

Unit 5: Security

Unit code D/618/7406

Unit type Core

Unit level 4

Credit value 15

Introduction

Security is one of the most important challenges modern organisations face. It is about protecting organisational assets, including personnel, data, equipment and networks, from attack through the use of prevention techniques in the form of vulnerability testing/security policies and detection techniques, exposing breaches in security and implementing effective responses.

The aim of this unit is to give students knowledge of security, the associated risks and how it has an impact on business continuity. Students will examine security measures involving access authorisation and regulation of use. They will implement contingency plans and devise security policies and procedures. The unit also introduces students to detection of threats and vulnerabilities in physical and IT security, and how to manage risks relating to organisational security.

This unit includes network security design and operational topics, including address translation, DMZ, VPN, firewalls, AV and intrusion detection systems. Remote access will be covered, as will the need for frequent vulnerability testing as part of organisational and security audit compliance. As a result, students will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Assess risks to IT security

LO2 Describe IT security solutions

LO3 Review mechanisms to control organisational IT security

LO4 Manage organisational security.

Essential Content

LO1 Assess risks to IT security

IT security risks:

Risks of unauthorised use of a system, including unauthorised removal or copying of data or code from a system, damage to or destruction of physical system assets and environment, damage to or destruction of data or code inside or outside the system, naturally occurring risks, internal and external sources of risk.

Legal restrictions on the access to data, including UK and international data laws (walled garden laws), e.g. General Data Protection Regulation (UK) (GDPR).

Organisational security, including business continuance, backup/restoration of data, audits, areas of systems to be secured, e.g. data, network, systems (hardware and software), WANs, intranets, wireless access systems, security culture and the approaches to security in the work place, operational impact of security breaches.

The concepts, main functions and features of a range of Operating Systems (OS) and their security functions and associated security features.

LO2 Describe IT security solutions

IT security solution evaluation:

Network security infrastructure, including evaluation of network address translation (NAT), demilitarized zone (DMZ), static and dynamic IP addresses.

Network performance: redundant array of inexpensive disks (RAID), Main/Standby, Dual LAN, web server balancing.

Data security, including asset management, image differential/incremental backups, storage area network (SAN) servers, encryption.

Data centre, including replica data centres, virtualisation, secure transport protocol, secure MPLS routing, segment routing and remote access methods/procedures for third-party access, physical mechanisms, e.g. air flow and cooling to prevent overheating.

Security vulnerability, including logs, traces, honeypots, data mining algorithms, vulnerability testing, zero-day exploits.

Educating staff and customers on IT security issues and prevention methods.

Understand how cyber security technology components are typically deployed in digital systems to provide security and functionality, including hardware and software to implement security controls.

LO3 **Review mechanisms to control organisational IT security**

Mechanisms to control organisational IT security:

Risk assessment and integrated enterprise risk management: network change management, audit control, business continuance/disaster recovery plans, potential loss of data/business, intellectual property, hardware and software.

Probability of occurrence, e.g. disaster, theft.

Staff responsibilities.

Legal mechanisms, both UK and international, including Data Protection Act 2018, Computer Misuse Act 1990 and amendments, ISO 31000 Risk Management standards.

Company regulations: site or system access criteria for personnel; physical security types, e.g. biometrics, swipe cards, theft prevention.

Awareness of common security architectures and methodologies that incorporate hardware and software components, and sources of architecture patterns and guidance.

Assess the security culture within an organisation (the approach to security, including how user actions impact on security).

Ensure system defences are informed by the most up-to-date legislation and guidance on best practice from professional bodies.

LO4 **Manage organisational security**

Manage organisational security:

Organisational security policies, e.g. system access, access to internet email, access to internet browser, development/use of software, physical access and protection, third-party access, business continuity, responsibility matrix.

Reviewing and monitoring of security risk assessments and ensuring stakeholder compliance with security procedures and standards.

Collect information from various sources (e.g. log files, system monitoring tools, Secure Information and Event Management (SIEM) tools, access control systems, physical security systems) and compare to known threat and vulnerability data to determine a digital system security breach.

Using enterprise risk management (as part of system management and lifecycle) for identifying, evaluating, implementing and follow up of security risks according to ISO 31000 standards.

Understand appropriate security tools and methods, e.g. user log-on profiles to limit user access to resources, online software to train and update staff.

Auditing tools to monitor resource access, security audits and penetration testing.

Investigate organisation policy on ethical hacking and bug bounties.

Gathering and recording information on security and initiating suitable actions for remediation.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Assess risks to IT security		LO1 and LO2 D1 Evaluate a range of physical and virtual security measures that can be employed to ensure the integrity of organisational IT security.
P1 Discuss types of security risks to organisations. P2 Assess organisational security procedures.	M1 Analyse the benefits of implementing network monitoring systems with supporting reasons.	
LO2 Describe IT security solutions		
P3 Discuss the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs. P4 Discuss, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve network security.	M2 Propose a method to assess and treat IT security risks.	
LO3 Review mechanisms to control organisational IT security		D2 Recommend how IT security can be aligned with an organisational policy, detailing the security impact of any misalignment.
P5 Review risk assessment procedures in an organisation. P6 Explain data protection processes and regulations as applicable to an organisation.	M3 Summarise an appropriate risk-management approach or ISO standard and its application in IT security. M4 Analyse possible impacts to organisational security resulting from an IT security audit.	

Pass	Merit	Distinction
LO4 Manage organisational security		D3 Evaluate the suitability of the tools used in the organisational policy to meet business needs.
<p>P7 Design a suitable security policy for an organisation, including the main components of an organisational disaster recovery plan.</p> <p>P8 Discuss the roles of stakeholders in the organisation in implementing security audits.</p>	M5 Justify the security plan developed giving reasons for the elements selected.	

Recommended Resources

Textbooks

Alexander, D. et al. (2020) *Information Security Management Principles*. BSC.

Collins, R. (2017) *Network Security Monitoring: Basics for Beginners. A Practical Guide* CreateSpace Independent Publishing Platform.

Sanders, C. Smith, J. (2013) *Applied Network Security Monitoring: Collection, Detection, and Analysis*. Syngress.

Steinberg, R. (2011) *Governance, Risk Management, and Compliance: It Can't Happen to Us – Avoiding Corporate Disaster While Driving Success*. Wiley.

Tipton, H. (2010) *Information Security Management Handbook*. 4th edn. Auerbach Publications.

Web

www.bcs.org BCS, The Chartered Institute for IT
(General Reference)

www.bsa.org Software Alliance
(General Reference)

www.fast.org.uk Federation Against Software Theft
(General Reference)

www.ico.org.uk Information Commissioners Office
(General Reference)

Links

This unit links to the following related units:

Unit 29: Network Security

Unit 30: Applied Cryptography in the Cloud

Unit 31: Forensics

Unit 32: Information Security Management.