BSB 7.0

BSBXCS405

CONTRIBUTE TO CYBER SECURITY INCIDENT RESPONSES

Aspire
Learning Resources

BSBXCS405

Contribute to cyber security incident responses

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.

BSBXCS405 Contribute to cyber security incident responses, Release 1

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

First published May 2021

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

e-ISBN 978-1-922466-53-2 (PDF version)
ISBN 978-1-922466-52-5

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 vi

Topic 1 | Confirm and contain cyber security incidents 1

1A Confirm nature and location of cyber incidents 2

1B Estimate risk, likelihood and potential consequence of cyber security incidents 12

1C Assist in containing cyber incidents and confirming no further risks 21

Summary 29

Learning Checkpoint 1: Confirm and contain cyber security incidents 30

Topic 2 | Communicate information on cyber security incidents 33

2A Escalate cyber security incident with workplace personnel 34

2B Consult with stakeholders on cyber incident communication needs 37

2C Assist in alerting external parties 44

Summary 50

Learning Checkpoint 2: Communicate information on cyber security incidents 51

Topic 3 | Contribute to post-incident activities 55

3A Support post-breach review and reporting 56

3B Assist in identifying lessons learnt and changes to response plan 62

3C Assist in updating cyber security response plan 68

3D Communicate lessons learnt and recommendations to personnel 71

Summary 78

Learning Checkpoint 3: Contribute to post-incident activities 79

Before you begin

This Learner Guide is based on the unit of competency *BSBXCS405 Contribute to cyber security incident responses*, 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 ▪ Understands developments within cyber security protection and is able to advise on which options are appropriate
Numeracy	▪ Interprets mathematical data ▪ Completes at times complex calculations and records mathematical data
Oral communication	▪ Asks open and closed probe questions and actively listens to clarify consult with business and ICT technicians ▪ Communicate findings of assessment of business impact to required personnel
Reading	▪ Recognises and interprets information from relevant sources to determine organisational expectations and legal requirements
Writing	▪ Uses clear, specific and industry-related terminology relating to cyber security ▪ Produce written reports on business impact of assessed threat
Planning and organising	▪ Manages cyber security incident response plan including protection strategies through to responding to breaches
Technology	▪ Uses appropriate technology platforms to assist with cyber security incident responses

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: Confirm and contain cyber security incidents	1A Confirm nature and location of cyber incidents	❑ Confident ❑ Basic understanding ❑ Not confident
	1B Estimate risk, likelihood and potential consequence of cyber security incidents	❑ Confident ❑ Basic understanding ❑ Not confident
	1C Assist in containing cyber incidents and confirming no further risks	❑ Confident ❑ Basic understanding ❑ Not confident
Topic 2: Communicate information on cyber security incidents	2A Escalate cyber security incident with workplace personnel	❑ Confident ❑ Basic understanding ❑ Not confident
	2B Consult with stakeholders on cyber incident communication needs	❑ Confident ❑ Basic understanding ❑ Not confident
	2C Assist in alerting external parties	❑ Confident ❑ Basic understanding ❑ Not confident
Topic 3: Contribute to post-incident activities	3A Support post-breach review and reporting	❑ Confident ❑ Basic understanding ❑ Not confident
	3B Assist in identifying lessons learnt and changes to response plan	❑ Confident ❑ Basic understanding ❑ Not confident
	3C Assist in updating cyber security response plan	❑ Confident ❑ Basic understanding ❑ Not confident
	3D Communicate lessons learnt and recommendations to personnel	❑ Confident ❑ Basic understanding ❑ Not confident

Topic 1 | Confirm and contain cyber security incidents

1A Confirm nature and location of cyber incidents

1B Estimate risk, likelihood and potential consequence of cyber security incidents

1C Assist in containing cyber incidents and confirming no further risks

1A Confirm nature and location of cyber incidents

Cyber security incidents can cause significant, and long-lasting, damage to organisations.

The Australian Cyber Security Centre (2021) defines cyber security incidents as 'an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.'

The following table outlines some of the main types of cyber security incidents.

Ransomware	Ransomware is a malicious form of software, or 'malware', that prevents users from accessing their files and systems. Typically, hackers demand a payment (or ransom) before they will unlock the user's files.
Malware	Malware is any form of malicious software that is designed to damage devices and networks. In addition to ransomware, other common forms of malware include: ▪ viruses ▪ worms ▪ spyware ▪ trojan horses (malware that is disguised as legitimate software). Some malware is designed to quickly spread across devices and networks to cripple performance.
Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks	DoS and DDoS attacks involve hackers overloading and shutting down a computer system by inundating the system with network traffic. In a DDoS attack, the traffic comes from many different sources. DoS and DDoS attacks can shut down networks for long periods, which can be very damaging to a business.
Phishing and social engineering	Phishing is a term used for attempts by hackers to obtain sensitive information via email. Hackers can be very clever at disguising their email addresses to look like those of other staff members or trusted figures. Phishing emails typically include one of the following: ▪ requests for login credentials ▪ online links that compromise security ▪ attachments that compromise security. In addition to phishing, hackers may use 'social engineering' techniques to trick staff into providing credentials or other sensitive information. An example of social engineering is hackers who call employees on the phone and pretend to be from the company's IT department.

Data breach	A data breach occurs when an organisation's information, such as customer data or trade secrets, is released to an unauthorised party. A data breach may arise from some of the incidents mentioned in this table. For example, if a hacker obtains login credentials via a phishing attempt, they may be able to gain access to a client database and extract sensitive customer data.

Cyber incidents can be caused by malicious actions of individuals and groups including:

- criminal organisations, both small and large
- people, both individuals and groups, hacking into systems for fun
- insiders, such as disgruntled employees of an organisation
- individuals or groups with an ethical or moral mission; these parties are sometimes referred to as 'hacktivists'
- nation-state actors: hackers supported and funded by international governments
- extremist groups.

The objectives and level of sophistication of these different parties may vary. However, their actions can all have harmful consequences and cause serious disruption to your organisation's systems.

Confirming cyber security incidents

In order to contain and eliminate cyber security incidents, they first need to be detected.

Hackers continually find new and better ways of covering their tracks, so cyber security incidents are not always evident to organisations. The unusual 2020 SolarWinds cyber breach, which penetrated multiple US Government departments, took around nine months to be detected. The longer an incident, such as a hack, remains undetected, the more time hackers have to steal data or cause other damage.

'Precursors' and 'indicators' are two methods used to detect cyber incidents.

Precursors	Precursors help to detect potential future cyber incidents. Common precursors include: ▪ news of the latest cyber threats, such as those published by the Australian Cyber Security Centre ▪ announcements by hacking groups about planned future hacks, or threatening emails received from such groups. While many cyber incidents are not detected until after they occur, the importance of precursors should not be discounted.

Indicators	Indicators identify the potential existence of an ongoing incident. They can be generated automatically by systems/software or can be raised by members of staff. While there are many potential indicators of cyber incidents, some common examples are: ▪ alerts generated by anti-malware software when a virus, or other malware, is detected ▪ an email administrator noticing large numbers of bounced emails containing suspicious content ▪ a system application generating an alert when multiple failed login attempts occur from an unfamiliar location ▪ a systems administrator identifying a filename with an unusual name or extension ▪ a network intrusion system generating an alert when an attack against a database server is identified ▪ a network administrator identifying a change in regular network traffic activity ▪ a staff member advising that they cannot login into the system using their normal credentials ▪ a customer reporting that the organisation's website is broken or functioning incorrectly.

Using mathematical data to identify indicators

You can use mathematical data, such as numbers and percentages, to help you identify whether an incident has occurred. Your organisation should have baseline data that shows system performance in normal circumstances. This may include data relating to:

- network traffic
- server speeds
- anti-malware software alerts
- login attempts
- incoming emails from outside the organisation.

If you find data that is significantly different to the baseline figures, it may help you identify a potential security incident.

The Australian Cyber Security Centre has suggested several data sources that can be used to help you detect, and investigate, a cyber security incident.

Domain Name System (DNS) logs	These logs can help you to check the existence of attempts to resolve harmful domains or Internet Protocol (IP) addresses. The presence of these may reveal an attempted or successful attack.

Email server logs	These logs can help you locate users who have been targeted via phishing emails.
Operating system event logs	These logs may reveal authentication events, security alerts and other file or network events relevant to a potential security incident.
Security software and appliance logs	These logs may help you identify unusual or harmful activity within your network security control.
Virtual Private Network (VPN) and remote access logs	These logs may help you identify any unusual addresses that have accessed your system. They can also help provide details about when malicious activity occurred.
Web proxy logs	These logs may help you identify HTTP (Hypertext Transfer Protocol) threat vectors and the traffic of malware in your system.

Source: Australian Cyber Security Centre (2021): Detecting cyber security incidents

Identifying the extent of an incident

When a cyber incident has been detected, the nature and extent of the attack needs to be determined. Understanding the incident will help identify an appropriate response.

Questions to ask when assessing an incident include:

- When did the incident occur, and is it still ongoing?
- What is the scope of the attack? This may include confirming what systems, networks and assets have been affected, what sets of data have been accessed, etc.
- What have the attackers already accessed, stolen or corrupted?
- What is the attackers' motivation? Possible motivations might be financial, such as in incidents of ransomware; theft of intellectual property, such as stealing trade secrets; personal attacks, such as stealing someone's sensitive photos; or disruption of services. Understanding the hackers' motivation may help you identify affected or threatened parts of your system more efficiently. If you know the attack is motivated by financial gain, your focus would be on the parts of your system that relate to money, such as customers' credit card details.
- Who has attacked us?
- How did the attackers gain access: was it via a phishing attempt or social engineering technique?
- Is the incident part of a broader attack, such as targeting comparable organisations or organisations that use a similar type of software?

Using an incident response plan

An incident response plan helps you to contain and manage a cyber incident.

In the event of a cyber incident, you need to follow your organisation's Cyber Incident Response Plan. As the name suggests, this plan will guide you through the process of responding to a current cyber threat.

Different organisations have their own incident response plans, developed to reflect their specific needs and system requirements. In addition, the Victorian Government has developed a generic cyber incident response plan template, which you can download from: aspirelr.link/vic-gov-prepare-cyber-incident

The key features of most incident response plans include:

Terminology and definitions	This section of a response plan gives definitions of the key terms used throughout the response plan. For example, it may include the organisation's definition of the difference between a 'cyber event' and a 'cyber incident'. Organisation-specific terminology and acronyms may also be defined here.
Common cyber incidents and responses	This section outlines the most common types of incidents faced by the organisation and details the initial response to each type. This section may also include common threat 'vectors' faced by the organisation. 'Vectors' are ways by which a cybercriminal can create an incident, such as via email or removable media.
Roles and responsibilities	This section details the team members responsible for managing cyber incidents. Each team member's details should be recorded including, at a minimum, their: – name – contact details – title – responsibilities when responding to an incident. Contact details for the senior executive management team may also be included in this section. These members may not have a hands-on role in managing a cyber threat but will need to be kept updated regarding the situation. They also may provide oversight and direction to the team.

Incident response process	This is the most important part of the incident response plan. It provides details about each step that should be followed in the event of a cyber incident. This process may vary between organisations. The process provided in the Victorian Government template includes the following main steps which are appropriate to many situations: ▪ Step 1: detection and analysis ▪ Step 2: containment and eradication ▪ Step 3: communications and engagement ▪ Step 4: recovery ▪ Step 5: learning and improvement.
Appendices	An incident response plan may also include appendices. These are forms and templates which should be filled out if an incident occurs. For example, appendices may include: ▪ situation update form ▪ incident log template ▪ resolution action plan ▪ evidence register ▪ IT assets and key contacts.

Other organisational policies and procedures

While your organisation's cyber incident response plan is the primary document you should refer to in the event of an incident, you also need to be familiar with several other policies relating to your organisation's information technology systems. In the event of a fast-moving cyber incident, you will need to comply with these policies to ensure sensitive information is not shared with unauthorised parties.

Acceptable Use Policy	This policy specifies how the information stored on an organisation's system is allowed to be accessed and used by staff. Typically, this policy specifies that organisational information: ▪ may be used only for the purpose of completing legitimate work tasks ▪ must not be used for any purpose other than in the context of performing work tasks. The policy may also specify activities which are classified as 'Unacceptable Use', such as: ▪ introducing malware onto an organisation's network ▪ sharing personal passwords ▪ using an organisation's devices and network to harass others. This policy helps organisations to maintain data confidentiality.

Access Control Policy	Not all employees of an organisation should have access to all the data held by the organisation. An access control policy outlines how access to sensitive information is managed. The policy may contain details about: ▪ the different types of account used in the organisation ▪ the conditions and access levels for each type of account ▪ the process for authorising new accounts and for changing the level of access for existing accounts ▪ the procedure for deactivating accounts that are no longer required ▪ the way system usage is monitored. This policy helps to ensure that sensitive information can only be accessed by authorised users and helps organisations to maintain data confidentiality.
Information Security Policy	An information security policy is a wide-reaching policy that may outline various controls relating to information security. This policy may include details such as: ▪ types of infrastructure and information that need to be protected ▪ classification of an organisation's information, from publicly accessible to highly confidential ▪ typical threats to the organisation's security ▪ staff responsibilities. This section may include similar information to the acceptable use policy ▪ access controls. This section may include similar information to the access control policy ▪ rules for connecting external devices to the organisation's network or for using remote access ▪ penalties for security violations ▪ procedures to be followed in the event of a security incident. This policy helps organisations to meet confidentiality, integrity and availability requirements.
Data Integrity Policy	The aim of a data integrity policy is to ensure that an organisation's information is both correct and complete. This may include identifying controls such as: ▪ reconciliation routines that check data has not been modified ▪ verification programs to check the consistency of data held on organisation networks ▪ processes to monitor system performance and identify attempts to corrupt the integrity of data ▪ methods to report suspected damage to data integrity. The policy helps organisations to maintain data integrity.

Gathering evidence

When a cyber incident is detected, you need to assist with gathering evidence. This evidence will help you and the team understand both how the incident occurred and the extent of the damage. If the incident is a cyber-crime, this evidence may be used when prosecuting the responsible party. Your organisation's cyber incident response plan may include a template for documenting collected evidence. Your organisation should also have an evidence collection process to ensure the integrity of evidence remains intact and therefore is admissible in a court of law.

Some types of evidence you may need to help gather include:

- system registers and logs
- cache data
- temporary file systems
- remote logging and monitoring data
- records of the physical configuration of system components
- archival media.

The most volatile evidence should be extracted first, as this is the evidence that hackers could potentially change or delete. The integrity of any evidence you gather must also be maintained. This could be done by storing it on a secure drive that cannot be accessed by unauthorised parties.

Example

Confirm nature and location of cyber incidents

Ramona works in the ICT department of AppTastic, a mobile app development company. She receives a call from another member of staff called Lewis. Lewis says that when he tried to turn on his computer this morning, he was faced with a screen which read: 'Oops! Your files have been encrypted. There is no way for you to access your files unless you send $1000 in bitcoin to the following address: shWHDUsoiwhdOIWSfj84729DHR. Your files will be deleted in 24 hours if you do not pay.'

Ramona knows that this appears to be a ransomware attack. She asks Lewis some more questions about his recent computer usage and performs some other system checks. She confirms that:

- the attack occurred overnight and is still active
- currently the scope of the attack is limited to Lewis's local computer
- last week Lewis clicked a link in an email which he thought was sent by AppTastic's CEO and this was probably a phishing attempt to gain his credentials
- the attacker's motivation seems to be financial.

The Australian Cyber Security Centre listed a recent alert about ransomware attacks on Australian IT companies, so this incident appears to be part of a broader attack.

Ramona knows this could be a serious incident and she needs to act fast.

Practice Task 1

Question 1

Which of the following are indicators of a potential cyber incident? Tick all that apply.

- ◯ A newspaper article about cyber-attacks on other organisations in your industry.
- ◯ Alerts generated by your organisation's anti-malware software.
- ◯ An announcement by a hacking group posted on Facebook about an upcoming malware attack.
- ◯ Unusual files in your system identified by a systems administrator.
- ◯ A helpdesk request from a staff member who cannot login using their normal credentials.

Question 2

List three questions you could ask when confirming the nature of a cyber incident?

Question 3

Which of the following would you expect to see in a cyber incident response plan?

- ◯ Appendices.
- ◯ Hacker's details.
- ◯ Terminology and definitions.
- ◯ Common cyber incidents and responses.
- ◯ Roles and responsibilities.

Question 4

In addition to the cyber incident response plan, what are two organisational policies you would comply with when responding to a cyber incident?

1B Estimate risk, likelihood and potential consequence of cyber security incidents

Accurately assessing risk enables us to effectively manage security incidents.

In the event of a cyber incident, one of the first steps is conducting a risk assessment. This process is sometimes referred to as 'triage'.

A risk assessment helps us to determine the incident's potential organisational damage, and respond accordingly. Risk assessments help organisations both to understand the existing system and environment, and to identify risks through analysis of the information/data collected. It is a continuous process which should not only happen once an incident occurs. A high-risk incident with the potential to cause major damage to the system will require a greater response in terms of urgency, resourcing and budget than a lower risk incident.

The two main elements of risk assessment are identifying:

- the likelihood of the risk occurring
- the potential impact (or consequence) on the organisation if the risk occurs.

Types of risk

A risk can be defined as an uncertain outcome. While risks can be positive or negative, in cyber security we generally focus on negative risks as these create unwanted outcomes for an organisation.

When evaluating the risk level of a cyber incident, the three main types of risk are:

Loss of confidentiality	▪ Your organisation's system is compromised by unauthorised parties, such as SAP ASE hackers. ▪ Your system's data is released to the public without authorisation.
Loss of integrity	▪ Your organisation's system cannot be trusted. ▪ Your system, and the data it contains, is no longer complete or correct.
Loss of availability	▪ Your organisation's system, and the data it contains, no longer exists. That is, the system has been destroyed. ▪ Your system does not respond to queries from authorised users. ▪ Your system and data cannot be restored by authorised users.

Source: Ulowa (2020): System risk analysis: Determining risk levels

Assess risk likelihood

You need to understand both threats and vulnerabilities in order to assess risk likelihood.

The first step in risk assessment is to estimate the likelihood (or probability) of the risk occurring.

Assessing risk likelihood requires you to consider two factors:

- the probability of a risk occurring
- the current vulnerability or weakness of your ICT system to the threat.

Some examples of this are:

- Australian financial planning companies are currently being targeted by financially motivated ransomware attacks. You work at a financial planning company which uses outdated anti-malware software. In this instance, both the probability of confidentiality loss and the vulnerability of your organisation's system is high. This means the overall likelihood of confidentiality loss is also high.
- Your organisation has recently set up two-factor authentication on all devices and network accounts and has just identified a phishing attempt on a member of staff. In this instance, the possibility of the hacker attempting to access company accounts using stolen credentials is high, but the company's vulnerability to the threat is relatively low, due to two-factor authentication. This would mean the overall likelihood of data being lost as a result of the phishing attempt may be either possible or somewhat unlikely.

Ranking risk likelihood

Consider both the probability of the threat occurring and your organisation's current vulnerability to the threat. Rank the overall risk likelihood using the following scale.

1	Highly unlikely
2	Unlikely
3	Possible
4	Likely
5	Almost certain

Risk management involves dealing with the unknown, so ranking the likelihood of each risk requires you to make some educated guesses. The accuracy of this process may be improved by asking:

- how often has our organisation experienced the same threat in the past?
- how vulnerable is our organisation to different types of threats?

It is a good idea to estimate risk likelihood in collaboration with colleagues and stakeholders to improve the quality and consistency of rankings assigned.

Assess risk consequences

What damage would occur in the event of a cyber threat?

Having estimated the risk likelihood, you now need to estimate the risk consequences, also referred to as 'impact'. The following table identifies some negative impacts an organisation may experience due to a cyber risk.

Revenue loss	▪ Significant revenue losses will immediately occur if an online store's website crashes due to a hacking attempt. ▪ Some cyber threats have more subtle impacts, such as system slowdown and increased downtime. While less immediately damaging, revenues lost because of IT downtime can quickly add up. ▪ In addition, significant spending may be required to repair or replace equipment damaged by a threat. ▪ The average cost of a data breach in Australia was estimated at around $3.35m in 2020.
Damage to brand reputation	▪ A business's reputation is often built on consumer trust. If sensitive customer data is hacked, customers will be less likely to do further business with that organisation. ▪ Previous hacks, such as the 2014 hack of film company Sony Pictures, have also resulted in embarrassing internal emails being shared publicly, further damaging organisations' reputations.
Loss of intellectual property	▪ As well as customer data, intellectual property (IP) can be the most valuable asset held by many organisations. The loss of IP, such as designs and strategies, may cost an organisation its competitive edge. ▪ As a result of the Sony Pictures hack mentioned above, a number of movies in production were leaked online prior to their official release.
Legal damage	▪ Data breaches may involve significant legal consequences both from regulators and from people whose data has been breached. This may include the issuance of fines and penalties. ▪ Following a major data breach resulting from a hack in 2017, Equifax was required to pay nearly $700 million in fines.

Source: The Ame Group (2020): Data security breach: consequences for your business

A single cyber risk may result in one or more of the above impacts. You can estimate the potential overall impact for each risk using the following scale.

1	Insignificant
2	Minor
3	Moderate
4	Major
5	Critical

Not every risk will result in a critical business impact.

Breaches of highly sensitive information, such as customer information or trade secrets, are more likely to have critical impacts on the organisation. Breaches of non-sensitive information, for example already publicly available information, are less likely to have serious impacts. Critical impacts could include legal, commercial, and reputational consequences.

Just as when estimating the risk likelihood, it is best to estimate risk impacts with colleagues and relevant stakeholders. You are unlikely to know everything about your organisation, so it is best to get a variety of viewpoints and insights in order to estimate impacts accurately.

Using a risk matrix

A matrix helps you to visualise each risk.

A single cyber incident may present a number of different risks. For example, an unauthorised user within your system may threaten the system's confidentiality, integrity and availability, or a combination of the above. It can be difficult to know what you need to fix first. Assigning levels to each risk helps to define the urgency of each threat. In turn, this enables decision-makers to identify how to best allocate resources to address the incident.

As discussed in the previous section, the likelihood and potential impact for each risk needs to be identified. A 5-point scale can be used for each.

This information can be presented in a risk matrix. Different organisations use different risk matrix templates, but a common format is shown below.

Likelihood \ Consequences	Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	High	High	Very high	Very high	Very high
Likely	Moderate	Moderate	High	Very high	Very high
Possible	Low	Moderate	High	High	Very high
Unlikely	Low	Low	Moderate	Moderate	High
Rare	Low	Low	Low	Low	Moderate

Each risk will be located in either the red, orange or green part of the graph, depending on the likelihood and risk ratings. For example:

- Risks with a likelihood of 4 and an impact rating of 3 will be located in the red part of the matrix.
- Risks with a likelihood of 2 and an impact rating of 4 will be located in the orange part of the matrix.
- Risks with a likelihood of 1 and an impact rating of 2 will be located in the green part of the matrix.

The following table outlines how different levels of risk should be managed.

Red risks (high level)	These are high level risks that need to be addressed urgently. In the next section, we will look at potential strategies for controlling and eradicating these risks.
Orange risks (medium level)	These are medium level risks that, while needing to be addressed, are not as urgent as high level risks. Potential strategies for controlling and eradicating these risks will be looked at in the next section.
Green risks (low level)	These are low level risks that can be accepted by the organisation with ongoing monitoring and routine management.

Calculating risk scores

Risk scores are another way of quantifying each risk.

A total risk score for each risk can be calculated by multiplying the risk likelihood by the risk impact. **Likelihood** × **Impact** = **Risk**. For example:

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

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

Risk score 12-25 (high level)	These are high level risks that need to be addressed urgently.
Risk score 3-11 (medium level)	These are medium level risks that, while needing to be addressed, are not as urgent as high level risks.
Risk score 1-2 (low level)	These are low level risks that can be accepted by the organisation with ongoing monitoring and routine management.

Classifying risks

Ordering risks by urgency helps us to focus on high risks.

During the risk assessment process, you may identify a number of different risks relating to a single security incident. Identifying the highest scoring risks enables you to make recommendations about which threats need to be addressed as quickly as possible.

A risk register can be used to document risks you have identified. Organisations may use a variety of risk register formats, but a standard template that includes examples is provided below.

Risk category	Likelihood	Impact	Risk score	Risk level
Loss of confidentiality	**High (5)** Hacker motivation appears solely to be stealing customer information. Initial logs show client databases have already been accessed.	**Critical (5)** Loss of sensitive information will have widespread financial, and legal, impacts on the business.	25	High
Loss of integrity	**Unlikely (2)** Corrupting data does not appear to be a motivation of the hacker. No changes have been made to system files.	**Major (4)** Back-ups of sensitive data are currently only run once a month, so significant amounts of data may be damaged if malware enters the network.	8	Medium

Risk category	Likelihood	Impact	Risk score	Risk level
Loss of availability	Highly unlikely (1) Compromising system availability does not appear to be a motivation of the hacker. All systems are currently online.	Minor (2) Redundant off-site servers are available and can be brought online within 2-4 hours if main server goes down.	2	Low

As shown in the example above, risks should be listed from highest to lowest. Once this part of the risk register has been completed, mitigation strategies for each risk can be identified and added.

Categorising the incident

Your organisation's cyber incident response plan may specify different categories for incidents, based on their level of risk. For example, the incident response plan template provided earlier includes 4 categories:

Cyber event	This category relates to suspected (or unconfirmed) threats which have not had any impact on organisational systems.
Cyber incident	This category is for incidents where security controls have been compromised resulting in minor impacts to organisational services, data and assets. However there has not been a data breach.
Significant cyber incident	This category refers to incidents which have had a limited or major impact on organisational services, data and assets. Any incident involving critical infrastructure, or where a data breach has occurred, automatically classifies as a significant incident.
Cyber emergency	This category is reserved for serious and exceptional incidents that may lead to extensive or permanent damage.

Source: Victorian Government Cyber Incident Response Plan Template (2021)

Example

Estimate risk, likelihood and potential consequence of cyber security incidents

Ramona is part of a team working to assess the risk level of a ransomware attack on her company. Based on their current knowledge of the incident, they complete the following risk register.

Risk category	Likelihood	Impact	Risk score	Risk level
Loss of confidentiality	Moderate (3) At this stage, stealing information does not appear to be the hacker's motivation. Initial logs show client databases have not been accessed.	Critical (5) Loss of sensitive information will have widespread financial, and legal, impacts on the business.	15	High
Loss of availability	Likely (4) One staff member has already lost access to their data. Attack appears to be limited to one staff member only at this stage.	Minor (2) Apart from some non-sensitive files saved on staff member's desktop, all files have been safely backed up and can be restored.	8	Medium
Loss of integrity	Unlikely (2) Corrupting data does not appear to be a motivation of the hacker. No changes have been made to system files.	Minor (1) Back-ups of sensitive data are run daily so can be restored without losing extensive information.	2	Low

Based on this assessment, the ransomware attack is classified as a cyber incident. Ramona's team now needs to consider how to contain and eradicate the threat.

Practice Task 2

Question 1

Which of the following statements are correct regarding risk assessment for a cyber incident? Select yes or no for each one.

a) If the likelihood of a risk is high, the consequence will also be high. » Yes » No

b) The consequences of a risk are measured in dollar amounts. » Yes » No

c) A cyber incident response plan should include information about how to classify an incident. » Yes » No

d) The main risks in a cyber incident are loss of confidentiality, integrity and availability. » Yes » No

Question 2

The likelihood of a risk event has been estimated as 4. The potential consequences of the risk have been estimated as 3. What is the total score for this risk?

1C Assist in containing cyber incidents and confirming no further risks

Cyber incidents must be contained, then eradicated.

If you are helping with the response to a serious cyber incident, you may think the focus should be on totally removing the threat from the system. However, the first step is usually to 'contain' the threat. Once the threat is contained, the team can focus on strategies for eradicating it.

Containment strategies

Containment helps to slow the spread of damage.

Containing damage caused by a cyber incident means preventing it from spreading to other parts of the system and causing more damage.

The objective of containment is typically not to eliminate the threat, or return to business as usual, but to make short-term alterations while planning longer-term solutions.

Some of many containment strategies available include:

- blocking unauthorised users from accessing systems
- blocking sources of malware, such as compromised emails or websites
- closing compromised ports and mail servers
- changing passwords if these have been, or are suspected of being, compromised
- updating firewalls
- isolating compromised systems from the network.

Matching containment strategies to the incident

The specific containment strategies chosen should reflect the nature of the cyber security incident. The following table identifies potential containment strategies for common cyber security incidents.

Type of incident	• Potential containment strategies
Ransomware	• Isolate infected device/application from the network to prevent ransomware from spreading.
Malware	• Isolate infected device/application from the network to prevent malware from spreading.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks	▪ Work with network team to apply filters or increase capacity.
Phishing and social engineering	▪ Change account passwords. ▪ Monitor accounts for unauthorised access.
Data breach	▪ Change passwords to data sources. ▪ Block compromised accounts from accessing data.

By performing containment strategies such as those identified above, you are essentially mitigating, or lowering, the risk level of the cyber incident. This is because you are reducing the level of damage that can occur as a result of the incident.

If you consider the risk assessment process, containment actions help to lower your system's vulnerability to further damage. This helps to reduce the likelihood and overall risk level of further damage arising from the incident.

Generally, the faster you are able to contain an incident, the less damage it can do to your systems.

Eradication strategies

Containment is just the first step. Threats need to be eradicated.

After the incident has been contained, your team can focus on eradicating the threat. Eradication means completely removing the root cause of the incident from your system. For example, if your system has been infected with malware, eradication strategies will focus on completely removing the malware from the system, then hardening the system, via patches and updates, to prevent reinfection. When eradication efforts have been completed, no further risk should exist.

Depending on the severity and complexity of the incident, members of your team or a third party might be involved in the eradication process.

Any eradication process must be thorough. Even small amounts of remnant malware can continue to cause damage to your system.

To confirm whether the eradication process has been successful, you should ask:

- Has the root cause of the incident, such as malware or other issues, been securely removed from the system?
- Has the system been hardened, through the use of patches and updates, to prevent the same issue from occurring again?
- Has all organisational documentation relating to eradication processes been completed?

Providing assistance

Depending on your role, and the structure of your team, you are likely to be assisting others in containing and eradicating cyber security incidents rather than doing it all yourself. Other members of the incident management team who you may need to assist include your organisation's:

- IT security manager
- business continuity manager
- chief information officer
- chief information security officer
- ICT team leader or manager.

Here are some tips to bear in mind when assisting other members of the team.

Ask questions if you are unsure

If you are unsure about what you are required to do during a cyber incident, ask questions. You can use open and closed questions as required in order to confirm the best way to help your team.

In a potentially high-risk situation, it is much better to take the time to be certain of what is needed rather than possibly do the task incorrectly.

Take notes and create a checklist

Do not try to memorise everything that is said to you. In a fast-paced situation such as a cyber incident you may forget important details. Write down the tasks that have been allocated to you, including any important information, such as when the task needs to be done by, who needs to be involved and so on.

Creating a checklist of your tasks will make it easier to keep track of what still needs to be done. It will also help you prioritise competing priorities. Consider using a resolution action plan.

Provide updates

Keep your team members updated about the status of the tasks you have been allocated. Your organisation or team may have specific protocols about how to keep the team informed. It may be as simple as sending an email or using another internal communication tool such as Teams, Trello or Hangouts.

Stay calm

Cyber security incidents, especially those that are ongoing, can be stressful events.

Stress can affect our ability to think critically, so it is important to remain calm when working with other members of the team. Even if other team members are stressed, keep your composure and provide support to find solutions.

Policies and procedures

Your organisation's cyber incident response plan should be the main piece of documentation you refer to when containing and eradicating a threat. Your organisation's plan should outline the steps to take when responding to a threat as this ensures a consistent approach to cyber threat management.

The cyber incident response plan may include a resolution action plan template, probably in the appendices. The resolution action plan outlines what actions the team will take to resolve the incident. Each action should include the following details:

- Details of the action.
- Category of the action: does it relate to containing or eradicating the threat?
- Date and time of the action.
- Team member who 'owns' the action and is responsible for ensuring the action is done.
- Current status of the action. Is it: in progress, unallocated or closed?

You can support your team by helping to complete the resolution action plan and ensuring allocated items are followed up by the team members responsible.

Legislative requirements

You need to comply with data laws when responding to a cyber incident.

When you respond to a cyber incident, you need to be aware of and comply with laws relating to sensitive data and information. In particular, these laws relate to the handling of personally identifiable information (PII). This is information that can be used to identify a person and could cause harm to them in the wrong hands, such as bank details, passport numbers, health records and so on. You may encounter these types of information during an incident response and must comply with relevant laws when doing so.

Legislation regarding sensitive information exists at Australian state, Australian Commonwealth, and international levels. You will generally need to comply with legal requirements at all three levels.

Australian Commonwealth requirements

The Privacy Act

The *Privacy Act 1988 (Cth),* is the most important piece of federal legislation relating to the management of personal information. The Privacy Act includes requirements around the:

- collection of personal information
- use of personal information
- storage of personal information
- disclosure of personal information.

The Privacy Act applies to:

- Australian Government agencies
- private organisations, such as companies, with an annual turnover more than $3 million.

The Privacy Act generally does not apply to:

- state and territory government agencies
- small businesses with a turnover less than $3 million*

* Some small businesses are covered by the Privacy Act. Please check the following link for full details of the types of businesses that are, and are not, covered: aspirelr.link/oaic-privacy-act

Australian Privacy Principles (APPs)

The Commonwealth *Privacy Act* provides 13 Australian privacy principles (APPs). These principles apply to all organisations that have responsibilities under the Privacy Act. The APPs relate to all stages of handling personal information including collecting, using, storing and disclosing information.

For a helpful summary of the 13 APPs, download the information poster from the Australian Government Office of the Australian Information Commissioner (OAIC) website: aspirelr.link/oaic-privacy-principles

Notifiable Data Breach (NDB) Scheme

The notifiable data breach (NDB) scheme commenced in 2018 and applies to organisations who have responsibilities under the Privacy Act. Under the NDB, organisations must report data breaches both to the individuals whose data is affected by the breach, and to the Office of the Australian Information Commissioner (OAIC).

A data breach occurs when personal information is:

- accessed or disclosed without authorisation
- lost.

Data breaches can be generally categorised into the following areas:

- a device with an individual's personal information is lost or stolen such as credit card theft
- a database with personal information is accessed without authorisation
- personal information is mistakenly given to a wrong party.

Implications of the NDB Scheme on an organisation

Failure to comply with notifiable data breach (NDB) laws, can incur penalties for organisations.

Non-compliance could mean serious fines, for example:

- companies can be fined up to $1.8 million
- individuals can be fined up to $360,000.

The NDB scheme means that organisations and individuals need to take proactive steps when dealing with personal information.

We will look at breach reporting in more detail in Topic 2.

Australian state and territory requirements

Commonwealth laws and state/territory laws have many similarities. However, there are specific differences in each state and territory. It is important to identify and adhere to the legislation under which your organisation operates. When state/territory and Commonwealth laws are in conflict, the overarching Commonwealth law prevails.

For more information on privacy laws in your jurisdiction please visit the Australian Government's Office of the Australian Information Commissioner (OAIC) here: aspirelr.link/oaic-state-privacy

Here is a list of Privacy legislation in each State and Territory.

ACT	*Information Privacy Act 2014 (ACT)*
NSW	*Privacy and Personal Information Protection Act 1998 (NSW)*
NT	*Information Act 2002 (NT)*
QLD	*Information Privacy Act 2009 (QLD)*
SA	*None, SA refers to Commonwealth Privacy Act 1988 (Cth)*
TAS	*Personal Information and Protection Act 2004 (TAS)*
VIC	*Privacy and Data Protection Act 2014 (VIC)*
WA	*Freedom of Information Act 1992 (WA)*

International requirements

In today's global world, you also need to be aware of international data protection laws.

On the 25th of May 2018, the General Data Protection Regulation (GDPR) was enacted by the European Union. The GDPR is designed to protect personal data of European (EU) citizens and residents by increasing the obligations of organisations who collect and process data.

The GDPR offers EU citizens more rights over:

- who has access to their data
- where and how their data is stored and used
- having their personal information removed or deleted from databases.

There are large potential fines for organisations that breach the GDPR, even if the organisation is not based in the EU.

Australian organisations and the GDPR

Australian organisations need to comply with the GDPR if they:

- have a presence in the EU
- offer goods or services in the EU
- process data and monitor EU citizens and residents.

This regulation is far reaching and does overlap with the Australian notifiable data breaches (NDB) scheme. For example, the GDPR also requires that data breaches are reported, much the same as the requirements of the NDB scheme. Both NDB and GDPR promote the confidentiality of personal identifiable data.

Example

Assist in containing cyber incidents and confirming no further risks

Ramona is working in a team responsible for containing and eradicating a ransomware attack on a member of staff named Lewis. To contain the incident, the team follows the company's cyber incident response plan and:

- isolates Lewis's computer from the network so that the ransomware cannot spread
- identifies the phishing email which Lewis clicked on and blocks the address from accessing the company network
- resets passwords for sensitive accounts to ensure these cannot be accessed by the source of the ransomware.

The ransomware is still installed on Lewis's computer. The team escalates the eradication process to a third party who specialises in ransomware deletion. After the specialist has completed their work, Ramona supports the team to check that all traces of the ransomware have been removed from Lewis's computer, and that all security software has been updated to prevent further attacks. Although this attack did not result in a data breach, Ramona is aware that her company has responsibilities to report any breaches of customer data under the NDB scheme.

Practice Task 3

Question 1

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

a) The notifiable data breach (NDB) scheme applies to all organisations with responsibilities under the Privacy Act. » Yes » No

b) Australian organisations must be registered overseas to comply with the GDPR. » Yes » No

c) Australian organisations may need to comply with Australian federal, state and international laws when handling data. » Yes » No

d) Failure to comply with the DDB scheme may result in large fines. » Yes » No

Question 2

Where would you locate your organisation's procedures for containing a cyber incident?

Question 3

In the event of a DDoS incident, what would be an appropriate containment strategy?

Question 4

What are two checks you would perform after an eradication process has been conducted?

Summary

- Cyber security incidents are unwanted or unexpected cyber security events that have a significant probability of compromising business operations.
- Without active monitoring, cyber security incidents may not be detected.
- 'Precursors' and 'indicators' are the two main ways of detecting potential incidents.
- An organisation's cyber incident response plan provides guidance on how to respond to an incident.
- All incidents, and suspected incidents, should undergo risk assessment to help identify their seriousness.
- Risk assessment involves estimating the likelihood and potential impact of different risks.
- Containing a cyber incident involves preventing it from spreading to other parts of the system and causing more damage.
- Containment strategies can mitigate the risk posed by an incident. These strategies need to be matched to the nature of the incident.
- Eradicating a threat means totally removing it from the system.
- When responding to a cyber incident, you need to comply with organisational and legislative requirements. You must be especially aware of requirements relating to the privacy of personal data.

Learning Checkpoint 1

Confirm and contain cyber security incidents

Part A

1. Number each step from 1 to 5 in the order you would follow when responding to a cyber incident according to an incident response plan.

   ◯ Perform recovery steps

   ◯ Detect and analyse the incident

   ◯ Engage in learning and improvement

   ◯ Perform communications and engagement

   ◯ Contain and eradicate the threat

2. List three sources of data you would access and analyse when confirming the nature and location of a cyber incident?

Part B

Read the case study, then answer the questions that follow.

Case study

Kris works in the ICT department of BetterNow, a health insurance company. An incident has been detected in which hackers have accessed company clients' sensitive information, including Medicare details.

1. Kris's team estimates the likelihood of confidentiality loss as '5' and the impact of this event as '5'. What is the total risk score?

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

   a) The cyber incident response plan should include details about how to classify the incident based on its risk profile. » Yes » No

   b) BetterNow will probably need to report this breach under the NDB scheme. » Yes » No

   c) If BetterNow's clients include EU citizens, it will need to comply with the GDPR reporting requirements. » Yes » No

   d) The threat must be contained and eradicated before it is escalated. » Yes » No

3. List **one** risk mitigation strategy that could be used to contain the data breach.

4. When assisting the team to confirm that no further risks exist, what strategies should Kris use? Tick all that apply.

   ◯ Do everything herself before seeking assistance.

   ◯ Keep the team updated on progress.

   ◯ Memorise all the details of the incident.

   ◯ Create a checklist of actions to be completed.

   ◯ Remain calm under pressure.

Topic 2 | Communicate information on cyber security incidents

2A Escalate cyber security incident with workplace personnel

2B Consult with stakeholders on cyber incident communication needs

2C Assist in alerting external parties

2A Escalate cyber security incident with workplace personnel

You are not expected to solve every issue yourself but to escalate when necessary.

When responding to a cyber security incident, you need to know how to escalate the issue. This means passing it on to a more senior or specialised employee or team. Escalation often occurs during normal ICT work and responding to incidents is no different.

For example, if you work in a general ICT helpdesk, your team may have the skills and knowledge required for responding to lower-level threats, such as an attempted phishing attempt on a member of staff. Serious incidents, such as a DDoS attack, may need to be escalated to a more senior member of your ICT department.

Using an Escalation Policy

Your organisation's escalation policy will outline how, and when, to escalate an issue.

While the cyber incident response plan should include some information regarding escalation, your organisation should also have an escalation policy in place. The escalation policy outlines:

- what events should trigger an incident to be escalated. For example, if there is a threat of data breach
- who incidents should be escalated to, such as the role or name of the responsible person
- how incidents should be escalated.

There are three different types of escalation which may be used, depending on the nature of the incident.

Hierarchical escalation

In hierarchical escalation, an incident is passed on to a more senior member of the organisation.

For example, a junior ICT technician may escalate an issue to the ICT team leader. If the team leader cannot resolve the issue, they may escalate it upwards to the manager of the department.

Functional escalation

In functional escalation, an issue is passed on to the person best equipped to resolve the issue. This person may not necessarily be in a senior position. For example, the ICT team leader may escalate an issue relating to a bug in an app to the junior who developed that app.

Automatic escalation

Some help desk platforms enable automatic escalation workflows. These workflows will automatically escalate an issue to a team member if it has not been addressed or closed in a timely manner. The workflows may use a combination of both hierarchical and functional escalation, depending on how they are configured.

Source: Atlassian, (2021): Escalation policies for effective incident management

Methods of escalation

The way you escalate a cyber incident should be specified in your organisation's escalation policy.

Unless your organisation is very small, it should have service desk, or helpdesk, software in place. This software helps you to manage and track the status of different issues and incidents. Escalating an issue via service desk software will typically require you to:

1. Allocate the ticket to a staff or team member according to the escalation policy.
2. Specify the status and urgency of the incident.
3. Add any information regarding the incident which is not already in the service desk system. This information will enable the person taking on the issue to quickly understand the issue.

In critical ongoing incidents where data is at risk of being compromised, it may also be beneficial to call the person whom the ticket is being escalated to. This will ensure the person is immediately aware of the issue and its urgency.

If you work for a very small organisation that does not have helpdesk software, the processes for escalating issues may be less formal. You may escalate the issue via email, phone call, or a combination of these.

Example

Escalate cyber security incident with workplace personnel

Toby works in the helpdesk team at Fly Fast, an online travel company. Toby receives a helpdesk request from a member of staff who says their computer is running sluggishly. When several similar requests come through, Toby's team suspects the company's server is being subjected to a DDoS attack.

Referring to Fly Fast's escalation policy, Toby escalates the potential incident to senior engineer Clara via the helpdesk system. Toby also gives Clara a call to make sure she is aware of the ongoing incident.

Practice Task 4

Question 1

Draw a line to match each term about incident escalation to its definition.

» Automatic escalation	» Issues are passed on to the next person up in the organisational structure.
» Hierarchical escalation	» Issues are passed on to the person with the most relevant skills to the issue.
» Functional escalation	» Issues are passed on based on system-defined workflows.

Question 2

Which of the following should be outlined in an escalation policy? Tick all that apply.

- ◯ To whom you should escalate an incident.
- ◯ Who could cause a cyber incident attack.
- ◯ What the risks of cyber incidents are.
- ◯ What cyber threats should be escalated.
- ◯ How you should escalate an incident.

2B Consult with stakeholders on cyber incident communication needs

Effective communication is an important part of a cyber incident response.

At this point, you have escalated the cyber incident to relevant staff members. Depending on the scale of the incident, there may be other internal and external stakeholders who need to be informed. Supporting your team to develop a communications plan is the best way to ensure that all relevant parties are kept aware of the situation.

An effective, structured communications plan may help your team to:

- limit the damage caused by an incident. For example, by alerting staff to a phishing attempt and thereby preventing further staff from being tricked, or by ensuring customers change their passwords as quickly as possible
- meet legislative requirements with regard to data breaches
- limit reputational damage caused by a cyber incident. For example, by showing your customers you are working to address the incident instead of covering it up.

Developing a communications plan

A communications plan provides a structured approach to communicating with your organisation's internal and external stakeholders about a cyber incident. Your organisation may have an existing format for a communications plan, or you may need to develop your own.

The communications plan should include the following details:

Stakeholders

The stakeholders you need to communicate with regarding a cyber incident may be either internal or external to your organisation.

Communication objective

Here is where you specify the purpose of your communication; that is, what you want to achieve from it. For example:

- you may want to communicate with customers to limit the extent of damage. This could be letting them know they should update their password if it has been compromised
- you may want to communicate with Government stakeholders to comply with legislative requirements
- you may want to communicate with managers to keep them aware of an ongoing incident.

Level of urgency

Assigning an urgency level (such as low, medium or high) to each stakeholder group will help you prioritise your actions. Communications that will help to contain or mitigate damage arising from an incident should be considered more urgent than communications simply designed to keep stakeholder groups aware.

Required actions

Here is where you specify how the communication will occur. Some urgent stakeholder communications may require several actions. For example, alerting customers about a data breach may involve:

- directly emailing affected customers
- putting a notification on your organisation's website
- setting up a hotline to manage telephone queries from affected customers.
- Ensure these actions are consistent with your organisation's policies and procedures for internal and external communications.

Due date/time

This is where you specify by when the communication action/s need to be completed. Any communications which have been identified as highly urgent should be addressed first.

Responsibility

Ensure the team is clear about who is responsible for completing each communication action. In some cases, a given action may involve several members of the team and other organisational staff. For example, posting an alert on your organisation's website may involve both public relations staff to write the message in consultation with the ICT about the incident, and the web development team to post the message.

Status

Track the progress of each communication item so that nothing is overlooked. Each item can be flagged as:

- not yet started
- in progress
- completed.

Considering stakeholders

Your communications plan should consider both internal and external stakeholders of your organisation. Stakeholders are individuals and groups who are affected by, and can affect, the organisation's actions.

Internal stakeholders	Internal stakeholders who may need to be included in the communications plan include: ▪ employees ▪ managers ▪ owners.
External stakeholders	External stakeholders who may need to be included in the communications plan include: ▪ government agencies ▪ customers ▪ shareholders ▪ suppliers ▪ society.

Consulting with your stakeholders

It is best to develop a communications plan as a team, incorporating feedback from multiple stakeholders. This may include ICT technicians and other business specialists who understand complex details of an incident.

Consulting with a variety of stakeholders will help ensure multiple perspectives and opinions are considered regarding communication requirements arising from a cyber incident. When consulting with stakeholders, use these communication strategies.

Ask open and closed questions	Asking a variety of closed-ended and open-ended questions will help you obtain the information you need to create a communications plan. Closed-ended questions have a limited set of answers such as yes or no. Examples of closed-ended questions you might ask your stakeholders include: ▪ has this incident compromised our customers' data? ▪ has this incident now been contained? ▪ do we need to communicate this incident to our government stakeholders? Open-ended questions cannot be answered with a yes or no, and generally require a longer response. You can use open-ended questions to draw out more information from your stakeholders. Some open-ended questions you might ask your stakeholders include:

Ask open and closed questions (cont.)	▪ which stakeholder groups do we need to communicate with urgently? ▪ what types of data were compromised because of this breach? ▪ what steps are being taken to contain the incident? Both closed-ended and open-ended questions have their advantages. Be sure to use a mix of both question types when consulting with your stakeholders.
Use active listening	Active listening enables you to focus on the stakeholder and stay engaged in the conversation. It involves: ▪ listening attentively to what the other person is saying ▪ using visual cues to show you are engaged such as nodding and avoiding looking at your phone ▪ paraphrasing what the other person says to show you have understood it ▪ waiting until the other person finishes speaking before you reply.
Take notes	In the context of a fast-moving cyber incident, consulting with stakeholders may be just one of many tasks you need to perform. Take notes of any discussions you have. Not only will this help you work from accurate information, but it also means there is less information you need to retain in your short-term memory.

Policies and procedures

When developing a communications plan for a cyber incident, you need to follow your organisation's policies and procedures relating to internal and external communications. An internal communications policy relates to communications with internal stakeholders and an external communications policy relates to communications with external stakeholders.

While addressing different audiences, both these policies should include the following details:

Approved communication channels	A complete list of the communication channels that can be used with the audience, whether internal or external stakeholders. A few examples of communication channels include: ▪ group emails ▪ social media posts ▪ publicly visible emails or announcements on an organisation's website ▪ messages posted to individuals within the organisation's system. For example, only visible to a customer after they login to a secure area on your website. Communication plans should also include an emergency communication channel, such as via SMS, to inform all internal stakeholders in case an incident disables all standard methods of communication.
Approved purpose for each communication channel	Each of your organisation's communication channels should have an approved purpose. For example, a communications policy may specify that information regarding a data breach must be sent directly to external stakeholders via email.
Specific details about how each channel should be used	The communications policy should provide details about the correct use of each communications channel. For example, with regard to using email to contact external stakeholders, the policy may specify: ▪ the company email address which is to be used ▪ who is authorised to send emails from this account ▪ rules around the use of BCC, so that customers cannot see other people's email addresses ▪ how replies to emails should be dealt with, for example, to whom they should be referred.

Example

Consult with stakeholders on cyber incident communication needs

Preeti works in the ICT team at HealRight, a medical centre. The organisation has just discovered a cyber-attack in which patients' medical records and appointment login information were accessed by hackers. Preeti consults with different members of the ICT team to find out more information about the hack and helps to develop a communications plan relating to the incident. A section of the communications plan is as follows:

Stakeholder group	Objective	Urgency	Required actions	Due date	Responsibility	Status
HealRight customers	Inform customers about breach and advise them to adjust personal credentials for other sites to avoid further compromise	High	Send email according to external communication policy	Today	ICT manager (in consultation with communications manager)	Not yet started
The Office of the Australian Information Commissioner (OAIC)	Notify OAIC as required under notifiable data breach (NDB) scheme	High	Complete NDB reporting form and lodge via OAIC website	Today	ICT manager	Not yet started

Practice Task 5

Question 1

Identify whether the following stakeholder groups are internal or external when communicating a cyber incident.

Customers	» Internal	» External
Owners	» Internal	» External
Society	» Internal	» External
Government agencies	» Internal	» External
Employees	» Internal	» External
Managers	» Internal	» External

Question 2

Which of the following details should be included in a communications plan? Tick all that apply.

- ◯ The purpose of communication.
- ◯ The level of urgency (high, medium or low).
- ◯ The email address of the ICT manager.
- ◯ The stakeholders being communicated to.
- ◯ By when communications need to be completed.

Question 3

Which of the following details would you expect to find in an organisation's communications policy? Tick all that apply.

- ◯ Email templates for communicating with customers.
- ◯ Approved purposes for different communication channels.
- ◯ Contact details for the organisation's stakeholders.
- ◯ Details about how approved communication channels can be used.
- ◯ A list of approved communications channels used by the organisation.

Question 4

What are two closed-ended questions you could ask an ICT technician about a cyber incident?

2C Assist in alerting external parties

Cyber incidents may require you to communicate with external stakeholders.

For lower-risk events your organisation's communications may be limited to internal stakeholders such as employees and managers. Higher-risk incidents, especially those involving data breaches, usually require communication with external stakeholders such as government bodies and customers.

Knowing how to communicate with these parties will help your organisation to meet its legal requirements.

Alerting the government

If a data breach or cyber-crime occurs, the Australian Government needs to be informed.

There are two main situations which require a cyber incident to be reported to the Australian Government:

1. When a data breach occurs
2. When a cyber-crime occurs

The government has created specific processes and websites for reporting in both these situations.

Reporting a data breach

Under the Australian Government's notifiable data breach scheme, organisations with responsibilities under the Privacy Act 1988 must report any incidents where personal information has been compromised.

In the context of a cyber incident, a data breach has occurred when:

- personal information held by your organisation has been accessed, disclosed or deleted without authorisation.

A serious data breach has occurred when:

- the unauthorised access, disclosure or deletion is likely to cause serious harm to individuals such as identity theft, financial loss, physical harm, psychological harm, and harm to their reputation
- your organisation has not been able to prevent likely harm from occurring, such as via risk mitigation strategies.

Serious data breaches must be reported to:

- individuals affected by the breach
- the Office of the Australian Information Commissioner (OAIC)

The OAIC provides a notifiable data breach form template for reporting breaches to both individuals and the OAIC. A practice version of this template that you can complete without needing to submit is available at: aspirelr.link/oaic-notifiable-data-breaches

The notifiable data breach form contains two parts:

Part one: Statement about an eligible data breach	The details you record in this part of the form should be reported to both the OAIC and to individuals whose information has been compromised. Information you record in this part of the form includes: ▪ details about your organisation ▪ description of the data breach ▪ information involved that has been compromised as a result of the breach. This may include financial details, tax file numbers, identity information, health information and so forth ▪ steps that individuals are recommended to take to reduce the risk of harm, such as changing passwords ▪ other entities or organisations affected by the breach.
Part two: Additional information	The details you record in this part of the form should be reported to the OAIC only. Information you record in this part of the form includes: ▪ your contact details ▪ dates on which the breach occurred and when it was discovered ▪ primary cause of the breach ▪ description of how the breach occurred ▪ number of individuals whose personal information was affected by the breach ▪ description of remedial action your organisation is taking, or plans to take, in order to assist individuals affected by the breach ▪ description of any actions taken by your organisation to prevent further breaches from occurring ▪ details about how your organisation will inform individuals affected by the breach ▪ details of any other authorities to whom the breach has been reported.

Remember that failure to report a data breach can result in large fines. For further detailed information about responding to a data breach, refer to the Office of the Australian Information Commissioner: aspirelr.link/oaic-responding-to-data-breaches

Reporting a cyber crime

If your organisation experiences an incident which may be a cyber-crime, you should assist in reporting the crime to authorities.

Incidents which may be classified as cyber-crimes include:

- incidents which involve identity theft and fraud, for example through phishing attempts
- incidents which involve attempts to extort money, such as by using ransomware
- attacks on IT systems and infrastructure by using malware or DDoS
- incidents which involve the malicious breach of sensitive information.

Cyber-crimes can be reported to Australian authorities using the ReportCyber tool on the Australian Cyber Security Centre website. Access the ReportCyber tool here: aspirelr.link/cyber-report

The reporting process in this service varies, including the details and information you need to provide, depending on whether you are reporting a crime as:

- an individual
- a small or medium business
- a large organisation
- a government department or agency.

The information you submit will be communicated to relevant authorities, for example the federal or state/territory police, who will investigate the potential crime. Note that the ReportCyber tool should not be used in situations:

- where a physical crime has occurred, such as thieves breaking into your organisation's server room
- where your organisation received a scam call but no loss of personal information or money occurred.

Tips for reporting

If you are involved in preparing reports or other communications regarding cyber incidents, here are some strategies for making them as effective as possible.

Be clear and specific

When reporting the details of an incident, it is important to provide clear and detailed information about what happened.

Where possible, provide specific data about the incident, for example:

- exactly when the incident occurred and how long it lasted
- how many people were affected by it
- what actions have been taken to contain and eradicate the threat.

Remember not to provide excess information or details which are not relevant to the incident.

Use the right language

When submitting a report to OAIC in the event of a breach, or the Australian Cyber Security Centre in the event of a cyber-crime:

- use industry-related language referring to your systems and infrastructure
- use formal language and avoid slang or abbreviations
- avoid using jargon and acronyms that may not be understood outside of your organisation.

Alerting clients and customers

You need to let your clients and customers know when they are affected by a cyber incident.

Serious data breaches will require your organisation to notify the individuals whose data has been compromised. In this situation, you need to complete part one of the notifiable data breach form and distribute this information to affected individuals.

Data breaches are not the only situation that require your organisation to communicate with customers. The following incidents may all necessitate some form of client communication:

- Hackers take the customer-facing section of your website offline.
- A DDoS attack prevents your website from being able to process orders.
- Hackers deface sections of your website with unwanted graphics and text.

The methods you use to communicate with customers in these situations should comply with your organisation's communications policy and be documented in the communications plan. These methods may include:

- direct emails to customers
- publishing information about the issue via your organisation's social media
- publishing information about the incident on your organisation's website
- creating a push notification if your organisation has an app.

The method/s you choose should be based on:

Expected duration of incident	If you expect the incident to be resolved quickly and services returned to normal, it may be sufficient to create a notification on social media that can then be removed once the incident is over.
Seriousness of incident	If the incident causes minor disruption, such as vandalism of your website, it may not be necessary to engage in extensive communications with your customers who may not otherwise be affected by the incident.
Customer preferences	Use the communication channels preferred by your customers. For example, younger people may be more likely to see a communication via social media than in their email.

Ensure the language used in communications to customers is clear, succinct and appropriate to the audience.

For an example of how Service NSW communicated with external stakeholders following a cyber incident, refer to: aspirelr.link/nsw-cyber-incident

Example

Assist in alerting external parties

Preeti works in the ICT team at HealRight, a medical centre where hackers recently obtained patients' medical records and appointment login information. Preeti supports the team to report this cyber-attack to external stakeholders. This involves:

- submitting a notification regarding the data breach to the Office of the Australian Information Commissioner
- completing a report to the authorities using the Government's ReportCyber tool
- alerting the patients whose records were compromised via email
- publishing details regarding the attack, and the steps being taken, on the HealRight website.

Practice Task 6

Question 1

When do Australian Government agencies need to be notified about a cyber incident? Tick all that apply.

- ◯ When your organisation's website has been taken completely offline.
- ◯ When a physical break-in results in damage to your network.
- ◯ When your organisation cannot access data stored in the cloud.
- ◯ When personal information has been breached and this breach may cause serious harm.
- ◯ When a potential cybercrime has occurred.

Question 2

List one way of reporting a serious cyber incident to the Australian Government.

Question 3

When communicating with your customers about a cyber incident, which of the following methods could be suggested in a communications policy? Tick all that apply.

- ◯ Publishing information about the incident on your website.
- ◯ Sending an email to affected customers.
- ◯ Writing a social media post.
- ◯ Publishing the details on the intranet.
- ◯ Creating an app notification.

Summary

- Responding to an incident may involve escalating it to other members of staff or a third party.
- Escalating incidents should be conducted in line with an organisation's escalation policy.
- Incident escalation is typically conducted via an organisation's helpdesk system.
- Cyber incidents need to be communicated to both internal and external stakeholders.
- All stakeholder communications should be documented in a communications plan.
- Stakeholder communications need to be in line with an organisation's internal and external communications policies.
- Incidents in which customer data is breached may necessitate a breach report to the Office of the Australian Information Commissioner.
- If an incident is the result of a cyber-crime, the authorities can be alerted using the Australian Cyber Centre's ReportCyber tool.
- Customers may be affected by a cyber incident in several ways, such as breach of their data or inability to access an organisation's website
- The way an organisation communicates with customers should reflect the duration and seriousness of the incident, as well as customer preferences.

Learning Checkpoint 2

Communicate information on cyber security incidents

Part A

1. What two items you would find in an organisation's escalation policy?

2. Identify two internal and two external stakeholder groups who may need to be communicated with regarding a cyber incident.

Part B

Read the case study and answer the questions that follow.

Case study

Nhan works in the ICT department of an investment bank. The bank experienced a hack that accessed customers' personal data. Nhan meets with the team to help develop a communications plan.

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

   a) Nhan should use a variety of open-ended and closed-ended questions to understand the details of the incident. » Yes » No

   b) Nhan should avoid taking notes as it may appear he is not listening attentively. » Yes » No

   c) Nhan should listen attentively and paraphrase to demonstrate understanding. » Yes » No

   d) Nhan should limit the number of people he talks to in order to avoid receiving conflicting stories. » Yes » No

2. What are four pieces of information Nhan and the team should include in their communications plan?

3. What document should Nhan refer to when deciding which channels should be used to communicate with the bank's customers?

4. Nhan is talking to a senior staff member regarding the incident to help understand the communication requirements. List one closed-ended and one open-ended question Nhan could ask this staff member.

5. Nhan's organisation has responsibilities under the Privacy Act 1988. Which of the following statements are correct? Select yes or no for each one.

a) Notifying the OAIC regarding a breach is voluntary.	» Yes	» No
b) Notifying the OAIC regarding the breach is mandatory.	» Yes	» No
c) This incident is unlikely to be considered a cyber-crime.	» Yes	» No
d) This incident should be reported using the government's ReportCyber tool.	» Yes	» No

6. Nhan is helping to draft a notifiable data breach form. Which of the following strategies should he use? Tick all that apply.

- ◯ Use internal jargon.
- ◯ Provide as much information as possible.
- ◯ Use formal language.
- ◯ Provide specific data about the incident.
- ◯ Complete part one of the document only.

Topic 3 | Contribute to post-incident activities

3A Support post-breach review and reporting

3B Assist in identifying lessons learnt and changes to response plan

3C Assist in updating cyber security response plan

3D Communicate lessons learnt and recommendations to personnel

3A Support post-breach review and reporting

After a threat is eradicated, you need to understand what happened so you can make improvements.

After a cyber threat is eradicated and normal operations have resumed, it is important to investigate how the incident occurred and what its impact was on the organisation and on stakeholders. This will help your team put measures in place to prevent the recurrence of similar incidents and improve the effectiveness of future incident responses. You may also need to complete reports and documentation relating to the incident.

Investigating how the incident occurred

You may need to look harder to understand the root cause of a cyber incident.

In the immediate aftermath of a cyber incident, your team may have a reasonable idea of what occurred. This could be as simple as knowing that an unauthorised user accessed your system. However, it may not be immediately obvious exactly how the incident occurred. Investigating the cause of the incident will help to prevent the same issue from happening again.

To understand how an incident occurred, you and your team need access to a variety of information. Sources of relevant information may include:

System logs	Logs can be used to help detect a cyber incident, such as: ▪ domain name system logs ▪ email server logs ▪ operating system event logs ▪ security software and appliance logs ▪ virtual private network and remote access logs ▪ web proxy logs. These logs can also help you to uncover details about how and when the incident occurred. For example, the exact date and time when an unauthorised user entered the system, how they moved around the system and so forth.
Digital evidence collected during incident	During an incident, relevant evidence must be collected and documented according to organisational policies and procedures. This may include using an evidence register template, which is included in some cyber incident response plans. The evidence gathered may provide further insights into the incident.

Stakeholders involved in the response	Members of the response team may have insights into how the incident occurred based on what they observed during the incident. For example, a network engineer who helped bring your system back online may be able to provide detailed information about which parts of the network were compromised.
Government sources	Your organisation may have experienced an incident which was part of a broader attack on comparable organisations, or organisations using similar software or systems. The Australian Cyber Security Centre publishes regular alerts regarding current and emerging threats online at: aspirelr.link/cyber-alert-register This information may help provide further insight into hackers' techniques and motivations when conducting an attack.

Identifying the root cause

Once you are equipped with more detailed understanding of the incident, you are in a better position to identify its root cause. The root cause is the fundamental problem, or combination of problems, that led to the incident occurring.

'5 whys' is a tool you can use to help identify the root cause of a cyber incident. This process involves repeatedly asking 'why' an issue occurred, helping you dig deeper into an issue. It is not always necessary to ask 'why' five times, but this is usually a good number to aim for.

Here is an example of the 5 whys process in action:

Problem: A hacker accessed our database and stole our clients' credit card information.

Why? The hacker had the username and password for one of our staff members.

Why? The hacker successfully phished the information from the staff member.

Why? The staff member clicked on a suspicious link which granted the hacker access to their login information.

Why? The staff member had not undertaken our organisation's cyber security training.

Why? Cyber security training is currently voluntary and only offered once a year.

In this example, the outcome of the 5 whys process may lead to recommendations for cyber security training to be made mandatory and delivered more regularly throughout the year. The process can be conducted several times on the same issue to uncover other root causes.

The details you find regarding the incident and its cause may need to be documented in a post-incident review (PIR).

Investigating the impact

A cyber incident can impact the organisation in many ways.

Previously, we looked at potential impacts of a cyber incident in terms of your organisational systems' confidentiality, integrity and continuity. During a post-incident review, you should consider the broader impacts of the incident on your organisation.

Some of the potential business impacts on your organisation arising from a cyber incident include:

Operational impacts	▪ Operational impacts relate to your organisation's ability to carry out normal business activities. ▪ For example, if your system is taken offline, this will limit or prevent business operations such as: – employees being able to login to the network – carrying out physical business tasks, such as performing credit card sales in physical stores – customers being able to access your website. These types of impacts can be quantified in terms of time; for example, the length of time when normal operations were unavailable.
Revenue impacts	▪ Operational impacts are likely to lead to revenue impacts. ▪ For example, if an online store's website crashes due to a hacking attempt, significant revenue losses will immediately occur because customers cannot pay for goods or services. ▪ Some cyber threats have more subtle impacts, such as system slowdown and increased downtime. While less immediately damaging, revenues lost because of IT downtime can quickly add up. In addition, significant spending may be required to repair or replace equipment damaged by a threat. ▪ Revenue impacts can be quantified in dollar amounts, that is, revenue lost because of the incident. The average cost of a data breach has been estimated at around $3.35 million.
Reputational impacts	▪ A business's reputation is often built on consumer trust. If an organisation's sensitive customer data is hacked, customers will be less likely to do further business with that organisation. ▪ Previous hacks, such as the 2014 hack of film company Sony Pictures, have also resulted in embarrassing internal emails being shared publicly, further damaging organisation's reputations. ▪ Revenue impacts are more difficult to quantify. Customer surveys where customers provide feedback about their level of trust in your organisation can help to gather this information.

Legal impacts	▪ Data breaches may involve significant legal consequences from both regulators and from people whose data has been breached. This may include the issuance of fines and penalties. ▪ Following a major data breach resulting from a hack in 2017, Equifax was required to pay nearly $700 million in fines.

Source: The Ame Group, (2020: Data security breach: consequences for your business

Completing post-incident reporting

Post-incident reporting helps document exactly what happened.

Following a cyber incident, there may be a number of documents that need to be completed to record all relevant information relating to the incident. Certain reports may also be required to be completed to comply with government legislation.

The specific documents required will vary depending on the nature of the incident and your organisation's policies and procedures. However, some of the reports to be aware of include:

Notifiable data breach reporting	▪ Breaches of personal information that are likely to cause harm to individuals must be reported to the Office of the Australian Information Commissioner (OAIC).
Cyber-crime reporting	▪ If the incident was probably a cyber-crime; that is, was not the result of an employee mistake, it should be reported to the authorities using the Australian Government's online ReportCyber tool.
Post-incident review (PIR)	▪ Your organisation may require your investigation of the incident and its impacts to be documented in a post-incident review (PIR). The format of a PIR may vary, but it should include the following details: – Sequence of events which led up to the incident. – Details of the incident. – Impact of the incident. – How the incident was detected. – How the team responded to the incident. – Details regarding incident recovery. ▪ The PIR may include a timeline of events to provide a full understanding of what happened. It may also include your analysis of the root cause of the incident; for example, using the 5 whys technique discussed above. For an example PIR, refer to: aspirelr.link/atlassian-postmortem-template
Lessons learnt report	▪ Lessons learnt reports help your organisation to learn from an incident and make improvements for the future.

Incident registers	▪ Your cyber incident response plan may include a number of registers that need to be completed. These registers document the details of the incident, such as: – situation update – incident log – resolution action plan – evidence register – assets and key contacts. ▪ Ensure these registers are complete, accurate and stored according to your organisation's policies and procedures.

Depending on your role in the team you may not be responsible for completing all these different documents. Some of the ways you might support your team in the reporting process include:

- gathering information as requested by senior members of the team
- tracking the completion of different reporting requirements and following up with stakeholders as required
- reviewing and proofreading reports prepared by other members of the team to ensure they make sense, are well-presented and follow organisational style guides
- ensuring reports and documents are stored and distributed according to your organisation's protocols.

Example

Support post-breach review and reporting

Lin works in the ICT department of ChargeCar, an electric automobile manufacturer. The company's client database was recently hacked. Although the threat has now been eradicated, Lin supports her team to review the incident.

The team's investigation gathered evidence that shows the hacker gained access due to a security vulnerability in the organisation's network security. Conducting analysis using the 5 whys technique reveals the root cause of the vulnerability was an absence of review and approval processes for security upgrades. This information will feed into the team's lessons learnt process.

Lin helps document the review process using ChargeCar's approved post-incident review (PIR) template. She also helps gather the information required to complete the team's incident reporting documentation, their evidence register and incident log. Because the incident involved a malicious breach of customer data, Lin is aware she will need to help to lodge an NDB report and to complete the ReportCyber alert to the authorities.

Practice Task 7

Question 1

What are four standard sections in an organisation's post-incident review (PIR) template.

Question 2

Which of the following are potential business impacts of a cyber incident? Tick all that apply.

- ◯ Lost revenue due to system downtime.
- ◯ Boost to reputation due to your organisation's honesty.
- ◯ Inability to carry out business operations.
- ◯ Increased revenue due to customer sympathy.
- ◯ Legal damages including serious fines.

3B Assist in identifying lessons learnt and changes to response plan

The lessons learnt from an incident will help your organisation grow stronger.

During the post-breach review, you and your team will have found out more about the details of the incident and how it occurred. This information can help you identify lessons learnt. These are key pieces of information which can help improve your response to future incidents. Undertaking lessons learnt is an important element of organisational learning.

Lessons learnt can be either positive or negative. Positive lessons can be learnt from actions that went well during the response. These can either be built upon or repeated during future incidents. Negative lessons can be learnt from actions that did not work well. These can be changed or improved upon to avoid similar mistakes in the future.

Organising a lessons learnt session

You can maximise the value and quality of information gained from the lessons learnt session by being well organised. Follow these steps when organising a session.

Create an agenda and identify attendees

Typically, a lessons learnt session runs for between one and two hours. Without an agenda, this time can easily be used up without generating any useful discussion. The amount of time spent on introductions and general information should be limited, and the majority of the time spent on discussing the lessons learnt and identifying action points. This could include specifying parts of the meeting to focus on detecting the incident, containing the threat, eradicating the threat, stakeholder communications and so on. Specifying time limits for each agenda item will help you stay on track and avoid running out of time.

You also need to identify the stakeholders to be invited to the session. This may include internal stakeholders such as members of the incident response team, as well as external stakeholders like company representatives for software that was compromised. Think about your stakeholders when you schedule the meeting and avoid scheduling it at a time when you know people are likely to be busy or preoccupied.

Distribute agenda and gather feedback

Include the agenda with the session invitation. It may be appropriate include some initial thoughts on what went well, and not so well, during the incident. You can collate these thoughts with input from others. This may help invitees to start generating their own ideas about the incident response in advance of the meeting, and some invitees may send you back feedback in advance.

Starting with existing ideas and feedback is a great way to get the conversation flowing and means you are not starting from scratch during the session itself.

Conduct the lessons learnt session

A lessons learnt session can be conducted either face to face or using online videoconferencing software such as Zoom, Skype or MS Teams.

Send a summary and seek additional feedback

After the lessons learnt session, a summary of the discussion and any agreed actions must be distributed to the session participants and to any invited stakeholders who were unable to attend. Stakeholders should also be invited to provide any additional feedback, because:

- there may not have been enough time during the meeting
- they may have thought of, or identified, further feedback after the meeting
- absentee stakeholders may have additional input based on the summary and agreed actions.

Source: 5 Easy Steps to the Perfect Lessons Learned Session (2020)

Questions to ask during the session

There are many questions you can ask during a lessons learnt session to help generate thoughts and feedback from session attendees. A selection of questions you could ask are provided below.

Questions to ask during a lessons learnt session
▪ How well did our staff perform when responding to the breach? ▪ Did the team follow our organisation's policies and procedures, such as the response plan? ▪ Did the team do anything which negatively affected the response? ▪ What information was the team lacking? ▪ Could the team or organisation have prevented any unexpected events? ▪ What should our team do differently the next time a situation like this occurs? ▪ What precursors or indicators helped identify this breach? Can we do anything to monitor these better? ▪ How accurate was our risk assessment?

Source: Cyber Security Incident Response Guide (2013)

Tips for assisting a lessons learnt session

To get the most out of a lessons learnt session, consider using these strategies.

Avoid blaming	▪ If an incident response went badly, some team members may try to blame other team members. Instead of focussing on individuals by name, encourage everyone to focus on behaviours that were successful or could be improved. This will help the conversation stay positive and productive, rather than negative and unproductive.
Seek input from everyone	▪ Everyone in the lessons learnt session should have been involved in the incident response. Therefore, each person will have valuable input about what they thought worked well or less well. Encourage quieter members of the team to share their thoughts. If input is only provided by the loudest person in the room, valuable lessons might be missed.
Do not spend too long on any one issue	▪ You are unlikely to have more than one or two hours to conduct a lessons learnt session, so you need to help the team to use the time wisely. This can be done by setting a time limit for discussing each issue and identifying when the discussion is not productive.
Be responsive to new information	▪ Attendees at the lessons learnt session may introduce new information regarding the incident which was not discovered during the post-incident review. This information may require you to quickly adapt and adjust the conversation.
Agree on actions	▪ A lessons learnt session may result in actions that members of the team need to follow up on after the meeting. For example, you may have an action to make updates to the organisation's incident response plan to improve the containment process. ▪ Ensure all the team is aware of, and agrees to, the planned actions that will occur after the meeting.

Take notes	
	▪ The conversation and outcomes that arise during a lessons learnt session should be documented and stored according to your organisation's policies and procedures. This will provide evidence of activities taking place to improve organisational processes. This is a requirement in many quality review systems. ▪ You may also need to report the findings of a lessons learnt session to other stakeholders such as senior managers, so you need to have an accurate record of the meeting.

Lessons learnt and recommendations

As a result of the lessons which have been learnt from the incident, you should support the team to identify recommendations. These recommendations should be designed to:

- reduce the risk of the same, or a similar, incident from occurring in the future. This will usually involve measures to reduce your systems' vulnerability to cyber threats. This could be, for example, by investing in new anti-malware software or improving processes for software patching
- improve the effectiveness of future incident responses. This will usually involve making updates to the cyber incident response plan.

You may need to communicate the outcomes and recommendations of a lessons learnt session to other stakeholders in your organisation, such as the senior management team.

Example

Assist in identifying lessons learnt and changes to response plan

Lin works in the ICT department of ChargeCar, an electric automobile manufacturer whose client database was recently hacked. Having supported her team to investigate the incident, Lin has now been asked to help organise and run a lessons learnt session.

The session will be 90 minutes long and Lin creates the following agenda:

- Introductions and housekeeping: 5 minutes.
- Lessons learnt (incident detection): 15 minutes.
- Lessons learnt (incident containment): 15 minutes.
- Lessons learnt (incident eradication): 15 minutes.
- Lessons learnt (stakeholder communications): 10 minutes.
- Lessons learnt (format/content of response plan): 10 minutes.
- Recommendations and actions: 15 minutes.
- Summary: 5 minutes.

When sending out the agenda, Lin, in consultation with members of her team, identifies some initial thoughts regarding what worked well and not so well during the response. These include:

- initial notifications regarding the incident were sent to the personal inbox of a staff member who was on leave. Future notifications should go to the support desk inbox
- the staff names and roles in the response plan were very out of date, causing confusion in the communications. These details need to be updated immediately
- our newly developed risk assessment process worked well and accurately identified the risk level of the incident. Ensure this process is followed in the future
- some members of the team were not familiar with the incident response plan or associated processes. We should do regular refresher courses on these to ensure no time is wasted during an actual incident.

Invitees to the session make additions to this list in advance of the actual meeting. This means the conversation moves quite quickly during the meeting, though Lin needs to keep an eye on the time to ensure all points are covered in sufficient detail. The team agrees on several actions, including changes to the incident response plan.

Afterwards, Lin distributes a summary of the meeting and agreed actions. This results in some of the stakeholders, including a couple who were unable to attend, providing further feedback on what improvements could be made for the future.

Practice Task 8

Question 1

What are four questions you could ask during a lessons learnt session to generate discussion?

Question 2

Which of the following are strategies for running a successful lessons learnt session? Tick all that apply.

- ◯ Focus on the person, not the behaviour.
- ◯ Gather information from the two most important people in the room.
- ◯ Agree on actions to be completed.
- ◯ Do not spend too long on any one issue.
- ◯ Take notes about the discussion and actions required.

3C Assist in updating cyber security response plan

A cyber incident response plan is not set in stone but requires ongoing improvement.

The lessons learnt session is likely to identify a number of recommended changes to your organisation's cyber incident response plan. When the next cyber incident occurs at your organisation, different staff, who were not involved in the previous response, may be required to respond. Updating the response plan helps ensure that the lessons learnt will be embedded in your organisation's incident response approach.

Making updates to the plan

Updating the response plan will help future response teams.

You may be responsible for drafting updates to the response plan, depending on your role in the team. The types of changes you make will vary depending on the lessons learnt from the incident. However, at this point you should have a thorough understanding of the response plan and you should be confident to make changes relating to:

- names and roles of people involved in a cyber incident response
- common cyber incidents faced by your organisation
- strategies for protecting the organisation from future attacks
- methods for detecting cyber incidents
- strategies for containing and eradicating cyber threats
- communication needs in the event of a cyber incident
- registers and templates contained in the plan.

When making updates to the cyber incident response plan, use these strategies.

Ensure the changes reflect the review	▪ The changes you make to the response plan must reflect the lessons learnt from the previous incident response. Avoid making additional changes that seem like a good idea to you, but were not discussed or agreed upon during the lessons learnt session.
Ensure consistency	▪ Ensure that if you make a change in one part of the document, any other relevant parts of the document are updated for consistency. ▪ For example, if you update the name of a piece of technology used in the response process in one part of the document, make sure the same change is made throughout the document.

Follow current industry practices	▪ Any changes you make to the response plan must be in line with current best practice relating to cyber security. Stay informed about the latest developments via online sources such as: – Australian Cyber Security Centre – Australian Cyber Security Magazine.
Follow policies and procedures	▪ Your organisation may have policies and procedures in place for updating documents. For example, you may need to follow procedures relating to document control, changes tracking and file naming. ▪ In addition, you need to ensure that any changes you make to the incident response plan itself comply with your organisation's policies and procedures. For example, if you are updating information relating to sensitive data management, you need to ensure this complies with your organisation's privacy policy.
Ask questions	▪ When dealing with technical information and specifications, you may need to ask questions and seek assistance from more senior members of the team. If you go over your notes from the lessons learnt session and are uncertain what was agreed upon, go back to attendees to confirm.
Seek approval	▪ After you make changes to the response plan, seek approval from the document 'owner'. This may be the ICT manager or another member of the senior management team. Follow your organisation's processes for seeking approval on workplace documentation. ▪ Your manager may have questions regarding the changes you have made or may suggest further changes. Be prepared to discuss these changes.

Example

Assist in updating cyber security response plan

Lin works in the ICT department of ChargeCar, an electric automobile manufacturer whose client database was recently hacked. Lin helped organise a lessons learnt session which helped to identify a number of required changes to ChargeCar's cyber incident response plan. These changes include:

- updating the names and roles of people involved in incident response
- updating methods for detecting cyber incidents
- updating communication protocols during a cyber event
- adding instructions about how to complete templates, such as the evidence register contained in the response plan.

Lin makes these changes in the document in line with ChargeCar's protocols for document updates, which involve tracking changes and updating the document versioning information. She seeks advice from other members of the team regarding some of the more technical changes required, such as the technical information about intrusion detection. Once she has finished making the updates, she sends the document to her team leader who is responsible for reviewing the updates and signing off on the document.

Practice Task 9

Question 1

Which of the following statements are correct in relation to updating a cyber incident response plan? Select yes or no for each one.

a) The updates you make should reflect the post-incident review and lessons learnt. » Yes » No

b) Follow your organisation's policies relating to document updates. » Yes » No

c) All feedback will have been finalised before starting the update process. » Yes » No

d) Check external sources, such as the Australian Cyber Security Centre, to ensure your updates reflect industry best practices. » Yes » No

3D Communicate lessons learnt and recommendations to personnel

The lessons learnt from a cyber incident need to be communicated beyond your team.

After conducting a post-incident review and undertaking a lessons learnt session, findings and recommendations will need to be shared with staff from outside your team, such as senior managers and other key decision makers. Two ways to communicate lessons learnt and recommendations are by writing a report and/or making a presentation.

Lessons learnt report format

While the findings and recommendations of each lessons learnt report will be unique, the reports typically follow a similar structure.

You should now understand the principles of conducting a lessons learnt session. These include gathering recommendations such as changes to the response plan, or to organisational systems and processes. You then compile this information into a user-friendly lessons learnt report.

Locate templates and/or style guides

When drafting a lessons learnt report, first check if there is a template used in your organisation. Using a template can save you time and also means your report will be in a format that is already familiar to your stakeholders.

If your organisation does not have a lessons learnt template, check if a style guide exists. A style guide provides guidance on font, format and spacing, and usually includes rules on the use of the organisation's brand and corporate identity.

Structure the report

Whether you are using your organisation's template or developing the lessons learnt report from scratch, it will generally include:

Lessons learnt report
▪ Executive summary. ▪ Introduction. ▪ Overview of the cyber incident including cause/s and impacts. ▪ Summary of the lessons learnt. ▪ Recommendations to prevent the incident from occurring in the future, or to improve the effectiveness of future incident responses. ▪ Summary including next steps. This may include seeking approval to carry out recommendations. ▪ Definitions of technical terms.

Use version control

It is a good idea to include version control information when drafting your report, as there are likely to be further updates required once you have received feedback from stakeholders.

Depending on your organisation's document versioning and sharing policies, version information can be tracked in two ways:

1. **Manually edit version information within the document**

Version information provided as a simple table at the front of the review document is often sufficient. The important information to include here is:

- who changed the document: the author
- when they changed it
- what changes were made.

Here is what a document version control table may look like:

Version	Date	Author/s	Rationale
0.1	1-Mar-21	Jane Smith	First Draft
0.2	14-Mar-21	Jane Smith	Reviewed by stakeholders

2. **Automatically manage version information using collaboration tools**

There are many collaborative working tools such as Dropbox, Google Drive, Microsoft One Drive. These tools usually track versioning information automatically, every time the document is changed. These tools also usually enable you to access previously saved versions of the document if required.

Ensuring the report is effective

A lessons learnt report should be clear, concise and avoid jargon in order to be effective.

The lessons learnt report is an important document that should recommend actions to improve the security of your organisation's ICT. The report may be read by a wide range of stakeholders, so it is essential to ensure the report is as effective as possible by writing clearly, concisely and avoiding jargon.

Write clearly

Clear writing is easy to understand. Always use plain English. This means avoiding complex language and using short sentences and short paragraphs. Never use a long or technical word if a simple word will do. Remember that your audience may not be familiar with technical terms so, if you have to use them, explain their meaning for your readers.

Paragraphs should only contain one thought or idea and be no longer than five or six lines. It is better to write a short paragraph than to confuse your audience by putting two or more ideas in one paragraph. Clear writing means the reader is less likely to get confused.

Write concisely

Concise writing uses the least number of words possible to relay information. To write concisely you need to explain exactly what is meant, while avoiding repetition or boring the reader with unnecessary information. Include specific details and definite statements. Think carefully about what needs to be communicated. Only include information that is relevant to the situation and the reader.

Avoid jargon and define terminology

Your report may be distributed to stakeholders who are not ICT security experts. This means you should avoid using jargon and use plain English wherever possible. In some situations, you may need to use industry terminology, such as malware, cloud storage, or two-factor authentication. Provide a simple definition for any terminology which may not be understood by your audience. This should also include providing definitions for any acronyms; for example, AES means Advanced Encryption Standard. These definitions should be included in a Definitions or Glossary section at the end of the report.

Communicating recommendations in person

In-person communication requires planning and preparation.

Communicating the findings and recommendations of a lessons learnt session is often done in person. This may involve both the presenter and audience being in the same physical space or using webinar technology, such as Zoom, MS Teams or Skype, to present to audience members in different locations.

Any presentation you give must provide your audience with accurate, clear, up-to-date information. And while you may have a good understanding of your organisation's incident response process, this does not instantly make you an expert presenter. You need to be a good communicator as well.

A competent presentation will ensure your audience gets a strong understanding of cyber threats facing the organisation, as well as appropriate strategies to address these threats. Using the strategies outlined in the following table will help you succeed when presenting.

Identify audience needs	▪ To communicate your findings to your audience as effectively as possible you should identify their needs. Consider the following questions: – How much prior knowledge does your audience have? For example, were they involved in the incident response? What do they already know about the incident? – What are the language skills of the audience? If their first language is not English, take care not to speak too fast or use needlessly complex language. – Does anyone in your audience have a disability? For example, it may be appropriate to print handouts with large text for people with visual impairment.
Select and order content	▪ If your information is relevant, clear and logically organised, then it will be easier for your audience to follow your presentation. ▪ All good presentations include: – Introduction: this is when you introduce yourself and outline the aim of the presentation. It is the opportunity to catch your audience's attention. – Body: here you should focus on talking about the incident that occurred, including causes and business impacts, the lessons learnt and proposed recommendations. – Conclusion: now you summarise your presentation and reinforce the recommendations you want the audience to remember. ▪ If your audience already knows something about the incident that occurred, start from that point and then introduce new concepts, such as the root cause of the incident. ▪ Starting with the known and moving onto to the unknown makes it easier for your audience to process and retain information.

Prepare slides	▪ Presentations often combine visual and verbal elements to engage an audience. For example, many presenters include a slide show using software such as Microsoft PowerPoint or Prezi. ▪ Complicated information, including numerical data, is best summarised visually. An image can often convey an idea more powerfully than text. ▪ Limit the number of slides you include in a presentation. Quickly moving from slide to slide can distract an audience. ▪ Ensure that you use a large font size and slides do not contain too much written information. Empty space on a slide improves its readability so include only key phrases and essential information.
Provide time for questions and feedback	▪ You should always provide time for questions and feedback. This gives your audience the opportunity to interact. ▪ You may invite the audience to ask questions and provide feedback as you go along, or you may request that any questions and feedback be asked at the end of your presentation. Your audience may consist of experts who will provide quality feedback and questions about the recommendations you have presented. ▪ If you are unable to answer a question, such as if it requires additional research, make a note and tell the audience member you will follow-up on their query. ▪ Be prepared to document any feedback or questions received, in case they require changes to be made to the lessons learnt report.
Set a time limit	▪ Confirm how long you have for your presentation and plan by allocating time to each section to ensure you do not go over the prescribed time. ▪ Avoid speaking for a long period of time as your audience may become bored and restless.
Rehearse the presentation	▪ It is always useful to rehearse your presentation, as practicing what you are going to say will help build your confidence. Time your rehearsal to make sure the length is appropriate. Allow for nervousness, the type of audience, the technology and questions. ▪ Read your presentation aloud and check whether you are using: – a clear, easy-to-follow structure – concise words with clear meanings – any jargon or terms that may confuse the audience – pauses to emphasise important points. ▪ You can rehearse your presentation with colleagues, friends or family to make sure the information is clear and interesting.

Deliver the presentation	▪ You might be nervous on the day of the presentation. To ensure your delivery is effective, consider using the following strategies: – Arrive early so you can set up equipment and check everything is working. Remember to have a glass of water close by in case your throat gets dry. – Use gestures and body language effectively. – Do not overdo hand gestures but use them effectively to emphasise key points. – Make eye contact and smile at various audience members to reach out and engage them from the start. – Refer to your notes only occasionally. ▪ Speak slowly and clearly and modify your voice so everyone can hear, especially if you are not using a microphone. ▪ Check that the audience understands what you are saying by observing their facial expressions; notice whether they are becoming restless.

Example

Communicate lessons learnt and recommendations to personnel

Lin works in the ICT department of ChargeCar, an electric automobile manufacturer whose client database was recently hacked. Lin's team recently conducted a lessons learnt session and Lin has been asked to communicate the lessons learnt and recommendations to ChargeCar's executive team. The presentation will take place via an online Zoom meeting.

Lin is aware that many of the executive team members are not highly technical, although all of them were provided with a briefing when the incident first occurred. She structures the presentation accordingly, avoiding technical jargon and building upon the information her audience already knows. Lin's preparation pays off; she delivers a highly engaging presentation to the stakeholders within her allocated time of 30 minutes.

Lin's audience has a number of questions regarding the recommendations she presented. She is able to answer some of these questions immediately. She takes notes regarding some of the more technical/complex questions and assures the relevant stakeholders her team will investigate and provide a response soon.

Practice Task 10

Question 1

Which of the following factors would impact the content of a lessons learnt presentation to stakeholders? Tick all that apply.

- ◯ Existing stakeholder knowledge of the incident.
- ◯ Stakeholders' understanding of technical terms.
- ◯ Your preferred presentation style to stakeholders.
- ◯ Details of the incident which reflect poorly on stakeholders.
- ◯ Stakeholders' language skills.

Question 2

List four sections you would expect to see in a lessons learnt report.

Summary

- A post-incident review helps identify how an incident occurred and its impact on the business.
- Techniques such as 5 whys are used to identify the root cause/s of a cyber incident.
- A cyber incident may have operational, financial, reputational and legal impacts on an organisation.
- Conducting a lessons learnt session can help improve your organisation's future response to cyber incidents and lower their risk of recurring.
- Strategies to maximise the effectiveness of a lessons learnt session include focusing on behaviours and not calling out individuals, seeking input from everyone, managing time and agreeing on actions.
- A lessons learnt session should generate recommendations, including recommended changes to the incident response plan.
- Updating the incident response plan will help future teams to respond more effectively.
- Lessons learnt can be communicated to stakeholders beyond the response team via a lessons learnt report and/or a presentation.
- A lessons learnt report should be clear, concise and avoid jargon.
- A lessons learnt presentation must be tailored to the information and communication levels of the audience.

Learning Checkpoint 3

Contribute to post-incident activities

Part A

1. What are two sources of data you might refer to when assisting with a post-incident review?

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

   a) Your organisation may have an approved template for documenting a post-incident review. » Yes » No

   b) You should conduct all post-incident reporting on your own. » Yes » No

   c) A post-incident review focuses on the monetary impact of the incident. » Yes » No

   d) External sources should be avoided when reviewing the incident. » Yes » No

Part B

Read the case study and answer the questions that follow.

Case study

Maggie works in the ICT department of a food wholesaler. Recently, malware took all the company's systems offline. Problems relating to the organisation's cyber incident response plan meant the issue was not resolved for several days. Maggie has been asked to help organise a lessons learnt session and communicate findings to the senior management team.

1. Which of the following are appropriate questions for Maggie to ask during the lessons learnt session? Tick all that apply.

   - ◯ Who should be blamed for errors in our incident response?
   - ◯ How well did the team perform when responding to the incident?
   - ◯ What information was the team lacking?
   - ◯ What indicators helped us to identify the incident?
   - ◯ How can we minimise the amount of change required to the response plan?

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

   a) Unstructured lessons learnt sessions are most successful. » Yes » No

   b) Lessons learnt sessions must be conducted face to face. » Yes » No

   c) A lessons learnt session should only use information gathered during the post-incident review. » Yes » No

   d) Stakeholders may provide additional input following a lessons learnt session. » Yes » No

   e) A lessons learnt session should focus on behaviours, not individuals. » Yes » No

3. What are three sections of the company's incident response plan that Maggie may need to update as a result of the lessons learnt session?

4. What is one online resource Maggie could check to ensure her changes to the response plan reflect best industry practice?

5. What are four communication techniques Maggie could use to maximise the effectiveness of a face to face lessons learnt presentation to senior management?