First published in 2026 by UE Campus

Unit specifications can be found on the UE Campus Portal: https://uecampus.com/

Contents

Using your Study Guide

Welcome to the study guide, designed to support you in completing your Level 4 Diploma in Cyber Security.

This study guide follows the order of the syllabus, which is the basis for your studies. Each chapter starts by listing the syllabus learning outcomes covered and the assessment criteria.

Level 4 Units

The Level 4 Diploma in Cyber Security consists of the following units:

Unit Title	Credits	Status
Cyber Security Threat and Risk	20	Mandatory
Network Security and Data Communications	20	Mandatory
Database Security and Computer Programming	20	Mandatory
Incident Response, Investigations and Forensics	20	Mandatory
Security Strategy: Laws, Policies and Implementation	20	Mandatory
Cyber Security Threats and Risk: Banking and Finance	20	Optional
Cyber Wars	20	Optional

The study guide includes a number of features to enhance your studies:

📝	**'Over to you:'** activities for you to apply what you have learned.
🌍	**'Industry Insights:'** discover up-to-date trends, expert opinions, and real-world examples from leading organisations in the cyber security industry.
🧭	**'Did you know?'** highlights interesting facts or surprising information to deepen your understanding of network security concepts.
💼	**'Case studies:'** realistic business scenarios to reinforce and test your understanding.
❗	**'Need to know:'** key pieces of information highlighted in the text.
💡	**'Examples:'** illustrating points made in the text to show how it works in practice.

Note: Website addresses current as of March 2026.

Level 4 Network Security and Data Communications

About this unit

This unit examines the component parts of digital communications and their interoperability with IT networks, hardware, firmware and software components. You will explore the inherent insecurity of the internet and understand the basics of how computers communicate with one another across local and wide area networks.

The unit addresses fundamental questions that every cyber security professional must be able to answer: How do computers and digital devices communicate? What makes networks vulnerable to attack? How can we design security architectures that are proactive and resilient rather than reactive and fragile?

The second half of this unit focuses on security planning and core concepts including security engineering, systems hardening and cyber resilience. You will evaluate both the technical and process-based defences available to organisations, and learn how to apply key security concepts such as the CIA triad, defence in depth, and change and configuration management within large, distributed organisations.

By the end of this unit, you will be able to analyse network vulnerabilities, evaluate security engineering approaches, assess internal risks, and recommend holistic strategies for network and systems resilience.

Unit code: **K/617/1130**

RQF level: **4**

Credits: **20**

Assessment: **Written Assignment – Network Security Architecture and Resilience Report**

Chapter One – How Computers and Digital Devices Communicate

Introduction

This chapter provides the foundational knowledge of computer networking that underpins all network security practice. You will explore how data is transmitted across networks, examine the protocols and standards that govern digital communications, and analyse the core vulnerabilities that exist within network and online environments. You will also investigate how the emergence of security thinking and tools has evolved to benefit network environments.

Understanding how networks operate is essential because you cannot defend what you do not understand. Every firewall rule, intrusion detection signature, and access control policy is ultimately about controlling how data moves between devices – and that requires a thorough grasp of networking fundamentals.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand how computers and digital devices communicate with one another over a network.**

Assessment Criteria

1.1 Analyse the core vulnerabilities within a network environment and an online environment.

1.2 Explain how the emergence of security thinking and tools can benefit a network environment.

1.1 Core vulnerabilities within network and online environments

Over to you – Video Watch: How the Internet Works

Watch this YouTube video:

Title: How Does the Internet Work? – Glad You Asked (Vox)

Link: https://youtu.be/x3c1ih2NJEg?si=pUddgYBx461R29Zr

After watching, draw a simple diagram showing how a request from your browser reaches a web server and returns a response. Label each key component (router, ISP, DNS server, web server). Identify at least two points in this journey where the data could be intercepted.

Network Fundamentals: How Computers Communicate

A computer network is a collection of interconnected devices that can exchange data and share resources. Networks range from small local area networks (LANs) connecting devices within a building to vast wide area networks (WANs) spanning continents. The internet is the largest WAN, connecting billions of devices globally through a complex infrastructure of cables, routers, switches, and wireless access points.

For devices to communicate, they must agree on a common set of rules, known as protocols. The most fundamental networking model for understanding these protocols is the OSI (Open Systems Interconnection) model, which divides network communication into seven layers:

Layer	Name	Function and Security Relevance
7	Application	End-user services (HTTP, HTTPS, FTP, SMTP, DNS). Vulnerable to SQL injection, cross-site scripting (XSS), phishing, and application-layer DDoS attacks.
6	Presentation	Data formatting, encryption, and compression (SSL/TLS). Vulnerable to SSL stripping and downgrade attacks.
5	Session	Session management and authentication. Vulnerable to session hijacking, cookie theft, and replay attacks.
4	Transport	End-to-end delivery and flow control (TCP, UDP). Vulnerable to SYN flood attacks, port scanning, and TCP session hijacking.
3	Network	Logical addressing and routing (IP, ICMP). Vulnerable to IP spoofing, routing table poisoning, and ICMP-based attacks (e.g. ping of death, smurf attacks).
2	Data Link	Physical addressing (MAC) and frame delivery (Ethernet, Wi-Fi). Vulnerable to ARP spoofing, MAC flooding, and VLAN hopping.
1	Physical	Transmission of raw bits over physical media (cables, wireless signals). Vulnerable to wiretapping, electromagnetic interference, and physical tampering.

Did you know?

The OSI model was developed by the International Organisation for Standardisation (ISO) in 1984. While no real-world protocol stack maps perfectly to all seven layers, the model remains the most widely used framework for understanding and troubleshooting network communications. The TCP/IP model, which condenses the seven layers into four (Network Access, Internet, Transport, and Application), more closely reflects how the internet actually operates.

Key Network Protocols and Their Vulnerabilities

Every network protocol was designed to solve a communication problem, but many were created before security was a primary concern. Understanding these protocols and their inherent weaknesses is essential for network security professionals.

- **TCP/IP (Transmission Control Protocol/Internet Protocol)** – the foundational protocol suite of the internet. TCP provides reliable, ordered delivery of data between applications, while IP handles addressing and routing. TCP was designed for reliability, not security – it transmits data in cleartext by default, and the three-way handshake (SYN, SYN-ACK, ACK) can be exploited through SYN flood attacks that exhaust server resources.

- **DNS (Domain Name System)** – translates human-readable domain names into IP addresses. DNS was designed without authentication, making it vulnerable to DNS spoofing (redirecting users to malicious sites), DNS cache poisoning, and DNS amplification attacks (using DNS servers to amplify DDoS traffic).
- **HTTP/HTTPS (HyperText Transfer Protocol)** – the protocol for web communication. HTTP transmits data in plaintext, allowing anyone monitoring the network to read the contents. HTTPS adds TLS (Transport Layer Security) encryption but is still vulnerable to certificate forgery, SSL stripping, and misconfigured cipher suites.
- **DHCP (Dynamic Host Configuration Protocol)** – automatically assigns IP addresses to devices on a network. Vulnerable to DHCP starvation attacks (exhausting the pool of available addresses) and rogue DHCP server attacks (directing clients to malicious gateways).
- **ARP (Address Resolution Protocol)** – maps IP addresses to MAC addresses on a local network. ARP operates on trust with no authentication, making it vulnerable to ARP spoofing (poisoning the ARP cache to redirect traffic through an attacker's machine).
- **SMTP (Simple Mail Transfer Protocol)** – used for sending email. Originally designed without encryption or authentication, SMTP is vulnerable to email spoofing, open relay abuse, and interception of email content in transit.
- **Wi-Fi (IEEE 802.11)** – wireless networking protocols that transmit data over radio waves. Older security standards such as WEP and WPA have been comprehensively broken, and even WPA2 was found to be vulnerable to the KRACK attack in 2017. WPA3 provides improved security but adoption remains incomplete.

> **! Need to know – The Inherent Insecurity of the Internet**
>
> The internet was designed in the late 1960s as ARPANET, a research network connecting trusted academic and military institutions. Security was not a design priority because the users were trusted and the network was small. Many of the protocols still in use today (TCP/IP, DNS, BGP, SMTP) inherited this trust-based design. The core challenge of network security is retrofitting security onto an infrastructure that was never designed to be secure.

Network Topologies and Their Security Implications

The physical and logical arrangement of a network (its topology) has significant implications for security. Common topologies include:

- **Star topology** – all devices connect to a central switch or hub. The central device is a single point of failure but also a convenient point for monitoring and applying security controls. Most modern LANs use this topology.
- **Bus topology** – all devices share a single communication line. Any device can see all traffic on the bus, creating significant eavesdropping risks. Largely obsolete in modern wired networks but conceptually similar to shared Wi-Fi.
- **Mesh topology** – devices are interconnected with multiple paths between them. Provides redundancy and resilience but increases complexity and the number of potential attack surfaces. The internet itself is a partial mesh.
- **Ring topology** – devices are connected in a circular chain. A single link failure can disrupt the entire network unless dual-ring redundancy is implemented.

In practice, most organisations use hybrid topologies that combine elements of these models. Understanding the topology of a network is essential for identifying potential attack paths and designing effective security controls.

Over to you – Network Mapping Activity

Using a free tool such as draw.io (https://app.diagrams.net/), create a network diagram for a small business with the following components: a broadband internet connection, a firewall, a managed switch, a Wi-Fi access point, a file server, a network printer, and ten desktop computers. Label each device and connection. For each connection, identify at least one potential vulnerability.

Common Network Vulnerabilities

Network vulnerabilities can be categorised into several broad areas:

- **Configuration weaknesses** – default passwords, unnecessary open ports, unpatched firmware, insecure protocol configurations, and overly permissive firewall rules. Misconfiguration is consistently cited as one of the top causes of security breaches.
- **Design weaknesses** – flat network architectures without segmentation, lack of network monitoring, absence of redundancy, and insufficient access controls. Poor network design can allow an attacker who compromises one device to move laterally across the entire network.
- **Protocol weaknesses** – inherent vulnerabilities in network protocols (as discussed above), including lack of encryption, weak authentication, and susceptibility to spoofing and injection attacks.
- **Wireless vulnerabilities** – rogue access points, evil twin attacks (setting up a fake Wi-Fi network with a legitimate-sounding name), deauthentication attacks, and weak encryption. Wireless networks extend the physical boundary of the network beyond the organisation's premises.
- **Physical vulnerabilities** – unsecured server rooms, exposed network cabling, unlocked network ports, and lack of physical access controls. Physical access to network infrastructure often enables complete compromise.
- **Human vulnerabilities** – social engineering, insider threats, poor password hygiene, and lack of security awareness training. The human element remains the weakest link in most network security implementations.

Case Study – The Target Data Breach (2013)

In late 2013, retail giant Target suffered a massive data breach that compromised 40 million payment card records and the personal information of 70 million customers. The attack began when hackers stole credentials from a third-party HVAC contractor that had network access to Target's systems. The attackers then exploited a flat network architecture to move laterally from the contractor's access point to Target's point-of-sale systems, where they installed malware to capture card data. Target's security monitoring system (FireEye) generated alerts, but they were not acted upon.

Task: (1) What network design failures allowed the attackers to reach the POS systems? (2) How would network segmentation have mitigated this attack? (3) Why were the security alerts not acted upon, and what organisational factors contributed? (4) Calculate

the estimated total cost of this breach (research the settlement amounts, legal fees, and lost revenue). Write your analysis in 500 words.

1.2 The emergence of security thinking and tools

Network security has evolved from an afterthought to a strategic business priority. Understanding this evolution helps contextualise why certain tools and approaches exist and how they complement one another.

The Evolution of Network Security

The history of network security can be traced through several distinct eras:

- **The Trust Era (1960s–1980s)** – early networks operated on trust. ARPANET connected a small number of known institutions, and security was primarily about physical access control. The Morris Worm (1988), one of the first major internet worms, exposed the vulnerability of this trust-based model.
- **The Perimeter Era (1990s–2000s)** – as the internet commercialised, organisations adopted a castle-and-moat approach: firewalls protected the network perimeter, and everything inside the perimeter was considered trusted. Intrusion Detection Systems (IDS) and antivirus software emerged during this period.
- **The Defence in Depth Era (2000s–2010s)** – organisations recognised that a single perimeter was insufficient. The defence in depth model introduced multiple layers of security controls, including network segmentation, DMZs (demilitarised zones), VPNs, and multi-factor authentication.
- **The Zero Trust Era (2010s–present)** – the dissolution of traditional network perimeters (driven by cloud computing, mobile devices, and remote work) has led to the Zero Trust model, which assumes no user or device should be trusted by default, regardless of their location. Every access request must be verified, validated, and authorised.

Industry Insight – Zero Trust Architecture

Major technology companies and government agencies have adopted Zero Trust as their primary security architecture. In 2022, the US Government issued Executive Order 14028, mandating that federal agencies adopt Zero Trust principles. Google's BeyondCorp initiative demonstrated that a large enterprise could operate securely without a traditional VPN-based perimeter. The core principle is 'never trust, always verify' – every user, device, and network flow must be authenticated and authorised before access is granted.

Read more: NIST SP 800-207 Zero Trust Architecture: https://csrc.nist.gov/publications/detail/sp/800-207/final

Key Network Security Tools

A comprehensive network security strategy employs multiple tools working in concert:

- **Firewalls** – control traffic flow between networks based on predetermined rules. Next-Generation Firewalls (NGFWs) add application awareness, intrusion prevention,

and threat intelligence capabilities. Firewalls can be hardware appliances, software-based, or cloud-native.

- **Intrusion Detection and Prevention Systems (IDS/IPS)** – monitor network traffic for suspicious activity. IDS detects and alerts; IPS detects and actively blocks. Signature-based systems match known attack patterns, while anomaly-based systems identify deviations from normal behaviour.
- **Virtual Private Networks (VPNs)** – create encrypted tunnels for secure communication over untrusted networks. Site-to-site VPNs connect office locations; remote access VPNs allow individual users to connect securely. Common protocols include IPsec, OpenVPN, and WireGuard.
- **Network Access Control (NAC)** – enforces security policies on devices seeking to access the network. NAC can check for updated antivirus, current patches, and compliance with security policies before granting access.
- **Security Information and Event Management (SIEM)** – aggregates and analyses log data from across the network to identify security incidents. Modern SIEMs use machine learning and user behaviour analytics to detect sophisticated threats.
- **Network segmentation and micro-segmentation** – dividing the network into isolated segments to limit lateral movement. Micro-segmentation applies this principle at the workload level, controlling traffic between individual applications and services.
- **Web Application Firewalls (WAF)** – specifically protect web applications by filtering and monitoring HTTP/HTTPS traffic, blocking common attacks such as SQL injection, XSS, and cross-site request forgery (CSRF).
- **Data Loss Prevention (DLP)** – monitors and controls data in motion, at rest, and in use to prevent sensitive information from leaving the organisation through unauthorised channels.

Over to you – Video Watch: Firewalls Explained

Watch this YouTube video:

Title: Firewalls Explained – PowerCert Animated Videos

Link: https://youtu.be/kDEX1HXybrU?si=uTMezdqqFyl5s_X3

After watching, explain the difference between a packet-filtering firewall, a stateful inspection firewall, and a next-generation firewall. Which would you recommend for a small business with 50 employees, and why?

Over to you – Tool Exploration Activity

Visit the Wireshark website (https://www.wireshark.org/) and download the free network protocol analyser. Capture network traffic from your own device for 5 minutes. Identify: (a) the protocols visible in the capture, (b) any unencrypted data being transmitted, (c) the IP addresses your device communicates with, and (d) any potential security concerns you observe. Write a 300-word analysis of your findings.

Note: Only capture traffic on networks you own or have permission to monitor.

Reading List

- Kurose, J.F. and Ross, K.W. (2022) *Computer Networking: A Top-Down Approach.* 8th edn. Harlow: Pearson.
- Stallings, W. (2024) *Network Security Essentials: Applications and Standards.* 7th edn. Harlow: Pearson.
- Tanenbaum, A.S. and Feamster, N. (2021) *Computer Networks.* 6th edn. Harlow: Pearson.
- Forshaw, J. (2023) *Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation.* 2nd edn. San Francisco, CA: No Starch Press.
- Sanders, C. (2022) *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems.* 4th edn. San Francisco, CA: No Starch Press.
- Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) *NIST SP 800-207: Zero Trust Architecture.* Gaithersburg, MD: NIST. Available at: https://csrc.nist.gov/publications/detail/sp/800-207/final (Accessed: 15 March 2026).

Summary

In this chapter, you have explored the fundamentals of computer networking, including the OSI model, key network protocols, and common network topologies. You have analysed the core vulnerabilities present within network and online environments at every layer of the OSI model, and examined how the evolution of security thinking – from the trust era to the zero trust era – has shaped the tools and approaches used to secure networks today. These foundations are essential for the security engineering and systems hardening topics covered in the following chapters.

Chapter Two – Network Architecture, Web Applications and Software Exploitation

Introduction

This chapter examines the relationship between network architecture and security engineering at a strategic level. You will explore how network design decisions directly influence an organisation's security posture, how web applications introduce specific vulnerabilities, and how software development practices can either create or mitigate cyber security risks. Understanding these interconnections is essential for evaluating and recommending security solutions.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand, at a strategic level, how computer networking, web applications and software can be exploited.**

Assessment Criteria

2.1 Evaluate the link between network architecture and security engineering concepts.

2.1 Network architecture and security engineering

Security Engineering Principles

Security engineering is the discipline of designing systems that are resistant to attack, misuse, and failure. It requires integrating security considerations into every stage of system design, from initial architecture through to deployment and ongoing maintenance. Key security engineering principles include:

> **! Need to know – The CIA Triad**
>
> The CIA triad is the foundational model of information security, comprising three principles:
>
> **Confidentiality** – ensuring that information is accessible only to those authorised to access it. Implemented through encryption, access controls, and data classification.
>
> **Integrity** – ensuring that information is accurate and has not been tampered with. Implemented through hashing, digital signatures, version control, and audit trails.
>
> **Availability** – ensuring that information and systems are accessible to authorised users when needed. Implemented through redundancy, backups, disaster recovery, and DDoS mitigation.
>
> Every security decision involves balancing these three principles. Excessive focus on confidentiality (e.g. overly restrictive access) can harm availability. The goal is to find the right balance for the organisation's needs.

Additional security engineering principles include:

- **Defence in depth** – implementing multiple, overlapping layers of security so that the failure of any single control does not compromise the entire system. Like the concentric walls of a medieval castle, each layer slows and deters an attacker.
- **Least privilege** – granting users and processes only the minimum permissions necessary to perform their functions. This limits the damage that can be caused by a compromised account or malicious insider.
- **Separation of duties** – dividing critical tasks among multiple people so that no single individual can compromise the system. For example, the person who approves firewall changes should not be the same person who implements them.
- **Fail-safe defaults** – when a system fails, it should default to a secure state. For example, a firewall that crashes should block all traffic (fail-closed) rather than allow all traffic (fail-open).
- **Security by design** – building security into systems from the outset rather than adding it as an afterthought. This principle is now a legal requirement under UK GDPR (Data Protection by Design and Default).

Secure Network Architecture

A well-designed network architecture is the foundation of an organisation's security posture. Key architectural components include:

- **Network segmentation** – dividing the network into isolated zones based on function, sensitivity, or trust level. Common segments include the corporate LAN, DMZ (hosting public-facing services), management network, and guest network. Segmentation limits lateral movement and contains breaches.
- **DMZ (Demilitarised Zone)** – a network segment that sits between the internet and the internal network, hosting services that need to be publicly accessible (web servers, email servers, DNS servers) while protecting the internal network.
- **VLANs (Virtual Local Area Networks)** – logically segment a physical network without requiring separate physical infrastructure. VLANs improve security by isolating traffic between departments or functions.
- **Bastion hosts and jump servers** – hardened systems that act as controlled access points between network zones. Administrators connect to a jump server, which then provides access to systems in more sensitive zones.
- **Software-Defined Networking (SDN)** – decouples the network control plane from the data plane, enabling centralised management and dynamic security policy enforcement. SDN allows rapid response to threats through automated reconfiguration.

Over to you – Video Watch: Network Segmentation

Title: Network Segmentation Explained – Sunny Classroom

Link: https://www.youtube.com/watch?v=ecCuyq-Wprc&list=PLSNNzog5eydueOR_p6dezKr2tosjGvdNH

After watching, design a segmented network architecture for a medium-sized hospital. Consider: patient records systems, medical devices (IoT), administrative systems, public Wi-Fi, and external-facing web services. Explain your design choices with reference to the CIA triad.

Web Application Vulnerabilities

Web applications are among the most frequently attacked components of an organisation's IT infrastructure. The OWASP (Open Web Application Security Project) Top 10 is the industry-standard awareness document listing the most critical web application security risks. Key vulnerabilities include:

- **Injection attacks (A03:2021)** – including SQL injection, NoSQL injection, and command injection. Attackers insert malicious code through user input fields to manipulate databases or execute arbitrary commands on the server.
- **Broken authentication (A07:2021)** – weaknesses in authentication mechanisms that allow attackers to compromise passwords, session tokens, or exploit implementation flaws to assume other users' identities.
- **Cross-Site Scripting (XSS)** – injecting malicious scripts into web pages viewed by other users. Stored XSS persists in the application; reflected XSS is delivered through crafted URLs.
- **Insecure direct object references** – exposing internal implementation objects (such as database keys or file paths) that allow attackers to access unauthorised resources by manipulating parameters.
- **Security misconfiguration** – insecure default configurations, incomplete or ad hoc configurations, open cloud storage, unnecessary features enabled, and verbose error messages that reveal system information.
- **Server-Side Request Forgery (SSRF, A10:2021)** – an attacker can induce the server to make HTTP requests to an arbitrary domain, potentially accessing internal services, cloud metadata endpoints, or sensitive internal resources.

Example – SQL Injection Attack

Consider a login form that constructs the following SQL query:

SELECT * FROM users WHERE username = '[input]' AND password = '[input]'

If an attacker enters ' OR '1'='1 as the username, the query becomes:

SELECT * FROM users WHERE username = '' OR '1'='1' AND password = ''

Since '1'='1' is always true, this returns all user records, bypassing authentication entirely. Prevention requires parameterised queries (prepared statements), input validation, and stored procedures.

Software Development and Cyber Security Risks

Software vulnerabilities are one of the primary entry points for cyber attacks. Understanding how software development practices relate to security risk is essential for building resilient systems.

- **Secure Software Development Lifecycle (SSDLC)** – integrating security activities into every phase of software development: requirements analysis (security requirements), design (threat modelling), implementation (secure coding standards), testing (security testing), deployment (secure configuration), and maintenance (patch management).
- **Common software vulnerabilities** – include buffer overflows, race conditions, insecure deserialization, hard-coded credentials, improper error handling, and use of components with known vulnerabilities.

- **DevSecOps** – the practice of integrating security into DevOps processes, automating security testing in CI/CD pipelines, and making security a shared responsibility across development, security, and operations teams.

Industry Insight – The OWASP Foundation

The Open Web Application Security Project (OWASP) is a non-profit foundation that works to improve the security of software. Their resources are freely available and widely used across the industry. The OWASP Top 10, updated every three to four years, is the most authoritative reference for web application security risks. OWASP also provides testing guides, cheat sheets, and free tools including ZAP (Zed Attack Proxy) for automated security testing.

Read more: https://owasp.org/www-project-top-ten/

Over to you – OWASP Research Activity

Visit the OWASP Top 10 website (https://owasp.org/www-project-top-ten/) and review the current list. Select two vulnerabilities from the list and for each: (a) explain the vulnerability in plain language, (b) provide a real-world example of the vulnerability being exploited, (c) describe three specific countermeasures. Present your findings in a 600-word report.

Reading List

- Anderson, R. (2020) *Security Engineering: A Guide to Building Dependable Distributed Systems.* 3rd edn. Indianapolis, IN: Wiley.
- Stuttard, D. and Pinto, M. (2021) *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.* 3rd edn. Indianapolis, IN: Wiley.
- Hoffman, A. (2020) *Web Application Security: Exploitation and Countermeasures for Modern Web Applications.* Sebastopol, CA: O'Reilly Media.
- OWASP Foundation (2021) *OWASP Top 10 – 2021.* Available at: https://owasp.org/www-project-top-ten/ (Accessed: 15 March 2026).
- Shostack, A. (2024) *Threat Modeling: Designing for Security.* 2nd edn. Indianapolis, IN: Wiley.
- Kim, D. and Solomon, M.G. (2022) *Fundamentals of Information Systems Security.* 4th edn. Burlington, MA: Jones & Bartlett Learning.

Summary

In this chapter, you have evaluated the critical link between network architecture and security engineering. You have examined the CIA triad, defence in depth, and other key security engineering principles. You have explored secure network design including segmentation, DMZs, and VLANs, and have analysed how web applications and software development practices introduce specific security risks. These concepts provide the strategic foundation for the practical defence measures covered in the following chapters.

Chapter Three – Security Prevention and Systems Hardening

Introduction

This chapter focuses on the practical methods of preventing cyber attacks and hardening systems against exploitation. You will learn to evaluate internal risks and exposure, and assess the process and physical defences available to protect against malicious network intrusions. Systems hardening – the process of reducing the attack surface by eliminating unnecessary functions, applying patches, and configuring systems securely – is one of the most effective and cost-efficient security measures available.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand methods of security prevention and systems hardening.**

Assessment Criteria

3.1 Evaluate internal risks and exposure.

3.2 Evaluate available process and physical defences against malicious network intrusions.

3.1 Internal risks and exposure

While much attention is given to external threats, internal risks represent a significant and often underestimated source of security exposure. Internal threats can be intentional (malicious insiders) or unintentional (careless or negligent employees).

Types of Internal Threats

- **Malicious insiders** – employees, contractors, or business partners who intentionally misuse their authorised access to harm the organisation. Motivations include financial gain, revenge, espionage, and ideological beliefs.
- **Negligent insiders** – well-meaning employees who inadvertently cause security incidents through carelessness, lack of training, or failure to follow security policies. This includes clicking on phishing links, sharing passwords, using unsecured personal devices, and mishandling sensitive data.
- **Compromised insiders** – authorised users whose credentials have been stolen through phishing, keylogging, or credential stuffing attacks. The attacker operates with the legitimate user's permissions, making detection particularly difficult.
- **Shadow IT** – the use of unauthorised hardware, software, and cloud services by employees without the knowledge or approval of the IT department. Shadow IT creates unmonitored and unprotected entry points into the network.

Did you know?

According to research by the Ponemon Institute, insider threats cost organisations an average of $15.4 million per year, with the average time to contain an insider incident being 85 days. Negligent insiders account for approximately 56% of incidents, while

malicious insiders account for around 26% and compromised credentials for 18%. These figures highlight the importance of comprehensive insider threat programmes.

Access Control Models

Access controls are the primary defence against both internal and external threats. They determine who can access what resources and under what conditions. The main access control models are:

- **Discretionary Access Control (DAC)** – the resource owner decides who has access. Common in consumer operating systems (e.g. file sharing permissions in Windows). Flexible but vulnerable to improper permission settings.
- **Mandatory Access Control (MAC)** – access is determined by a central authority based on security labels and clearance levels. Used in military and government environments. Highly secure but rigid and complex to manage.
- **Role-Based Access Control (RBAC)** – access is assigned based on organisational roles rather than individual identities. When an employee changes role, their access permissions change automatically. The most widely adopted model in enterprise environments.
- **Attribute-Based Access Control (ABAC)** – access decisions are based on attributes of the user, the resource, and the environment (e.g. time of day, location, device type). More granular than RBAC and well-suited to dynamic environments.

Over to you – Access Control Design Exercise

You are the security consultant for a law firm with 200 employees across three offices. The firm handles highly sensitive client data. Design an access control strategy that addresses: (a) how new starters are granted access, (b) how access changes when an employee changes role, (c) how access is revoked when an employee leaves, (d) how temporary contractors are handled, and (e) how privileged access (IT administrators) is managed. Specify which access control model(s) you would use and justify your choice. Present your strategy in a 500-word briefing.

Vulnerability Assessment and Penetration Testing

Proactive identification of vulnerabilities is essential for managing internal risk. Two complementary approaches are widely used:

- **Vulnerability assessment** – a systematic process of identifying, quantifying, and prioritising vulnerabilities in a system. Automated scanning tools (such as Nessus, Qualys, and OpenVAS) compare system configurations and software versions against databases of known vulnerabilities. Vulnerability assessments are typically non-intrusive and can be conducted frequently.
- **Penetration testing** – an authorised simulated attack on a system to evaluate its security. Unlike vulnerability assessments, penetration tests attempt to actively exploit vulnerabilities to determine whether they can be used to gain unauthorised access. Penetration tests can be black box (no prior knowledge), white box (full knowledge), or grey box (partial knowledge).

3.2 Process and physical defences against malicious network intrusions

Systems Hardening

Systems hardening is the process of reducing the attack surface of a system by removing or disabling unnecessary features, applying patches, and configuring the system according to security best practices. Hardening should be applied to every component of the IT infrastructure:

Component	Key Hardening Measures
Operating Systems	Remove unnecessary services and applications, apply security patches promptly, configure strong password policies, disable unused user accounts, enable logging and auditing, implement host-based firewalls.
Network Devices	Change default credentials, disable unused ports and protocols, enable secure management protocols (SSH instead of Telnet), implement access control lists, keep firmware updated, disable unnecessary services (SNMP v1/v2).
Servers	Remove unnecessary roles and features, place in appropriate network segments, implement strict access controls, configure secure remote management, enable comprehensive logging, use application whitelisting.
Databases	Change default ports and credentials, implement input validation, use parameterised queries, encrypt sensitive data at rest and in transit, restrict database user privileges, enable audit logging.
Web Servers	Remove default pages and sample applications, configure TLS with strong cipher suites, implement security headers (CSP, HSTS, X-Frame-Options), disable directory listing, restrict HTTP methods.
Endpoints	Enable full disk encryption, install and maintain endpoint detection and response (EDR) software, configure automatic updates, disable USB auto-run, implement application whitelisting, enable secure boot.

Over to you – Video Watch: Systems Hardening

Title: How to Harden Your Attack Surface – IBM Technology

Link: https://youtu.be/NqKid53v5x8?si=fwBizcGLhAPB7k7l

After watching, create a hardening checklist for a newly installed Windows Server that will host a corporate intranet application. Include at least 15 specific hardening steps.

Security Frameworks and Benchmarks

Several established frameworks provide detailed guidance for systems hardening:

- **CIS Benchmarks** – the Center for Internet Security publishes detailed configuration benchmarks for over 100 technologies. CIS Benchmarks are consensus-based best practices developed by global communities of security professionals and are freely available.
- **DISA STIGs** – the US Defence Information Systems Agency publishes Security Technical Implementation Guides (STIGs) that provide prescriptive configuration standards for military and government systems.
- **NIST SP 800-123** – provides general guidance for securing servers, including planning, installing, configuring, and maintaining them securely.

Physical Security

Physical security is a critical but often overlooked component of network security. If an attacker gains physical access to network infrastructure, most logical security controls can be bypassed. Key physical security measures include:

- **Data centre security** – access control systems (biometric, card readers, PIN codes), security cameras (CCTV), man-traps, visitor logs, and environmental controls (fire suppression, temperature monitoring, UPS systems).
- **Network infrastructure protection** – locked server racks, secured network closets, tamper-evident seals on equipment, and physical port security (disabling unused network ports).
- **Device security** – cable locks for laptops, encrypted USB drives, screen privacy filters, and clear desk policies.
- **Environmental controls** – fire detection and suppression, water leak detection, temperature and humidity monitoring, and uninterruptible power supplies (UPS) with backup generators.

Case Study – Insider Threat at Tesla (2020)

In 2020, a Tesla employee was approached by a Russian national who offered $1 million to install malware on Tesla's internal network at the Gigafactory in Nevada. The malware was intended to exfiltrate sensitive data, which would then be used as leverage for a ransomware demand. The employee reported the approach to Tesla, who involved the FBI. The Russian national was subsequently arrested.

Task: (1) What type of insider threat does this case represent? (2) What security controls could have detected this if the employee had not reported it? (3) What does this case tell us about the importance of security culture and employee awareness? (4) Design a three-point insider threat programme that could help organisations detect and prevent similar attacks.

Reading List

- Weidman, G. (2024) *Penetration Testing: A Hands-On Introduction to Hacking.* 2nd edn. San Francisco, CA: No Starch Press.
- Cole, E. (2022) *Defensive Security Handbook: Best Practices for Securing Infrastructure.* 2nd edn. Sebastopol, CA: O'Reilly Media.
- Muniz, J. and Lakhani, A. (2023) *Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide.* 2nd edn. Indianapolis, IN: Cisco Press.

- CIS (2024) *CIS Critical Security Controls v8.1.* Available at: https://www.cisecurity.org/controls (Accessed: 15 March 2026).
- Stewart, J.M. (2022) *CompTIA Security+ Review Guide: Exam SY0-701.* 6th edn. Indianapolis, IN: Sybex.

Summary

In this chapter, you have evaluated internal risks and exposure, including malicious insiders, negligent insiders, and shadow IT. You have examined access control models (DAC, MAC, RBAC, ABAC) and the role of vulnerability assessment and penetration testing. You have also assessed the process and physical defences available against malicious network intrusions, including comprehensive systems hardening across all infrastructure components, physical security measures, and established security frameworks and benchmarks.

Chapter Four – Network Security Tools, Terminology and Resilience

Introduction

This final chapter brings together the knowledge from previous chapters to examine how key security concepts are applied in practice within large, distributed organisations. You will explore the tools, terminology, and models that underpin network security and systems resilience, with a particular focus on change management, configuration management, and building an holistic approach to cyber resilience.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand key network security and systems resilience tools, terminology and models.**

Assessment Criteria

4.1 Explain how key security concepts can be applied in a large and distributed organisation.

4.2 Assess how key factors are applied to enhance and embed an holistic approach to network and systems resilience.

4.1 Applying security concepts in large and distributed organisations

Large and distributed organisations face unique security challenges. They typically have multiple office locations, cloud services, remote workers, complex supply chains, and diverse technology stacks. Applying security concepts consistently across such environments requires strategic planning, strong governance, and robust tools.

Security Operations Centres (SOCs)

A Security Operations Centre is a centralised facility that monitors, detects, analyses, and responds to cyber security incidents in real time. A SOC typically employs security analysts who monitor SIEM dashboards, investigate alerts, coordinate incident response, and produce threat intelligence reports. For large organisations, the SOC is the nerve centre of cyber security operations.

SOCs operate at different maturity levels, from basic log monitoring (Level 1) through to advanced threat hunting with artificial intelligence and automation (Level 4). The effectiveness of a SOC depends on its people, processes, and technology working in concert.

Over to you – Video Watch: Inside a SOC

Title: What is a SOC? Security Operations Center Explained – IBM Technology

Link: https://youtu.be/WOFJzVdkkhI?si=BIlMoQgyRpOFwAqG

After watching, list the three tiers of SOC analysts and describe the key responsibilities of each tier. What skills and qualifications would you need to work in a SOC?

Encryption and Cryptographic Protocols

Encryption is the cornerstone of data confidentiality in network communications. Key encryption concepts include:

- **Symmetric encryption** – uses the same key for encryption and decryption. Fast and efficient for large volumes of data. Algorithms include AES (Advanced Encryption Standard, the current gold standard), Blowfish, and ChaCha20. The challenge is securely distributing the shared key.
- **Asymmetric encryption (public-key cryptography)** – uses a pair of keys: a public key for encryption and a private key for decryption. Slower than symmetric encryption but solves the key distribution problem. Algorithms include RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman key exchange.
- **TLS/SSL** – Transport Layer Security (successor to SSL) provides encrypted communication channels for web traffic (HTTPS), email, and other network services. TLS uses a combination of asymmetric encryption (for key exchange) and symmetric encryption (for data transfer).
- **Hashing** – a one-way mathematical function that converts data into a fixed-length digest. Used for verifying data integrity and storing passwords. Common algorithms include SHA-256, SHA-3, and bcrypt (specifically for passwords). Hashing is not encryption – it cannot be reversed.
- **Digital certificates and PKI** – Public Key Infrastructure provides a framework for managing digital certificates that bind public keys to identities. Certificate Authorities (CAs) issue certificates that enable secure HTTPS connections, digital signatures, and email encryption.

Did you know?

The AES encryption algorithm was selected through an open international competition organised by NIST. The winning algorithm, Rijndael (developed by Belgian cryptographers Joan Daemen and Vincent Rijmen), was selected in 2001 from fifteen candidates. AES-256 is approved by the US National Security Agency for protecting classified information up to the Top Secret level.

Incident Response in Distributed Environments

Effective incident response in large, distributed organisations requires a coordinated approach. The NIST Incident Response framework (SP 800-61) describes four phases:

- **Preparation** – establishing incident response policies, forming the incident response team (IRT), deploying monitoring tools, and conducting tabletop exercises and simulations.
- **Detection and Analysis** – identifying potential security incidents through monitoring, alerting, and investigation. This phase involves triage (prioritising incidents based on severity and impact) and initial analysis.

- **Containment, Eradication, and Recovery** – isolating affected systems to prevent the incident from spreading, removing the threat, and restoring normal operations. Short-term containment provides immediate protection, while long-term containment provides a stable environment for forensic analysis.
- **Post-Incident Activity** – conducting a thorough review (lessons learned) to identify what happened, how it was handled, and what can be improved. This phase feeds back into the preparation phase, creating a continuous improvement cycle.

Case Study – Maersk and the NotPetya Attack (2017)

In June 2017, the shipping giant A.P. Moller-Maersk was hit by the NotPetya malware, which destroyed nearly all of the company's IT infrastructure. Within minutes, 49,000 laptops, 3,500 servers, and thousands of applications were rendered inoperable. Operations at 76 port terminals in 17 countries were disrupted. Maersk was forced to reinstall its entire IT infrastructure over ten days, working around the clock. The estimated cost was $300 million.

Task: (1) How did NotPetya spread so rapidly through Maersk's network? (2) What network segmentation measures could have limited the damage? (3) Using the NIST Incident Response framework, evaluate how Maersk responded to the incident. (4) What resilience measures should Maersk implement to prevent a similar catastrophe? (5) Draft a 500-word executive summary for Maersk's board explaining the lessons learned.

4.2 Enhancing network and systems resilience

Cyber Resilience

Cyber resilience goes beyond traditional security by accepting that breaches will occur and focusing on the organisation's ability to anticipate, withstand, recover from, and adapt to adverse conditions. While security aims to prevent incidents, resilience ensures the organisation can continue to operate despite them.

Key components of cyber resilience include:

- **Business continuity planning (BCP)** – developing plans that ensure critical business functions can continue during and after a disruptive event. BCPs identify essential services, establish recovery time objectives (RTOs) and recovery point objectives (RPOs), and define roles and responsibilities.
- **Disaster recovery (DR)** – specifically focused on restoring IT systems and data after a disruptive event. DR plans include backup strategies (3-2-1 rule: three copies of data, on two different media, with one offsite), failover procedures, and testing schedules.
- **Redundancy and high availability** – eliminating single points of failure through redundant components (dual power supplies, RAID storage, clustered servers), load balancing, and geographically distributed data centres.
- **Regular testing and exercises** – conducting tabletop exercises, simulation drills, and full-scale tests to validate that resilience plans work in practice. Untested plans provide false assurance.

Change Management

Change management is the systematic process of controlling changes to IT systems and infrastructure to minimise disruption and maintain security. Uncontrolled changes are a significant source of security incidents – a misconfigured firewall rule, an improperly tested patch, or an unauthorised system modification can create vulnerabilities that attackers exploit.

An effective change management process includes: raising a change request with a clear description of the proposed change and its business justification; risk assessment of the change's potential impact on security, performance, and availability; approval by a Change Advisory Board (CAB); implementation planning including rollback procedures; testing in a non-production environment; scheduled implementation during approved change windows; and post-implementation review to verify the change was successful.

Configuration Management

Configuration management is the process of systematically managing, recording, and controlling the configuration of IT assets throughout their lifecycle. It ensures that every device, system, and application is configured consistently and securely. Key elements include:

- **Configuration Management Database (CMDB)** – a centralised database that records the configuration of all IT assets (Configuration Items or CIs), their relationships, and their current state.
- **Baseline configurations** – documented, approved standard configurations for each type of system. New systems are built from these baselines, ensuring consistency and compliance with security policies.
- **Configuration auditing** – regularly comparing actual system configurations against approved baselines to identify unauthorised changes or configuration drift.
- **Infrastructure as Code (IaC)** – defining infrastructure configurations in machine-readable files that can be version-controlled, tested, and automatically deployed. Tools such as Ansible, Terraform, and Puppet enable consistent, repeatable, and auditable configuration management at scale.

Industry Insight – ITIL and Service Management

The IT Infrastructure Library (ITIL) is the most widely adopted framework for IT service management. ITIL v4 (2019) integrates modern practices including Agile, DevOps, and Lean into traditional service management processes. ITIL's change management and configuration management practices provide mature, well-documented processes that support security objectives. Many organisations use ITIL as the operational backbone for their cyber security programmes.

Read more: https://www.axelos.com/best-practice-solutions/itil

Over to you – Resilience Planning Exercise

You are the cyber security manager for a large online retailer with data centres in London and Manchester. Design a cyber resilience strategy that covers: (a) business continuity planning for a ransomware attack, (b) disaster recovery with specific RTO and RPO values, (c) change management process for deploying a critical security patch, and

(d) configuration management approach for 500 web servers. Present your strategy as a 750-word executive briefing.

Over to you – Video Watch: Business Continuity

Title: Business Continuity and Disaster Recovery – Professor Messer

Link: **https://www.youtube.com/watch?v=NaXMohP4-vU**

After watching, explain the difference between RTO and RPO. Why are these metrics critical for a financial services organisation? Give specific examples.

Reading List

- Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2022) *NIST SP 800-61 Rev. 3: Computer Security Incident Handling Guide.* Gaithersburg, MD: NIST.
- Axelos (2020) *ITIL Foundation: ITIL 4 Edition.* 2nd edn. London: The Stationery Office.
- Grimes, R.A. (2022) *Hacking the Hacker: Learn from the Experts Who Take Down Hackers.* Indianapolis, IN: Wiley.
- Greenberg, A. (2020) *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.* New York: Anchor Books.
- NCSC (2024) *10 Steps to Cyber Security.* London: National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/collection/10-steps (Accessed: 15 March 2026).
- Ross, R. et al. (2021) *NIST SP 800-160 Vol. 2: Developing Cyber-Resilient Systems.* Gaithersburg, MD: NIST.

Summary

In this chapter, you have explored how key security concepts are applied within large, distributed organisations. You have examined the role of Security Operations Centres, encryption and cryptographic protocols, and structured incident response frameworks. You have also assessed how change management, configuration management, business continuity planning, and disaster recovery contribute to an holistic approach to network and systems resilience. These concepts are essential for building organisations that can not only prevent cyber attacks but also withstand and recover from them.

Glossary

Word / Term	Explanation
AES	Advanced Encryption Standard – a symmetric encryption algorithm and the current standard for data encryption.
ARP	Address Resolution Protocol – maps IP addresses to MAC addresses on a local network.
Asymmetric Encryption	Encryption using a key pair: a public key for encryption and a private key for decryption.
CIA Triad	Confidentiality, Integrity, Availability – the three core principles of information security.
CMDB	Configuration Management Database – a centralised record of all IT assets and their configurations.
DDoS	Distributed Denial of Service – an attack using multiple compromised systems to flood a target.
Defence in Depth	A security strategy using multiple overlapping layers of protection.
DMZ	Demilitarised Zone – a network segment between the internet and the internal network.
DNS	Domain Name System – translates domain names into IP addresses.
Firewall	A network security device that monitors and controls traffic based on predetermined rules.
IDS/IPS	Intrusion Detection/Prevention System – monitors network traffic for suspicious activity.
Least Privilege	Granting only the minimum permissions necessary to perform a function.
MAC (Access Control)	Mandatory Access Control – access determined by security labels and clearance levels.
NAC	Network Access Control – enforces security policies on devices accessing the network.
OSI Model	Open Systems Interconnection – a seven-layer reference model for network communication.
OWASP	Open Web Application Security Project – a non-profit providing web security resources.
RBAC	Role-Based Access Control – access assigned based on organisational roles.
RTO/RPO	Recovery Time Objective / Recovery Point Objective – key metrics for disaster recovery planning.
SIEM	Security Information and Event Management – aggregates and analyses security log data.

SOC	Security Operations Centre – centralised facility for monitoring and responding to cyber threats.
SQL Injection	An attack that inserts malicious SQL code through user input to manipulate databases.
Symmetric Encryption	Encryption using the same key for both encryption and decryption.
TCP/IP	Transmission Control Protocol/Internet Protocol – the foundational protocol suite of the internet.
TLS	Transport Layer Security – a cryptographic protocol for secure network communications.
VLAN	Virtual Local Area Network – logically segments a physical network.
VPN	Virtual Private Network – creates encrypted tunnels over untrusted networks.
WAF	Web Application Firewall – protects web applications by filtering HTTP/HTTPS traffic.
XSS	Cross-Site Scripting – injecting malicious scripts into web pages viewed by other users.
Zero Trust	A security model that assumes no user or device should be trusted by default.

MCQs and True & False Questions (self-assessment)

True or False Questions

1. The OSI model has five layers.
2. TCP was designed with security as a primary concern.
3. DNS translates domain names into IP addresses.
4. ARP spoofing exploits the lack of authentication in the Address Resolution Protocol.
5. A DMZ sits between the internet and the internal network.
6. Zero Trust means trusting all devices inside the corporate network.
7. Defence in depth relies on a single, strong security control.
8. SQL injection is an attack against web application databases.
9. RBAC assigns access permissions based on individual user identities.
10. WPA3 provides improved wireless security over WPA2.
11. The CIA triad stands for Confidentiality, Integrity, and Availability.
12. A vulnerability assessment actively exploits system weaknesses.
13. Systems hardening aims to reduce the attack surface.
14. Change management helps prevent security incidents caused by uncontrolled modifications.
15. RTO measures how much data loss an organisation can tolerate.
16. A SIEM aggregates and analyses log data from across the network.
17. Symmetric encryption uses different keys for encryption and decryption.
18. Hashing is a reversible process that can be used to recover original data.
19. A botnet can be used to conduct DDoS attacks.
20. Infrastructure as Code enables consistent, repeatable configuration management.
21. OWASP Top 10 is a list of the most critical web application security risks.
22. A packet-filtering firewall operates at the application layer of the OSI model.
23. Shadow IT creates unmonitored entry points into the network.
24. The Morris Worm of 1988 was one of the first major internet worms.
25. Physical security is irrelevant if strong logical security controls are in place.

Multiple Choice Questions

1. Which layer of the OSI model handles logical addressing and routing?

A. Data Link
B. Transport
C. Network
D. Session

2. What does the CIA triad stand for?

A. Control, Identity, Access
B. Confidentiality, Integrity, Availability
C. Compliance, Investigation, Audit
D. Configuration, Implementation, Administration

3. Which protocol operates without encryption by default?

A. HTTPS
B. SSH
C. HTTP
D. SFTP

4. What is the primary purpose of network segmentation?

A. Increasing network speed
B. Limiting lateral movement after a breach
C. Reducing hardware costs
D. Simplifying network management

5. Which access control model is most commonly used in enterprises?

A. DAC
B. MAC
C. RBAC
D. PBAC

6. What does a SIEM system do?

A. Encrypts network traffic
B. Aggregates and analyses security log data
C. Blocks malware at the endpoint
D. Manages user passwords

7. The OWASP Top 10 addresses security risks in:

A. Network infrastructure
B. Physical security
C. Web applications
D. Cloud storage

8. What is the '3-2-1 backup rule'?

A. 3 users, 2 passwords, 1 server
B. 3 copies, 2 media types, 1 offsite
C. 3 firewalls, 2 VPNs, 1 SIEM
D. 3 layers, 2 zones, 1 DMZ

9. Which encryption algorithm is considered the current gold standard?

A. DES
B. RC4
C. AES
D. Blowfish

10. Zero Trust architecture is based on the principle of:

A. Trust but verify
B. Never trust, always verify
C. Trust all internal users
D. Verify once, trust always

11. What type of attack uses a fake Wi-Fi network to intercept traffic?

A. SYN flood
B. Evil twin
C. DNS poisoning
D. Buffer overflow

12. The NIST Incident Response framework has how many phases?

A. Two
B. Three
C. Four
D. Five

13. Which tool is commonly used for network traffic analysis?

A. Nessus
B. Wireshark
C. Metasploit
D. Terraform

14. Configuration drift occurs when:

A. Systems run out of storage
B. Actual configurations deviate from approved baselines
C. Networks lose connectivity
D. Encryption keys expire

15. What does RPO measure?

A. Time to restore systems
B. Maximum tolerable data loss
C. Network bandwidth
D. Number of security incidents

16. Systems hardening includes:

A. Adding new features to a server
B. Removing unnecessary services and applying patches
C. Increasing network bandwidth
D. Installing additional software

17. Which protocol replaced SSL for secure web communications?

A. SSH
B. IPsec
C. TLS
D. AES

18. NotPetya caused approximately how much damage to Maersk?

A. $3 million
B. $30 million
C. $300 million
D. $3 billion

19. CIS Benchmarks provide:

A. Legal compliance certificates
B. Detailed security configuration guidelines
C. Network speed optimisation tips
D. Software development frameworks

20. A WAF specifically protects:

A. Wireless networks
B. Web applications
C. Database servers
D. Email systems

Answers to True/False Questions

1. *False.* The OSI model has seven layers, not five.

2. *False.* TCP was designed for reliability, not security. It transmits data in cleartext by default.

3. *True.* DNS resolves human-readable domain names to machine-readable IP addresses.

4. *True.* ARP has no built-in authentication, enabling cache poisoning attacks.

5. *True.* A DMZ is a network segment between the external and internal networks.

6. *False.* Zero Trust assumes no user or device should be trusted by default, regardless of location.

7. *False.* Defence in depth uses multiple overlapping layers of security.

8. *True.* SQL injection inserts malicious SQL through user input fields in web applications.

9. *False.* RBAC assigns access based on organisational roles, not individual identities.

10. *True.* WPA3 addresses known vulnerabilities in WPA2, including KRACK.

11. *True.* The CIA triad is the foundational model of information security.

12. *False.* Vulnerability assessments identify weaknesses; penetration tests actively exploit them.

13. *True.* Hardening removes unnecessary features and applies secure configurations.

14. *True.* Uncontrolled changes are a significant source of security incidents.

15. *False.* RTO is Recovery Time Objective. RPO (Recovery Point Objective) measures tolerable data loss.

16. *True.* SIEM systems aggregate, correlate, and analyse security events across the network.

17. *False.* Symmetric encryption uses the same key for both encryption and decryption.

18. *False.* Hashing is a one-way function; it cannot be reversed to recover original data.

19. *True.* Botnets are frequently used to conduct distributed denial-of-service attacks.

20. *True.* IaC tools like Ansible and Terraform enable automated, repeatable configuration.

21. *True.* OWASP Top 10 is the industry-standard list of critical web application risks.

22. *False.* Packet-filtering firewalls operate at Layers 3 and 4 (Network and Transport).

23. *True.* Shadow IT creates unmanaged and unprotected access points.

24. *True.* The Morris Worm (1988) was one of the first widely recognised internet worms.

25. *False.* Physical access can bypass most logical controls; physical security is essential.

Answers to Multiple Choice Questions

1. (C) Network
2. (B) Confidentiality, Integrity, Availability
3. (C) HTTP
4. (B) Limiting lateral movement after a breach
5. (C) RBAC
6. (B) Aggregates and analyses security log data
7. (C) Web applications
8. (B) 3 copies, 2 media types, 1 offsite
9. (C) AES
10. (B) Never trust, always verify
11. (B) Evil twin
12. (C) Four
13. (B) Wireshark
14. (B) Actual configurations deviate from approved baselines
15. (B) Maximum tolerable data loss
16. (B) Removing unnecessary services and applying patches
17. (C) TLS
18. (C) $300 million
19. (B) Detailed security configuration guidelines
20. (B) Web applications