BSB 7.0

BSBXCS401

MAINTAIN SECURITY OF DIGITAL DEVICES

Aspire Learning Resources

BSBXCS401

Maintain security of digital devices

Release 1

Learner Guide

Aspire Version 1.1

Aspire
Learning Resources

Aspire also has learning resources available in these areas:

- Foundation skills
- LLN and employability skills (non-competency)
- Community services
- Early Childhood Education and Care
- Allied health

Aspire is committed to developing quality resources that meet the needs of our customers. However, occasionally Aspire finds, or is notified of, errors. Please refer to our website at www.aspirelr.com.au to see if there are any updates that may be relevant to you.

Every effort has been made to ensure the information in this book is accurate; however, the author and publisher accept no responsibility for any loss, damage or injury arising from such information.

Except where an information source is acknowledged, the names and details of individuals and organisations used in examples are fictitious and have been devised for learning purposes only. Any similarity to actual people or organisations is unintentional.

All websites referred to in this unit were accessed and deemed appropriate at time of publication.

Aspire Training & Consulting apologises unreservedly for any copyright infringement that may have occurred and invites copyright owners to contact Aspire so any violation may be rectified.

Acknowledgement

Aspire Learning Resources wishes to acknowledge Hivint for providing an industry validation review of this Learner Guide. Hivint is a cybersecurity consultancy with offices in Melbourne, Sydney, Perth and Brisbane that provides leading edge security advisory and assurance services. We are grateful for their contribution.

BSBXCS401 Maintain security of digital devices, Release 1

Level 1, 464 St Kilda Road
MELBOURNE VIC 3004 AUSTRALIA
Phone: (03) 9820 1300

First published December 2020

Cover design: Anne-Marie Reeves Design
Printer: Doculink Australia Pty Ltd, 1d/28 Rogers Street, Port Melbourne VIC 3207

e-ISBN 978-1-76075-979-7 (PDF version)
ISBN 978-1-76075-978-0

Contact details

Participant
Name:
Start date:
Phone number:
Email:
Work location
Name:
Address:
Postal address:
Workplace supervisor name:
Phone number:
Fax:
Email:
Registered Training Organisation (RTO)
Name:
Address:
Postal address (if different):
Phone number:
Fax:
RTO contact name:
Mobile:
Email:

CONTENTS

Before you begin

This Learner Guide is based on the unit of competency *BBSBXCS401 Maintain security of digital devices*, Release 1. Your trainer or training organisation must give you information about this unit of competency as part of your training program. You can access the unit of competency and assessment requirements at:
www.training.gov.au.

How to work through this Learner Guide

This Learner Guide contains a number of features that will assist you in your learning. Your trainer will advise which parts of the Learner Guide you need to read, and which Practice Tasks and Learning Checkpoints you need to complete. The features of this Learner Guide are detailed in the following table.

Feature of the Learner Guide	How you can use each feature
Learning content	Read each topic in this Learner Guide. If you come across content that is confusing, make a note and discuss it with your trainer. Your trainer is in the best position to offer assistance. It is very important that you take on some of the responsibility for the learning you will undertake.
Examples	These highlight key learning points and provide realistic examples of workplace situations.
Practice Tasks	Practice Tasks give you the opportunity to put your skills and knowledge into action. Your trainer will tell you which practice tasks to complete.
Summaries	Key learning points are provided at the end of each topic.
Learning Checkpoints	There is a Learning Checkpoint at the end of each topic. Your trainer will tell you which Learning Checkpoints to complete. These checkpoints give you an opportunity to check your progress and apply the skills and knowledge you have learnt.

Foundation skills

As you complete learning using this guide, you will be developing the foundation skills relevant for this unit. Foundation skills are the language, literacy and numeracy (LLN) skills and the employability skills required for participation in modern workplaces and contemporary life.

The following table provides definitions for each foundation skill.

Foundation skill area	Foundation skill description
Learning	▪ Modifies behaviour following exposure to new information
Numeracy	▪ Interprets mathematical data ▪ Completes at times complex calculations and records mathematical data
Reading	▪ Recognises and interprets information from relevant sources to determine organisational expectations relating to cyber security
Technology	▪ Uses appropriate technology platforms to assist with protection strategies relating to cyber security

What do you already know?

Use the following table to identify what you may already know. This may assist you to work out what to focus on in your learning.

Topic	Key outcome	Rate your confidence in each section
Topic 1: Identify security for digital devices	1A Create and maintain a device register	❑ Confident ❑ Basic understanding ❑ Not confident
	1B Identify device risks	❑ Confident ❑ Basic understanding ❑ Not confident
	1C Manage device risks	❑ Confident ❑ Basic understanding ❑ Not confident
Topic 2: Apply protection strategies to digital devices	2A Install and run anti-malware	❑ Confident ❑ Basic understanding ❑ Not confident
	2B Create strong passwords	❑ Confident ❑ Basic understanding ❑ Not confident
	2C Use two-factor authentication	❑ Confident ❑ Basic understanding ❑ Not confident
	2D Encrypt devices	❑ Confident ❑ Basic understanding ❑ Not confident
	2E Develop and communicate a physical security plan	❑ Confident ❑ Basic understanding ❑ Not confident

Topic	Key outcome	Rate your confidence in each section
Topic 3; Evaluate protection strategies	3A Review breaches and business impact	❑ Confident ❑ Basic understanding ❑ Not confident
	3B Monitor digital security development	❑ Confident ❑ Basic understanding ❑ Not confident
	3C Support the selection of security strategies	❑ Confident ❑ Basic understanding ❑ Not confident
Topic 3; Patch software and configure new devices	4A Patch software and applications	❑ Confident ❑ Basic understanding ❑ Not confident
	4B Configure new devices	❑ Confident ❑ Basic understanding ❑ Not confident

Topic 1 | Identify security for digital devices

1A Create and maintain a device register

1B Identify device risks

1C Manage device risks

1A Create and maintain a device register

A device register enables relevant personnel to effectively manage the security of an organisation's devices.

Organisations, even small ones, are likely to possess many digital devices. Every device used by an organisation presents a risk, as it may be the means by which sensitive data is leaked. A crucial step in managing information security is to get a complete understanding of the devices used in the organisation. This means creating a device register.

Creating a device register

Device registers contain detailed information about each device used in the organisation.

A device register is a list of the digital devices on an organisation's network. This list should be populated with details about the specifications of each device, and other relevant information. A device register is the starting point for identifying and managing risks relating to each digital device.

Identifying devices that store information

The first step is to identify which kinds of devices to add to the register. The focus of this unit is managing those digital devices that can store information.

The following table provides some examples of digital devices that store information.

Examples of digital devices that store information:
▪ Personal computers (PCs) ▪ Laptop computers ▪ Smartphones ▪ Tablets ▪ Servers

Note: Some organisations may also include in their register digital devices that do not store information. These include peripherals such as keyboards, mouses, stand-alone monitors etc. As mentioned above, this unit focuses on devices that do store information.

Methods for identifying devices

Depending on an organisation's size, it may own a lot of devices that need to be added to the register. Even in a smaller organisation, you may not know the full list of digital devices that are used. The following table identifies methods for identifying devices.

Conduct a visual inspection	Especially in smaller workplaces, it may be possible for you to simply walk around the workplace and document all the devices you see. Be aware that some devices may not be visible; this method is best used in conjunction with one or more of the other strategies.
Talk with department heads	In larger organisations (especially those spread across multiple locations), it may not be possible to do a visual check of the devices being used. It may be appropriate to ask the leaders of different divisions of your organisation for assistance. Provide them with a copy of the register template (we'll look at this template shortly) and ask them to populate it with as much information as possible. Department heads may not always be tech-savvy, so be sure to provide them with assistance and support to gather the information you need.
Refer to existing registers	Your organisation may already have some of the information you need on existing lists and registers. Using this information will make your life easier. For example, the purchasing or finance departments may be able to provide a report of devices purchased each year for the last XX number of years. These lists may not be complete or accurate, so you need to crosscheck this information using one or more of the other strategies.
Check your list with the chief information security officer	The 'owner' of the digital device register will usually be an organisation's chief information security officer. This person should know the organisation's IT infrastructure in detail. You should therefore check your list with this person, as they will be able to check for any gaps.
Asset discovery tools	There are a variety of asset discovery programs available. They are used to identify connected devices and to automatically update asset inventory.

No single strategy from the list above is likely to result in an accurate list. You need to use a selection of these strategies in order to get the most accurate and complete information possible.

Populating the register

You need to add detailed information about the devices listed. There is no standard format for a device register, and your organisation may already have its own format for recording this information. The following table identifies some of the details you should record for each digital device.

Details to record in a device register:
▪ device type (e.g. desktop computer, laptop, tablet) ▪ brand (e.g. Dell, Apple, Acer) ▪ model (e.g. Swift 3, MacBook Air, 14" Chromebook Celeron) ▪ serial number (e.g. 11WSZZZ3) ▪ assigned to (staff name, e.g. Hazel Brown) ▪ department and/or location (e.g. marketing department, Melbourne office) ▪ operating system (e.g. Windows 10, OS10.15.5) ▪ memory (e.g. 4GB RAM) ▪ anti-virus software (e.g. Norton 360 Standard) ▪ licensed software installed (e.g. MS Office Suite 2016, Adobe Premier Pro) ▪ purchase date (e.g. 1 August 2019) ▪ warranty period (e.g. 3 years) ▪ expected life (e.g. 4 years) ▪ information held and classification (this will be covered shortly)

While there is no standard format for an asset register, they are generally created using spreadsheet software (such as Microsoft Excel). Using spreadsheet software makes it easier to use the information held in the register. For example, you might want to quickly check:

- which devices are running a certain operating system
- which devices are being used in a particular department
- which devices were purchased prior to a particular date.

Creating a device register using a spreadsheet will enable you to filter and sort the information so you can quickly find what you need to know.

Maintaining the register

It may take you some time to identify all the digital devices used in your organisation and add all the necessary details to the register. Once it's complete, it's also important to regularly check and update the register. The following table outlines the questions to ask to ensure the register stays accurate and complete.

Questions to ask when maintaining a device register:

- What devices has the organisation acquired since the register was last updated?
- What devices have been retired since the register was last updated?
- Have any staff members left or joined the organisation since the register was last updated?
- Have any updates been performed (e.g. updates to operating systems, software or anti-virus protection) since the register was last updated?

When updating the register, make sure you record when it was updated (and by whom) so anyone looking at the register can see at a glance how up-to-date it is.

Identifying what information is held on devices

In addition to the technical details of the devices held by an organisation, the information stored on each device also needs to be identified.

As mentioned earlier, the device register should identify what types of information are held on each device. Specifically, the register should specify the classification level of the information held on each device. This will help you identify the risk level of each device.

The following table identifies four levels of information classification, and examples of each.

Public

This is workplace information that can be freely shared inside and outside the organisation.

Public information includes:

- marketing materials
- contact details for sales representatives
- price lists for retail products.

Internal

This is workplace information that is potentially sensitive and should not be shared outside the organisation. Generally, this information should be available for all employees of the organisation.

Examples of internal information include:

- organisational charts
- recordings of staff meetings.

Confidential

This is workplace information that is sensitive and could negatively affect the organisation's operations if compromised. This information should not be shared outside the organisation and should only be available to employees on a need-to-know basis.

Confidential information includes:

- supplier contracts
- salary details for members of staff.

Restricted

This is workplace information that is extremely sensitive. It must not be shared outside the organisation and must be handled extremely carefully inside the organisation. If this information is compromised, it could put the organisation at financial or legal risk.

Restricted information may include:

- customer information such as credit card details, passwords and other personally identifiable information
- certain kinds of intellectual property, such as trade secrets.

How to identify information on each device

It's likely that you won't know exactly what kinds of information are held on each of the digital devices on the register. You also might not have permission to view confidential or restricted information. In order to get a better understanding of what types of information are stored on each device you should talk to:

- staff who use the device
- department heads
- the chief information security officer.

For the purposes of populating the device register, it is sufficient to include:

- a list of the type of information held (e.g. customer data) as opposed to specific file names
- the classification level of the most sensitive information held on the relevant device (i.e. if a device holds customers' credit card information, it should be classified as 'restricted').
- When identifying the information held on a device, you should also ask:
- Is information physically stored on this device (e.g. on a computer's hard drive)?
- Is this device used to access data held on another device (e.g. a server)?

Example

Create and maintain a device register

Stephanie works in the ICT department of Timepiece, an online watch retailer with offices in Melbourne and Adelaide. Stephanie is asked to create a register of the digital devices used on Timepiece's network. To create the register, Stephanie:

- obtains a list of IT equipment procured since 2013 from the purchasing department
- does a physical check of all the devices being used in the Melbourne office where she works
- asks the department heads in Adelaide to populate the register with information about the devices used in the Adelaide office
- checks her compiled register with the company's chief information security officer.

Stephanie creates her register in an Excel spreadsheet that records details such as serial number, model, operating system, purchase date, etc. In addition to this, Stephanie includes details about the types of information stored on each device and their classification levels. To do this, she talks with staff, department heads and the chief information security officer. The kinds of information being held on Timepiece devices include:

- sensitive customer information including shipping addresses and passwords to the Timepiece online store that is stored in a database on one of the Melbourne-based servers and classified 'restricted'
- artwork files for Timepiece's upcoming Christmas catalogue that is stored on the desktop PC assigned to Maria in the marketing department, which is classified 'internal'.

Practice Task 1

Question 1

Which methods can be used to identify the digital devices in an organisation? Tick all that apply.

- ◯ Describe what you see in use across the organisation
- ◯ Talk with department heads
- ◯ Obtain a list of equipment purchased from the relevant department
- ◯ Refer to existing registers
- ◯ Email all employees asking them to report back on their use of digital devices

Question 2

Draw a line to match each of the following types of information held on digital devices to the correct classification.

- Contracts with suppliers
- Customer information
- Marketing materials
- Organisational charts

- Public
- Internal
- Confidential
- Restricted

Question 3

What method or methods should you use to confirm the type of information held on digital devices within the organisation?

1B Identify device risks

Every digital device held by an organisation presents a risk.

Creating a digital device register that specifies what classification of information is held on an organisation's devices is the first step in identifying the risks related to those devices. Risk is the possibility of something happening that causes danger, harm or loss. In this unit, we're looking at the risks associated with digital devices, specifically, of the information contained on an organisation's devices being breached.

Calculating risk levels

Identifying the risk level for each device involves thinking about both risk likelihood and risk impact.

There is a risk related to every device held by an organisation, however, different devices will have varying levels of risk. For example, the consequences of a laptop computer containing marketing brochures being breached will be less serious than the breach of a company server containing sensitive customer information. Calculating the risks relating to each device will enable you to manage these risks effectively. Calculating risk involves identifying the likelihood and impact of the harmful event occurring.

Estimate risk likelihood

To calculate the risk level of a device, the first step is to identify the likelihood (or probability) of the risk occurring.

As noted earlier, we are mainly concerned with the likelihood of information stored on a device being breached. To determine risk likelihood, you need to consider how vulnerable the device is to threats that may result in a breach. The following table identifies common threats to the security of information held on digital devices.

General threats
General threats to digital devices include: ▪ hardware and software failure – via power loss or data corruption ▪ human error – including accidental breaches such as sending information to the wrong person ▪ physical damage – caused by overheating, fire, flood, etc. ▪ malware – software designed to disrupt normal device operation ▪ viruses – disruptive computer code that copies itself and can spread across devices.

Criminal threats

Criminal threats to digital devices include:

- hackers – people who break into computer systems to access sensitive information using methods such as:
  - phishing scams (tricking people into providing their passwords)
  - denial-of-service attacks (hacks that prevent organisations from accessing their own information)
- physical theft – in which digital devices and equipment are stolen from a person or workplace
- staff dishonesty – employees accessing/stealing sensitive information or the device itself.

Consider how likely a digital device is to receive one (or more) of the threats above and rank it using the following scale.

1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost certain

Risk management involves dealing with the unknown, so ranking the likelihood of each risk will involve making some educated guesses. It's also a good idea to consult with colleagues and business stakeholders when assessing the likelihood of a given event occurring to improve the quality and consistency of the rankings assigned. The following table outlines some questions you might ask when considering the risk likelihood of a given device.

Questions to ask when estimating risk likelihood:

- How old is the device? (Older devices may not be compatible with the latest security updates)
- Is the most current operating system and software installed? (Devices that are not running current OS and software are more vulnerable)
- What anti-virus / anti-malware software is installed?
- What security controls does the device have in place? Does it have:
- password protection
- encryption
- multi-factor authentication
- physical security?
- Have people using the device received training in potential threats?

Estimate risk impact

Having estimated the risk likelihood, you now need to estimate the risk impact. Impact relates to the negative consequences to the organisation if the information stored on the device is breached.

Estimate the potential impact of a data breach on each device using the following scale.

1	Insignificant
2	Minor
3	Moderate
4	Major
5	Critical

Breaches of highly sensitive information (such as customer information or trade secrets) are more likely to have critical impacts to the organisation (e.g. legal, commercial and reputational issues) than breaches of non-sensitive information (e.g. information that was already publicly available). In other words, devices containing more sensitive information should receive higher impact ratings.

As with estimating the risk likelihood, it is best to estimate risk impacts in consultation with colleagues and relevant stakeholders. You are unlikely to know everything about your organisation, so it's best to get a few viewpoints and a range of perspectives in order to estimate the impact accurately.

Create a risk matrix

You have now estimated the risk likelihood (from 1–5) and risk impact (from 1–5) for a given digital device. This information can be presented in a risk matrix. Different organisations use different risk matrix templates, but a common format is shown below.

		Consequences				
		Insignificant (1)	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Critical (5)**
Likelihood	**Almost certain (5)**	High	High	Very high	Very high	Very high
	Likely (4)	Moderate	Moderate	High	Very high	Very high
	Possible (3)	Low	Moderate	High	High	Very high
	Unlikely (2)	Low	Low	Moderate	Moderate	High
	Rare (1)	Low	Low	Low	Low	Moderate

Depending on the likelihood and risk ratings, each risk will be located within certain shades of the graph. For example:

- risks with a likelihood of 4 and an impact rating of 3 will be located in the darkest (very high) part of the matrix
- risks with a likelihood of 2 and an impact rating of 4 will be located in the middle range (high to moderate) of the matrix
- risks with a likelihood of 1 and an impact rating of 2 will be located in the lightest (low) part of the matrix.

The following table outlines what the matrix tells us about how the risk should be managed.

Dark risks	These are high-level risks that need to be very carefully managed. In the next section, we'll look at potential methods for mitigating these risks.
Middle risks	These are medium-level risks that, while needing to be managed, are not as critical as high-level risks. Methods for mitigating these risks will be outlined in the next section.
Light risks	These are low-level risks that can be accepted by the organisation and addressed by ongoing monitoring and routine management.

Calculate risk scores

Total scores for each risk can be calculated by multiplying the risk likelihood by the risk probability. For example:

- Devices with a risk likelihood of 4 and an impact rating of 3 have a risk score of 12.
- Devices with a risk likelihood of 2 and an impact rating of 4 have a risk score of 8.
- Devices with a risk likelihood of 1 and an impact rating of 2 have a risk score of 2.

Similar to the matrix approach, calculating the total risk score can be used to identify if a risk is low, medium or high level.

Risk score 12-25	These are high-level risks that correspond to the red section of the chart and need to be very carefully managed. In the next section, we'll look at potential methods for mitigating these risks.
Risk score 3-11	These are medium-level risks that correspond to the orange area of the chart. While needing to be managed, they are not as critical as high-level risks. Methods for mitigating these risks will be looked at in the next section.
Risk score 1-2	These are low-level risks that can be accepted by the organisation with ongoing monitoring and routine management. They correspond to the green section of the chart.

Using this scoring method can help you to rank the risks of a large number of different devices. For example, in an organisation with 100 devices, calculating the total risk for each device enables all devices to be classified as low, medium or high risk and managed accordingly.

Example

Identify device risks

Luis works in the ICT department of SureFarm, a farming supplies company with 50 staff. Luis has created a register of all the digital devices on SureFarm's network. This includes 147 devices such as servers, staff PCs, laptops, smartphones and tablets. In consultation with several colleagues in the ICT team, Luis estimates the risk likelihood and risk impact for each device. Devices and their ratings include:

- a recent smartphone with an up-to-date operating system and strong password protection, which contains non-sensitive internal information about an upcoming promotional campaign. It is ranked as Likelihood 1 / Impact 2.
- a server purchased eleven years ago that hosts SmartFarm's client database. It is not compatible with the latest operating systems and has not been patched for some time. It is ranked as Likelihood 4 / Impact 5.

Using the risk matrix approach, Luis classifies each device as high, medium and low risk. The smartphone identified above was classified as low risk. On the other hand, the server was identified as high risk and in need of urgent management.

Practice Task 2

Question 1

If a risk is estimated to have a likelihood of 3 and an impact of 5, what is the total risk score and ranking? Show your calculation.

Question 2

Which of the following events constitute a risk to digital devices? Tick all that apply.

- ◯ Employees accessing sensitive information without authorisation
- ◯ Updates to anti-virus software being installed on company devices
- ◯ Employees receiving phishing emails from hackers
- ◯ Digital devices overheating due to poor storage conditions
- ◯ Employees accidentally disclosing sensitive information

1C Manage device risks

Identifying risks means that they can then be managed.

Generally, risks cannot be left unmanaged. If risks related to information storage on devices are not addressed, they are likely to result in negative consequences (such as a data breach). One strategy for managing risk involves identifying ways to mitigate (reduce the severity of) the level of risk for each device.

Mitigating risk

Mitigating risk involves reducing risk impact, risk likelihood or both.

In the previous section, we explored how the total risk score for a device is calculated by multiplying risk likelihood (ranked from 1–5) and risk impact (ranked from 1–5). The total risk can therefore be reduced by:

- reducing the likelihood of the risk occurring
- reducing the impact of the risk event if it does occur
- a combination of the two.

Reduce risk impact

In terms of digital devices, the potential impact of a risk is directly related to the sensitivity of the information stored on the device. The organisational consequences of a device containing personally identifiable customer information being hacked are much worse than a hack of a device containing non-sensitive information.

While organisations will always hold some information that is confidential or restricted, it is possible to reduce the risk of breaches on individual devices. The following table outlines strategies to achieve this.

Consider location of sensitive data	Identify which devices are being used to store the organisation's most sensitive data (these should be the devices with the highest risk impact ratings) and ask the following questions: ▪ Is it essential for sensitive data to be stored on this device? ▪ Could the sensitive data be stored more securely on a different device? By removing highly sensitive data from a device, the potential risk impact relating to the device is also reduced.

Consider whether data needs to be stored	Data can be an organisation's most valuable asset, but it also contributes to increased risk impacts if it is breached. Many organisations hold on to sensitive data long after it useful. The Australian Privacy Principles specify that when data no longer serves an approved purpose, it should be destroyed or de-identified. By destroying or de-identifying sensitive data held on a device, its risk impact is usually reduced. Any proposed destruction or de-identification of organisational information must be discussed with (and approved by) senior management.

Reduce risk likelihood

The risk likelihood rating reflects the vulnerability of a particular device to threats that may result in a data breach. These threats may be criminal, but they can also result from human error, technical malfunctions or physical damage resulting from fire or flood.

To reduce the risk likelihood, identify the major threat/s and select appropriate security protocols. The following table outlines common threats and suggested security protocols for each.

Common threats	Suggested security protocols
Physical damage to device	▪ Ensure devices are housed in appropriate facilities to protect them from heat and water.
Outdated operating system or software	▪ Ensure all operating systems and software are updated to the current version. ▪ Retire devices that cannot support latest version of operating systems and software.
Human error	▪ Provide staff training to ensure devices are used correctly. ▪ Implement controls to prevent human error where possible (e.g. prevent emails from being sent outside the organisation's network or white-listed recipient domains).
Malware and viruses	▪ Ensure latest anti-virus and anti-malware software is installed and functioning. ▪ Provide staff training to reduce likelihood of staff downloading malware and viruses to devices.
Physical theft of devices	▪ Ensure access to devices is controlled by physical security (e.g. locks, physical barriers). ▪ Train staff to take care of work mobile devices.
Staff dishonesty and corruption	▪ Avoid using shared passwords to ensure transparency of who is accessing/downloading information. ▪ Inform staff that their accessing of sensitive information will be monitored.

Common threats	Suggested security protocols
Hacking attempts	• Implement password policies to prevent hackers guessing passwords to sensitive data. • Use multi-factor authentication methods to protect access even if a password is obtained. • Use encryption to protect data. • Provide training to staff in how to identify phishing attempts and other suspicious emails. • Train staff to avoid connecting to unsecured public Wi-Fi.

A number of the security protocols identified (e.g. using strong passwords and multi-factor authentication) will be explained in more detail in the next Topic.

Example

Manage device risks

Chris works in the ICT department of a medium size homewares company. Chris has created a register of the company's digital devices and has analysed the risks relating to each device. Several high-risk devices were identified, for which Chris has recommended treatment strategies.

These include:

- A desktop computer containing confidential contracts, which was accessible to staff using a shared password ('Password123'). Chris recommends the risk likelihood for this device can be reduced by ensuring that each staff member who uses this computer logs in with their own credentials. Chris also recommends a policy for stronger passwords to be introduced.
- A server containing the company's client database, which was not stored in a climate-controlled area or protected by physical security. Chris recommends that the server be moved to a locked, climate-controlled room to reduce the risk likelihood for this device.

By reducing the risk likelihood ratings for these devices, their overall risk scores are lowered to acceptable levels.

Practice Task 3

Question 1

Draw a line to match each of the following threats to the most appropriate treatment strategy.

- Physical theft of digital devices
- Human error
- Inappropriate data access by staff members
- Hacking attempts by external parties

- Encrypt data and devices
- Control access to devices using physical locks and barriers
- Provide training to ensure staff use devices properly
- Remove usage of shared passwords

Question 2

Which of the following strategies can be implemented to reduce the total risk level of a digital device? Select all that apply.

- ◯ Reduce the risk impact.
- ◯ Reduce the risk likelihood.
- ◯ Increase the risk impact.
- ◯ Increase the risk likelihood.
- ◯ Reduce the risk impact and the risk likelihood.

Summary

- A device register is a list of all the digital devices on an organisation's network.
- Methods for identifying devices include conducting a visual inspection, talking with department heads and the chief information security officer, referring to existing registers, and using asset discovery tools as a method to identify connected devices and to automatically update asset inventory.
- The register should include technical details for each device (e.g. serial number, operating system, anti-virus software) and the types of information held on the device.
- The sensitivity of information held on devices ranges from 'Public' to 'Restricted'.
- By rating risk likelihood and risk impact from 1–5, a risk matrix can be used to identify the overall risk level for the device.
- Every digital device has a risk score, calculated as likelihood multiplied by impact.
- The likelihood of data being breached from a device is related to the device's vulnerability to threats.
- The impact of data being breached is related to the sensitivity of the data stored on the device.
- Risk can be mitigated by reducing the risk impact, the risk likelihood, or both.
- Reducing risk likelihood involves using treatment strategies to address threats to the device.

Learning Checkpoint 1

Identify security for digital devices

Part A

1. What are five pieces of information you would record for each device listed on a digital device register?

2. Which of the following statements are correct? Select yes or no for each one.

   a) To identify the information held on each device, talk to the staff member/s who use that device. » Yes » No

   b) You should include the names of all files stored on a device in the register. » Yes » No

   c) A device that stores sensitive customer information should be classified as 'Restricted'. » Yes » No

   d) You need to visibly check each piece of information stored on a device before it can be added to the register. » Yes » No

Part B

Read the case study and answer the questions that follow.

Case study

Phillipa works for SweetCuts, a wholesale fabric supply business. She has created a register of all the digital devices used in the organisation, and is about to conduct a risk assessment of these devices.

1. Which of the following statements are correct? Select yes or no for each one.

   a) Phillipa should be mainly concerned with estimating the likelihood of each risk. » Yes » No

   b) Phillipa should involve colleagues and relevant staff when estimating risk levels. » Yes » No

   c) Calculating total risk scores will help Phillipa to analyse the large number of devices. » Yes » No

   d) The likelihood of risks occurring may be related to the age of devices. » Yes » No

   e) Devices holding sensitive information are likely to have a lower risk impact score. » Yes » No

2. Phillipa identifies one device that is vulnerable to hacking attempts. What are three strategies she could recommend to reduce the likelihood of this occurring?

Topic 2 | Apply protection strategies to digital devices

2A Install and run anti-malware

2B Create strong passwords

2C Use two-factor authentication

2D Encrypt devices

2E Develop and communicate physical security plan

2A Install and run anti-malware

Malware can cause serious damage to a business, but there are tools to prevent it.

Malware is a combination of the words 'malicious' (harmful) and 'software'. Malware is any software designed to damage devices and steal the information held on them. There are several different types of malware, outlined in the following table.

Viruses	Viruses attach themselves to clean files and rapidly spread to other files. This can result in system corruption and file deletion or corruption.
Trojans	Trojans are disguised as legitimate software, or is hidden in legitimate software that has been hacked. Trojans are not always obvious or visible – they exist to create vulnerabilities in a device to allow other malware to enter.
Spyware	Spyware is malware that spies on your actions. It can record everything you do on your computer, including taking your passwords, personal information, browsing history and more.
Worms	Worms infect networks of digital devices, using network interfaces to spread the infection.
Ransomware	Ransomware locks a user out of their system and demands a payment in order to reinstate access to files.
Adware	Adware usually bombards the user with pop-up ads. Although these ads might not corrupt systems or files, they can create vulnerabilities for other malware to enter a device. Excessive ads can also be very frustrating for the user.

Malware can cause enormous damage if it is not managed effectively. It can affect both desktop/server devices and mobile devices. Fortunately, anti-malware software is designed to identify malware and remove it from devices. This software needs to be correctly installed and run to be useful.

Installing and running anti-malware

All organisations should be running some form of anti-malware software.

Anti-malware software (sometimes also referred to as anti-virus software) is one of the best ways to protect your organisation's digital devices from dangerous software.

Select an anti-malware product

Many different companies offer anti-malware software – some require paid subscriptions while others are free. Some of the most popular anti-malware products are outlined in the following table.

Popular anti-malware software:
▪ Malwarebytes Anti-malware ▪ Avast anti-virus ▪ Kapersky Anti-virus ▪ Panda ▪ F-Secure SAFE ▪ Trend Micro Antivirus+ Security ▪ McAfee AntiVirus Plus ▪ Norton AntiVirus Plus ▪ Bitdefender Antivirus Plus ▪ Webroot SecureAnywhere

Some devices and operating systems also have in-built anti-malware protections, although these can be supported with specific anti-malware software for extra protection.

When selecting an anti-malware software product, there are several questions to ask. Consider these questions in consultation with your manager.

Is the product compatible with all our devices?	Malware can damage both mobile and non-mobile devices from different manufacturers using different operating systems. Check that the anti-malware product will cover all the devices you use. You may need to use a couple of different products to protect all the devices on your network.
How often is the product updated?	New malware is being developed every day, so anti-malware products need to be updated regularly. Look for a product that is updated at least every day.
Does the product run continuously?	Products that offer 'real-time scanning' can detect malware as it tries to enter your devices. This is preferable to anti-malware software that only runs periodically and may only detect malware after it has entered and infected your device.
Will the product slow your system down?	Some products may slow system and device performance significantly, and therefore reduce productivity.
What level of support is provided?	Check how much support is provided with the product. For example, how quickly are support requests answered? Is support available 24/7?

Install anti-malware software

Anti-malware software must be installed onto a digital device in order to be effective. The exact process for installing anti-malware software may vary slightly depending on the software you choose and the device you're installing it onto.

Organisations generally deploy anti-malware software to their device population using pre-configured operating system image which includes pre-installed anti-malware software. They may also roll it out using automated software deployment tools. Similarly, the anti-malware software agents running on user devices are typically managed with updates and logs, and controlled using a central anti-malware software/solution console.

The process for installing anti-malware software, if your organisation is not using a centrally controlled method, is outlined in the following table.

Step 1: Download the anti-malware software
You will usually need to download the anti-malware software directly from the software publisher's website onto the device. Depending on your organisation's policies, you may need to be logged into the device as an administrator in order to download the software.
Step 2: Find and run the installer
Find the software installer you downloaded to the device. The software may be located in the device's downloads folder or another specified drive. The software may be in a zip folder, or it may be an executable file (with a '.exe' extension on PC devices or an '.app' extension on Mac devices). Open the software file – you may need to re-enter your administrator credentials to run the software.
Step 3: Go through the setup menus
Most anti-malware software will walk you through a series of setup menus that contain a number of configuration menus you can adjust. Generally, the default options can be used – but you should read through each option carefully. Be very careful to check whether the software will install additional programs or toolbars onto your computer – it is recommended not to install anything outside of the core anti-malware software.
Step 4: Close the install menu and check that the software works
When you have gone through the setup menus, the software may take some time to completely install. Be patient. After the software has finished installing, you will be prompted to close the install menu. Check the software has downloaded by opening it and checking it is running. You may need to restart the computer.

Anti-malware software often includes auto-update settings to ensure it can detect the latest threats to security. Updates (also referred to as 'patches') can be run manually. Patching will be covered in more detail in Topic 4.

Run anti-malware software

Most anti-malware software will run automatically and make you aware of any threats that have been detected and removed. However, you can also run the software manually. The exact steps for running anti-malware will depend on the product you are using, but the following table outlines the general steps.

Step 1: Open the software and run a scan
Open the anti-malware software from the applications menu on your device. Most software has a very prominent 'scan now', 'run scan' or 'scan for viruses' button visible when the software is opened. You may need to select between two options: ▪ A full scan checks the entire device for malware and takes a longer time. ▪ A quick scan checks only the areas on the device that are most commonly targeted by malware, and is quicker than a full scan.
Step 2: Review the findings
When the scan has finished, the anti-malware software will present a list of suspicious files that may be malware. The software should identify the names and locations of affected files.
Step 3: Address suspicious files
There are generally two options to address the suspicious files identified by the software: ▪ 'Delete' will completely remove the problematic file/s from the device. ▪ 'Quarantine' will move the problematic file/s to a location on the device where it cannot be executed or cause damage to other files. Quarantine should be used when: – a malware file cannot be deleted from the device – a file containing sensitive data has been infected and efforts need to be made to recover the data.

Example

Install and run anti-malware

Claudia works in the ICT department of a small fashion company. The company's digital devices (desktop computers) currently have no anti-malware protection installed. Claudia works with her manager to identify an appropriate anti-malware software. After purchasing the software, Claudia:

- downloads the software to each computer
- installs the software, adjusting the default settings to prevent unnecessary toolbars from being added to internet browsers
- runs the software to identify if any malware already exists on the company's computers
- deletes the malware files detected by the software. Some files cannot be deleted and Claudia quarantines these.

Practice Task 4

Question 1

Number each step from 1 to 4 in the order you would follow to install anti-malware software

- ◯ Find and run the software installer
- ◯ Go through the setup menus
- ◯ Download the anti-malware software
- ◯ Close the install menu and check the software works

Question 2

Which of the following are reasons to quarantine a suspicious file? Tick all that apply.

- ◯ You don't want to upgrade your free anti-malware software.
- ◯ The suspicious file cannot be deleted.
- ◯ The suspicious file contains sensitive data you want to recover.
- ◯ You want to back-up the suspicious file.
- ◯ You want to prevent the suspicious file from damaging other files.

2B Create strong passwords

Passwords are often the first line of defence against hacking attempts.

A 2018 report conducted by Verizon found that 81% of data breaches related to hacking were a result of either stolen or weak passwords. Common passwords people use are '123456', 'qwerty' and 'Password123'. These are all very easily guessed by hackers, providing them with access to sensitive information. Following a few simple practices will help reduce the risk of data breaches relating to weak passwords.

Best practices for passwords

Following some simple practices can strongly increase the strength of passwords.

Creating strong passwords (also referred to as 'passphrases') is an essential part of protecting the security of both work and personal devices. Using strong passwords makes it much more difficult for them to be guessed by hackers. The following table outlines best practice for creating and managing passwords.

Create strong passwords	A 'strong' password uses a combination of: ▪ uppercase letters ▪ lowercase letters ▪ numbers ▪ symbols. Avoid using dictionary words or passwords that can be easily guessed (e.g. '123456', 'abcde', 'qwerty', your name, etc.). It can be difficult thinking of totally random combinations of letters, numbers and symbols. There are a number of secure password generators online that can be used to create truly random and complex passwords. You can also check the strength of your password using an online password-checking tool.
Create long passwords	Passwords should be at least 8 characters in length. However, longer passwords (up to 64 characters) provide even more security. Each additional character added to a password makes the job of guessing it significantly more difficult.
Use different passwords for every account	If you use the same password for all your personal and work accounts, you create the risk of having all your accounts compromised if one service is hacked. Also avoid using similar passwords for different accounts (e.g. using the same complex password with 'gmail', 'dropbox' or 'facebook' added to the end) – if one password is hacked, it will be easy for the hacker to work out the rest. The best practice is to maintain completely different passwords for each account you use.

Don't use shared passwords	Passwords must not be shared between staff. Each staff member should have a personal account and their own password for devices or services they need to use. This provides transparency around which accounts are logging onto devices and accessing sensitive data. If a password is used in a data breach, using individual accounts and passwords helps to track the source of the breach.
Change passwords when staff leave the organisation	Avoid the risk of ex-employees accessing sensitive data or sharing passwords with others by changing passwords as soon as a staff member leaves your organisation.
Don't use personal information in passwords	Avoid using personal information in your password such as date of birth, postcodes, tax file number, etc. If your password is hacked, this information will be helpful to the hacker in creating a fake identity in your name.
Use a password manager	Avoid keeping a list of all your passwords in a notepad or file on your phone. These methods are highly prone to being compromised. A password manager stores the passwords you use for all your accounts in one highly secure place. A good password manager can also help you to generate highly secure unique passwords. You'll just need to remember the one password to access the password manager.
Don't use your passwords on others' devices	Do not enter your password on other people's digital devices. These devices may contain malware or be vulnerable to other forms of attack.

Example

Create strong passwords

Bernadette works in the ICT department of a medium-size furniture company. The company does not have any standard password practices in place, and Bernadette is aware that many devices can be accessed using the password 'PassWord-123!'. Bernadette receives permission to increase the security of the company's devices and assists staff to set up passwords that:

- are at least 12 characters long
- do not use dictionary words or personal information
- use a combination of uppercase, lowercase, numbers and symbols.

She supports staff to understand that different passwords should be used on each of their devices and helps them to set up password managers, to stop staff from writing their passwords on post-it notes next to their computer.

Practice Task 5

Question 1

Provide an example of a strong password.

Question 2

Which of the following are good practices when it comes to password management? Tick all that apply.

- ◯ Use different passwords for every device and account.
- ◯ Create a single strong password that can be used by multiple staff.
- ◯ Change passwords when staff leave the organisation.
- ◯ Don't use passwords on other users' devices.
- ◯ Use personal information in passwords to make them easy to remember.

2C Use two-factor authentication

Two-factor authentication adds an extra layer of protection if a hacker obtains a password.

Creating a strong password is a great way to reduce the risk of other people accessing sensitive devices and accounts. However, if a password does fall into the wrong hands, using two-factor authentication (also known as 'two-step authentication' or 'two-factor verification') provides an extra layer of security. As the name suggests, two-factor authentication requires a user to have a secondary 'factor' in addition to a password in order to gain access.

There are a wide range of 'factors' – these are outlined in the following table.

Something you know	A factor can be a piece of knowledge only known to the user, such as: ▪ a password ▪ a PIN. 'Secret questions' (such as your mother's name or the street you grew up on) are poor examples of 'something you know' factors, as this information may be known to others or easily researched.
Something you have	A factor can be a physical object owned by the user, such as: ▪ a USB key inserted into the device ▪ a specific device (e.g. a mobile phone) ▪ a key card (in the case of using an ATM).
Something you are	A factor can be a piece of biometric information that is part of the user, such as their: ▪ fingerprint ▪ iris ▪ voice.
Somewhere you are	A factor can be the location of the user, identified using a GPS (global positioning system) or IP address.

Two-factor authentication requires a combination of two different types of factors. Common examples of two-factor authentication include:

- typing in a password (something you know) and then entering a confirmation code sent to your mobile device (something you have) to access an online account
- entering an access code (something you know) and then allowing your device to take a picture of your face (something you are) to access a mobile device
- putting in your bankcard (something you have) and then entering your PIN (something you know) to withdraw money from an ATM.

Switching on two-factor authentication

Two-factor authentication is now commonplace.

Two-factor authentication can be turned on for many online services and apps (email, social media, cloud storage, etc.), as well as software and devices themselves. This unit is all about ensuring the security of devices, and the following table outlines how to turn on two-factor authentication on some commonly used devices.

PC running Windows 10

Steps for setting up two-factor authentication:

1. Log into the device
2. Go to the 'Security Basics' page
3. Select 'More security options'
4. Under the 'Two-step verification' menu, select 'Set up two-step verification'
5. Follow the set-up instructions to activate two-step authentication. This will involve scanning a QR code with your mobile device to confirm you are in possession of the device being used as an authentication method.

Mac computer running macOS

Steps for setting up two-factor authentication:

1. Log into the device
2. Go to the 'System Preferences' page and select 'Apple ID'
3. Select 'Password & Security'
4. Select 'Turn on Two-Factor Authentication'
5. Follow the set-up instructions to activate two-factor authentication. If you're using a recently created Apple ID, you may find that two-factor authentication is already on (by default).

Android phone or tablet

Steps for setting up two-factor authentication:

1. Log into the device
2. Go to the 'Settings' menu and select 'Google'
3. Select 'Manage your Google account'
4. Select 'Security'
5. Select '2-step Verification'
6. Select 'Get Started'
7. Follow the set-up instructions to activate two-factor authentication.

iPhone or iPad (iOS 10.3 or later)

Steps for setting up two-factor authentication:

1. Log into the device
2. Go to Settings -> [your name] -> Password & Security
3. Select 'Turn on Two-Factor Authentication'
4. Select 'Continue'
5. Follow the set-up instructions to activate two-step authentication.

The exact steps for the devices you use may vary depending on the model and operating system used. However, most devices have two-factor options – check online for the specific instructions for setting up your devices.

When switching on two-factor authentication for someone else (i.e. another member of staff), make sure they know how the authentication process will work.

Potential risks of two-factor authentication

The most common form of two-factor authentication for protecting devices is for the user to receive a confirmation code on their mobile device (something they have) in addition to entering a password (something they know). While this does provide additional security when compared to using a password alone, the approach is not totally risk-free. This is because:

- hackers can clone SIM cards, which may enable a hacker to receive security codes
- text messages containing security codes that are sent to mobile phones can be intercepted
- if the user loses their mobile device, they may not be able to receive a security code
- successful phishing attempts can trick someone into providing both their password and a security code.

Despite these risks, two-factor authentication does provide greater security than a password on its own.

Example

Use two-factor authentication

Hannah works in the ICT department of a food wholesaler. The company uses desktop devices (running Windows) and Apple mobile devices. Two-factor authentication has not been activated for a number of these devices. Hannah works with the staff who use each device to set up two-factor authentication within the preferences and security settings for each device. Hannah makes sure each staff member knows how the authentication process will work (i.e. which phone the person will receive the authentication code on).

Practice Task 6

Question 1

Draw a line to match each type of 'factor' to the correct example..

- Something you have
- Somewhere you are
- Something you are
- Something you know
- Password
- USB key
- Location the device is accessed from
- Fingerprint

Question 2

What are two potential risks associated with two-factor authentication that involves sending a security code to a mobile device?

Question 3

Number each step from 1 to 5 in the order you would follow to set up two-factor authentication on an iPhone or iPad (or another brand of smartphone and tablet).

- ◯ Select 'Turn on Two-Factor Authentication'
- ◯ Select 'Continue'
- ◯ Log into the device
- ◯ Follow the set-up instructions to activate two-step authentication.
- ◯ Go to Settings -> [your name] -> Password & Security

2D Encrypt devices

Encryption converts sensitive information into a highly complex code.

'Encryption' involves converting data into a code (called 'ciphertext') that can only be read by authorised people who have the secret key to read it. In addition to individual files and programs, entire devices can be encrypted.

Encryption means that even if sensitive data is accessed by unauthorised parties (e.g. via a digital hacking attempt or physical theft), it cannot be used unless the hacker also has the secret key. A secret key is similar to a highly complex password. The longer the key (measured in bits), the stronger it is.

Encrypting a device

If a device isn't encrypted, it should be.

As a strong method of security, encryption is activated by default on many current devices.

The following table outlines steps to check whether encryption is turned on.

PC running Windows 10

Steps to turn on encryption:

1. Log into the device (using an administrator account)
2. Go to the 'Settings' page
3. Select 'Update & Security' -> 'Device Encryption'
4. If device encryption is turned off, select 'Turn on'

Mac computer running macOS

Steps to turn on encryption:

1. Log into the device
2. Go to the 'System Preferences' page
3. Select 'Security & Privacy'
4. Select the 'FileVault' tab and check if FileVault encryption is turned on
5. If 'FileVault' encryption is turned off, select 'Turn on FileVault'.

Android phone or tablet device

Steps to turn on encryption:

1. Log into the device
2. Go to the 'Settings' menu
3. Select the 'More' tab
4. Select 'Security'
5. If Encryption is not already turned on, select 'Encrypt Device'

iPhone or iPad

Data on Apple mobile devices is encrypted by default, whenever the device is locked with a passcode or touch ID. If the device does not already have a Touch ID or passcode set up:

1. Open the 'Settings' menu
2. Select 'Touch ID & Passcode'
3. Follow the set-up instructions to create a passcode – use the passcode strategies outlined earlier in this topic to create a passcode that is both strong and long.

The exact steps for the devices you use may vary depending on the model and operating system used. However, most devices have encryption options. Check online for the specific instructions for setting up your devices.

Example

Encrypt devices

Leon works in the ICT department of an architecture and design firm. Staff do the majority of their work on iMacs and MacBook Pro laptops. The firm has won a project to develop plans for a government building and these need to be stored securely. Leon checks the 'Security & Privacy' settings for each device, and ensures FileVault encryption is turned on.

Practice Task 7

Question 1

Succinctly define 'encryption'. Try and keep your answer to one or two sentences.

Question 2

Number each step from 1 to 4 in the order you would follow to encrypt a device.

- ( ) Navigate to the device's Settings or Preferences page
- ( ) Navigate to the device's Security or Privacy settings
- ( ) Log into the device
- ( ) If encryption is off, turn it on
- ( ) Check if encryption is already turned on

2E Develop and communicate a physical security plan

Digital security measures must be supported by a physical security plan.

The security strategies examined so far in this topic have all related to increasing the digital security of devices. However, digital devices also face physical threats of theft and damage. A physical security plan describes the methods used to ensure the physical security of digital devices.

Developing the plan

A physical security plans should be developed so that it meets the needs of the organisation.

To ensure the ongoing security and functionality of digital devices, organisations must have a plan that details methods for securing digital devices against:

- intrusion
- unauthorised access
- vandalism.

The physical security plan outlines the level of security required for each device, and the measures that will be used to ensure security at each level.

Defining the level of security required

Depending on the size of the organisation, it may own and operate many different digital devices. As discussed in Topic 1, devices contain information at varying levels of sensitivity and devices containing sensitive data have a greater negative risk impact if they are accessed by unauthorised parties. These high-risk devices require higher levels of physical security than devices that contain non-sensitive information.

Security levels will vary from organisation to organisation. A simple way to categorise devices by security level is to group together:

- critical digital devices
- devices that are important but not critical
- other digital devices.

Another way to categorise security levels is to consider the impact of the device being compromised. This approach is similar to the risk impact rating system discussed in Topic 1. Impacts range from:

- catastrophic business impact if device is compromised
- extreme business impact if device is compromised
- high business impact if device is compromised
- low to medium business impact if device is compromised
- low business impact if device is compromised.

Whichever approach you use to define the level of security required, appropriate physical security measures should be defined for each level.

Defining the physical security measures to be used

A variety of measures can be used to ensure the physical security of digital devices. Physical measures should do one or more of the following:

- deter unauthorised parties from attempting to access digital devices
- detect unauthorised parties if they attempt to access devices
- prevent unauthorised parties from accessing devices
- delay unauthorised parties as they attempt to access a device.

A security measure such as a video camera could deter an unauthorised person from accessing a digital device as well as detecting a person if they make an attempt.

The following table outlines some common physical security measures to consider when developing a physical security plan.

Physical security measures for digital devices:

- restrict access to rooms containing devices by using identifiable swipe cards or a unique keycode
- ensure rooms are locked at all times
- use full-height walls to prevent people from climbing into rooms containing devices
- use security cameras outside and inside rooms containing devices
- use monitored alarms that are activated upon unauthorised access to the room (or when a device is disconnected)
- bolt devices to desks or onto racks
- lock computer cases to prevent hard drives from being easily removed
- use security personnel to guard rooms containing devices (or locate rooms near staff who can keep an eye out for unusual parties)
- store devices in rooms without windows (or use bars on windows)
- position computer screens so they are not visible by others
- lock mobile devices in secure cupboards/containers when not in use
- avoid signposting where servers are located – don't make it easy for outsiders to find rooms containing devices
- ensure that staff policies specify mobile that devices are not to be left unattended
- develop processes for authorising access to areas containing sensitive devices (this may be via the ICT security manager or chief information security officer).

No single measure is likely to be sufficient to protect every device in an organisation from every possible threat (especially the high-risk devices). Work with your manager to identify the most appropriate selection of measures required for each level of device.

Documenting the plan

The physical security plan documents the measures to be applied for the devices of each level of security. An extract taken from a plan (relating to devices classified as 'critical') is provided below.

Extract of a physical security plan:

- For digital devices classified as critical, [Company name] employs the following physical controls:
- electronic lock (identifiable via keycard)
- video surveillance
- monitored alarms (motion sensing and forced entry).
- Authority to access areas containing critical digital devices may only be provided by the ICT security manager.

A full plan would identify the security measures required for each level of device.

Other information to include in the plan would be:

- a brief statement outlining the objective of the plan
- a brief statement outlining the scope of the plan
- definitions of any specialist terms or acronyms used in the plan
- version history (including when the latest version was made).

After drafting the plan, you should discuss it with management and receive their sign-off before communicating it to other staff.

Communicating the plan

Physical security plans must be communicated to all staff.

All staff in an organisation need to be aware of the physical security requirements relating to digital devices. This is because the plan:

- outlines the physical security requirements for devices used by all staff (e.g. that mobile devices are not to be left unattended)
- identifies the process to follow if access to sensitive devices is required (e.g. gaining authorisation from the ICT security manager to access the server)
- contains security measures that may deter staff from any attempts at unauthorised access.

Methods to communicate the physical security plan to staff are outlined in the following table.

Methods to communicate the physical security plan:
▪ introduce the plan to new staff during the on-boarding process ▪ send the plan to all staff via email – consider requesting a 'read receipt' to ensure staff have read the document ▪ communicate the contents of the plan at staff meetings ▪ communicate the plan using internal online communications channels (such as a staff newsletter) ▪ add the plan to the organisation's document management system.

Using a combination of these methods will help ensure the plan has been read and is understood by all staff.

Example

Develop and communicate physical security plan

Georgie works in the ICT department of an investment firm and has been given the job of developing a physical security plan for the digital devices used in the company. Georgie first defines the different levels of security for the organisation's devices, and categorises them as:

- critical devices containing customer information and systems required for running operations
- devices that are important but not critical
- other digital devices

With her manager, Georgie identifies the appropriate measures to be applied for each level of security. For critical devices, this includes the use of security cameras, alarm systems, locked doors and security guards. This information (together with the required measures for the other security levels) is documented in a physical security plan. After the plan is reviewed and signed off by management, Georgie distributes the plan to all staff via email – the plan is also discussed at the next all-staff meeting.

Practice Task 8

Question 1

Which of the following are physical security measures? Tick all that apply.

- ◯ Preventing access to server rooms using a security code
- ◯ Installing security cameras in rooms containing sensitive devices
- ◯ Installing anti-virus software on all devices
- ◯ Requiring that no staff leave mobile devices unattended
- ◯ Implementing complex passwords on all mobile devices

Question 2

What are two appropriate methods for distributing a physical security plan?

Summary

- Anti-malware software protects digital devices from dangerous software (known as malware).
- Anti-malware detects harmful software so it can be deleted or quarantined (which prevents the software from harming other files).
- Using strong passwords makes it much more difficult for them to be discovered by hackers.
- Best practice with passwords involves using a random combination of characters, using long passwords and using different passwords for different accounts.
- Two-factor authentication requires a user to have a secondary 'factor' in addition to a password in order to gain access.
- The most common form of two-factor authentication is a security code sent to the user's phone that is needed in addition to a password.
- Encryption involves converting data stored on a device into a code that can only be read by authorised people who have the secret key to read it.
- Most current devices are encrypted by default, but this can be checked within device settings.
- A physical security plan describes the methods used to ensure the physical security of digital devices.
- Developing a physical security plan requires different levels of device security to be identified, together with appropriate measures for each level.

Learning Checkpoint 2

Apply protection strategies to digital devices

Part A

1. Why is it important for anti-malware software to be updated at least once a day? Succinctly summarise your answer.

2. What are three good practices for creating and managing passwords?

3. Which of the following indicate that two-factor authentication is switched on?
Tick all that apply.

- ◯ You need to enter a 4-digit passcode to access your mobile device.
- ◯ You need to create a strong password to access Windows on a desktop computer.
- ◯ Your registered mobile phone is sent a verification code as part of the login process.
- ◯ When you log in, you are asked to verify your identity with a fingerprint.
- ◯ You need to insert a USB into the device you are trying to access.

Part B

Read the case study and answer the questions that follow.

Case study

Hayley works in the ICT department of an online homewares and gardening store. Following a recent risk assessment, Hayley is implementing a number of security protocols to improve the security of company information. She has already installed anti-malware software, implemented strong password practices and activated two-factor authentication.

1. Hayley is now considering the encryption of all company devices including recently purchased iPhones and desktop PCs running Windows 10. Which of the following statements are correct? Select yes or no for each one.

   a) Many devices are unlikely to have encryption available. » Yes » No

   b) Current generation iPhones with a passcode are encrypted by default. » Yes » No

   c) Specialised encryption software will need to be purchased. » Yes » No

   d) Encryption can protect data accessed via hacking attempts or physical theft. » Yes » No

2. In addition to the digital security methods she has implemented, Hayley needs to ensure the physical security of the organisation's devices. What are three physical security measures she might consider?

Topic 3 | Evaluate protection strategies

3A Review breaches and business impact

3B Monitor digital security developments

3C Support selection of security strategies

3A Review breaches and business impact

Data breaches need to be closely monitored and their impact assessed.

Planning effective security strategies for an organisation's devices requires that you assess how the organisation is currently performing in this respect. By knowing the number of times data has been breached (and its associated impact), lessons can be learned and better strategies can be formulated.

Identifying breaches and their impact

Responding to data breaches first requires that they be identified – this doesn't always happen quickly.

Research conducted by Bitdefender in 2019 suggests that six in ten organisations experienced a data breach within the past three years. While some data breaches may be quickly identified and recorded by an organisation, others may not be noticed for many months.

Ensuring breaches are tracked

To ensure your organisation is accurately tracking the number of breaches that have occurred in a given period (e.g. the last 12 months), consider whether the following strategies are being used.

Monitor the latest digital security development

- Staying aware of the latest threats is one of the best ways for organisations to identify potential and actual data breaches. This will be discussed in more detail in Sub-topic 3B.

Use technology to detect and track breaches

- Technology such as an intrusion detection system can be used to detect potential and actual threats to sensitive data.

Train employees about data breaches

- While hacks and technical errors are a considerable threat to data, human error can lead to unintentional data breaches. Keeping employees up-do-date in their training helps to reduce the number of breaches and improves staff performance in reporting breaches that do occur.

Hire cybersecurity specialists

Data security professionals play an important role in identifying and monitoring breaches due to their specialist knowledge of the potential threats to your organisation's data.

Recording breaches

When an actual or potential breach is identified, it should be logged according to the organisational processes and procedures. This may include the use of a 'data breach incident form'. At a minimum, the information indicated in the following table should be recorded.

Details to be included when reporting a data breach:

- name and contact details of the person reporting the breach
- date, time or period when the breach occurred
- a description of the breach – including which devices were affected
- summary of the data breached (i.e. the number of records and the sensitivity of the information)
- immediate actions taken to contain the breach
- staff and third parties involved in the breach.

Understanding the business impacts of data breach

In addition to the technical details about a given data breach, the impacts or potential impacts to the business also need to be assessed and recorded. The following table outlines the most significant potential effects of a data breach on an organisation.

Revenue loss	If an online store's website crashes due to a hacking attempt, significant revenue losses will immediately occur. However, some hacking attempts result in more subtle effects such as system slowdown. While less immediately devastating, revenues lost as a result of IT downtime can quickly add up.
Damage to brand or reputation	A business's reputation is often built on consumer trust. If an organisation's sensitive customer data is hacked, customers will be much less likely to return to that organisation. Hacks can also result in embarrassing internal emails being shared publicly, which does significant reputational damage.
Loss of intellectual property	Alongside customer data, intellectual property (IP) is the most valuable asset held by many organisations. The loss of IP such as designs, trade secrets and strategies may cost an organisation its competitive edge.

Legal damage	Data breaches may involve significant legal consequences from both regulators and people whose data is leaked. It may result in the issuance of fines and penalties that come at financial cost to the organisation.

Serious breaches may result in an organisation suffering several of these consequences (e.g. financial, reputational and legal damage).

Analysing the information about the breaches

Information about an organisation's data breaches may not always be easy to understand or analyse. The following table outlines how to assess the data breaches that occur in a given period of time.

Step 1: Obtain the information	First, you need to gather the information available about data breaches in your organisation during the period you are investigating. This may involve accessing data breach incident forms, security logs, or other tools used in your workplace to record information about data breaches.
Step 2: Collate the information	The information you gather might not be in a format that's easy to analyse. You will probably need to collate the details of each data breach into a single spreadsheet. To make the data easy to sort and analyse, consider using column headings such as: ▪ date the breach occurred ▪ duration of the breach ▪ date the breach was identified/reported ▪ device/s related to the breach ▪ sensitivity of data breached (e.g. Internal, Restricted, etc.) ▪ number of data records breached ▪ impact on the organisation – this could include commercial, reputational, legal costs and other negative impacts.
Step 3: Analyse the information	After you have added the information regarding breaches to your spreadsheet, you can use the tools within the spreadsheet to conduct an analysis. For example, you could identify: ▪ how many breaches occurred during a given time period ▪ the average length of time between when a breach was identified and when it was reported ▪ the total and average number of records compromised in each breach. This analysis will form the first part of the process for conducting a gap analysis, which will be covered next.

Performing a gap analysis

A gap analysis measures the distance between an organisation's target state and its actual performance.

You should now have a clear understanding of the data breaches that occurred during a given period. But how does that data compare to the organisation's strategy and goals? The process of conducting a 'gap analysis' helps an organisation to identify:

- the actual status (with regard to data security)
- the organisation's target state (i.e. ideal status)
- how to close the gap between the actual and target status.

A gap analysis helps an organisation to understand how effective the techniques used to manage data security were, and where changes need to be made.

The gap analysis process involves four steps, which are outlined in the following table.

Step 1: Identify the current status
As mentioned earlier, by gathering and analysing the information relating to the data breaches and identifying their impact on the business, you should have a good picture of the organisation's current status. If you haven't already done so: obtain, collate and analyse the organisation's existing data breach information.
Step 2: Identify the target state
What does the target state look like for organisation, with regard to data security? Every organisation will be different, but the goals of the target state should be measurable. For example, a target state might include: ▪ no breaches of restricted data over a 12 month period ▪ that all data breaches are identified within 24 hours of the breach occurring ▪ no legal or reputational damage resulting from data breaches over a 24 month period. ▪ Identifying the target state may involve other stakeholders such as information security specialists and managers in the organisation.
Step 3: Identify the gaps
There is likely to be at least some gaps between the organisation's actual and target states. Again, these gaps should be quantifiable. You can identify the size of the gap by subtracting the target state from the actual state. For example: ▪ Actual number of breaches over the past 12 months: 3 ▪ Target number of breaches for the next 12 months: 0 ▪ Gap = 3 (actual) – 0 (target) = 3

Step 4: Analyse the gaps to identify improvements

Each gap needs to be investigated to understand why the gap exists. Dig deeper and ask questions to get to the bottom of the problem. Using the example above (a gap of three breaches), you need to analyse why these breaches occurred by asking questions such as:

Were the breaches a result of hacking, technical issues or human error?

- If they were the result of hacking, was this due to a phishing attempt, social engineering or security vulnerability?
- If the hacks were a result of a security vulnerability, was this related to hardware or software?
- If it was a software issue, was it a result of manual patches not being applied correctly?
- If it was a result of manual patches not being applied correctly, how can we avoid this occurring in the future?

At this point, it starts to become possible to pinpoint specific improvements. In this case, they might include moving to automatic (instead) of manual patching wherever possible, or updating processes to ensure all manual patches are double-checked after application. Any recommendations should:

- be based on the findings of the gap analysis
- include timelines for implementation
- consider the cost of implementation.

Coming up with sound recommendations and communicating them will be covered in more detail later in this topic.

Example

Review breaches and business impact

Chai works in the ICT department of a large mining company. Chai has been asked to conduct a gap analysis of the company's information security performance over the past 12 months. He locates eight data breach incident forms that were completed during the reporting period and compiles them into a spreadsheet. By analysing the data, Chai finds that:

- five actual breaches of data occurred over the previous 12 months
- it took, on average, 58 days for data breaches to be identified.

Chai organises a meeting with stakeholders and identifies that the organisation's ideal state is to have zero data breaches over the next 12 months (i.e. a gap of 5 breaches). If a breach does occur, the target is to identify it within 2 days (i.e. a gap of 56 days). Chai analyses these gaps to identify the root of the current issues and identifies a range of improvement actions.

Practice Task 9

Question 1

Number each step from 1 to 4 in the order you would follow to perform a gap analysis.

- ( ) Identify the gaps
- ( ) Identify the current state
- ( ) Analyse the gaps
- ( ) Identify the target state

Question 2

What are two ways a business might be negatively affected by a data breach?

Question 3

Which of the following tools could be used to conduct a gap analysis? Tick all that apply.

- ◯ Spreadsheet for collating information
- ◯ Risk assessment matrix
- ◯ Anti-malware software
- ◯ Data breach incident forms
- ◯ Security logs

3B Monitor digital security developments

Staying on top of the latest developments in cybersecurity enables you to respond to potential threats in a timely manner.

Technology is rapidly evolving, and digital security is no exception. Hackers are constantly inventing new ways to attack devices and networks, and security experts are responding with defence strategies. Monitoring the latest developments in digital security will help you stay ahead of the curve in keeping your organisation's devices secure.

Finding relevant information

There's a lot of information out there, so you need to know where to look.

New information about developments in digital security is being published every day. Cybersecurity information is usually time-sensitive, so the internet is the best place to check for the latest developments (as opposed to monthly print magazines, etc.).

The following table identifies several online sources of information you can check.

Commonwealth and state government sources
Australian government sources generally publish high-quality information that is closely aligned to local laws and regulations. The first place to check should be the Australian Cyber Security Centre, which includes information about the latest cyber threats facing Australians: aspirelr.link/cyber-security-centre-news

Australian ICT news sources
There are a number of Australian news sites that specialise in cybersecurity. These sites are regularly updated and publish information about emerging threats to Australian organisations. Websites to check include: **IT News Australia:** aspirelr.link/it-news **Australian Cyber Security Magazine:** aspirelr.link/australian-cybersecurity-magazine **Security Brief Australia:** aspirelr.link/security-brief-australia

International ICT news sources

Many global cyber threats target Australian individuals and organisations, so stay updated on international cybersecurity developments. The following international news sites are all focussed on cybersecurity and are regularly updated. Be aware that not all the developments discussed are relevant to Australian regulations and/or practices.

Websites to check include:

Threat Post: aspirelr.link/threat-post

CyWare: aspirelr.link/cyware

The Hacker News: aspirelr.link/the-hacker-news

Wired: aspirelr.link/wired-security

Cyber Security News: aspirelr.link/cyber-security-news

Dark Reading: aspirelr.link/dark-reading

Hardware and software developer sources

A number of major hardware and software developers, in particular anti-malware software publishers, publish news and developments regarding cybersecurity. These articles may not always be entirely objective and should be approached with caution. However, they may provide accurate updates and information regarding the hardware and software you use in your organisation.

Websites to check include:

IBM: aspirelr.link/ibm-security

Microsoft: aspirelr.link/microsoft-security

Norton: aspirelr.link/norton-internet-security

Kaspersky: aspirelr.link/kaspersky-news

You're unlikely to have time to read every one of these websites daily, and there may be some crossover in the news presented on the different sites. Identify a handful of sites that are most appropriate to your organisation's needs, and make time to check these at least once a week. Some sites also offer a weekly newsletter which contains all the most important news in one digest.

Questions to ask when reviewing information

When faced with a lot of different information sources, it can be difficult to quickly identify which pieces of information are relevant and should be considered.

The following table provides some questions to ask yourself when reviewing a piece of cybersecurity information – the more of these questions you can answer 'Yes' to, the better.

Is the information current?	The world of cybersecurity moves rapidly. You need to make sure that any information you refer to is current (e.g. from within the last month).
Is the information relevant?	Certain articles and information may be about threats to software or hardware that are not used in your organisation. Focus on articles which talk about threats to the infrastructure being used in your organisation.
Is the information reputable?	Information published on reputable websites is more likely to be accurate than rumours and unverified information published on social media. Even if you see an article on a news site that you believe is reputable, check some other sites to confirm the information is accurate.
Is the information local?	If you're working for an Australian organisation, you need to comply with local laws and regulations. So it's important to consider whether the information you're reading is relevant to the Australian context.

Communicating information to colleagues

As you review the latest developments in digital security, you may find information that you believe will have implications for your organisation's security practices. For example, you might learn that:

- companies have been hacked due to a vulnerability in their database software – and your organisation uses the same database
- companies in your state have been the target of social engineering hacks, in which hackers call employees and attempt to trick them into handing over their usernames and passwords.

In these situations, you should make relevant colleagues aware of the development in case urgent action needs to be taken. Relevant colleagues may include your manager and ICT security staff. When communicating digital security developments to colleagues, consider the guidance identified in the following table.

Practices for communicating digital security developments:

- Email is generally the best method of communication to ensure a clear record is kept of communication.
- Only email relevant staff.
- Use an appropriate subject heading.
- Flag the email as 'important' if the information you have found suggests an immediate threat to your organisation.
- Provide a link to the information so colleagues can learn more.
- Provide some detail as to why you believe the information is important (e.g. if it indicates a threat to the organisation).
- Suggest some next steps (e.g. propose a meeting to discuss how to address an immediate threat).
- Use appropriate language for the audience.

Example

Monitor digital security developments

Daniela works in the ICT department of an online financial management company. She regularly checks several local and international cybersecurity news websites in addition to the Australian Cyber Security Centre and the McAfee website (Daniela's company uses McAfee anti-malware software).

One day, Daniela sees an alert on the Australian Cyber Security Centre website about a series of DoS (denial of service) attacks on Australian companies in the banking and finance sector. The alert was published that morning, and has also been reported on several other reputable news websites. Daniela believes her company may be a potential target of this attack, so emails a link to her colleagues who specialise in information security. In the email, Daniela outlines why she believes this threat needs to be acted upon, and suggests a meeting to discuss a course of action.

Practice Task 10

Question 1

What are two sources of information you can check for developments regarding digital security?

Question 2

Which of the following questions would you ask when considering information about digital security? Tick all that apply.

- ◯ Is the information free?
- ◯ Is the information commercial?
- ◯ Is the information relevant?
- ◯ Is the information reputable?
- ◯ Is the information current?

3C Support the selection of security strategies

Keeping your organisation's data secure requires appropriate security strategies to be identified and implemented.

As technology evolves and changes (and hackers develop new ways of stealing data), so must the security strategies used by an organisation be kept up-to-date. People with an understanding of current security gaps and who are keeping abreast of the latest developments in cybersecurity are in a great position to recommend security strategies.

Selecting and recommending strategies

Following a logical process for making recommendations helps you identify the best strategies for keeping data secure.

The first step is to identify and evaluate possible security strategies, so you are in a position to recommend the most appropriate ones for your organisation. The following table outlines a process for preparing a recommendations report.

Step 1: Describe the problem	The first step is to provide an overview of the problem. You might have found, for instance, that: ▪ a particular device having an unacceptably high level of risk (such as a server which is not running up-to-date anti-malware software) ▪ an unacceptably large gap in security performance (e.g. four data breaches in the past 12 months instead of the target state of zero breaches) ▪ an wide-scale hacking attack on organisations similar to yours, which needs to be responded to quickly. When describing the problem: ▪ be clear and use straightforward language ▪ specify the information used to identify the problem (e.g. breach reports) ▪ identify any previous attempts to solve the problem ▪ state how urgent the problem is.
Step 2: Identify potential solutions	Identify potential security strategies that will address the problem. Aim for at least three quality solutions. Outline each strategy and specify: ▪ how it addresses the problem at hand ▪ the details about how it would be implemented ▪ your justification as to why it would work. Different types of security strategies are explored later in this sub-topic.

Step 3: Evaluate each option	Rate each strategy against evaluation criteria. These may include: ▪ how effectively the strategy will address the problem ▪ the cost of implementing the strategy ▪ the ease of implementation ▪ timelines for implementation ▪ the riskiness of the strategy (e.g. using an unproven anti-malware software vs a well-known provider). The criteria used (and the weighting of each criteria) may vary depending on the problem at hand. For example, addressing an urgent and major threat to security may place greater importance on timeliness than on cost. Rank each strategy using the evaluation criteria to determine the best option.
Step 4: Make a recommendation	Provide more detailed information about the strategy that you have evaluated to be the best option. This section should include all information decision-makers would need to either accept or reject the recommendation.

When the draft recommendations report is complete, send it via secure email to the relevant decision-makers in your organisation. This may include the manager of information security, the ICT manager and others. Specify the next steps. These could include requesting feedback of stakeholders by a certain date, or confirming their availability to discuss the recommendation in a meeting.

The recommendations report may need to be updated based on stakeholder feedback.

Choosing the best strategy based on data location

The strategies selected must relate to the location of the organisation's data.

When considering potential security strategies for an organisation (Step 2 of the recommendation process), it may be helpful to consider where and how the organisation's sensitive data is stored. It could be stored data (also referred to as 'data at rest'), data in transit and data in third-party applications. The following table explains each of these in more detail, along with some appropriate security strategies.

Stored data

Stored data (or 'data at rest') is any data that is stored on a digital device, including online and offline devices. Examples of stored data include:

- Word documents stored on the desktop of a laptop computer
- a customer data base housed on a server
- notes files stored on a mobile device.

Stored data can be compromised by hacking attempts, device defaults and human error. A number of strategies for protecting stored data were discussed in Topic 2. These include:

- ensuring anti-malware software is installed and running correctly
- using strong passwords on network devices
- using two-factor authentication
- encrypting digital devices
- protecting the physical safety of digital devices
- ensuring policies and procedures exist for protecting data stored on devices
- ensuring staff are trained in how to use devices to avoid accidental data breaches.

Data in transit

Data in transit (also referred to as 'data in motion') is any data moving from one location to another. This includes data moving through a network or the internet. Examples of data in motion include:

- data being transmitted from a local device to the cloud
- email data as it travels from one account to another
- data being downloaded from a network server to a desktop computer.

Data in transit is vulnerable to hacking attempts which aim to access the data as it moves from one place to another. Strategies to protect data in transit include:

- ensuring data is encrypted prior to being moved
- ensuring the connections being used to move data are encrypted
- using network access controls and firewalls to prevent attacks during transit
- checking the security measures for incoming and outgoing data of any cloud-storage provider you are using.

Data in third-party applications

Organisations don't always store all sensitive data within their own infrastructure. Third-party applications (i.e. apps developed outside of the organisation) may be used to house and transmit sensitive data to help reduce the organisation's bandwidth and perform specialised tasks.

Examples of third-party applications may include your email provider, network manager and customer management apps. Using third-party apps can create system vulnerabilities that may be targeted by hackers.

Strategies to protect the data contained in third-party applications include:

- maintaining an inventory of all third-party apps used (including purpose of app and data contained)
- ensuring the security of third-party apps is in line with your organisation's ICT policies and procedures
- checking that app developers are certified according to relevant security standards
- ensuring the developer has a disaster recovery plan for data stored in their apps
- checking that all apps utilise encryption and developers have an encryption policy
- ensuring all third-party apps are regularly updated (or 'patched') to address new and emerging security threats. Patching will be covered in more detail in the next topic.

No single strategy will be enough to protect all data at rest, in transit and stored on third-party applications. Using and implementing a range of strategies is the best way to ensure data security across an organisation's devices.

Example

Supporting the selection of security strategies

Edwin works in the ICT department of a large agriculture equipment company. Having conducted a gap analysis of the company's data security performance over the past 12 months (in which two breaches of stored data occurred), Edwin is aware of a problem with the security of stored data. Edwin prepares a recommendations report containing:

- an overview of the problem (including a summary of his gap analysis)
- details of three potential strategies to improve the security of data at rest, including: increasing the strength of encryption used on devices, moving to a different anti-malware software product, and implementing two-factor authentication on all devices
- an evaluation of each option using criteria based on implementation costs, time, and likelihood of success. This evaluation indicates that increased encryption is the best strategy to pursue.
- a final recommendation detailing the level of encryption that needs to be implemented and details about how this would be done (including impacts on the organisation's operations).

Edwin emails his recommendation report to senior ICT security staff members and suggests a meeting be held in the following week to discuss the next steps.

Practice Task 11

Question 1

What three criteria could you use to evaluate a potential security strategy?

Question 2

Draw a line to match each of the security strategies to the correct type of data.

» Install anti-malware software	» Data in third-party applications
» Encrypt connections used for moving data	» Data in third-party applications
» Maintain an inventory of apps used	» Stored data
» Use network access controls and firewalls	» Stored data
» Check that external developers have a disaster recovery plan	» Data in transit
» Protect the physical safety of digital devices	» Data in transit

Summary

- Data breaches and their impacts on a business must be proactively monitored and measured.
- Potential business impacts of data breaches include damages or loss to revenue, brand reputation, intellectual property and legal status.
- Information regarding breaches must be obtained (e.g. from incident forms), collated and analysed.
- A gap analysis measures the distance between an organisation's target state and its actual performance, and outlines strategies to reduce the gap.
- Sources of information about digital security must be monitored to gain an understanding of emerging threats and solutions.
- Sources of information about developments include government sources, local and international news sources, and hardware/software vendors.
- When reviewing information, you should check whether it is current, relevant, reputable and local.
- The process for selecting security strategies involves describing the problem, identifying potential strategies to address the problem, evaluating each option and making a final recommendation.
- Effective strategies differ, depending on the location of organisational data – whether it is stored data, data in transit or data held in third-party applications.

Learning Checkpoint 3
Evaluate protection strategies

Part A

1. Which of the following sources provide the latest developments in digital security? Tick all that apply.

- ◯ Social media
- ◯ Australian Cyber Security website
- ◯ Official websites for the software and hardware used by an organisation
- ◯ International cybersecurity news websites
- ◯ Monthly magazines

Part B

Read the case study and answer the questions that follow.

Case study

Sian works in the ICT department of an online wine retailer. She is conducting a gap analysis of the company's performance with respect to data breaches.

1. Which of the following steps would Sian take to gain an understanding of the company's current performance? Tick all that apply.

- ◯ Upload data breach information.
- ◯ Obtain data breach information.
- ◯ Analyse data breach information.
- ◯ Collate data breach information.
- ◯ Distribute data breach information.

2. Over the past nine months, the company experienced 27 data breaches. The company has a target state of zero breaches over the next year. What is the size of the gap? Show your calculation.

3. Sian has been asked create a recommendations report to address the gaps identified. What steps should Sian follow to develop this report?

4. Sian's investigation has identified that security threats exist to the company's:
   - stored data
   - data in transit
   - data in third-party applications.

   For each of these types of data, identify a potential security strategy.

Topic 4 | Patch software and configure new devices

4A Patch software and applications

4B Configure new devices

4A Patch software and applications

'Patching' means applying a set of changes to software and applications to update, improve or fix it.

Applying 'patches' (i.e. software/application updates) protects devices from vulnerabilities. Leaving devices unpatched leaves them open to the risk of a cyber attack. Some studies suggest that up to 57% of data breaches are the result of hackers targeting a known vulnerability that had not been patched. In 2018, the personal data of 1.5 million Singaporeans customers of SingHealth was hacked because an unpatched version of Microsoft Outlook was being used on a company computer. This highlights the importance of ensuring software and applications in your organisation are patched.

Identify software and apply patches

The first step in the patching process is to identify the software and applications used in your organisation.

Software and applications installed on both desktop and mobile devices need to be patched to ensure ongoing security. The following table gives examples of commonly used software that will need to be patched.

Operating systems	▪ Windows ▪ Mac OS ▪ iOS ▪ Android
Anti-malware and security software	▪ Malwarebytes Anti-malware ▪ Avast Anti-virus ▪ Trend Micro Antivirus+ Security ▪ McAfee AntiVirus Plus ▪ Norton AntiVirus Plus
Internet browsers	▪ Chrome ▪ Firefox ▪ Internet Explorer ▪ Edge ▪ Safari

Web plugins	▪ Adobe Flash ▪ Adobe Reader ▪ Skype ▪ Apple QuickTime ▪ iTunes ▪ Java ▪ ActiveX
Other applications and software	▪ Microsoft Office suite (Word, Excel, PowerPoint, etc.) ▪ Adobe Creative Cloud (Photoshop, Illustrator, etc.) ▪ other software used in your organisation

Your organisation is likely to be using a number of different applications, so you need to have systems in place to ensure that each application is regularly patched.

Automate updates where possible

Automating software updates (i.e. patches) helps to eliminate or minimise the amount of time that software and applications remain unpatched. Organisations may have their own patching cycle and procedures that take into account risk assessments of security vulnerabilities and prioritise patch deployment. Patches are typically tested in a 'sand box' environment before they are rolled out to general devices. The following table outlines some best practices for automating updates.

Best practices for automatic updates:
▪ Turn on automatic software updates wherever possible (noting that automatic updates may not be possible on some older devices and applications). ▪ Automatic updates can usually be scheduled to download and install outside of business hours. This minimises slowdowns during business hours. ▪ When configuring a new device, turn on automatic updates (as discussed in the next sub-topic).

Turning on automatic updates is slightly different for each piece of software. For operating systems, automatic updates can generally be set within the system preferences or settings on the device.

To access specific steps for turning on automatic updates for a variety of devices and applications, refer to the Australian Cyber Security Centre website: aspirelr.link/update-software-regularly

Software and application publishers also publish steps to turn on automatic updates on their websites. This is usually the best place to get the latest information on how to configure the software used in your organisation.

Apply manual patches

Patches should be configured to install automatically wherever possible. However, in some situations (especially when running older applications or hardware) you may need to manually download and install patches.

The specific steps for applying patches manually varies between different types of software and applications. However, the general process is as follows:

- Step 1: Log into the device with an administrator account
- Step 2: Navigate to the 'Settings', 'Preferences' or other similar menu within the relevant software or application.
- Step 3: Navigate to the 'Security', 'Updates' or similar sub-menu.
- Step 4: The software or application should inform you whether you are up-to-date, or if there is an update that can be installed.
- Step 5: If there is an update available, download and run it.
- Step 6: Check that the patch has been applied correctly by re-opening the software/application, going to the 'Security' or 'Updates' menu, and checking that you are now up-to-date.

If you need to manage manual updates for many devices and/or applications, you may wish to keep a record of updates in the digital device register (see Topic 1). However, wide-scale manual patching is much riskier than using automated patching so if manual patching is required due to outdated hardware, it may be time to consider an upgrade.

Audit patches

After a patch is applied (automatically or manually) monitor any system performance issues, such as slowdown and software functionality/incompatibility. There should also be a mechanism for scanning if any devices are missing critical/defined patches. Users who have received updates on their devices may also alert you if they are experiencing unexpected issues. Report any patching issues to management so an appropriate course of action can be taken.

Example

Patch software and applications

Ramesh works in the ICT department of an online music distribution company. The company has a number of desktop computers (Mac and PC) that run a variety of applications (including operating systems, web browsers, anti-malware software, web plugins and specialised music publishing applications). Ramesh checks the update settings for each application (referring to the instructions available on the websites for each application's publisher) and sets applications to update automatically wherever possible.

Practice Task 12

Question 1

What are three types of software or applications that need to be patched?

Question 2

Number steps 1 to 5 in the order you would follow to apply updates to software and applications used on desktop computers.

- ( ) Navigate to the 'Settings', 'Preferences' or other similar menu within the relevant software or application.
- ( ) Check the patch has been applied correctly by re-opening the software/application, going to the 'Security' or 'Updates' menu, and checking that you are now up-to-date.
- ( ) Navigate to the 'Security', 'Updates' or similar sub-menu.
- ( ) Log into the device using an administrator account.
- ( ) The software or application should inform you whether you are up-to-date, or if there is an update that can be installed. If there is an update available, download and run it.

4B Configure new devices

Spending the time to set up the security features of a new device will help protect it from future threats.

When starting up a brand new device, it can be tempting to speed through the setup process in order to start using the device as quickly as possible. However, there are a number of ways you can maximise the security of a device during the setup process. Taking the time to configure devices properly will reduce the security risk of the device and prevent headaches down the line.

Following the setup process

Every device is different, but the best practices for data security are similar.

The exact steps to follow when setting up a new mobile or desktop device will vary, depending on the type of device. Organisations may have their own hardened baseline configuration of operating system images that will be installed on its devices. However, the following table outlines the main steps you should take when configuring a new device.

Adjust default password settings	New devices may include a default password, or let you enter a weak password. Be sure to apply a strong access password for the device, following the guidelines outlined in Topic 2. If you're setting up multiple devices, create a unique, strong password for each one.
Activate two-factor authentication	Two-factor authentication provides an additional layer of security than relying on a password alone. Follow the steps for activating two-factor authentication provided in Topic 2.
Remove unnecessary software	New devices often come with a lot of in-built software. As discussed previously, every piece of software needs to be patched to ensure it does not create security vulnerabilities on the device. Uninstalling software that you're unlikely to use is the best method for reducing associated security risks.
Turn on automatic security updates	For each piece of in-built software that will be used on the new device, check that automatic software updates are turned on. During the setup process, you may also be prompted to download and install the latest security updates. Ensure this process is able to run before using the device.
Install anti-malware software	The purpose and installation process of anti-malware software was discussed in Topic 2. Anti-malware software should be installed on new devices to provide ongoing protection from potential threats.

Disable location services	Location services (such as GPS and Bluetooth) may enable undesirable parties to see where the device user is located. Turning these feature off provides an additional safeguard for private information. Turning off Bluetooth also reduces the risk of unwanted parties attempting to connect to your device.
Disable cameras	If they are unlikely to be used in the course of work, consider disabling or physically covering cameras on devices such as phones or laptops. Hackers can take control of in-built cameras in order to spy on users, so taking these steps will reduce the risk of being spied on.

Router settings

When setting up a new desktop device, you may also be required to configure an internet router. A router is connected to a modem, and enables a Wi-Fi network to be created. This network can be accessed by your different devices. If a network is not secure, hackers may be able to enter the network and access private information. Therefore, it's important to ensure the internet router is properly configured to provide security across the network.

The following table provides good practices for setting up a router securely.

Enable automatic security updates
If possible, enable automatic security updates. This will enable the router to be automatically patched by the hardware manufacturer as any vulnerabilities arise.
Change the router login credentials
Some routers have default usernames and passwords that are used across different devices. Update these (using good password practices) to make it harder for hackers to gain access to the network.
Disable the broadcasting of your Wi-Fi network name
Preventing your Wi-Fi network name or Service Set Identifier (SSID) from being broadcast will make it more difficult for hackers to discover your network. At a minimum, change the Wi-Fi network name from the manufacturer's default name (which tells hackers the type of router you are using).

Install a firewall

Firewalls monitor and control incoming and outgoing network traffic. A firewall will help prevent malicious traffic (such as hacking attempts) from entering your network. Some router devices have an in-built firewall, but you need to check that it is turned on and correctly configured.

Use a virtual private network (VPN)

A virtual private network (VPN) encrypts the connection between devices. A VPN masks the internet protocol (IP) address on devices connected to the network, and goes some way to hiding them from hackers. A VPN also allows for greater privacy over the data that is sent and received by devices in your network.

Use WPA2

WPA2 (Wi-Fi Protected Access 2) is a form of secure encryption for data as it is communicated across your wireless network. If possible, use WPA2 instead of other encryption types such as WEP and WPA as it has additional security features.

Example

Configure new devices

Maryam works in the ICT department of an online toy retailer. She is setting up some new devices that have been purchased for the company's Sydney office, including desktop PC computers and a network router.

When setting up the PCs, Maryam adjusts the default password to a strong password, activates multi-factor authentication, turns on automatic security updates and installs anti-malware software. The PCs come with a lot of unnecessary inbuilt software that isn't required, which she uninstalls.

When setting up the internet router, Maryam activates WPA2 encryption, enables automatic security updates, installs a firewall and changes the login credentials from the username and password that are printed on the device. She also changes the network name (which was previously set to the device name) and prevents it from being broadcast.

Practice Task 13

Question 1

What are three things you could do to maximise the security of a mobile device when configuring it for the first time?

Question 2

Which of the following steps would you take when setting up a router to improve network security? Tick all that apply.

- ◯ Use WEP encryption if possible.
- ◯ Use a Virtual Private Network.
- ◯ Install a firewall.
- ◯ Ensure the network name is broadcast.
- ◯ Enable automatic security updates, if possible.

Summary

- Applying 'patches' (software/application security updates) protects devices from vulnerabilities.
- Patches need to be applied to operating systems, security software, internet browsers and plugins, and other workplace software.
- Automatic security updates should be used where possible.
- New devices should be properly configured to maximise their security.
- Measures to increase the security of a new device during the setup process include adjusting password settings, activating two-factor authentication, removing unnecessary software and turning on automatic security updates.
- Internet routers should also be configured to increase the level of security provided across a network.

Learning Checkpoint 4

Patch software and configure new devices

Part A

1. Which of the following statements regarding patching are correct? Select yes or no for each one.

   a) Desktop devices need to be patched, but mobile devices do not. » Yes » No

   b) The main reason for patching is to ensure that users have access to all the latest features and options. » Yes » No

   c) Automatic security updates should be activated whenever possible. » Yes » No

   d) After installing a patch, the device should be checked for correct operation. » Yes » No

Part B

Read the case study and answer the questions that follow.

Case study

Martina works for Puff'n'Stuff, an online stuffed toy retailer. Martina is configuring a number of new devices that have been purchased for company staff, including Windows PCs, iPhones and iPads. A new internet router has also been purchased.

1. Which of the following actions should Martina take when configuring the iPhones? Tick all that apply.

   ◯ Adjust the default password settings used on the device.

   ◯ Enable location services.

   ◯ Disable two-factor authentication.

   ◯ Install anti-malware software.

   ◯ Turn on automatic security updates.

2. Which of the following statements are correct? Select yes or no for each one.

   a) The main reason for configuring the router is to increase network security. » Yes » No

   b) Routers have built-in passwords that are hard to guess or identify. » Yes » No

   c) A VPN can increase data security across the Wi-Fi network. » Yes » No

   d) Data sent within a Wi-Fi network does not need to be encrypted. » Yes » No

   e) Martina should set the network name as the router model number. » Yes » No