T-LEVELS
THE NEXT LEVEL QUALIFICATION

DIGITAL PRODUCTION, DESIGN & DEVELOPMENT

Mo Everett
Sonia Stuart

CORE

Boost

HODDER EDUCATION
LEARN MORE

Contents

Guide to the book

Learning outcomes

Summaries of the knowledge outcomes that you need to learn in each content area.

Key term

Definitions of key terms.

Industry tip

Tips and advice to help you in the workplace.

Important point

Important points that you need to be aware of.

Activity

Short activities that encourage you to apply the knowledge and skills covered in the Student Book.

Research

Research-based activities – either stretch-and-challenge activities, enabling you to go beyond the course, or industry placement-based activities encouraging you to discover more about your placement.

Case study

Scenarios that place content into real-world contexts.

Test yourself

Short questions designed to test your knowledge and understanding.

Assessment practice

Knowledge-based practice questions to help you to prepare for the core exams.

Skills practice

Short scenarios and focused activities that allow you to apply the skills you have learned in each content area.

Content area 8: Security

In this content area you will learn about the potential risks and threats to the digital systems used by organisations. You will apply your understanding of the implications of these to digital systems, as well as to organisations and their stakeholders. You will also learn about the relationships between the different aspects of the data and information that an organisation stores and uses, including confidentiality, integrity and availability (CIA).

Each of these risks or threats can be mitigated against to limit its impact and to reduce the threat of it happening again. You will learn about a range of measures that can be used to do this. You will learn about several types of security. Cyber security is the most important type in relation to digital systems, data and information. Physical security can also be used to protect digital systems, data and information, including CCTV and access badges.

Learning outcomes

In this content area you will learn about:

8.1 Security risks

8.2 Threat mitigation

8.1 Security risks

8.1.1 Maintaining privacy and confidentiality of an organisation's information and that of stakeholders

Industry tip

All businesses and organisations will have data and information which needs to be kept secure, classified and confidential, which should be covered by the CIA triad. What data and information is stored will depend on the function of the organisation and will differ from sector to sector.

Confidentiality relates to data, while privacy relates to the individual. In this context, an 'individual' can be a single person, a business or an organisation.

The GDPR is covered in Content area 4, section 4.1.2.

The CIA triad is covered in section 8.2.1 of this content area.

Typically, an organisation will store information about:

- employee salaries
- employee perks
- client lists
- trade secrets
- sales numbers
- customer information
- news about pending restructuring.

It is important that this information is kept confidential. Any breaches relating to the information can have a serious impact leading to the possible loss of clients or business. This in turn can lead to a downturn in the health of the organisation which may, ultimately, lead to the organisation's failure.

Employee salaries and perks

Salaries and perks should only be known by the employee and the HR department. It is important that this information is kept confidential as different employees carrying out the same task may be paid different salaries based on the number of years they have worked for the organisation, their experience and other factors such as qualifications and training courses attended. It is not acceptable to pay different salaries on the basis of gender or certain other protected characteristics (see Content area 4, section 4.1.4) as this would contravene the Equality Act.

Client lists and customer information

All organisations interact with people – clients and customers. Client lists and customer information are business-sensitive information that result from these interactions.

A client list may include individuals but also a named representative from a different organisation or business. Client lists show anyone who interacts with the organisation and they should not be accessed by employees unless absolutely necessary. Clients may interact with the organisation by using the services provided. For example, a client may use the services of an organisation that provides cloud-based storage facilities. Many organisations will have a client relationship team that looks after clients so this team will need access to this information.

Customer information usually relates to those who buy goods or services. The information held about customers will typically include personal details such as name and contact details but may also include order history.

If the privacy and confidentiality of client lists and customer information are not maintained, the organisation could lose clients and customers. People should expect that any organisation storing their personal data will keep it safe and secure to limit any breaches. The breach of personal data can impact on the organisation and also the people whose data has been leaked.

Activity

Select an online retailer. Define the data that would be held about the customers. What would the impact on the retailer and customers be, including the consideration of relevant legislation (see Content area 4), if there was a data breach leading to the loss of this data?

Create a digital communication detailing your findings. Present your findings to your group.

Sales numbers and trade secrets

Most organisations have stakeholders. Depending on the size and type of the organisation these may be shareholders – **external stakeholders**. Employees can also be classed as **internal stakeholders**. Some organisations may have a policy of keeping stakeholders informed about sales numbers as this may have a financial impact. Some organisations provide a financial bonus to employees or a dividend to investors or shareholders based on the previous year's sales numbers. Sales numbers can also be used to determine the goods that are bought and sold by the organisation. For example, goods that have low sales numbers may be reduced in price and not stocked again, while goods with high sales numbers will be restocked to continue the sale of them to customers.

Where an organisation sells specific goods, these could be classed as a trade secret. Trade secrets often apply to a patent.

Patents are covered in Content area 4, section 4.1.5.

The IPA also covers software processes in addition to patents for tangible items. This means that if the function of the organisation is to provide cloud-based services then the software processes used by the organisation could be covered by the IPA.

Key terms

External stakeholders: groups outside an organisation, for example shareholders.

Internal stakeholders: groups within an organisation, for example owners and employees.

Activity

Using the same online retailer as in the previous exercise, define the data that could be held about the goods that are sold. What would the impact on the retailer and stakeholders be if the data was breached?

Create a digital communication detailing your findings. Present your findings to your group.

Pending restructuring

Many organisations carry out restructuring of departments and employees. This may be because of either an increase or a decrease in clients/customers. However, any leak of the news of a pending restructuring can have an impact on the organisation and its internal and external stakeholders.

If news of a restructure is leaked to employees, it could cause panic. Employees may worry that they could lose their job and may start to look for a different employer. Customers' and clients' confidence in the organisation may decrease and they may look for a different organisation to interact with. This will, obviously, lead to a downturn in finances.

Protecting privacy and confidentiality

One method of maximising the privacy and confidentiality of data is to use access controls, privileges, authorisation and other security procedures to limit the access to the data and information. All important data and information should also be regularly backed up to a secure location to minimise the impact of a data breach. This ensures that any data can be reinstated as soon as possible to keep the organisation functioning smoothly.

The use of data its access and the impact on organisations and stakeholders is covered in Content area 6, section 6.4.4.

Security processes and procedures are covered in this content area, section 8.2.3.

Test yourself

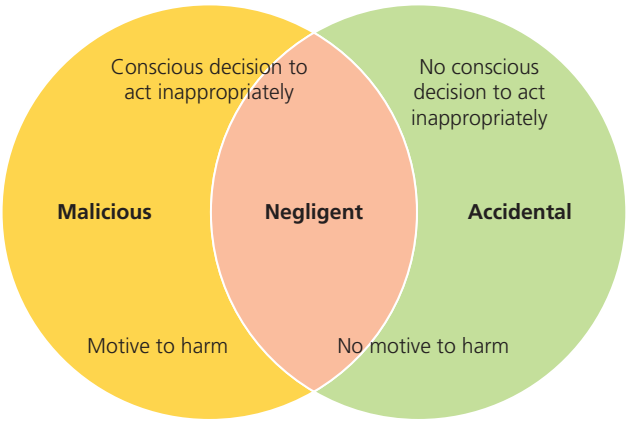
1. What is meant by privacy?
2. What are the two different types of stakeholders?
3. How do clients interact with an organisation?
4. Who should access employee salaries?
5. Describe one possible impact of a restructure being leaked.

8.1.2 The potential impact of failing to maintain privacy and confidentiality

Every business and organisation stores data and information. What data and information is stored will depend on the function of the business and organisation. The failure to maintain privacy and confidentiality is most often the result of an attack. The attack may take many forms and some of these will be covered in section 8.1.3.

The impact(s) of failing to maintain privacy and confidentiality can be wide ranging but includes financial and reputational impacts.

Human threats include:
- human error
- malicious employees
- disguised criminals
- targeted attack.



▲ Figure 8.2 Types of human threats

Figure 8.2 shows the differences between malicious, negligent and accidental human threats to digital systems, data and information.

Human error

Human error can lead to an accidental loss of data. This is a loss of the data itself rather than a loss of a copy or backup version of the data. For example, the loss of a hard copy of the data would not result in the loss of the source of that data.

Human error can include:
- accidentally deleting a file containing the data, or shredding the final hard copy of a data file
- saving files and folders to a different location
- sending emails to the wrong recipients with attachments containing data
- accidentally making changes in documents.

While every person is capable of making an error, businesses and organisations should attempt to minimise the likelihood of these errors happening. This may be through the use of regular employee training, high-profile reminders to employees, for example on splash screens on digital devices, and ensuring that all policies and procedures are read and understood by all employees.

Malicious employees

Malicious employees can be another threat to digital systems, data and information. Malicious employees are also known as Turncloaks. They typically use their access details in a malicious and deliberate way to steal information and data for financial or personal reasons. An individual may become a Turncloak as a result of a social engineering attack.

While many employees take no further action if they are disciplined or sacked, a Turncloak employee will hold a grudge against their employer. This type of threat is often difficult to trace as they are familiar with the security procedures of the business as well as any vulnerabilities.

Research

In 2015 a US health insurance company, Anthem, suffered a data breach. Social engineering was thought to have provided the access codes to the customer database.

Identify the different types of social engineering and describe how each type could have been used to gather the required access codes. Make notes about your findings.

Disguised criminals (social engineering) are covered in Content area 4, section 4.1.3.

Targeted attacks (hackers) are covered in Content area 4, section 4.1.3.

8.2 Threat mitigation

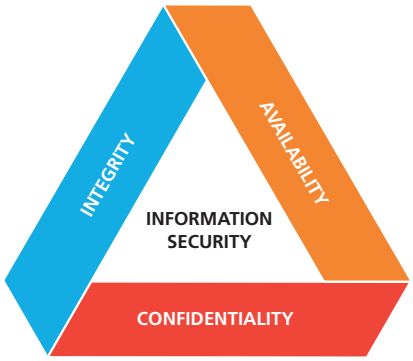
8.2.1 Understand the concept of the CIA and how it can be applied to define security aims

Security, in particular cyber security, aims to protect digital systems, data and information. Cyber security attempts to:
- act as a deterrent against attackers and hackers
- prevent an attack from happening
- detect and warn users of the digital systems that an attack is happening.

The main purpose of cyber security is to maintain the **confidentiality, integrity and availability (CIA)** of digital systems, data, and information.

Key term

Confidentiality, integrity and availability (CIA): also known as the CIA triad.



▲ Figure 8.3 The CIA triad

Figure 8.3 shows the CIA triad, viewed here as a triangle with security in the centre. The CIA triad is a security model developed to define the important parts of cyber security and how they are interlinked.

- **Confidentiality** means that the digital systems, data and information resources are protected from unauthorised viewing and access (**hacking**).
- **Integrity** means that data is protected from unauthorised changes to ensure that it is reliable and correct.
- **Availability** means that authorised users have access to the digital systems, data and information they require.

The CIA triad shows the clear relationship between these three parts of cyber security. Looking at these in a triangle we can see that they overlap, but they can also work against each other when deciding which types of mitigation to use. Visualising things in this way enables an organisation to plan and prioritise the implementation of new security policies and processes.

A good example of how confidentiality, integrity and availability interact can be found in online banking:

- Confidentiality – it is important to a customer that their financial details are kept confidential between them and the bank. One strategy that can be used to maintain the confidentiality of the financial data is through access-level login. When a customer logs into the bank website their login details provide access only to their bank account (and no one else's).
- Integrity – the financial data of the customer must demonstrate integrity. This means that the customer can expect their financial data to be correct. For example, their recent transactions using their debit or credit cards should be true and accurate. The financial data should also be reliable, which is linked to its accuracy.
- Availability – customers should be able to access both the bank website and their financial records when they want and need to. If the website or personal financial data is not available, then this part of the CIA triad has been broken.

Activity

In Content area 4, section 4.1.3 details were given about data breaches of three high-profile businesses – Adobe, eBay and BA.

For each of these breaches, explain how the CIA triad was broken. Consider the impact on the customers of these businesses.

Create a presentation showing the results of your findings. Present your findings to your group.

8.2.2 The interrelationship between security, identity, confidentiality, integrity, availability, threat, vulnerability and risk management within a business context

Security aims to protect digital systems, data and information. Part of this is to ensure that the digital systems, data and information are not compromised when/if a critical threat happens.

By using security, the likelihood of a threat being successful is reduced because the identified vulnerabilities of the digital system, data, information and people will also be reduced.

Security must be used to maintain the CIA triad. There is a strong relationship between all the different components, but using security reduces the chance of any of the components being compromised.

Test yourself

1. What does the I in CIA stand for?
2. How is the CIA security model represented graphically?
3. Define confidentiality.
4. What is meant by availability?
5. What does security aim to protect?

8.2.3 Processes and procedures to mitigate threats and ensure security

Research

Find and watch the video called 'What is penetration testing' at www.cisco.com. What are the main points related to the importance of cyber security raised in the video? Make notes about your findings.

Data and information are very valuable assets, not only to the businesses and organisations that collect, store, process and use them, but also to each individual.

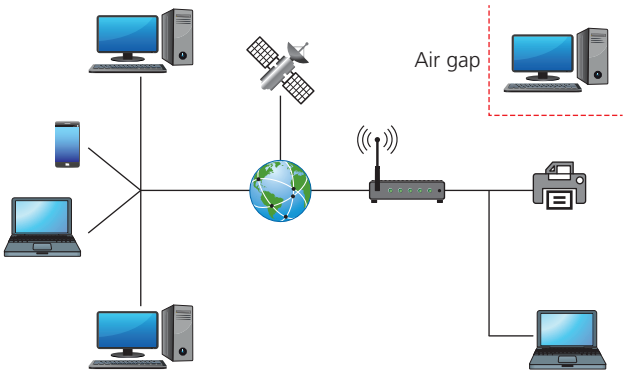
Data and information, such as customer shopping records, financial data and health data and information, are used for a variety of purposes. What is important is that all data and information are kept secure and protected from the large range of threats that could occur.

Some of the ways that threats can be mitigated against include:

- air gapping
- anti-virus and anti-malware programs
- certification of APIs
- configuration and management of software-based access control
- device hardening
- encryption
- user access restrictions
- multi-factor authentication
- firewalls
- password managers
- policy, policy enforcement and training
- SYN cookies
- virtual private networks (VPNs)
- security testing (penetration testing, white/grey hat hackers).

Air gapping

Air gapping is a digital system that is physically isolated from potentially dangerous networks, such as the internet. Basically, air gapping is having a digital system that works offline.



▲ Figure 8.4 An air-gapped digital system

As shown in Figure 8.4, an air-gapped digital system is one that is not connected, either physically or wirelessly, to other systems or networks. It is usually a standalone system or a network of digital systems that has no external links to any other system.

Air gapping refers to the concept that there is air between the digital system and any other system or network, including the internet. This means that the air-gapped system cannot be the victim of a threat or attack through another network. To carry out an attack on an air-gapped system would require the attacker to be physically sitting at the system.

There are still threats to an air-gapped system. The main threat is the use of removable storage devices. For example, a user downloads an infected file from a network onto a USB memory stick. The memory stick is then used to upload the infected file to the air-gapped system. This means that the air-gapped system is now infected and has been the victim of a threat.

However, to some businesses and organisations, using the air-gapping technique to mitigate against threats is not always feasible. The reason digital systems are used in business is because they can share information and data, and access this data and information, from a centralised storage area.

But air gapping, if done properly, can provide complete protection to the air-gapped digital system The other main advantage to using an air-gapped digital system to mitigate against threats is that once the air gapping has been carried out, there are no ongoing, recurring costs.

Research

Investigate the types of industries, businesses and organisations that use air-gapped networks and the reasons why. Make notes about your findings.

White box testing

This is when the people carrying out the penetration tests are provided with full and complete information about the digital system to be tested. White box testing aims to identify any existing vulnerabilities in the software and any incorrect configurations within the digital system.

Black box testing

This is when the people carrying out the penetration tests are provided with no information except the name of the business or organisation. Black box testing is carried out from an external perspective with the aim of identifying ways that the digital systems could be accessed by attackers. The main disadvantage of using black box testing is that, because full and complete details have not been provided, vulnerabilities within the digital system may not be identified.

Test yourself

1. Who are the NCSC?
2. What is ethical hacking?
3. What does network penetration testing aim to test?
4. Identify two other types of penetration testing.
5. What is the difference between white box and black box testing?

Skills practice

An online games company provides games to its customers. Customers need to register their personal and payment details to buy and play the games.

Different options are available for the games. Some games are played online with the players' progress being stored on a dedicated games server. Other games are available to buy and download, meaning they can be played offline.

Some of the games are single player while others can be played by several players at once. If several players want to play the same game at once, each player must be a registered user.

Each customer has a username and password. The password is provided when registration is completed. The players can change their password to something more memorable. The username and password are stored on the games company's server.

The games company has been the victim of several data breaches and threats, including a DDoS attack, malware and social engineering attempts.

You have been asked to:

- Explain to the owner of the games company the importance of maintaining the CIA triad relating to customers' personal and payment details.
- Provide details about the threats that have happened and other potential threats to the games company.
- Explain the possible human threats to the digital systems, data and information stored by the games company.
- Provide details of possible processes and procedures that could be implemented to mitigate against future attacks, including recommendations.

Assessment practice

1. Explain why it is important to maintain the confidentiality of employees' salaries.
2. Discuss the financial impacts of an organisation failing to maintain privacy and confidentiality of its customer data and information.
3. Explain what is meant by a man-in-the-middle attack.
4. Identify and describe two different types of social engineering.
5. Explain the threats a malicious employee could pose to an organisation's digital system, data and information.
6. Explain the CIA triad (triangle).
7. Define hashing and asymmetric encryption, explaining the difference between them.
8. Discuss how user access restrictions can be used to mitigate against threats and ensure security.
9. Compare the use of a password and a passphrase.
10. Explain the process of location-based multi-factor authentication.

T-LEVELS
THE NEXT LEVEL QUALIFICATION

DIGITAL PRODUCTION, DESIGN & DEVELOPMENT

CORE

Boost knowledge, understanding and skills with this student textbook that comprehensively covers the Digital Production, Design and Development T Level core component content areas.

Written by highly respected authors, Mo Everett and Sonia Stuart, this clear, accessible and thorough textbook will guide students through the key principles, concepts and terminology, plus provide the insight track into what it takes to be successful in a chosen career path.

- Track and strengthen knowledge using learning outcomes at the beginning of every unit and Test Yourself questions throughout each unit.
- Improve understanding of important terminology and key terms, plus contextualise learning with research tasks and practice points.
- Develop the skills required and explore guidelines for good practice that will fuel an interest into starting a career in the digital world.
- Confidently prepare for the examinations with assessment practice questions.
- Boost understanding of how to approach the Employer Set Project with project practice tasks.

HODDER EDUCATION
t: 01235 827827
e: education@hachette.co.uk
w: hoddereducation.co.uk

ISBN 978-1-3983-4678-9
9 781398 346789
FSC