
- **Database servers** host database applications and share requested data with authorised users.
- **Monitoring and management servers** monitor network traffic in order to ensure the smooth functioning of the network.

Activity

If you were setting up a small business network that included a file server, an email server, four PCs, a printer and a router, which topology would you use and why? Write down your answer and include a supporting diagram to illustrate your choice of topology.
Time allocation: 15 minutes

More recent server models include blade servers, which are smaller and easier to maintain than traditional servers; mirroring, which makes it possible to perform maintenance without shutting down the entire server; and virtual servers, where hardware and software are spread across multiple servers and storage devices.

Activity

Study the following:
The information provided in section 1.3 is based on online content available at:
Link: https://www.paessler.com/it-explained/server
Time allocation: 15 minutes

1.4 THE OSI MODEL AND THE IEEE 802 STANDARDS

1.4.1 The OSI reference model

The Open Systems Interconnection (OSI) reference model is a **conceptual** (theoretical) model, which describes the functions of the various communication layers that participate in the transmission of data across computer networks. The OSI reference model comprises seven distinct layers, each of which is responsible for a specific activity that prepares the data for the subsequent layer.

Activity

Watch the following video:
Title: What is the OSI Model (Open Systems Interconnection Model)?
Link: https://www.youtube.com/watch?v=jlp8HL_iIqo
Discuss this with your fellow students and lecturer.
Time allocation: 02:06

- **Physical layer** (Layer 1): This layer represents physical components such as network interface cards, and logical components such as network media and transmission speeds. In this layer, the Protocol Data Units (PDUs) are referred to as bits.
- **Data Link layer** (Layer 2): This layer is responsible for assigning the physical protocols to be used for communication and preparing data for transmission via the Physical layer. In this layer, the PDUs are referred to as frames.
- **Network layer** (Layer 3): This layer provides the routing mechanism between networks, based on logical elements such as IP addresses. In this layer, the PDUs are referred to as packets.
- **Transport layer** (Layer 4): This layer is responsible for transporting data between network devices and adds reliability by controlling for errors. In this layer, the PDUs are referred to as segments.
- **Session layer** (Layer 5): This layer manages and controls the synchronisation of data between applications. In this layer, the PDUs are referred to as data.
- **Presentation layer** (Layer 6): This layer receives data from the application layer, and represents it in the desired format such as text, sound or video. This layer also provides security through encryption. In this layer, the PDUs are referred to as data.

- **Application layer** (Layer 7): This layer is responsible for interacting with the operating system or application, to ensure that applications are able to utilise required network services. In this layer, the PDUs are referred to as data.

Note

To remember the order of layers 1-7 of the OSI reference model, you can use the first letter of each word in the sentence: *Please Do Not Throw Salted Peanuts Away*.

The Institute of Electrical and Electronics Engineers (IEEE) has developed a set of standards for PANs, LANs and MANs, which together are known as the IEEE 802 standards. The services and protocols specified in IEEE 802 apply only to networks that carry variable-sized packets, and map to the physical layer and the data link layer of the OSI networking reference model.

1.4.2 The TCP/IP model

The Transmission Control Protocol/Internet Protocol (TCP/IP) model is a **practical** model that combines two communication protocols. The TCP protocol ensures that the data being transmitted is reliable and correctly ordered, while the IP protocol forwards data packets from the source computer to the destination computer. The actual communication process between two computers (PC1 and PC2) works as follows:

- **Application layer**: If the user of PC1 uses a browser to access an Internet website, the Hypertext Transfer Protocol (HTTP) will process the request and forward the response to the transport layer.
- **Transport layer**: The TCP protocol packages the data received from the HTTP protocol into segments called datagrams, before forwarding them to the Internet layer.
- **Internet layer**: The IP protocol adds the source and destination IP addresses to the datagrams that have been received, at which stage they are referred to as packets. The packets are then transmitted to the network access layer.
- **Network access layer**: The Ethernet protocols (which are mostly used in LANs) organise the data into frames by adding the source and destination MAC addresses. These frames are then carried over the network to their destination.

Note

To remember the order of layers 1-4 of the TCP/IP model, you can use the first letter of each word in the sentence: *Access The Intended Network*.

Refer to Chapter 2 of Dauti (2018) for additional information and illustrations related to the OSI and TCP/IP models.

Activity

Watch the following videos:
Title: what is TCP/IP and OSI? // FREE CCNA // EP 3.
Link: https://www.youtube.com/watch?v=CRdL1PcherM
Time allocation: 12:03

Title: OSI and TCP IP Models - Best Explanation.
Link: https://www.youtube.com/watch?v=3b_TAYtzuho
Time allocation: 19:19

Summary

This topic identifies different categories of computer network, ranging in size from personal and local area networks to wide area networks including the Internet. A variety of network topologies are also described, such as bus, ring and mesh networks. This is followed by an overview of networking hardware and transmission media, as well as some examples of software that is used to support networking services. Functions that are commonly performed by computer servers are listed, accompanied by a brief explanation of the purpose of each function.

The seven layers of the Open Systems Interconnection (OSI) reference model are identified together with a brief description of the purpose of each layer. It is emphasised that the OSI reference model is a conceptual model which provides the foundation for a variety of different communication protocols. In practice, the most used of these protocols is the Transmission Control Protocol/Internet Protocol (TCP/IP) model which comprises four layers: the application layer, transport layer, internet layer, and network access layer. Supporting links to websites and YouTube videos are provided to enhance your understanding of topic 1.

Self-Assessment Questions

1. How does the OSI model help in understanding the flow of data in a computer network?

2. What are the differences between peer-to-peer and client-server network architectures?

3. What are the essential hardware and software components that make up a computer network?

Topic 2
Principles of Information Security

2.1 INTRODUCTION

This topic relates to the following module outcome:

3. Participate in the implementation of the basic principles that underpin the protection of information assets (identification, authentication, etc).

In the last two decades, computer technology has changed the way that we access and use information. Smartphones, tablets, laptops and other digital devices make it possible for us to search for information, conduct business or connect with friends 24 hours a day. However, our constant connectedness also puts us at risk; for example, hackers can gain access to confidential data, and malware such as viruses and ransomware can infect our computing devices. As an information systems practitioner, you need to understand the risks to which organisational or personal computer systems may be exposed, and the measures that are available to prevent or address those risks.

Information security "… is a set of practices intended to keep data secure from unauthorized access or alterations, both when it's being stored and when it's being transmitted from one machine or physical location to another" (Fruhlinger, 2020).

In this topic, you will gain knowledge in the following areas:
1. Confidentiality, integrity and availability
2. Identification, authentication, authorisation and access control
3. Auditing, accountability and legal/regulatory compliance

2.2 CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

Prescribed reading

Chapter 1 (pages 1-22) (Andress, 2019).

2.2.1 The CIA Triad

Confidentiality, integrity and availability (commonly referred to as the CIA Triad) are key principles that underpin information security.

- **Confidentiality** refers to the ability to prevent unauthorised users from accessing private data. Confidential data may be protected by the use of strong passwords and PIN codes, and by ensuring that the physical devices on which such data is stored are appropriately secured.
- **Integrity** refers to the ability to prevent unauthorised changes from being made to existing data, and to reverse any unauthorised changes that may have been made. Data integrity can be protected by implementing read/write restrictions or by placing restrictions on file access.
- **Availability** refers to the ability to access organisational or personal data when it is needed. Non-availability may be due to internal causes such as power outages or file corruption, or to external causes such as denial-of-service attacks.

2.2.2 The Parkerian Hexad

The Parkerian Hexad (Parker, 1998) extends the CIA Triad by adding three related principles: possession (or control), authenticity and utility. Parker also employs a slightly different definition of integrity, which for him refers to data that remains completely unchanged from its previous state; whereas the CIA Triad allows authorised changes to be made.

- **Possession** (or control) refers to the physical storage of data on media such as disk drives or magnetic tapes. If a disk drive crashes or a magnetic tape is lost, and if no backup of that data exists, then you will no longer have possession of the corresponding data.
- **Authenticity** refers to having the ability to verify the source of a particular item of information, such as an email message.
- **Utility** refers to the usefulness of an item of data. Utility is measured in terms of degree (slightly useful/extremely useful) and not in binary terms (yes/no).

2.2.3 Security attacks

In this section we consider four different types of security attack: interception, interruption, modification and fabrication. Furthermore, security attacks can be carried out on ‘data at rest’ (e.g. data that is stored on a hard drive) or ‘data in motion’ (e.g. data that is in the process of being transferred from one computer to another via email).

- **Interception attacks** allow unauthorised users to access confidential data and/or software applications, and can be difficult to detect.
- **Interruption attacks** prevent authorised users from accessing information assets, either temporarily or permanently. Such attacks may affect the integrity as well as the availability of data.
- **Modification attacks** result in unauthorised changes being made to the content of affected files. This could compromise the availability, integrity and/or confidentiality of the file contents.
- **Fabrication attacks** generate random data, fake email communications or additional processes that serve no useful purpose. Such attacks affect the integrity of the system and may also impact its availability.

2.2.4 Threats, vulnerabilities and risk

The following section explains the differences between a threat, a vulnerability, a risk, and impact.

- A **threat** is an activity that has the potential to undermine an organisation’s information security by damaging, modifying or in other ways negatively affecting an organisation’s hardware, software, data or processes.
- A **vulnerability** is a weakness within an organisation’s hardware or software systems that can result in operational inefficiency or can be exploited by external agents.
- **Risk** refers to the likelihood of an event occurring that has an undesirable outcome. For risk to exist, a threat and a vulnerability must both be present: for example, a hacker tries to access your customer database (threat) and finds that the database has been protected using a weak password (vulnerability).
- Some organisations regard **impact** as an additional risk factor that should be considered. Impact considers the value of the asset that is under threat.

Activity

Study the following article:
Title: What is the difference between a threat, a vulnerability, and a risk?
Link:https://www.sectigo.com/resource-library/what-is-the-difference-between-a-threat-a-vulnerability-and-a-risk
Time allocation: 10 minutes

2.2.5 Risk management

The risk management process usually comprises the following five steps:

1. **Identify business assets**, evaluate their importance to the organisation, and determine which business functions require the use of those assets.
2. **Identify potential threats** to the most critical assets, using a framework such as the CIA Triad or the Parkerian Hexad as a starting point.
3. **Identify vulnerabilities** based on the threats that were identified in the previous step.
4. **Assess risks** by identifying vulnerable situations that could expose the organisation to corresponding threats.
5. **Mitigate risks** by putting suitable physical, logical (technical) or administrative controls in place, and making sure those controls are enforced.

2.2.6 Incident response

What do you do if despite your best efforts, the security of your information is breached? You refer to your organisation’s **incident response plan**. The incident response plan is a document (prepared before it is needed!) that outlines the steps that should be taken to counteract a security breach that has occurred.

The incident response process has six stages:

1. In the **preparation stage**, policies and procedures are prepared that document how security breaches should be handled. The incident response plan may need to be updated after a breach has been resolved.
2. During the **detection and analysis** phase, a breach is detected, its severity is assessed, and a decision is made about how to address it.
3. The incident is resolved during the **containment, eradication and recovery** phase. Containment limits the impact of the security breach; eradication removes the threat from your system; and recovery may be required to e.g. restore data from backup media.

4. In the **post-incident** phase, you analyse how and why the breach occurred, and you determine how future occurrences can be prevented.

A comprehensive approach known as **defence in depth** is based on the creation of targeted strategies that defend individual elements of the overall computer system. For example, different defence tactics could be used to protect the external network, the internal network, the host computer, software applications and data stores. Table 1-1 on page 18 of the prescribed textbook by Andress (2019) provides a detailed overview of this approach.

Note

Table 1-1 on page 18 of the prescribed textbook by Andress (2019) provides a detailed overview of the 'defence in depth' approach.

Activity

Identify a personal 'business asset' such as a smartphone or laptop. Write notes outlining how threats, vulnerabilities and risks could affect this asset and suggest ways in which the impact of those threats, vulnerabilities and risks could be addressed.
Time allocation: 10 minutes

2.3 IDENTIFICATION, AUTHENTICATION, AUTHORISATION AND ACCESS CONTROLS

Prescribed reading

Chapters 2 and 3 (pages 23-50) (Andress, 2019).

2.3.1 Identification and authentication

The methods used to identify a person are not always reliable. Documents can be altered or forged, and the sender of an email may not be who they claim to be. For this reason, methods of **identification** may be insufficient on their own, and often require **verification**; for example, you could ask a friend or neighbour to verify your identity. However, although verification may be used to confirm a claim of identity, it is not proof. In fact, identity theft based on false information has become a business in its own right.

Authentication factors range from the use of PIN codes to authenticate the holder of an ATM card, to complex physical attributes such as fingerprints. **Multifactor authentication** uses a combination of two or more factors to establish whether a claim of identity is true. **Mutual authentication** is a software-based approach in which the client authenticates themselves to the server; and the server, in turn, authenticates the client.

Activity

Watch the following video:
Title: What is Multifactor Authentication (MFA)?
Link: https://www.youtube.com/watch?v=_3rlQVXGKZc
Time allocation: 02:30

The most used methods of identification and authentication are passwords, biometrics and hardware tokens. **Complex passwords** can provide a relatively high level of security if they are securely managed and the same password is not used for multiple accounts. **Biometric identifiers** compare a physical characteristic such as a fingerprint against a stored copy of the legitimate user's own fingerprint. A **hardware token** (sometimes called a dongle) is a physical device containing a unique identifier, that is inserted into a USB port to ensure security.

Activity

Study the following article:
Title: How identification, authentication, and authorization differ.
Link:https://www.kaspersky.com/blog/identification-authentication-authorization-difference/37143/
Time allocation: 15 minutes

Prescribed Reading

Refer to pages 29-31 of the prescribed textbook by Andress (2019) for a discussion of the characteristics of biometric factors and the metrics that are used to measure the performance of biometric systems.

2.3.2 Authorisation and access controls

After the identity of an individual has been authenticated, a decision must be made about the hardware and software resources they are allowed to access.

- **Authorisation** defines what an authenticated individual is allowed to do.
- **Access controls** determine which systems, tools and devices an authenticated individual can access. Access controls may be used to allow access to a resource, to deny access to a resource, to limit access to a resource, or to revoke existing access to a resource.
- **Physical** access controls include items like keys.
- **Logical** access controls include items like computer passwords.

Access control is generally implemented through **access control lists** (ACLs), which limit users’ access to hardware, software and physical devices. ACLs are mostly used to control access to software files and to control the flow of traffic within the network.

Note

Refer to pages 38-41 of the prescribed textbook by Andress (2019) for a detailed discussion of ACL functions and vulnerabilities.

Access control may also be based on specific capabilities that are governed by a physical or logical **token** that defines a particular set of permissions. In this case, permission to access a resource (e.g. entering a specific building or using a particular software application) is available to anybody who holds a corresponding token.

Access control models are used to manage access to organisational resources. The most used **logical** access control models are listed below.

- **Discretionary access control** (DAC): Access to a resource is determined by the owner of that resource.

- **Mandatory access control** (MAC): Access to resources is determined by a group or individual that has been authorised to grant access.
- **Rule-based access control**: Access to resources is determined by a set of rules defined by the system administrator.
- **Role-based access control**: Access to resources is based on the role of a particular user group within the organisation, e.g. salespeople and accounting staff will have different access rights.
- **Attribute-based access control** (ABAC): Access to resources is based on the attributes of a person, resource or environment. Subject attributes relate to an individual, e.g. skills and experience. Resource attributes relate mainly to operating systems and software application, e.g. required communication protocols. Environmental attributes may be used to control user access to resources, e.g. limiting the length of time for which users can access a particular resource before they need to log in again.
- **Multi-level access control**: Access to resources is managed by combining several access control models. This approach is mainly used to protect critical or highly sensitive data.

Physical access controls can be used to manage the movement of individuals or vehicles and often depend on physical barriers such as locks and booms. Access cards or badges that can be used to unlock doors are a common example. **Tailgating** refers to a situation where a user obtains legitimate access to a building or other restricted area but is immediately followed into the same building or area by an unauthorised person or vehicle. More complex systems such as airport security may involve a combination of access control methods and artefacts such as proof of identification plus a boarding pass.

Note

Refer to pages 43-49 of the prescribed textbook by Andress (2019) for a detailed discussion of access control methods and their strengths and vulnerabilities.

Activity

Identify three different examples of access controls that exist within your home and/or work environment. For each access control example, write down its purpose, evaluate its effectiveness, and make a note of any additional measures that could be taken to increase the level of security that it provides.
Time allocation: 15 minutes

2.4 ACCOUNTABILITY, AUDITING AND LEGAL/REGULATORY COMPLIANCE

Prescribed reading

Chapter 4 (pages 51-60) and Chapter 6 (pages 79-94) (Andress, 2019).

2.4.1 Accountability

The principle of **accountability** requires individuals who have access to your resources to be held responsible for their actions and to adhere to the rules that govern the use of those resources. To determine accountability, you need to refer back to the identification, authentication and authorisation rules that are associated with a particular individual. Holding people accountable is an important factor in preventing security breaches: it enables non-repudiation, it deters people from abusing organisational resources, and it helps to detect and prevent intrusions.

- **Non-repudiation** implies that you have sufficient evidence to be able to prove who was responsible for a particular activity or occurrence.
- **Deterrence** implies that people will be more likely to follow rules governing the use of resources, if they know that their actions are being monitored.
- **Intrusion detection and prevention** tools monitor organisational systems and alert technical staff to unusual or undesirable activities.

Activity

Watch the following video:
Title: How To Prevent a Security Breach in Your Business.
Link: https://www.youtube.com/watch?v=ZEl1SEa5hhA
Time allocation: 05:10

When evidence is collected for use in a legal dispute, it is important for the chain of custody to remain unbroken. A tracking system allows the original evidence to be tracked, monitored and reported.

When evidence is collected for use in a legal dispute, it is important for the chain of custody to remain unbroken. A tracking system allows the original evidence to be tracked, monitored and reported.

Prescribed reading

Refer to pages 51-55 of the prescribed textbook by Andress (2019) for a detailed discussion of methods and principles related to accountability.

2.4.2 Auditing

Internal auditing is the process of reviewing organisational records to ensure that rules governing the use of corporate resources have been complied with. In large organisations, **external audits** may be performed to ensure that your organisation meets statutory financial and regulatory requirements. Organisations may also conduct audits of software licenses and of websites that are frequently visited by employees.

- A **computer log** generates a history of the digital activities that have occurred within a specific system.
- **Monitoring** usually involves reviewing computer logs in order to identify unusual activities, usage patterns or traffic volumes.
- An **assessment audit** searches for vulnerabilities in the system in order to resolve any potential or existing problems.

Prescribed reading

Read pages 55-59 in the prescribed textbook by Andress (2019) for a detailed discussion of methods and principles related to auditing.

2.4.3 Regulatory compliance

Organisations need to comply with externally imposed rules and regulations that may affect their internal systems and processes. **Compliance** refers to an organisation’s adherence to the rules and regulations that govern a particular industry, including the information that is typically handled within that industry.

In this context, compliance is a business need, not an issue of technical security.

- **Regulatory compliance** requires adherence to the laws governing the industry in which your organisation operates. The demonstration of regulatory compliance is based on regular audits and assessment.
- **Industry compliance** involves adherence to practices that are not mandated by law, but are essential for organisations operating within a particular business context. For example, organisations must comply with the standards that have been defined for processing credit card transactions.

Activity

Watch the following video:
Title: Why good compliance equals good business.
Link: https://www.youtube.com/watch?v=MlKWd84TuzI
Time allocation: 05:07

Physical, administrative and technical controls are used to support compliance with standards and regulatory requirements.

- **Physical controls** are used to prevent or deter unauthorised access; examples include security cameras and locked doors.
- **Administrative controls** refer to processes and procedures that are implemented in order to reduce or avoid risk. For example, you may have an information security policy plus supporting documentation showing how this policy has been implemented.
- **Technical controls** use technical measures to manage risk, such as intrusion detection systems and firewalls.

The primary controls used to mitigate risk within a particular environment are referred to as **key controls**. The failure of a key control will usually affect an entire process, and it is unlikely that another control will be able to compensate for this failure. **Compensating controls** are used as a (less effective) substitute for impractical or unfeasible key controls. **Maintaining compliance** relies on a four-step process that includes monitoring existing controls, reviewing their effectiveness, documenting and analysing the review results, and reporting on the overall state of controls in the organisation.

2.4.4 Legal compliance

Relevant legislation must be taken into account when evaluating compliance. In the United States, the National Institute of Standards and Technology (NIST) promulgates standards that often provide the basis for corresponding laws and regulations. Security professionals subsequently ensure that organisations comply with these standards.

Note

Compliance standards and regulations promulgated by US government agencies fall outside the scope of this module, i.e. **you are not required to familiarise yourself** with the Federal Information Security Management Act, the Federal Risk and Authorisation Management Program, or the Health Insurance Portability and Accountability Act (outlined on pgs. 84-85 of the prescribed textbook). You are also not required to familiarise yourself with the Gramm-Leach-Bliley Act (pg. 85), the Children's Internet Protection Act (pg. 85), the Children's Online Privacy Protection Act (pg. 86), and the Family Educational Rights and Privacy Act (pg. 87).

However, the **Sarbanes-Oxley Act** (SOX) of 2002 is relevant to South African organisations. SOX regulates financial data, operations, and assets for publicly held companies, and includes specific requirements related to the gathering, retention and storage of electronic records. In addition, organisations that operate internationally need to ensure that they are familiar with relevant laws, regulations and security practices in the countries where they conduct business. For example, the **General Data Protection Regulation** (GDPR) of 2018 applies to anybody collecting data about citizens of the European Union, regardless of the country in which your own organisation is based.

Activity

Watch the following video:
Title: The Fall of Enron - Sherron Watkins.
Link: https://www.youtube.com/watch?v=v26mGyNyDpE
Time allocation: 04:13

Compliance frameworks make it easier for organisations to ensure compliance across several unrelated regulations. Use of a tried and tested framework also simplifies the audit process, since it facilitates the auditor's understanding of the program controls that have been implemented. Some internationally accepted compliance frameworks and standards are listed below.

Standards promulgated by the International Organisation for Standardisation (ISO):

- ISO/IEC 27000: Information security management systems – Overview and vocabulary.
- ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements.
- ISO/IEC 27002: Code of practice for information security controls.

Special publications issued by the US National Institute of Standards and Technology (NIST):

- SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems.
- SP 800-53: Security and Privacy Controls for Federal Information Systems and Organisations.

Note

Further information about these standards and publications is available on page 88 of the prescribed textbook by Andress (2019).

Compliance in the Cloud encompasses several different models that offer differing levels of control over the computing environment. Organisations can choose the best configuration based on their needs.

- **Infrastructure as a Service** (IaaS) provides access to virtual servers and storage. The cloud provider is responsible for risks associated with the host servers and the networks that connect those servers.
- **Platform as a Service** (PaaS) provides prebuilt servers such as database and web servers. The cloud provider is responsible for the security of the server infrastructure, as well as server configuration, backup and maintenance.
- **Software as a Service** (SaaS) provides access to specific applications or software suites. The cloud provider is responsible for the security of the servers and accompanying infrastructure including software applications.

Activity

Watch the following video:
Title: IaaS vs. PaaS vs. SaaS.
Link: https://www.youtube.com/watch?v=KgL3BfAc9Cs
Time allocation: 03:00

Some cloud providers allow clients to audit the security of their cloud environment, subject to certain conditions such as the timing and frequency of audits. Other cloud providers may share the results of their own annual external audit with their clients.

Note

You are not required to familiarise yourself with the discussion of blockchain and cryptocurrency compliance on pages 91-92 of the textbook by Andress (2019). Blockchain and cryptocurrency are addressed later in the programme.

Summary

This topic begins with a concise introduction to fundamental concepts and principles of information security, focusing on models such as the CIA Triad and the Parkerian Hexad. Four categories of security attack are identified and the potential impact of each type of attack is briefly outlined in terms of the CIA Triad. The difference between a threat, a vulnerability and a risk is explained, and the activities that are typically undertaken during the risk management and incident response processes are summarised. The concepts of identification, authentication, authorisation and access control are then defined and discussed, supported by relevant examples.

The next section of this topic emphasises the importance of accountability, explains the need for regular audits, and differentiates between regulatory versus legal requirements. It also draws attention to the importance of preserving an unbroken chain of custody when collecting evidence related to legal disputes. Finally, attention is drawn to standards promulgated by the International Organisation for Standardisation (ISO) which are particularly relevant to information security; and the risks and responsibilities of cloud-based service providers and their client organisations are clarified.

Self-Assessment Questions

1. Why are confidentiality, integrity, and availability considering the foundational principles of information security?

2. How do identification, authentication, authorisation, and access control work together to protect information systems?

3. What role do auditing, accountability, and legal compliance play in maintaining information security?

Topic 3
Operations and Human security

3.1 INTRODUCTION

This topic relates to the following module outcomes:

4. Identify the different stages of the operations security process, and the activities that occur within each stage.
5. Identify common threats affecting information security at the human level, the physical level, the network level and the application level; and outline preventative measures that can be used to eliminate or manage these threats.

Organisational data is constantly exposed to threats originating from a variety of sources, ranging from hackers, viruses, and denial of service attacks to the use of weak passwords by employees, deliberate data manipulation, or the theft of organisational data or equipment. The operations security process is intended to minimise the impact of potential threats on the security of organisational information, as illustrated in Figure 1 below:

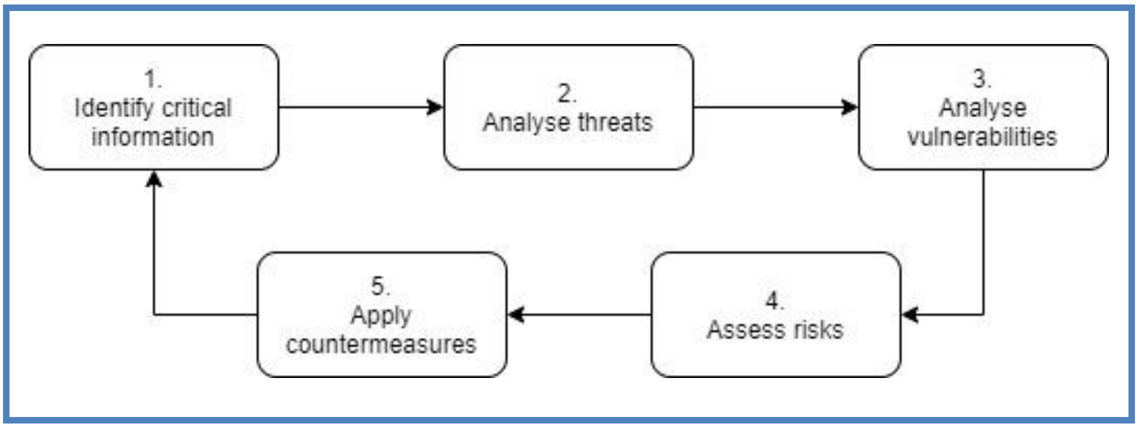

Figure 1 – The operations security process

Employees may unintentionally assist potential intruders to gain unauthorised access to organisational computing facilities; for example, criminals may gain access to confidential information by claiming to be senior managers within the organisation. In other cases, weak passwords provide easy access to hackers, or employees may be persuaded to copy confidential data for sale to outside agents.

These examples highlight the need for security training to be provided to organisational staff.

Physical threats such as intrusion by outsiders and fire or water damage also need to be anticipated and prevented. In this type of situation, the protection of human life through the implementation of efficient evacuation procedures is even more important than the protection of data and equipment.

On their own, none of these options provides a complete solution to the problem of enforcing network security. However, when the information security practices identified above are carefully planned and implemented, they can provide an effective defence against unwanted intruders.

In this topic, you will gain knowledge in the following areas:
1. Protecting the organisation against vulnerabilities and risks
2. Recognising and addressing social engineering attacks
3. Identifying physical threats and appropriate security controls

3.2 PROTECTING THE ORGANISATION AGAINST VULNERABILITIES AND RISKS

Prescribed reading

Chapter 7 (pages 95-104) (Andress, 2019).

3.2.1 The operations security process

The operations security process comprises five stages:
1. Identify information that needs to be protected.
2. Identify potential threats to that information.
3. Analyse existing system vulnerabilities.
4. Assess the potential impact of identified threats.
5. Implement countermeasures to prevent or mitigate the impact of threats.

Implementing an operations security policy is not a simple 'one size fits all' process. The security measures that you put in place should be selected based on the value to the organisation of the information that is to be protected, and the level of risk that it is likely to be exposed to.

The first step in planning an information security strategy is to assess the significance and value of the information that is generated, stored and used within your organisation. This will help you to identify the information assets that would cause the most damage to your organisation if they were exposed.

For each item of critical information that has been identified, you should consider how competitors or other outside agents might make use of it, to evaluate the potential impact of an information security breach. You will then be able to decide on appropriate countermeasures that can be implemented to either avoid or else reduce the impact of each of the threats.

It is important to remember that information security is a process, and not a once-off activity. After information security measures have been put in place, the security of the system should be monitored on an ongoing basis so that any weaknesses in the system can be identified and addressed.

Activity

Watch the following video:
Title: Operations Security.
Link: https://www.youtube.com/watch?v=c8s44iRuW6o
Time allocation: 03:00

3.2.2 The 'laws' of operations security

Three 'laws' of operations security are discussed in a paper by Haase (1992). Haase explains how these laws operate by using the analogy of a set of tools that can be used to navigate a maze that has a dragon at its centre. He summarises the three laws of OPSEC as follows:
1. If you don't know the threat, how do you know what to protect?
2. If you don't know what to protect, how do you know you are protecting it?
3. If you are not protecting it (the information), … the dragon wins!

Activity

Read the contents of the text box entitled "Operations Security and Social Media" on pages 100-101 in the prescribed textbook by Andress (2019). Then make notes outlining how social media users may unintentionally expose themselves to unwanted risks and suggest steps they can take to reduce their exposure to these risks.
Time allocation: 15 minutes

Written records that refer to operations security principles date as far back as the 6th century BCE. (BCE is the abbreviation for 'Before Common Era', a term that is replacing the old 'BC' which had religious connotations. The abbreviation 'CE' for Common Era is similarly replacing the old abbreviation of 'AD'.)

The Chinese general Sun Tzu emphasised the importance of learning as much as possible about the enemy while protecting one's own information. George Washington highlighted that small items of information that are of little value individually, can be of great value when considered in combination. And during the Vietnam war, U.S. attention was drawn to the amount of information being leaked to the enemy, from which the first operations security group emerged. Principles of operations security and competitive intelligence have since been adopted by many large organisations to inform their decisions and protect their business processes.

Prescribed reading

Read about the application of operations security principles in different contexts on pages 101-104 of the textbook by Andress (2019).

3.3 RECOGNISING AND ADDRESSING SOCIAL ENGINEERING ATTACKS

Prescribed reading

Chapter 8 (pages 107-119) (Andress, 2019).

3.3.1 Sources of information for social engineering attacks

Not all security threats can be addressed using technical solutions. For example, employees may employ weak passwords that are easily hacked – or may even record their complex password on a Post-It note stuck to their computer monitor! The office door might be left unlocked with the computer logged on, while an employee takes a coffee break. Or support staff may be fooled by somebody claiming to be a senior manager who requires urgent access to confidential data.

The best way to reduce this type of risk is by setting and enforcing appropriate policies, and by providing effective training for all staff, since social engineering attacks target people rather than technologies. Social engineers employ a variety of persuasive tactics to gain access to sensitive data. For example, social media can provide a useful starting point for identifying employees who are new to their job and may not yet be familiar with the organisational systems and senior staff; or employees who intend leaving their current employment and might be persuaded to enrich themselves at the organisation's expense. The internet makes it easy for social engineers to identify individuals who might be able to provide access to an organisation's networks or data.

Activity

Watch the following video:
Title: What is Social Engineering?
Link: https://www.youtube.com/watch?v=Vo1urF6S4u0
Time allocation: 02:02

Important sources of information used for planning social engineering attacks are human intelligence (HUMINT) and open-source intelligence (OSINT). HUMINT data is collected by talking to people about their jobs and by monitoring their routine movements and activities. OSINT data is extracted from sources such as social media, online job postings, public records, and the targeted organisation's own website. The use of search engines and other information gathering tools is discussed on pages 109-113 of the textbook by Andress (2019), along with a list of other less common approaches to intelligence gathering.

3.3.2 Types of social engineering attacks

Pretexting, phishing and tailgating are three common methods employed for social engineering attacks.

In **pretexting**, the attacker pretends to be a trusted member of the targeted organisation and uses a credible story to persuade their target (usually an employee) to perform an action that they would not be likely to do for a stranger. The success of this approach depends on having relevant information about the organisation that can be mentioned in the conversation, supported by persuasive communication skills.

Simple **phishing** attacks use phone calls to collect personal and/or organisational information from a human target. In more sophisticated phishing attacks, text messages or emails persuade the target to click on a link that will take them to a fake website that looks very similar to the 'real' site that the target thinks they are visiting. When the fake website is accessed, malware is downloaded and installed on the target's computer. However, the success rate of phishing attacks has dropped as the public has become more aware of this threat. A new variant known as **spear phishing** targets specific organisations or people and appears to originate from somebody who the target knows and trusts.

Tailgating (also known as 'piggybacking') is the practice of following a legitimate user through a controlled access point, often by pretending to have lost their access card, forgotten the password, or left the key at home.

3.3.3 Developing employee security awareness

Security training should be provided to employees at regular intervals and can be reinforced by using options like online quizzes. Important topics that should be included in a security training course include safe password management practices; the need to verify the source of suspicious phone calls or emails from unknown sources; the danger of allowing visitors or strangers to access your corporate network; and the risk of unintentionally sharing confidential information when connected to a public network.

Users should also be taught to be suspicious of malware, in particular email attachments sent by people they don't know, web links based on very short or misspelled URLs, pirated software, and smartphone applications that are not available from official download sites.

In addition, corporate policies should include rules such as:

- Whether employees may use their personal computing equipment in the workplace.
- Whether computing equipment belonging to the organisation may be taken home by employees.

- How sensitive data that is recorded on physical media should be stored and disposed of.

Security awareness can be promoted using emails or posters to inform staff of security threats that are currently doing the rounds.

3.4 IDENTIFYING PHYSICAL THREATS AND APPROPRIATE SECURITY CONTROLS

Prescribed reading

Chapter 9 (pages 121-132) (Andress, 2019).

3.4.1 Identifying physical threats and security controls

Physical security measures are intended to protect people, equipment, and data storage facilities. All relevant security threats should be identified in order for appropriate controls to be implemented. Examples of physical threats include extreme temperatures, gases, liquids, living organisms, projectiles, movement, and energy anomalies. The physical security controls that are put in place to counter these threats may have a deterrent, detective and/or preventive function.

- **Deterrent controls** are intended to discourage potential intruders from trying to gain access to your property, whether physical or digital.
- **Detective controls** monitor and report physical intrusions, or undesirable events such as a smoke alarm going off.
- **Preventive controls** such as locks, electric fences or guard dogs, make it difficult for an intruder to enter a building or other business premises.

The level of security control that is implemented in a particular location should be in decided based on the people, equipment, data and/or other assets occupying those premises.

Business continuity plans ensure that the business will continue to function despite disruptions that interfere with normal business processes. **Disaster recovery planning** anticipates the possible impact of an unforeseen disaster and lays out the steps that should be followed if a disaster occurs.

Activity

Watch the following video:
Title: What is Business Continuity Planning (BCP)?
Link: https://www.youtube.com/watch?v=ZetTrqWFE_w
Time allocation: 02:30

3.4.2 Protecting people

Humans are vulnerable to a wide range of physical threats. These include extreme temperatures (either hot or cold); fire, floods, earthquakes and hurricanes; smoke inhalation; poisonous liquids, gases or other toxins; living organisms (including the Covid-19 coronavirus); collapsed buildings; and exposure to radiation or poorly insulated energy sources. Intruders could use social engineering techniques to gain access to your physical facilities and data, or could physically attack your staff.

Evacuation plans should be updated regularly, and employees should be aware of the procedures to be followed if an emergency occurs. Essential information includes where evacuated employees should gather, the safest route for them to get the gathering place, and alternative routes in case some exits from the building are blocked or unsafe to use. In the event of an emergency evacuation, one person should be responsible for ensuring that everybody leaves the building safely; while a second person is responsible for ensuring that everybody reaches the agreed gathering point safely. All employees should understand the urgency of responding to an evacuation order as soon as the alarms have sounded, without first taking time to shut down their computers or lock their office doors.

Administrative controls that are intended to protect employees include requiring new job applicants to undergo background checks and drug tests; as well as implementing relevant policies, procedures, guidelines, regulations and laws.

3.4.3 Protecting data and equipment

Encryption is the most used method of **data protection**. However, encryption will not protect your data from damage caused by adverse physical conditions. Temperature changes, humidity, magnetic fields, electricity and physical impact can all affect the integrity of physical media.

- Strong magnetic fields can corrupt data that is stored on magnetic media.

- Magnetic media may become unusable if it is jolted while it is being read from or written to.
- Optical media may become unusable if the surface of the optical disc is scratched.

Data may still need to be accessible during a power outage or after an emergency evacuation has occurred, and the inability to access data could have serious consequences for large businesses. Implementing a redundant array of independent disks (RAID) means that your data can be reconstructed even if one of those disks fails. Replicating your data from one machine to another over a network is an even safer option. It is equally important for businesses (and individuals) to ensure that confidential data that has been stored on a computer's hard drive is destroyed before the computer is sold or otherwise disposed of.

Computer equipment may also be exposed to physical threats. The temperature inside server rooms should be monitored, since extreme temperatures can affect magnetic media. High levels of humidity can cause corrosion or lead to short-circuits in electrical equipment. Insects that find their way inside computer equipment can create unexpected problems – the original 'computer bug'. Uninterruptible power supplies remove the risk of brief power outages or damage caused by voltage fluctuations. Earthquakes and fire are particularly undesirable, and these risks should be considered when selecting a data facility site.

Security measures should be implemented both inside and outside data facilities. These measures could include vehicle control, fencing, security guards, cameras, locks, and sophisticated access control systems. Suitable environmental conditions also need to be maintained within the facility, to avoid fluctuations in temperature and humidity levels. Larger facilities are likely to include generators to ensure a constant supply of electrical power.

Activity

Create a diagram such as a mind map that illustrates the relationship between the physical threats that are identified in Chapter 9 of the prescribed textbook by Andress (2019), and the security controls that can be used to address or mitigate those threats.
Time allocation: 15 minutes

Summary

This topic opens by identifying the five stages that occur within the operations security (OPSEC) process and discussing the purpose of each stage. This is followed by a brief discussion of the three 'laws of OPSEC' defined by Haase (1992), and an example of how the operations security process can be applied in our personal lives. Additional background information provides insight into the origins of OPSEC.

Employees are often the target of social engineering attacks used by intruders to gain access to confidential information, or to persuade the employee to unintentionally download malware by clicking on a particular website link. Several commonly used social engineering techniques and their impact are discussed. This is followed by an explanation of the importance of security training programs for employees, and some policies that should be implemented to ensure that employees do not expose the organisation to social engineering attacks.

The topic ends with an overview of the physical security measures that are available to protect an organisation's employees, equipment and data facilities. Several physical threats are identified, and corresponding preventive or mitigating controls are discussed. The role of an emergency evacuation plan is explained, and key elements of the evacuation plan are outlined. Finally, issues of data availability and accessibility are discussed, together with options for securing access to data facilities and for ensuring the maintenance of suitable environmental conditions within those facilities.

Self-Assessment Questions

1. How can preventative measures be applied to manage or eliminate common information security threats?

2. What types of threats affect information security at various levels, and what are some examples?

3. How can organisations protect themselves against vulnerabilities and risks?

Topic 4
Network and Operating System security

4.1 INTRODUCTION

This topic relates to the following module outcomes:

1. Demonstrate an understanding of the Open Systems Interconnection (OSI) model and common network architectures.
2. Identify the key hardware and software components found in computer networks.
5. Identify common threats affecting information security at the human level, the physical level, the network level and the application level; and outline preventative measures that can be used to eliminate or manage these threats.

Network security is a critical component of any organisation's overall security strategy. The protection of sensitive information can be enhanced by dividing the overall network infrastructure into multiple smaller networks (also referred to as subnets). Firewalls can be used to control traffic flowing between the internet and an internal network, or to prevent unauthorised access to a subnet that contains critical data. Data traffic that is transmitted via wireless networks is particularly vulnerable and should be encrypted using a secure protocol. A variety of network scanners and tools are also available to improve network security. Events that affect network connectivity can have a significant negative impact on critical business activities; for this reason, it is important for network reliability and security to be appropriately maintained.

Operating system software manages and supports the functioning of network, data and application servers. Operating system applications play an important role in supporting network security by detecting attempted network intrusions, protecting your computer systems from malware, and blocking or reporting unauthorised traffic. Vulnerability assessment tools will inspect your systems in order to identify any weaknesses that need to be addressed. When used appropriately and monitored frequently, these types of application play an important role in ensuring network security.

In addition, the security of mobile, Internet of Things (IoT) and embedded devices needs to be protected. Mobile and fixed devices that are either permanently or semi-permanently connected to the internet are at risk of hacking or data theft. Unauthorised manipulation of embedded devices, such as sensors that activate the airbags in your car or that adjust the rate of a cardiac pacemaker, can have serious or even fatal consequences. Monitoring the security of digital appliances is likely to become increasingly important as their number and variety grows.

In this topic, you will gain knowledge in the following areas:
1. Network security
2. Operating system security
3. Security for mobile, embedded and IoT devices

4.2 NETWORK SECURITY

Prescribed reading

Chapter 10 (pages 133-144) (Andress, 2019).

4.2.1 Network design, firewalls and intrusion detection systems

Principles and technologies that support network security should be included in the design and operation of any organisational network. A relatively simple but effective option is to segment the physical network into multiple smaller networks called subnets. Network segmentation also makes it easier to monitor network traffic and identify technical problems. Choke points can be used to filter and control traffic moving from one subnet to another. The flow of data traffic into and between subnets can be controlled based on factors such as a user's level of authorisation or the department in which they are employed. The inclusion of redundancies in your network design facilitates the rerouting of network traffic in the event of e.g., the failure of a router.

Firewalls are used to control traffic that flows into and out of a network, for example where data moves from the internet into your corporate network. Internal firewalls may be used to prevent access to particular subnets in order to prevent unauthorised users from accessing sensitive data. In general, firewalls analyse the data that is moving through the network in order to determine whether it should be blocked.

- Packet filtering examines the structure of each packet of data.
- A stateful firewall only allows traffic that is part of a new or established connection.
- Deep packet inspection analyses the actual content of packets moving through the network.
- Proxy servers log the traffic that passes through them and filter out spam and malware.
- A demilitarised zone (DMZ) provides additional protection by using multiple layers of firewalls to control access to internal servers. This approach is illustrated on page 137 of the prescribed textbook by Andress (2019).

Network intrusion detection systems (IDSs) are hardware or software tools that monitor networks, hosts or applications for unauthorised activity (Andress, 2019). They detect intrusion attacks using either signature-based detection or anomaly-based detection.

- A signature-based IDS relies on a database of familiar signatures that have been used in previous intrusion attacks. However, this approach is unlikely to detect new attacks that do not match an existing signature.
- An anomaly-based IDS compares the present network traffic with 'normal' traffic to identify unusual patterns or activities. This method is good at detecting new types of attack, but it may incorrectly flag legitimate network activity that displays unusual traffic patterns.

A combination of both methods can detect unwanted attacks more reliably, but is likely to slow down the speed of network transmission.

Note

A network host is a computer device that is connected to an IP-based network. A host may also act as a server, by providing data, applications and other services to programs or devices (which are referred to as clients).

4.2.2 VPNs and wireless networks

Because attackers may be able to intercept data from either wired or wireless networks, sensitive data should always be encrypted prior to transmission. A **virtual private network** (VPN) connects a VPN application (the client) with a VPN concentrator at the other end (the server). Once the VPN client application has authenticated itself to the VPN concentrator, traffic will flow through an encrypted VPN tunnel. VPNs can also be used to protect or anonymise traffic that is being sent over untrusted or insecure connections.

Activity

Watch the following video:
Title: What is a VPN and How Does it Work? [SHORT Video Explainer]
Link: https://www.youtube.com/watch?v=_wQTRMBAvzg
Time allocation: 04:19

Locations that offer free public wireless networks may present significant security risks, since they are often set up without passwords and they do not usually provide encryption. Similar risks apply if all users share the same password, since in that case other users on the same network could potentially access your data. The Secure Shell (SSH) protocol, which is discussed in Chapter 13 of Andress (2019), provides a useful method for securing communications.

4.2.3 Network security tools

Network security should be monitored and assessed regularly, to ensure that any vulnerabilities are identified and resolved. You can test the security of your network by using the same tools that attackers would employ. Unauthorised wireless devices can present a significant security threat, and specialised detection tools should be used to identify hidden wireless access points.

Useful tools for testing the security of your network include:

- **Scanners**: hardware or software tools that search for hosts on a network, identify the operating systems in use, and detect the software versions running on open ports.
- **Packet sniffers**: specialised tools that are able to intercept, filter, sort and analyse network traffic.
- **Honeypots**: software applications that can be configured to resemble vulnerabilities in the system; they are used to attract potential attackers to identify their methods and activities.
- **Firewall tools**: these map the topology of firewalls within your system and help to locate vulnerabilities within them.

A combination of secure network design, appropriate use of firewalls, and regular monitoring using up-to-date security tools, will go a long way towards protecting the security of your network.

4.3 OPERATING SYSTEM SECURITY

Prescribed reading

Chapter 11 (pages 145-157) (Andress, 2019).

4.3.1 Managing operating system security

An operating system is a software application that supports the basic functionality of a computing device. The most commonly used operating systems for servers and desktop computers include different varieties of Linux, as well as operating systems provided by Microsoft and Apple.

The security of your operating system is a key factor in protecting your data, processes and applications against attack. Options that are available for protecting the security of your operating systems include operating system hardening, anti-malware tools, and operating system security tools.

4.3.2 Operating system hardening

Operating system hardening aims to reduce the exposure of your operating system to potential attacks. The 'attack surface' of your network refers to the number of vulnerabilities through which your operating system might be attacked. The attack surface can be reduce by implementing the following six strategies:

1. Remove all unnecessary software: Software that is seldom used and is not regularly updated, may present a vulnerability that exposes your system to attack.
2. Remove all non-essential services: Service applications are usually loaded automatically when the system starts. If you determine the purpose of each of these services, then you can then reconfigure the start-up process to exclude unwanted services.
3. Alter the default accounts: Most operating systems include default accounts such as 'guest', with standard passwords and permissions. Any such accounts

that are not actually needed should be turned off or removed. Default accounts that serve a useful purpose should have their passwords changed, and should preferably be renamed.

4. Apply the principle of least privilege: User accounts should only provide the minimum set of permissions that are needed to carry out required functions. If ordinary system users have access to administrative privileges, they could expose the network to a wide range of security vulnerabilities.
5. Perform regular software updates: This is essential to 'patch' any vulnerabilities in older software and to protect your system against new forms of malware.
6. Turn on logging and auditing features: You should record (and review) events such as users logging into and out of the system, failed login attempts, and any changes made to the operating system. Use monitoring tools to identify unusual activities.

4.3.3 Anti-malware tools

Several anti-malware tools are available to protect operating systems from attack.

- **Anti-malware applications** work by matching a file to a known malware signature, or (less effectively) by detecting unusual activity on the network. Problem files are then either deleted or 'quarantined'.
- **Executable space protection** uses a combination of hardware and software components to prevent the operating system and applications from using certain portions of the memory to execute code. This prevents some types of malware attack from functioning.
- **Software firewalls** and **host intrusion detection** add a specialised layer of intrusion detection functions to the built-in features that are provided by firewall hardware. These specialised functions generally include more complex rules and management options.

4.3.4 Operating system security tools

Security tools that can be used to assess the security of your hosts include scanners, vulnerability assessment tools and exploit frameworks.

- **Scanning tools** can be used to discover ports (devices) on which the system is listening for network connections and can then obtain information about the services and versions that are running on those ports.
- **Vulnerability assessment tools** search for network services on connected devices and then list their known vulnerabilities.
- **Exploit frameworks** are collections of network mapping tools and sniffers that take advantage of software flaws to gain access to target systems.

Activity

Watch the following video:
Title: Basics for building a System Security Plan - SSP
Link: https://www.youtube.com/watch?v=DEr5SS66Ko4
Time allocation: 03:43

The implementation of firewalls and the hardening of your operating system, supported by regular monitoring based on anti-malware and vulnerability assessment tools, are key steps towards effective network security management.

4.4 SECURITY FOR MOBILE, EMBEDDED AND IOT DEVICES

Prescribed reading

Chapter 12 (pages 159-171) (Andress, 2019).

4.4.1 Security for mobile, embedded and IoT devices

Your information security practices should extend beyond computer networks, desktop and laptop computers. Mobile phones and tablets, Internet of Things appliances and embedded monitoring devices are also vulnerable to attack.

Mobile devices include smartphones, tablets and smartwatches, most of which run iOS or Android-based operating systems. These appliances can store and transmit data and are almost always connected to a network.

- **Mobile device management systems** provide tools and features that support the centralised management of mobile devices that are owned or supplied by an organisation. These systems generally impose a predefined configuration on the device, which governs access to business resources and can disable access for devices that are non-compliant. Mobile device management solutions include options that can force users to install updates and to change their password at regular intervals, or that can block the installation of non-business-related apps.

- **Bring your own device (BYOD) policies** regulate the use of personal devices in the workplace but are more difficult to monitor.
- Most mobile devices contain a **baseband operating system** that is proprietary to the device manufacturer and handles the device's hardware. Unfortunately, operating system updates are generally provided at infrequent intervals, which leaves mobile devices vulnerable to attack.
- **Jailbreaking** a mobile device involves removing restrictions that were placed on it by the device manufacturer, which usually disables the original security features and leaves the device open to malicious apps (including some that have been designed specifically to attack jailbroken devices).

Embedded devices are 'computers' that run inside some other device, such as the controllers that activate a car's airbags in the event of a crash, or medical implants that monitor blood glucose levels in diabetic patients. Embedded devices are often used in industrial control systems (e.g., to monitor the quality of the domestic water supply). Medical devices such as cardiac pacemakers also include embedded systems.

Activity

Watch the following video:
Title: What is an Embedded System and What Does it Do?
Link: https://www.youtube.com/watch?v=d3N_Zuu2bqA
Time allocation: 01:33

Internet of Things (IoT) devices are internet-connected devices that don't run a 'full' desktop operating system. Examples of IoT devices include network printers, home security systems and environmental monitoring systems. However, because all IoT devices have a network connection, they can be difficult to secure.

Activity

Write down two innovative features involving IoT devices that could enhance the functioning or performance of self-driving vehicles.
Time allocation: 10 minutes

Summary

Careful network design is a key aspect of network security. A secure network is appropriately segmented, includes redundancies where necessary, and is protected by means of firewalls and intrusion detection systems. Network traffic is monitored and controlled, and the network as a whole is regularly tested for vulnerabilities. VPNs are used to secure data transmission across untrusted networks.

Network operating systems can be hardened by removing unnecessary software and services, changing the names (and if necessary, the privileges) of default accounts, and applying regular software updates. Anti-malware tools should be used to prevent, detect and remove malware; and any unusual network traffic or user activity should be logged.

The use of mobile devices within corporate environments should be monitored and controlled, based on organisational policies. Embedded devices, IoT devices, and other devices that have a network connection are more difficult to monitor and secure.

Self-Assessment Questions

1. How does the OSI model help in designing and securing computer networks?
2. What are the key components of network and operating system security, and why are they important?
3. What security risks are associated with mobile, embedded, and IoT devices, and how can they be mitigated?

Topic 5
Application security

5.1 INTRODUCTION

This topic relates to the following module outcomes:

3. Participate in the implementation of the basic principles that underpin the protection of information assets (identification, authentication, etc).
5. Identify common threats affecting information security at the human level, the physical level, the network level and the application level; and outline preventative measures that can be used to eliminate or manage these threats.

Ensuring that your local and web applications and databases are protected from intruders is an important aspect of network security. Application and data vulnerabilities are not always the result of inadequate network design; they may instead be a result of insecure coding practices. Appropriate input validation, combined with strong user authentication and authorisation mechanisms, will help to protect the security of your applications. In addition, encryption should be used to secure sensitive data. Software development vulnerabilities include buffer overflows, race conditions, input validation attacks, authentication attacks, authorisation attacks, and cryptographic attacks, all of which are discussed in this topic.

Web applications are particularly vulnerable to attack. Client-side web attacks often work by inserting a malicious link on a web page that is hosted on a client computer; when a user clicks on that link, the hidden code is executed. Server-side attacks are facilitated by poor input validation, inappropriate user permissions, the use of default directory names and structures, and the existence of old backup copies of source code. Databases are a common target for intruders, since they often contain sensitive data including users' personal and financial information. Potential sources of database vulnerability include the network protocols that are used to communicate with the database; the provision of database access without appropriate user credentials; insecure SQL coding practices; and privilege escalation through SQL injection. Useful tools for assessing and improving the security of your applications include sniffers, which are used to monitor patterns of network traffic; web application analysis tools, which search for insecure settings and other common vulnerabilities; and 'fuzzers', which attempt to cause an application to fail or to produce unexpected results.

Specialised vulnerability assessment tools are used to scan for vulnerabilities and assess their severity; the vendor will usually provide information regarding how to address any vulnerabilities that are detected. Vulnerability assessment usually includes at least three elements: mapping and discovery, scanning for vulnerabilities, and addressing the technological challenges presented by a cloud environment. Penetration testing is used to test a system for potential vulnerabilities, and involves five stages: scoping, recon, discovery, exploitation and reporting.

In this topic, you will gain knowledge in the following areas:

1. Software development vulnerabilities
2. Web, database and application security
3. Conducting a vulnerability assessment

Prescribed reading

Chapters 13 and 14 (pages 173-205) (Andress, 2019).

5.2 SOFTWARE DEVELOPMENT VULNERABILITIES

5.2.1 Buffer overflows, race conditions and format string attacks

Application vulnerabilities may be introduced during the software development process. The most common of these are buffer overflows, race conditions and input validation attacks (Figure 2).

- A **buffer overflow** occurs when no limit has been set on the size of a data input field. The resulting excess characters may then be used overwrite other areas in memory.
- A **race condition** occurs when multiple processes share access to a single resource that participates in a time-dependent transaction. In this situation, two processes may attempt to perform different operations on the same resource at the same time.
- **Input validation** ensures that the input submitted to an application is in the expected format. When input validation is absent, unusual input characters

might cause an application to crash or could even affect the functioning of the operating system.

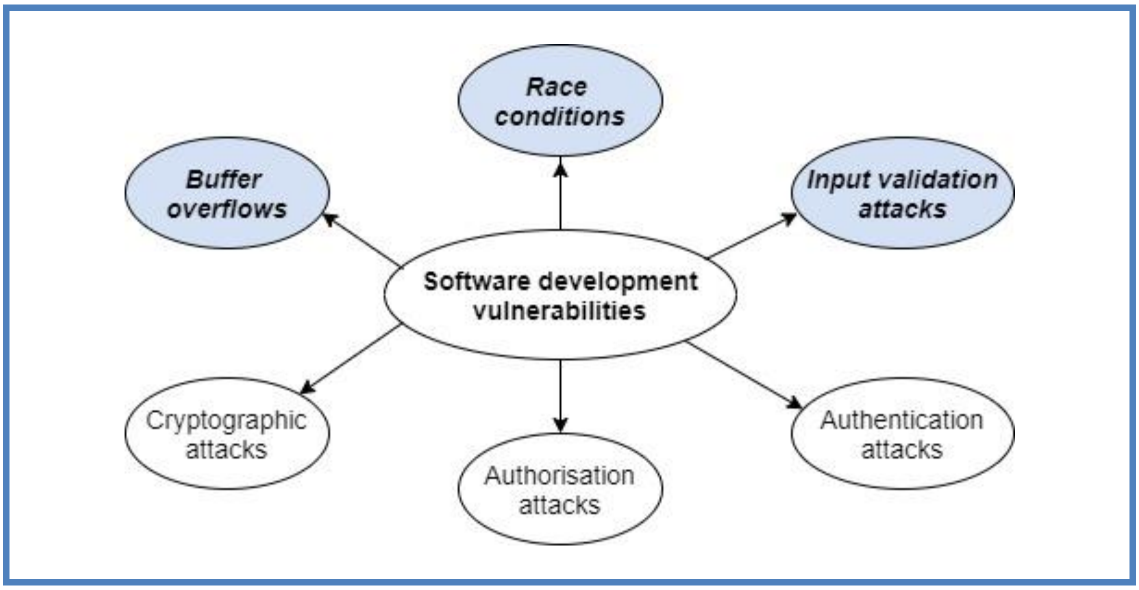

Figure 2 – Software development vulnerabilities

5.2.2 Authentication and authorisation attacks

The goal of an authentication or authorisation attack is to gain access to computing resources or privileges that the intruder is not entitled to access. These attacks relate to illegitimate attempts to gain access to restricted software applications and are not result of a flaw in the software development process (Figure 3).

- An **authentication attack** occurs when an unauthorised entity tries to impersonate a legitimate user to gain access to computing resources. To minimise this risk, legitimate users should always employ strong passwords that are difficult to crack.
- In an **authorisation attack**, an intruder tries to gain access to privileges that they are not entitled to, such as being able to perform transactions on the organisation's bank account.

Network monitoring reports should be reviewed regularly to identify any attempted security breaches related to application access.

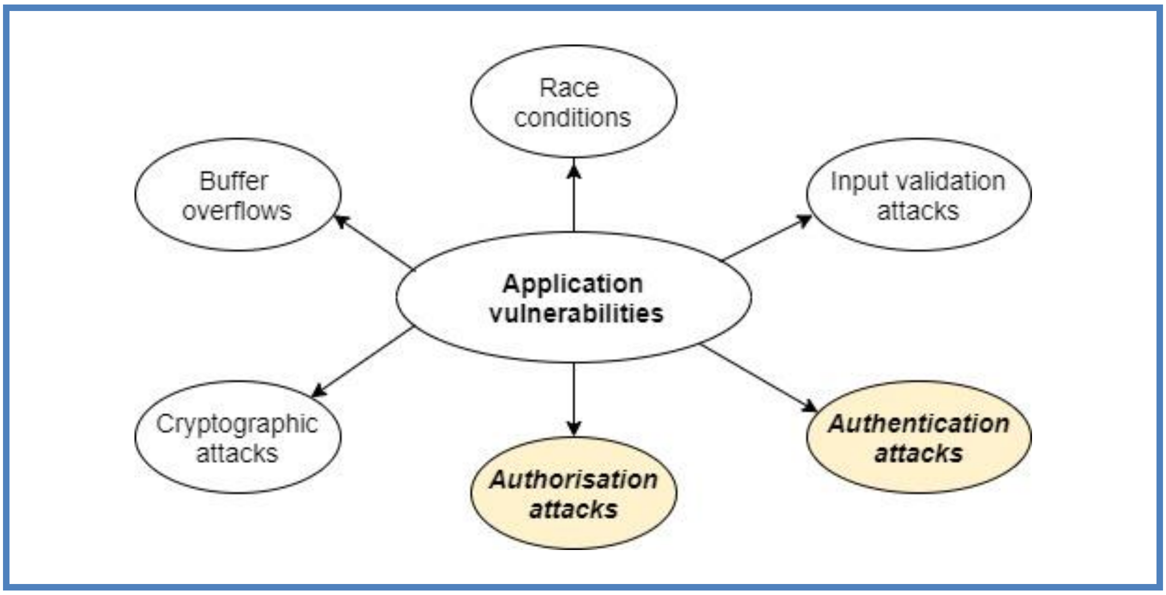

Figure 3 – Application vulnerabilities

Activity

Watch the following video:
Title: The Five Stages of Vulnerability Management.
Link: https://www.youtube.com/watch?v=LkAptpCZDlc
Time allocation: 04:19

5.2.3 Cryptographic attacks

A cryptographic attack is unlikely to succeed if you have implemented a reputable and trusted algorithm. However, you should ensure that the encryption keys can be changed if they have been exposed. The biggest risks related to cryptographic systems emerge when they have been badly implemented, or (even worse!) when individuals or organisations develop their own cryptographic algorithms.

5.3 WEB, DATABASE AND APPLICATION SECURITY

5.3.1 Web security

There are two kinds of attack that target web applications: client-side attacks and server-side attacks.

Client-side attacks usually exploit weaknesses in software applications that are loaded on client devices. Alternatively, they may use social engineering techniques to elicit user information such as logins and passwords. Common techniques that use the web to launch an attack are cross-site scripting (XSS), cross-site request forgery, and clickjacking. Installing regular browser updates will help to protect you against these threats.

- **Cross-site scripting** incorporates code written in a scripting language into a web page or other media. When a user views the web page or media, the embedded code is executed.
- **Cross-site request forgery** relies on a link located on a web page, that will execute automatically when the web page is opened, and initiate an activity on another web page where the user is currently authenticated.
- **Clickjacking** tricks users by linking a malicious control to an apparently innocent button on a web page.

Server-side attacks are generally linked to poor quality control during software development; the assignment of inappropriate user permissions; or the existence of unprotected backup of copies of source code or other technical documentation.

- **Lack of input validation** - invalid input data can be used to change directories within the server and view files that would not usually be accessible. Filtering out special characters during input validation will usually defeat this type of attack.
- **Configuration files** are used by many web applications to store user credentials for accessing the databases linked to specific applications. If these configuration files have not been secured, the related databases could be accessed and exploited.
- **'Extraneous files'** include files that were created during development, backups of earlier versions of documents or applications, technical notes, and so on, which are not currently in use. If these files need to be retained, then they should be moved to a secure directory; and unwanted files should be removed from the server.

5.3.2 Database security

Organisations have a legal responsibility to protect sensitive personal data stored in application databases. Database security issues fall into four major categories: protocol issues, unauthenticated access, privilege escalation, and arbitrary code execution (Figure 4).

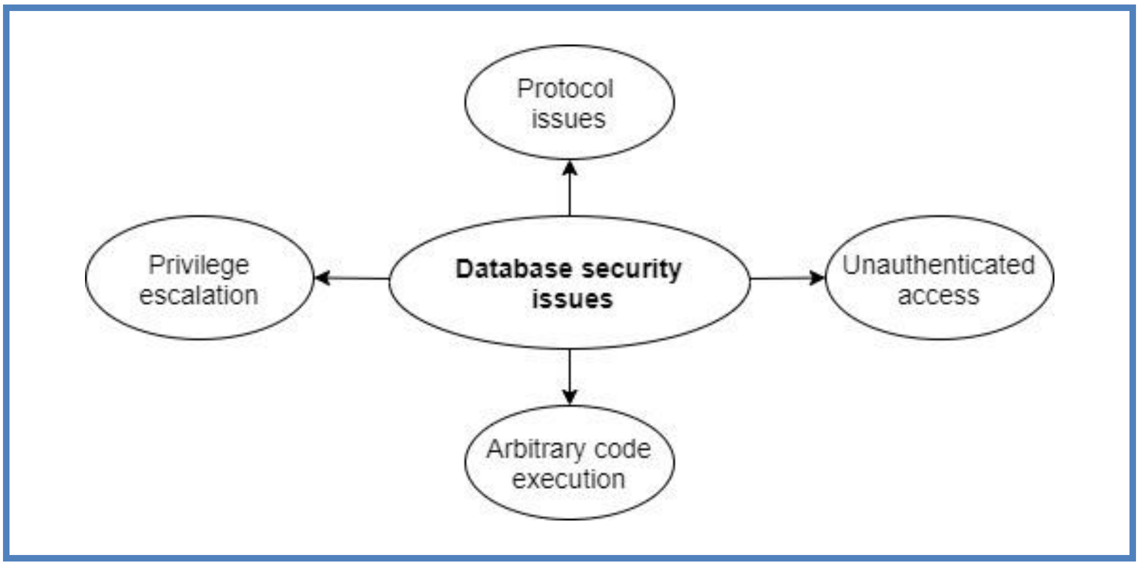

Figure 4 – Database security issues

- **Protocol issues**: The network protocols that are used to communicate with a database may contain vulnerabilities, which could be linked to software development issues such as buffer overflows. Three important steps towards protecting your organisation from protocol issues are: always use the latest version of your database software; control access to your database over the network; and limit the accounts and privileges controlling database access.
- **Unauthenticated access**: Allowing users to query a database without first supplying the appropriate access credentials is an obvious recipe for disaster. All database interactions should be restricted to authenticated and/or authorised users or processes.
- **Arbitrary code execution** allows attackers to take advantage of security weaknesses in the Structured Query Language (SQL) that is used to communicate with databases. Your best defence is to implement secure coding practices and ensure that your database software is kept up to date.
- **Privilege escalation** attacks can be carried out by submitting a SQL command to the database that allows an intruder to escalate their level of privilege. Database administrators must ensure that the privileges associated with user accounts provide an appropriate level of access and are regularly monitored.

Activity

Watch the following video:
Title: The Dangers of a Data Breach.
Link: https://www.youtube.com/watch?v=0kK902-ZvNM&t=51s
Time allocation: 02:00

5.3.3 Application security tools

A variety of tools are available for evaluating the security of your applications. These include sniffers, web application analysis tools, and fuzzers.

Sniffers monitor the network traffic that is exchanged with an application or protocol. Some sniffing tools also identify the corresponding network destinations and generate diagrams that illustrate traffic patterns.

Web application analysis tools search for vulnerabilities in web pages and applications, such as inappropriate permission settings, outdated software versions, unnecessary files, and other weaknesses that could allow an intruder to access your applications. All issues that are reported by an analysis tool must be manually verified before any action is taken.

Fuzzers identify software problems of which you were previously unaware. They operate by submitting a variety of random inputs to an application to see whether any errors or unexpected results are generated.

Activity

Study the following article:
Title: Best 10 Packet Sniffer and Capture Tools.
Link: https://www.dnsstuff.com/packet-sniffers
Summarise the “packet sniffing best practices”; briefly explain how sniffer software is used by hackers; and suggest how IT staff can protect their organisation from hackers who use packet sniffers.
Time allocation: 15 minutes

Application security can be enhanced by following secure coding guidelines, monitoring web applications for potential client-side and server-side issues, ensuring that your databases are secure, applying the principle of least privilege, and keeping your software up to date. Application security tools should be used to monitor the data that interacts with your applications and identify potential vulnerabilities that need to be addressed.

5.4 CONDUCTING A SECURITY ASSESSMENT

5.4.1 Vulnerability assessment

Vulnerability assessment tools are used to detect vulnerabilities in your platforms and applications. The assessment process includes two stages: mapping and discovery, and scanning.

The mapping and discovery stage identifies the devices that exist within your environment. Active discovery is a slow process because it is based on checking every IP address on the network; while passive scanning works by monitoring the network traffic to discover devices that are active on the network.

During the scanning stage, either an unauthenticated scan or an authenticated scan is performed on all the network devices that have been identified. An unauthenticated scan identifies all the open ports on the network, together with the services listening on those ports, and will try to determine the applications and operating systems in use. An authenticated scan requires administrative credentials so that it can collect internal information about the software that is installed, the contents of configuration files, file and directory permissions, and software patches that need to be installed.

Variations of authenticated scanning include agented scanning and application scanning. An agented scan is a simpler option than an authenticated scan. The "agent" is a small piece of software that is installed on each host; because it impersonates a system user, it doesn't require a separate set of credentials. An application scan lets you perform a deep scan on specific applications or technologies. Some challenges may be encountered when implementing and using vulnerability scanners. Providers of cloud services may restrict customers' scanning access, for example by excluding devices or software products. In addition, a cloud provider may install new hardware or applications, which could change some earlier IP addresses. Another complication relates to the use of "containers" in virtualised environments; because containers allow web servers to be easily scaled up or down depending on their level of load, they require specialised vulnerability scanning tools.

5.4.2 Penetration testing

Penetration testing is an in-depth process that uses the same tools and techniques as hackers use, in order to find and resolve any security weaknesses. It is usually performed by somebody from outside the organisation, who simulates the activities of a potential hacker. The penetration testing process has five stages: scoping, reconnaissance, discovery, exploitation, and reporting.

1. In the **scoping** stage of a penetration test, the organisation and the tester agree on what will be tested, when testing will be conducted, and the procedures to be followed when a vulnerability is detected.
2. During the **reconnaissance** ('recon') stage, the tester conducts research to find out as much as possible about the organisation that will be targeted, its environment and its systems.
3. **Discovery** is the first stage that involves active testing. Vulnerability assessment tools are used to detect open ports and associated services, and identify any that might be vulnerable to attack. Additional research may follow, based on the findings that emerge.
4. During the **exploitation** phase, the tester tries to exploit any vulnerabilities that were detected during reconnaissance or discovery. Further research may be needed if further vulnerabilities are exposed.
5. In the **reporting** stage, the tester documents the process that was followed and what was discovered. The final report describes the steps that were followed when carrying out the penetration attacks, and includes a list of issues that have a high chance of being exploited or that resulted in an actionable attack against the system.

Activity

Watch the following video:
Title: A day in the life of a Penetration Tester.
Link: https://www.youtube.com/watch?v=_NVxgQdA45g
Time allocation: 03:42

Penetration tests fall into three different categories: black-box testing, white-box testing, and grey-box testing.

- In **black-box** testing, the tester is not familiar with the testing environment, i.e., they go through the same process as a hacker would.
- In **white-box** testing, the tester is provided with detailed information about the organisation and its systems. This allows the tester to identify and focus on likely vulnerabilities.
- In **grey-box** testing, the tester is given limited information to familiarise them with the environment within which they will be testing.

Penetration tests are sometimes referred to as either internal or external. One definition state that internal testers operate from within an organisation's network environment, and external testers focus on internet-facing components. An alternative definition refers to internal testing as being conducted by in-house staff, while external testing is conducted by an independent third party. If you need to refer to either internal or external testing, it's probably a good idea to clarify which definition is being used.

The possible targets of penetration testing include web applications, networks and hardware.

Network penetration tests generally have a broad scope, ranging from hosts and web applications to engineering techniques. They are often conducted within limited time frames, in which case they are likely to be relatively superficial.

Application penetration testing focuses on applications and relies on specialised tools and skills. Static analysis examines source code and related resources; while dynamic analysis tests an application while it is running.

Physical penetration testing refers to the testing of physical security measures such as locks and alarm systems.

Social engineering penetration tests commonly include phishing attacks that target employees, and the use of tailgating to gain access to secured areas.

Hardware testing not only tests the actual device, but also tests its firmware, associated mobile apps, and the APIs (application programme interfaces) that are used to communicate with a server. Devices that are equipped with UART (Universal Asynchronous Receiver/Transmitter) or JTAG (Joint Test Action Group) debug ports, can often be manipulated without any form of authentication being required.

Vulnerability analysis and penetration testing face similar challenges. Cloud providers are often reluctant to allow testing of their resources; and skilled testers are in high demand, which means that they may not be available when needed. To counteract the latter problem, some organisations offer a reward to anybody who discovers a vulnerability in their resources (this is known as a **bug bounty program**). The organisation defines the scope within which testing can occur and then rewards the first person who identifies a new issue.

5.4.3 How realistic is your test environment?

At a simple level, the effectiveness of your existing security system can be evaluated by monitoring your everyday security tools while you are running vulnerability tools and penetration tests. These everyday security tools should include (at least) intrusion detection systems, firewalls, and anti-malware protection; and should identify and report the 'attacks' that are taking place. Effective alerting mechanisms are also needed to inform you if a security breach has been attempted.

However, more realistic testing must be performed if you want to get accurate results. In other words, vulnerability assessments and penetration tests should be approached in the same way as an attacker would conduct them. If testing is likely to have a negative impact on an organisation's production systems, then a 'mirrored' environment that matches the production environment should be set up and used for testing. Locating this replicated environment in the cloud will make it easy to test and then remove.

Since your 'attack surface' represents all the points that an attacker can use to interact with your environment, it will be changing continuously (for example, when software updates are installed) and should be retested at regular intervals. Such tests need to take into account any new tools that have become available to attackers.

You may also encounter the terms 'blue team' and 'red team' in your studies. When evaluating the security of an organisation's systems, the blue team is responsible for defending the organisation, while the red team assumes the role of the attacker. While the red team attacks the system, the blue team will record and document evidence of the red team's activities. This documentation should enable the organisation to identify and fix any security gaps that were exposed. A 'purple team' consisting of senior security personnel may sometimes be used to oversee and optimise the activities of the red and blue teams.

Activity

Study the following article:

Title: The Roles of Red, Blue and Purple Teams.

Link: https://www.advania.co.uk/blog/security/understanding-the-roles-of-red-blue-and-purple-security-teams/

Time allocation: 15 minutes

Summary

Secure coding practices play a critical role in protecting application software from vulnerabilities such as buffer overflows, race conditions, input validation attacks and authorisation attacks. Secure coding practices in conjunction with the principle of least privilege will also help to maintain database security. The enforcing of strict permissions can help to reduce server-side attacks, while patches and updates should be applied as soon as possible to client software. Application security tools can be helpful in uncovering application vulnerabilities.

Vulnerability assessment tools play a valuable role in identifying security issues in hosts and applications. Penetration testing is a more complex five-stage process that can encompass (web) applications, networks, hardware, social engineering, and physical security measures. The use of in-house 'red' and 'blue' teams builds in-house experience among employees. However, intrusion detection systems, firewalls, anti-malware and traffic monitoring systems remain essential components for providing effective protection against penetration attacks.

Self-Assessment Questions

1. Why is it important to implement identification and authentication in protecting information assets?

2. What are some common vulnerabilities in software development, and how do they affect application security?

3. What is a vulnerability assessment, and how does it help manage information security threats?

Glossary of terms

Access control list: A set of rules that determines which users can access specific folders and files.

Blade server: A chassis that can accommodate multiple server modules, thus optimising power and space usage.

Blockchain: A system that distributes transaction information across a network of linked computers, making it almost impossible to edit or delete any single entry.

Chain of custody: A record of the control, transfer and analysis of physical or electronic evidence in legal cases.

Choke point: A device such as a firewall that prevents unauthorised access to an organisational network.

CIA triad: Ensures the confidentiality, integrity and availability of data.

Data packet: An individual segment of a larger message, which is sent over the Internet and then recombined with other segments to form the complete message.

Data protection: Ensures that important data is protected from loss or corruption and can be restored to a functional state if it becomes unusable.

Domain: A network of computers and other devices that are controlled by a specific organisation and are linked to a particular IP address.

Ethernet: A wired connection that allows local area networks (LANs) and/or wide area networks (WANs) to communicate with each other.

Firewall: Controls the traffic that flows into and out of a network. Internal firewalls may be used to prevent unauthorised users from accessing sensitive data.

Fuzzer: A tool that is used to perform vulnerability assessments. It operates by submitting a variety of random inputs to an application, operating system or network to see whether any errors or unexpected results are generated

HUMINT (Human intelligence)**:** Intelligence that has been gathered from human sources.

Incident response plan: A document that outlines the steps that should be taken to counteract the impact of a security breach.

Intrusion detection system (IDS): A combination of hardware and software tools that monitor networks, hosts or applications for unauthorised activity.

IoT device (Internet of Things device): An internet-connected device such as a security camera, that doesn't run a 'full' operating system and can be difficult to secure.

Local area network (LAN): A set of computers and peripheral devices that are linked to a server either wirelessly or via a common communications line.

Logical topology: How data flows within the physical network infrastructure.

Mirroring: Allows data from a single source to be sent to multiple destinations.

Network interface card (NIC): Connects each individual computer to the network, allowing it to transmit and receive data.

Network operating system (NOS): Provides network services such as access control; file, data and application sharing; and sharing of hardware devices.

Network segmentation: Divides a physical network into multiple smaller networks (subnets), making it easier to monitor data traffic and identify problems.

Network topology: The arrangement of network nodes, cables and firewalls that can be found within a computer network. Common network topologies include bus, star, ring, mesh and tree networks.

Operations security (OPSEC): A set of practices that are intended to minimise the impact of potential threats on the security of organisational information.

Optical fibre: A technology that can send digital information over long distances, in the form of light pulses transmitted within a hollow glass or plastic 'wire'.

OSI model (Open Systems Interconnection reference model): a theoretical model that describes the functions of the various communication layers that participate in the transmission of data across computer networks.

OSINT (Open-source intelligence)**:** The analysis and interpretation of data that has been gathered from a variety of sources to generate intelligence.

Packet sniffer: Specialised software tool that can intercept, filter, sort and analyse network traffic.

Parkerian hexad: Adds the principles of possession (control), authenticity and utility to the elements of the CIA triad.

Penetration testing: An in-depth process that uses the same tools and techniques as hackers use, in order to find and resolve any security weaknesses.

Physical topology: How the different physical components within a computer network are arranged and connected.

Race condition: A situation that occurs when a system attempts to execute two sequential operations simultaneously.

Ransomware: A form of malware that encrypts the victim's files, which will only be restored to their original form after a ransom has been paid by the victim.

Repeater: A device that amplifies an existing wi-fi signal in order to cover a wider area.

Router: A switching device that is used to transmit network packages between networks and other devices.

Server: A computer that provides resources, data, services or application programs to other computers (known as clients) over a network.

Social engineering attack: A strategy employed by hackers to gain access to sensitive data by targeting people rather than technologies.

Stakeholder: A person or group of people who will be affected by the outcome of a business activity or project.

TCP/IP model (Transmission Control Protocol/Internet Protocol model): A practical model that combines two communication protocols. The TCP protocol ensures that the data being transmitted is reliable and correctly ordered, and the IP protocol forwards data packets from the source computer to the destination computer.

VPN (virtual private network): A way of protecting or anonymising data traffic that is being sent over untrusted or insecure connections.

References

Acunetix. 2017. The difference between vulnerability assessment and penetration testing. Online available: https://www.acunetix.com/blog/articles/difference-vulnerability-assessment-penetration-testing/ [Accessed: 28 June 2025].

Andress, J. 2019. Foundations of information security: A straightforward introduction. San Francisco, CA: No starch press.

APB Speakers. 2017: The fall of Enron - Sherron Watkins. [Online video] Available from: https://www.youtube.com/watch?v=v26mGyNyDpE [Accessed: 28 June 2025].

Ascend Technologies. 2020. The Five Stages of Vulnerability Management. [Online video] Available from: https://www.youtube.com/watch?v=LkAptpCZDlc [Accessed: 28 June 2025].

Careersnz. 2021. A day in the life of a Penetration Tester. [Online video] Available from: https://www.youtube.com/watch?v=_NVxgQdA45g [Accessed: 28 June 2025].

Dauti, B. 2018. CCENT/CCNA: ICND1 100-105 certification guide. Birmingham, UK: Packt Publishing Ltd. (Available via Proquest.)

DNSstuff. 2019. Best 10 packet sniffer and capture tools. Online available: https://www.dnsstuff.com/packet-sniffers [Accessed: 28 June 2025].

Drozhzhin, A. 2020. How identification, authentication, and authorization differ. Online available: https://www.kaspersky.com/blog/identification-authentication-authorization-difference/37143/ [Accessed: 28 June 2025].

Drunk_Engineer_. 2017. OSI and TCP IP models - Best explanation. [Online video] Available from: https://www.youtube.com/watch?v=3b_TAYtzuho [Accessed: 28 June 2025].

Eye on Tech. 2019. What is an Embedded System and What Does it Do? [Online video] Available from: https://www.youtube.com/watch?v=d3N_Zuu2bqA [Accessed: 28 June 2025].

Eye on Tech. 2020. What is Business Continuity Planning? [Online video] Available from: https://www.youtube.com/watch?v=ZetTrqWFE_w [Accessed: 28 June 2025].

Eye on Tech. 2020. What is Multifactor Authentication (MFA)? [Online video] Available from: https://www.youtube.com/watch?v=_3rlQVXGKZc [Accessed: 28 June 2025].

Eye on Tech. 2020. What is the OSI Model? [Online video] Available from: https://www.youtube.com/watch?v=jlp8HL_iIqo [Accessed: 28 June 2025].

Fruhlinger, J. 2020. What is information security? Definition, principles, and jobs. Online available: https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html [Accessed: 28 June 2025].

GraVoc. 2017. What is Social Engineering? [Online video] Available from: https://www.youtube.com/watch?v=Vo1urF6S4u0 [Accessed: 28 June 2025].

Haase, K.W. 1992. Kurt's laws of OPSEC. NCMS Viewpoints, 2: 46-50. Available online from: https://fas.org/sgp/library/ncms/ [Accessed: 28 June 2025].

Hargreaves, A. & Chamberlain, J. Not dated. The roles of red, blue and purple teams. Online available: https://www.itlab.com/blog/understanding-the-roles-of-red-blue-and-purple-security-teams [Accessed: 28 June 2025].

IntegrantSoftware. 2013. IaaS vs. Paas vs. Saas. [Online video] Available from: https://www.youtube.com/watch?v=KgL3BfAc9Cs [Accessed: 28 June 2025].

International Compliance Association. 2018. Why good compliance equals good business. [Online video] Available from: https://www.youtube.com/watch?v=MIKWd84TuzI [Accessed: 28 June 2025].

Kaspersky. 2017. The Dangers of a Data Breach. [Online video] Available from: https://www.youtube.com/watch?v=0kK902-ZvNM&t=51s [Accessed: 28 June 2025].

Let's Talk About I.T. 2021. How To Prevent a Security Breach in Your Business. [Online video] Available from: https://www.youtube.com/watch?v=ZEl1SEa5hhA [Accessed: 28 June 2025].

Lush, J. 2019. Basics for building a System Security Plan. [Online video] Available from: https://www.youtube.com/watch?v=DEr5SS66Ko4 [Accessed: 28 June 2025].

Melnick, J. 2019. Network devices explained. Online available: https://blog.netwrix.com/2019/01/08/network-devices-explained/ [Accessed: 28 June 2025].

NetworkChuck. 2020. What is TCP/IP and OSI? [Online video] Available from: https://www.youtube.com/watch?v=CRdL1PcherM [Accessed: 28 June 2025].

Ordr.net. Not dated. 10 internet of things (IoT) healthcare examples. Online available: https://ordr.net/article/iot-healthcare-examples/ [Accessed: 28 June 2025].

Paessler. Not dated. IT explained: Server. Online available: https://www.paessler.com/it-explained/server [Accessed: 28 June 2025].

Parker, D. B. 1998. Fighting computer crime. Wiley, Hoboken, NJ.

PowerCert Animated Videos. Not dated. Network Topologies (Star, Bus, Ring, Mesh, Ad hoc, Infrastructure, & Wireless Mesh Topology). [Online video] Available from: https://www.youtube.com/watch?v=zbqrNg4C98U&t=4s [Accessed: 28 June 2025].

PowerCert Animated Videos. Not dated. Network Types: LAN, WAN, PAN, CAN, MAN, SAN, WLAN. [Online video] Available from: https://www.youtube.com/watch?v=4_zSIXb7tLQ [Accessed: 28 June 2025].

PowerCert Animated Videos. Not dated. What is a Server? Servers vs Desktops Explained. [Online video] Available from: https://www.youtube.com/watch?v=UjCDWCeHCzY [Accessed: 28 June 2025].

Sectigo. 2020. What is the difference between a threat, a vulnerability, and a risk? Online available: https://sectigo.com/resource-library/what-is-the-difference-between-a-threat-a-vulnerability-and-a-risk [Accessed: 28 June 2025].

Sophos. 2020. The state of ransomware 2020. Online available: https://www.ccsmedia.com/partnernews/the-state-of-ransomware-2020/ [Accessed: 28 June 2025].

Staying Safe LLC. 2018. Operations Security. [Online video] Available from: https://www.youtube.com/watch?v=c8s44iRuW6o [Accessed: 28 June 2025].

Symanovich. 2020. What is a VPN? Online available: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html [Accessed: 28 June 2025].

Varteq Inc. Not dated. Unveiling the potential of embedded development for healthcare. Online available: https://varteq.com/unveiling-the-potential-of-embedded-development-for-healthcare/ [Accessed: 28 June 2025].

vpnMentor. 2017. What is a VPN and How Does it Work? [Online video] Available from: https://www.youtube.com/watch?v=_wQTRMBAvzg [Accessed: 28 June 2025].

Wikipedia. 2020. Host (network). Online available: https://en.wikipedia.org/wiki/Host_(network) [Accessed: 28 June 2025].

Wikipedia. 2020. Internet of things. Online available: https://en.wikipedia.org/wiki/Internet_of_things [Accessed: 28 June 2025].

Wikipedia. 2020. Parkerian hexad. Online available: https://en.wikipedia.org/wiki/Parkerian_Hexad [Accessed: 28 June 2025].

Answers to Self-Assessment Questions

TOPIC 1 – SELF-ASSESSMENT ANSWERS

1. How does the OSI model help in understanding the flow of data in a computer network?

The OSI model provides a structured framework that breaks down the process of data communication into seven distinct layers, from the physical transmission of bits (Layer 1) to the application-level interactions (Layer 7). This model helps students and IT professionals conceptualise how data travels across a network, identify where problems may occur, and understand the roles of various protocols and devices at each layer. By studying the OSI model, learners can more easily diagnose network issues and design efficient communication systems.

2. What are the differences between peer-to-peer and client-server network architectures?

Peer-to-peer (P2P) networks allow all devices to share resources directly without a central server, making them cost-effective and easier to set up for small environments. In contrast, client-server networks centralise services and data through one or more dedicated servers, enhancing scalability, security, and manageability, which is ideal for larger or enterprise-level networks. Understanding these architectures helps in selecting the appropriate network setup based on an organisation’s size, budget, and security needs.

3. What are the essential hardware and software components that make up a computer network?

A typical computer network includes key hardware components such as routers, switches, network cables, and network interface cards (NICs), which enable connectivity and data routing. On the software side, components like network operating systems, firewalls, and protocol software (e.g., TCP/IP) manage communication, enforce security, and ensure reliable data transfer. Recognising these elements and how they interact is crucial for building, maintaining, and troubleshooting effective networks.

TOPIC 2 – SELF-ASSESSMENT ANSWERS

1. Why are confidentiality, integrity, and availability considering the foundational principles of information security?

Confidentiality, integrity, and availability—collectively known as the CIA triad—form the cornerstone of information security. Confidentiality ensures that sensitive information is accessible only to authorised users, integrity guarantees that data remains accurate and unaltered, and availability ensures that information and systems are accessible when needed. These principles guide security policies and controls, helping organisations protect their information assets from threats such as data breaches, tampering, or service disruptions.

2. How do identification, authentication, authorisation, and access control work together to protect information systems?

These four elements function as a layered approach to safeguard systems. Identification establishes who a user claims to be, authentication verifies that claim (e.g., through passwords or biometrics), authorisation determines what resources the user is allowed to access, and access control enforces those permissions. Together, they help prevent unauthorised access, ensuring that only legitimate users can interact with systems and data according to their roles and privileges.

3. What role do auditing, accountability, and legal compliance play in maintaining information security?

Auditing and accountability ensure that all actions within a system can be traced to specific users, promoting transparency and deterring malicious behaviour. Logs and audit trails allow organisations to detect and investigate suspicious activities. Legal and regulatory compliance, such as adherence to POPIA or GDPR, ensures that organisations meet mandatory data protection standards. These elements not only support internal security practices but also build stakeholder trust and reduce the risk of legal penalties.

TOPIC 3 – SELF-ASSESSMENT ANSWERS

1. How can preventative measures be applied to manage or eliminate common information security threats?

Preventative measures should be tailored to the level of threat. For human threats, user education and strict access control are key. Physical threats can be mitigated with locked server rooms, CCTV, and environmental controls. Network threats require firewalls, intrusion detection/prevention systems, and secure protocols, while application-level threats are best managed through secure coding practices, regular updates, and vulnerability scanning. By applying the appropriate safeguards at each level, organisations can significantly reduce the risk of security breaches.

2. What types of threats affect information security at various levels, and what are some examples?

Threats exist at multiple levels: human threats include social engineering, phishing, and insider negligence; physical threats involve theft, damage, or unauthorised access to hardware; network-level threats include denial-of-service (DoS) attacks, eavesdropping, or IP spoofing; and application-level threats may involve SQL injection, malware, or insecure coding. Each threat type exploits specific vulnerabilities, making it essential to implement layered defences such as employee training, physical security measures, firewalls, encryption, and secure software development practices.

3. How can organisations protect themselves against vulnerabilities and risks?

Organisations can protect against vulnerabilities and risks by adopting a proactive, layered security approach. This includes conducting regular risk assessments, patching software promptly, implementing strong access controls, and using firewalls and encryption to safeguard data. Security policies should be regularly updated, and employees should be trained to follow best practices. By identifying potential weaknesses before they are exploited, organisations can reduce their attack surface and improve their overall resilience to cyber threats.

TOPIC 4 – SELF-ASSESSMENT ANSWERS

1. How does the OSI model help in designing and securing computer networks?

The OSI model breaks network communication into seven layers, from the physical layer to the application layer, allowing for a structured approach to both network design and security. By understanding each layer's function, network administrators can implement targeted security controls, such as encryption at the transport layer or firewalls at the network layer, to protect data and manage traffic effectively. This layered understanding also helps in diagnosing issues and ensuring that vulnerabilities are addressed at the appropriate level.

2. What are the key components of network and operating system security, and why are they important?

Key components of network security include firewalls, intrusion detection and prevention systems, secure protocols (e.g., HTTPS, VPN), and strong authentication methods. Operating system security involves regular updates, patch management, user account control, file system permissions, and antivirus software. Together, these components protect the network infrastructure and endpoints from unauthorised access, malware, and exploitation, ensuring that systems remain stable, secure, and compliant with security policies.

3. What security risks are associated with mobile, embedded, and IoT devices, and how can they be mitigated?

Mobile, embedded, and IoT devices often lack robust security features, making them vulnerable to unauthorised access, data interception, and malware. Common risks include weak passwords, unpatched firmware, and lack of encryption. To mitigate these risks, organisations should enforce strong authentication, apply regular updates, segment IoT devices on the network, and disable unnecessary services. Security policies must also account for the unique challenges posed by these devices, especially as they increasingly interact with critical systems and sensitive data.

TOPIC 5 – SELF-ASSESSMENT ANSWERS

1. Why is it important to implement identification and authentication in protecting information assets?

Identification and authentication are essential for verifying user identities and controlling access to sensitive systems and data. Identification establishes who the user is, while authentication ensures that the user is who they claim to be, typically through passwords, biometrics, or multi-factor methods. Together, they help prevent unauthorised access, reduce insider threats, and support auditing and accountability. Properly implemented, these mechanisms form the first line of defence in safeguarding an organisation's digital assets.

2. What are some common vulnerabilities in software development, and how do they affect application security?

Common software development vulnerabilities include buffer overflows, insecure input handling (such as SQL injection), weak authentication, and poor session management. These flaws can be exploited by attackers to gain unauthorised access, modify data, or disrupt system functionality. Secure coding practices, regular code reviews, automated testing, and adherence to secure development frameworks are critical to minimising these vulnerabilities and ensuring application security throughout the development lifecycle.

3. What is a vulnerability assessment, and how does it help manage information security threats?

A vulnerability assessment is a systematic process of identifying, evaluating, and prioritising weaknesses in an organisation's systems, networks, or applications. It helps uncover known flaws that could be exploited by attackers, such as outdated software, misconfigured settings, or exposed services. By conducting regular assessments, organisations can proactively address these issues through patching, configuration changes, or additional security controls; ultimately reducing their risk exposure and strengthening overall security posture.