BSB 7.0

BSBXCS402

PROMOTE WORKPLACE CYBER SECURITY AWARENESS AND PRACTICES

Aspire
Learning Resources

BSBXCS402

Promote workplace cyber security awareness and practices

Release 1

Learner Guide

Aspire Version 1.2

Aspire

Learning Resources

Version control and modification history

Version	Release date	Modification
Release 1, version 1.1	October 2020	First release
Release 1, version 1.2	November 2020	Question 7 added to Learning Checking 1, Part A. New question 3 added to Practice Task 4. New questions 4 and 5 added to Learning Checkpoint 2, Part A. Minor corrections as part of our continuous improvement process.

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.

BSBXCS402 Promote workplace cyber security awareness and practices, Release 1

© 2020 Aspire Training & Consulting
Level 1, 464 St Kilda Road
MELBOURNE VIC 3004 AUSTRALIA
Phone: (03) 9820 1300

First published October 2020
Reprinted (with amendments) November 2020

e-ISBN 978-1-76075-885-1 (PDF version)
ISBN 978-1-76075-884-4

Contact details

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

CONTENTS

Before you begin

This Learner Guide is based on the unit of competency *BSBXCS402 Promote workplace cyber security awareness and practices*, 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 ▪ Shares insights gained from cyber security trend analysis
Oral communication	▪ Consults with stakeholders to inform decision making
Reading	▪ Interprets information from relevant sources to determine organisational expectations
Writing	▪ Uses clear, specific and industry-related terminology relating to cyber security in workplace documents
Planning and organising	▪ Maintains records and documentation relating to cyber security protection
Teamwork	▪ Works collaboratively with interdisciplinary teams to promote cyber security
Technology	▪ Uses appropriate technology platforms to assist with promoting cyber security within work area

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: Develop cyber security awareness in your work area	1A	Cyber security awareness at work	□ Confident □ Basic understanding □ Not confident
	1B	Create and maintain best practice programs	□ Confident □ Basic understanding □ Not confident
	1C	Contribute to and communicate policies and procedures	□ Confident □ Basic understanding □ Not confident
Topic 2: Support effective cyber security practices at work	2A	Review practices according to organisational policies and procedures	□ Confident □ Basic understanding □ Not confident
	2B	Arrange training, updates and maintain records	□ Confident □ Basic understanding □ Not confident
	2C	Present insights to mitigate impacts on workplace	□ Confident □ Basic understanding □ Not confident
Topic 3: Review cyber security awareness in your work area	3A	Review latest threats and trends	□ Confident □ Basic understanding □ Not confident
	3B	Review outcomes and suggest improvements	□ Confident □ Basic understanding □ Not confident
	3C	Communicate review outcomes and improvements	□ Confident □ Basic understanding □ Not confident

Topic 1 | Develop cyber security awareness in your work area

1A Cyber security awareness at work

1B Create and maintain best practice programs

1C Contribute and communicate policies and procedures

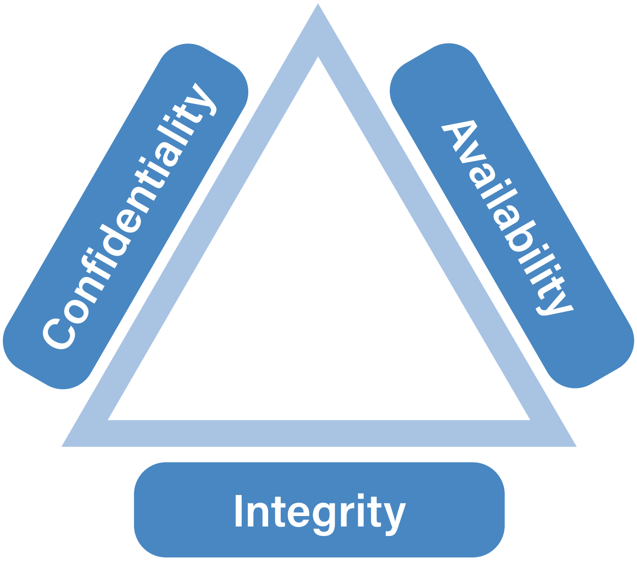
1A Cyber security awareness at work

Cyber security is the protection of computer systems and digital devices from attack, damage and unauthorised access to data.

Cyber security includes the application of technologies, processes and practices to protect systems, networks, programs, devices and data from cyber attacks.

The Australian Cyber Security Centre (ACSC) is a government initiative designed to improve security and inform Australians of cyber threats, and to promote awareness through education and free resources. They define cyber security as 'measures used to protect the confidentiality, integrity and availability of systems and information'. The terms: confidentiality, integrity and availability (CIA) are the pillars of a model for organisations to use when designing cyber security policies and procedures, and are known as the CIA triad.

The CIA triad



Confidentiality

Confidentiality relates to authorisation to access information. In cyber security, it relates to the level of permission someone has to access information. Medical records are examples of private and confidential records requiring strict protocols to protect people's health records.

Some common methods used to manage confidentiality include staff access lists, file encryptions and file permissions.

Integrity

Integrity defines the requirement that information should be stored accurately and unchanged without authorised modifications or deletions. 'Integrity' in the CIA triad stands for preventing unauthorised or accidental alteration of data at rest or in transit.

Alteration of *data at rest* happens when you have unauthorised data modifications, such as someone accessing your workstation and altering contents without your knowledge; whereas alteration of *data in transit* is the modification of data usually sent over the internet.

Some common methods used to manage integrity of information include version control, locking files, modification records and authorisation lists, file encryptions and file permissions.

Availability

Information is only valuable when you can access it. In cyber security, availability of information means information on demand and when you request it. In the CIA triad, availability is the production of information:

- when you need it
- provided by authorised parties
- unmodified or changed.

Some common methods used to manage availability include central management systems, backup systems and architecture designed to target hardware failures, upgrades or power outages.

Example

Denial of service or resource exhaustion?

Denial of service can be accidental and non-malicious, but still disruptive to an organisation.

In 2016 the Australian Bureau of Statistics (ABS) faced a service outage during its national census survey. The ABS held the survey at a specific time to survey Australia's population.

The surge in web service use overwhelmed information systems and caused the ABS survey to become unavailable. In the cyber security space, when you request a webpage and it is unexpectedly unavailable, this is called a Denial of Service (DoS). If this is unscheduled, it is an unwanted interruption to operations and could have a negative impact on an organisation.

Cyber security myths and reality

The media often reports on cyber security incidents, mostly labelling hackers with a notorious reputation.

There are three main actors involved in hacking, which are referred to as white hat, grey hat and black hat hackers.

White hat hackers	Specialised security professionals with permission to test the security of a target. They are usually known as ethical pen-testers and ethical hackers.
Grey hat hackers	IT experts who hack into systems without authority and communicate the security weaknesses they have exploited to the owners. Grey hat hackers pose a legal issue as they have not been given permission; this could cause that person to be treated as a black hat hacker.
Black hat hackers	Criminals who have not been authorised to access information systems. Black hat hackers are usually unethical technicians who have malintent, with criminal outcomes punishable by law.

Why cyber security is important

With the increase usage and reliance on information systems, it is important employees are cyber aware of their activities in the workplace, as there may be legal consequences.

Workers caught accessing information without permission is a criminal offence under the *Criminal Code ACT 1995* (Cth). It is every employee's responsibility to understand their organisation's cyber security policies and procedures; and, if in doubt, to ask their manager.

A 2020 report published by the ACSC, surveyed small and midsize businesses (SMB) and found the following:

- 62% had previously encountered a cyber security incident
- 40% said their cyber security understanding was average
- 46% thought they could resume normal operations with a few days if an incident occurred.

Legislative requirements relating to cyber security

Australian data protection laws are spread over several Commonwealth, state and territory Acts.

Privacy Acts are data protection legislation that govern the use of personal, identifiable data about individuals. Other legislation, such as the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth), need to comply with these privacy Acts.

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

The *Privacy Act 1988* (Cth) promotes the protection of privacy for individuals, whereas in different states, privacy is governed through several Acts. For example, in New South Wales, privacy laws are spread over several Acts such as the following:

- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Health Records and Information Privacy Act 2002* (NSW)
- *Workplace Surveillance Act 2005* (NSW)
- *Surveillance Devices Act 2007* (NSW).

Here are examples of privacy legislation in each state and territory.

Commonwealth	*Privacy Act 1988* (Cth)
Commonwealth	*Privacy Amendment (Private Sector) Act 2000* (Cth)
ACT	*Information Privacy Act 2014* (ACT)
NSW	*Privacy and Personal Information Protection Act 1998* (NSW)
NT	*Information Act 2002* (NT)
Queensland	*Information Privacy Act 2009* (Qld)
SA	Has none; SA refers to Commonwealth *Privacy Act 1988* (Cth)
Tasmania	*Personal Information and Protection Act 2004* (Tas)
Victoria	*Privacy and Data Protection Act 2014* (Vic)
WA	*Freedom of Information Act 1992* (WA)

Notifiable Data Breach scheme

Organisations are required under Commonwealth law to report any data breaches, intentional or otherwise.

The Notifiable Data Breach (NDB) scheme is part of federal legislation, which individuals and Australian organisations must comply with under the *Privacy Act 1988* (Cth). The NDB is a notification protocol where individuals and organisations must report data breaches, or those that are likely to occur, to the Office of the Australian Information Commissioner (OAIC). The guiding principle is that if data breaches have caused, or are likely to cause, serious harm to individuals, usually as a result of personal information being revealed, then a notifiable data breach incident must be reported.

Data breaches can be generally categorised in the following areas:

- a device with an individual's personal information that is lost or stolen (e.g. a credit card theft)
- a database with personal information, which has been accessed without authorisation
- personal information mistakenly given to a wrong party.

Personal information includes any information, which could identify an individual's credit information, health records, address, signature, date of birth, phone number and more.

Implications of NDB laws on an organisation

Failure to comply with NDB laws can incur penalties for organisations.

Below is a list of entities that must comply with the NDB scheme.

- Entities that fall under the Australian Privacy Principles (APP)
- Small operators with an annual turnover of greater than $3 million dollars in any financial year since 2001
- Credit reporting entities that handle private information
- Credit providers that handle private information
- Entities who are in possession of Tax File Numbers (TFN)
- Overseas entities with Australian links, which fall under the above-mentioned categories.

Non-compliance could mean serious fines; for example:

- companies face fines of up to $1.7 million
- individuals face fines of up to $340 000.

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

International data protection laws and Australia

In today's global world, compliance with international data protection laws may also be required.

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

The GDPR offers EU citizens more rights regarding:

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

There are large fines associated with breaches of the GDPR, even if the organisation does not reside in the EU.

Australians and GDPR

Australians 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 overlaps with NDB laws. Both promote the confidentiality of identifiable data on individuals; unauthorised sharing of individual data is in breach in both the GDPR and NDB laws.

Organisations need to be aware of federal, state and territory, and international laws that affect their business and data collection and storage.

Practice Task 1

Question 1

Which of the following statements about workplace cyber security are correct?
Select all that apply.

○ Cyber security at work is the responsibility of IT departments and managers.

○ Organisations' cyber security policies and procedures are governed by federal and state laws.

○ Data breaches likely to cause serious harm must be reported to the OAIC.

○ Australian companies need to comply with the GDPR if they have outlets in the USA.

○ It is a criminal offence for employees to access client information without permission.

Question 2

What does the CIA triad stand for? Explain how they can be addressed in organisations' cyber security policies and procedures.

Question 3

Draw a line to match the type of cyber hacker to its definition.

- White hat
- Grey hat
- Black hat

- Hackers with extensive knowledge of bypassing security systems in order to retrieve data. Often authors of malware.
- Ethical hackers who have permission to test the security of a system.
- Hackers who have hacked into security systems via a weakness they have found, who then notify the owners.

1B Create and maintain best practice programs

One of an organisation's most important assets is its staff, but they can also be one of the weakest links in cyber security.

Cyber awareness throughout an organisation is essential to create a cyber-safe work culture. Organisations today invest large amounts of capital to create, promote and maintain cyber-safe programs in the workplace.

Best practice in promoting cyber security within organisations include:

- assessing vulnerabilities to cyber attacks
- identifying weaknesses or vulnerabilities within an organisation
- designing policies and procedures to mitigate risks
- implementing procedures
- ensuring procedures are followed
- evaluating the procedure.

It is important that cyber security policies and procedures are made available to all staff members, are promoted, shared and enforced.

Implementing and promoting awareness programs

The Australian Cyber Security Centre (ACSC) provides a number of programs to keep Australian businesses safe online.

Read through their program *Stay Smart Online* for some tips on creating a cyber-safe culture at work. aspirelr.link/acsc-security-awareness

Below are some steps that can help you to create a cyber security awareness program for your organisation.

Step 1: Conduct a survey of the organisation's biggest threats.

Conducting a staff survey allows an organisation to build cyber awareness and collect different perspectives on problems that occur. It is a way to determine the type of practices used by staff and their awareness of cyber security threats and measures.

It allows management to hear about cyber security issues occurring in the workplace, and to identify strengths and weaknesses in dealing with them.

Weaknesses and strengths in the staff's knowledge of cyber security threats, procedures and responsibilities can be addressed. Results from staff surveys should form the basis of cyber awareness training or workshops.

Example

Cyber awareness survey questions

Surveys should be brief, easy to read and relevant to a worker's job role and daily activity. There are many free online survey builders or off-line paper-based surveys, which make the collection of primary data cheap and efficient.

Some sample questions to include are shown below.

Security is integrated into my daily work routine.

Answer by circling one of the items below.

- Strongly agree
- Neutral
- Disagree
- Strongly agree

Do you handle customers' personal information?

Answer by circling one of the items below.

- I do not know what customer personal information is.
- I am unaware if I do.
- Yes, I do, and I am confident that personal information is secure.
- Yes, I do, and I do not know if that information is secure.
- No, I do not.

Does your company have cyber security policies?

Answer by circling one of the items below.

- I am unaware if we do.
- No, we do not.
- Yes, we do, but I do not understand them.
- Yes, we do, and I understand them.
- Yes, we do, but they are outdated.

Step 2: Design a training program

Once you know the organisation's strengths and weaknesses, a cyber awareness program can be designed. Training can be provided for:

- existing staff or new staff such as a work team or department
- contractors or suppliers
- the Board of Directors
- refresher training for all staff members.

Developing a training plan for the delivery of the training program will provide a detailed overview of the sessions and the topics to be covered. A training plan may include:

- objectives of the training session
- profile of staff who will participate
- key terminology to be used
- resources required
- the topics to be covered with a time and description of the activity
- a space to include an evaluation of the activity such as feedback from participants.

Examples of information covered in a training program may include:

- privacy laws and requirements of the organisation
- legal responsibilities for privacy and storage
- intranet storage and access permissions
- file management protections and password protections
- avoiding pop-ups
- general cyber hygiene at work and home
- firewall protections.

Step 3: Gain management support

Management will need to sign off on the training program, especially if staff require time away from work to complete the training. They may want to see the training plan and be given an overview of the objectives of the training, expected outcomes and the cost involved in resources or staff removed from their work while undertaking the training.

Often management needs to be informed and educated on cyber issues within the organisation. It is important to keep managers up to date and gain their support to prioritise long-term training plans for staff on cyber awareness in the workplace.

Step 4: Use reminders, examples and multimedia

Cyber security awareness is an ongoing practice for workplaces. Once you have raised awareness of possible cyber security issues for workers and their role in identifying cyber threats and mitigating them, it's important to reinforce key messages regularly. A schedule of reminders to staff should be kept and updated regularly so staff are not overwhelmed with updates.

Depending on the size and type of business, this may be via:

- pop-up reminders
- email alerts
- notifications of updates
- posters around the office
- screensavers, etc.

These messages should be tailored to the audience and may need to be developed in languages other than English. An organisation's intranet, such as SharePoint, can be a good medium to promote the latest news and countermeasures to cyber security issues.

Step 5: Reward good cyber hygiene

Promoting cyber security awareness and offering incentives could have a huge impact on your organisation's security. Smaller companies may reward good behaviour by publicly acknowledging safe cyber practices. Larger organisations may have whole departments responsible for digital hygiene, backup systems and archiving information and data. A reduction in cyber attacks may be rewarded with financial bonuses.

Example

Rewarding secure behaviours in the workplace

Managers can reward staff by noticing cyber security practices and acknowledging them in public meetings, emails, newsletters etc.

Organisations with technical departments or teams responsible for handling sensitive information could reward staff for a reduction in incidents, by offering bonus payments, free lunches etc.

Reprimanding staff in front of others should be avoided, but when serious breaches of security policies occur, performance evaluation procedures need to be followed, as the organisation's reputation is at stake.

Step 6: Measure results

It is important to collect data on cyber attacks and measure any increase or decrease to identify the effectiveness (or ineffectiveness) of cyber security programs. By measuring any decreases in attacks due to cyber safety policies and procedures, an organisation is able to measure its return on investment in the cyber security awareness program.

Example

Training for staff

Profile

BizOps is a small manufacturing company with 20 employees. Many of the couriers use their own devices log in to the Wi-Fi when on site.

Issue

In the past, it has been known that malware and malicious applications have been introduced by poor cyber hygiene on employees' own devices. Luckily, the firewalls and anti-virus software caught all viruses and no damage was inflicted.

Safety program implemented

Short of banning the use of personal devices at work and enforcing stricter cyber security policies, the IT department or security team decided to:

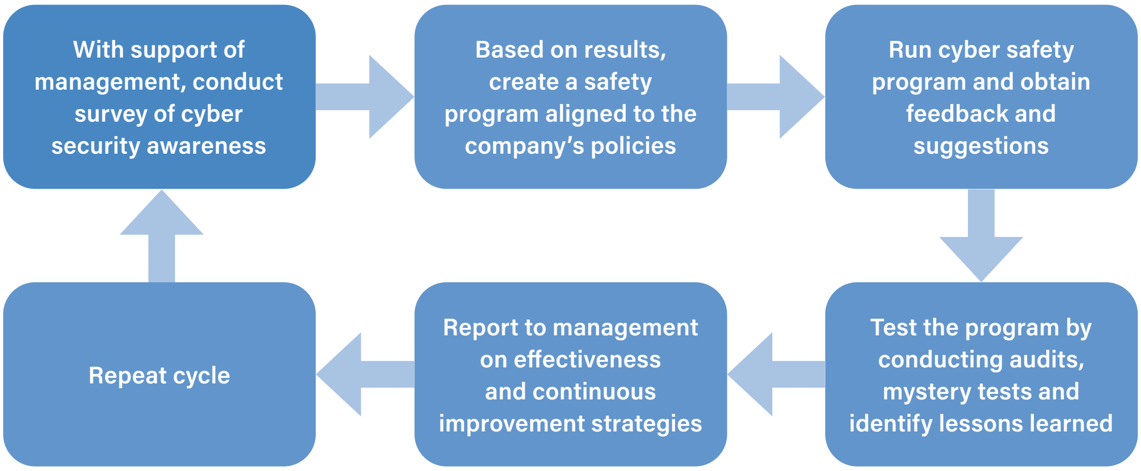
- text *employee-friendly policy reminders* when using the corporate wi-fi
- set up interactive feeds where staff had to accept and watch a 15–30 second video clip explaining cyber security measures in the organisation
- introduce consent forms to be signed by staff, accepting any new terms and conditions before being allowed to use the organisation's wi-fi
- implement training sessions for all staff, both at induction and periodically, to ensure they remain cyber alert and understand the organisation's policies and procedures
- hang posters in the staff room to remind workers to be cyber aware
- gather feedback from staff via surveys about their understanding of the cyber policies and how to record attacks or unusual online behaviour.

Cyber awareness is cyclical

Developing and maintaining cyber security in the workplace is a cyclical process.

All organisations need to invest in educating themselves and their staff on cyber security issues, its impact on the business and their role in reducing the risks.

Surveying staff, adapting policies and procedures, designing and conducting training, reinforcing policies and auditing continuous improvement strategies are on-going strategies for businesses today.


With support of management, conduct survey of cyber security awareness
Based on results, create a safety program aligned to the company's policies
Run cyber safety program and obtain feedback and suggestions
Test the program by conducting audits, mystery tests and identify lessons learned
Report to management on effectiveness and continuous improvement strategies
Repeat cycle

Practice Task 2

Question 1

List four common ways that cyber threats can be introduced to a workplace.

Question 2

Number each step from 1 to 6 in the order you would follow, to plan and create a cyber safety program in your workplace.

○ Test effectiveness of program via audits

○ Implement continuous improvement

○ Survey the staff on cyber security awareness

○ Conduct staff training

○ Create cyber safety policies and procedures

○ Send reminders and email alerts

Question 3

List four topics likely to be covered in a cyber safety training session for office staff.

1C Contribute to and communicate policies and procedures

Policies and procedures that govern an organisation's cyber security are important for every employee to follow.

A policy is developed by an organisation and outlines its own specific requirements, processes and rules in keeping with legislated requirements. Policies can take the form of practical guidelines for ensuring compliance with privacy laws, discrimination laws, monitoring, surveillance acts, etc. Like an act, a policy must always be followed carefully and exactly.

While it is not expected that employees read every piece of legislation related to their job role, it is very important that they become familiar with the organisation's policies. In many cases, following policy means that you are also following the law.

Policies and procedures might be accessed via a printed copy, such as a policy folder, or online, such as via the organisation's intranet. If you can't locate the policies, ask someone to show you where they are kept.

Discussing policies and procedures

Policies and procedures need to be living documents, which means they inform and require interaction from staff and are continually edited and updated.

As changes are made to processes or the working environment, or cyber threats are identified, policies and procedures should be updated to reflect this. Procedures tend to be updated more frequently, whereas policy documents are high-level statements that do not change as often. For example, when the COVID-19 virus arrived in many countries in 2020, many organisations had to allow employees to work from home. Policies and procedures had to be updated to ensure guidelines for safe work practices in the home and secure work communications could be maintained. Updating or developing a policy or procedural document will require the input of management, other colleagues and a review by specialists in other departments such as People and Culture or IT. Always check with a supervisor the organisational requirements for the workplace.

Policies and procedures are often introduced to workers during induction training. IT policies, such as acceptable usage policies, are usually required to have compliance to and understanding of signed off by new employees during their induction.   You should be informed of the location of the policies and once you have read through them, discuss with your manager or colleagues how they directly relate to you and your job tasks.

Ongoing training and refreshers in cyber security policies and procedures should also be periodically scheduled for new and existing employees.

Content of a policy document

A policy document is structured into clear sections, outlining the rules, guidelines and regulations an organisation requires employees to follow.

A policy should include, but is not limited to, the following information.

- **Purpose:** What is the purpose of the policy?
- **Scope:** Who does the policy apply to?
- **Relevant legislation:** What legislation is being adhered to?
- **Policy statements:** Details of the policy inclusions
- **Supporting resources:** Any documents both internal and external that support the policy
- **Responsibility:** Who in the organisation is responsible for the policy?
- **Promulgation:** Official communication of the policy's ratification

Procedural document contents

Procedures outline the way policies statements are executed to support operational activities and compliance with relevant legislation.

The procedures provide a step-by-step guide in how to complete a task; for example: how to save a document or report a cyber threat. These guidelines often include flowcharts and diagrams to clearly explain a process. Adherence to procedures is expected by management to ensure cyber security is practised across the organisation.

A procedure document should include, but is not limited to, the following information.

- **Procedure:** What is the purpose of the procedure?
- **Scope:** Who does the procedure applies to?
- **Relevant legislation:** What legislation is being adhered to?
- **Actionable steps:** Details of the procedure including responsibilities
- **Supporting resources:** Any documents, both internal and external, which support the procedure
- **Responsibility:** Who in the organisation is responsible for the procedure?
- **Promulgation:** Official communication of the procedure

All policies and procedures are companywide and are set by management or authorised personnel only. Unauthorised personnel contribute to policies and procedures by making suggestions.

Cyber security fundamentals

When creating policies and procedures for cyber security, it is important you understand the terminology.

Cyber security issues often use specific terminology and this language will be reflected in the policies and/or procedures used by staff. Having these terms clearly defined, means staff will better understand the policies and the relevance of the policies and procedures to their job role. Some policies may include a glossary of terms.

Some terminology for cyber security is explained below:

Secure storage	Secure storage ensures that information assets are protected within company policy. They could include locked screens, encrypted data and authorisation mechanisms, such as fingerprint technology.
Sharing	Sharing in the context of cyber security is sending company information to others. A problem may arise when certain parties are not allowed permission to access information, so it is important to always check the data classification to guide you as to what is acceptable use.
Managing information	Managing information refers to the management of information created; its distribution and decisions regarding its confidentiality, availability and integrity.
Encryption	Encryption is the process of encoding data or scrambling text in a way that makes it illegible to unauthorised parties (also known as cipher text). Encryption works with the use of public and private keys; encoders who hold public keys can encode data to cipher text and private key holders are able to encrypt data to cipher text in order to access the information.
Protocols	Protocols are sets of rules or standards that govern the transfer of data and information between two or more devices or computing systems.
Media	Media, commonly known as digital media or mediums, is a method of storage on computing devices. Examples are USBs, CD-ROMs, flash cards and portable hard drives.
Document labelling	Document labelling is a method used to name files or reports for easy retrieval within an organisation. In information management, a uniform approach is important, as different colleagues or departments may rely on efficient access to the same files. Appropriate and uniform document labels and file paths are identified as per policy standards.
Data governance	Data governance refers to an organisation's collection of policies and processes, which guide its use, protection and storage of data.
Acceptable usage	Acceptable usage policies outline what is and is not acceptable usage of IT resources within an organisation. For example, they set guidelines for email and internet usage, how devices are to be used within the workplace and while off-site, and outline conditions of usage.
Bring your own device (BYOD)	BYOD refers to an organisation's policy allowing personnel to bring their own computing devices such as mobile phones, tablets, laptops, computers, smart watches and anything else into the workplace.

Data classification

In cyber security, information is categorised on a continuum from confidential to public and anything in between.

Protecting the CIA triad of information is important for organisations, as it can lead to criminal charges or a risk to their brand and reputation if information is not protected.

The Australian Attorney-General's department has created a security classification guide to assess the sensitivity of information and its impact on businesses if it is not handled securely and confidentiality is not maintained.

The Attorney-General's Data Classification Guide is shown below.

Classification	Business impact level	Compromise of information a breach would be expected to cause
Unofficial	No business impact	No damage; information is intended for public view
Protected	High business impact	Damage to business interests, organisations or individuals involved
Secret	Extreme business impact	Serious damage to business interests, organisations or individuals involved
Top secret	Catastrophic business impact	Exceptionally grave damage to the business interests, organisations or individuals involved

Below is an example of a policy for managing information.

Example

A policy for storing, sharing and managing information

1.	Purpose and scope
1.1	*Purpose.* The purpose of this policy is to highlight secure storage, sharing and managing information at BizOps Enterprises. These rules are in place to protect the employees and BizOps Enterprises.

1.2	***Scope.*** The scope of this policy applies but is not limited to: ▪ the use of computing related equipment ▪ collecting, storing, accessing and sharing information ▪ electronic and network resources owned by BizOps Enterprises. This scope includes employees and third parties. All employees, contractors, consultants, temporary and other workers at BizOps Enterprises and its subsidiaries are responsible for exercising good judgment regarding appropriate use of this policy at BizOps Enterprises.
2.	**Relevant legislation**
2.1	In accordance with the *Privacy Act 1988* (Cth)
3	**Policy statements**
3.1	Storage
3.1.1	***Physical storage.*** Storage of BizOps Enterprises data on physical devices, removable devices such as but not limited to USB drives, flash cards, memory cards or external storage devices must be approved by the IT department before usage in BizOps Enterprises property.
3.1.2	***Cloud storage.*** BizOps Enterprises information/data should never be stored in cloud storage applications or accounts that are not provided by BizOps Enterprises. You will be directed to a user account with login credentials and all information/data remains the property of BizOps Enterprises. As a procedural policy, the IT department has approved the following for usage, for which accounts will be created on your behalf: ▪ URL or application of service ▪ guidance, permissions and usage procedures; these will be provided to you upon request.
3.2	Sharing
3.2.1	***Sharing policy*** applies to all data owned by BizOps Enterprises, which is classified by data classification and management policy. This policy includes, but is not limited to, computing equipment, servers, databases and information systems (including computing devices which access email, web services, third-party application data and other data owned by BizOps Enterprises which may not be computer-related, such as physical information).
3.3	Managing information The purpose of this section is to provide guidance to staff on the creation and management of information assets.

3.3.1	BizOps Enterprises information created should include all required information for adequate business decision making, which include but is not limited to names, dates and other information required for BizOps Enterprises.
3.3.2	All information created and received for BizOps Enterprises should be within compatible formats, language, versions and other requirements in context for regular business use by BizOps Enterprises.
3.4	Access to information
3.4.1	Information is owned by BizCorp Enterprises, which should facilitate staff members to complete their job responsibilities where access is permitted, unless restricted by the data classification and management policy.
4.	**Supporting resources**
4.1	Data classification and management policy.
5.	**Responsibility**
5.1	Departmental managers
6	**Promulgation**
6.1.	The policy is to be announced via official electronic communication sent to company email addresses followed by the current policy repository, which can be accessed via the company intranet.

For more information on creating cyber security policies and procedures, see the Australian Government Business website: aspirelr.link/business-cyber-security

Practice Task 3

Question 1

Which of the following statements are correct for cyber security policies and procedures? Select all that apply.

○ Cyber security policies should refer to privacy Acts and other relevant legislation.

○ Cyber security procedures offer a step-by step approach to managing information.

○ Cyber security policies and procedures need scheduled reviews and updates.

○ Cyber security policies and procedures are the same thing.

○ Cyber security policies and procedures may help employees understand how to prevent a cyber attack.

Question 2

Draw a line to match each term about cyber security to its definition.

» Encryption	» An external device used to store data such as a USB or portable hard drive
» Secure storage	» To announce, publish or divulge the information or policy
» Media	» Method of holding data to maintain CIA; for example: locked screens, encrypted data and authorisation mechanisms such as fingerprint technology
» Promulgation	» Encoding data or scrambling text in a way to make it illegible to unauthorised personnel

Question 3

List seven sections included in a cyber security policy.

Question 4

To your previous answer, add one extra section you would find in a cyber security procedure.

Summary

- Cyber security is the protection of information collected and stored on computers or digital systems and networks.
- The CIA triad stands for: confidentiality, integrity and availability.
- There are three classifications used to describe hackers:
  - white hat hackers – personnel with permission to test security of a target
  - grey hat hackers – IT experts who have hacked into a system without authorisation and then notify the organisation of the threat
  - black hat hackers – hackers who deliberately hack into systems for criminal purposes, punishable by law.
- Cyber security awareness at work includes:
  - legal Acts and other laws to which employees and organisations must adhere when collecting, storing and sharing client information and data
  - responsibilities of all employees to ensure information is managed securely
  - notification of data breaches (NDBs); these are mandated by law, which requires every employee or organisation to report possible or actual data breaches to the OAIC. Penalties such as fines are imposed on organisations that do not comply with the NDB laws.
  - an understanding of international data protection laws and how they affect Australians and Australian organisations.
- Practical step-by-step guides to promoting cyber awareness programs at work are created by ACSC to protect cyber security, including staff surveys, training, procedures, notification reminders, cyber cleaning and measuring results of cyber safety programs.
- Contributing and communicating policies and procedures at work include:
  - creating and maintaining current cyber security policies and procedures
  - using terminology common to cyber security policies and procedures
  - using the security classification guide, designed by the Australian Attorney-General's department, to assess the sensitivity of information and its impact on businesses if confidentiality is not maintained.

Learning Checkpoint 1

Develop cyber security awareness in your work area

Part A

1. Define the purpose of the *Privacy Act 1988* (Cth).

2. The Victorian *Privacy and Data Protection Act 2014* sets out the minimum standard for how Victorian public organisations should manage personal information. List the ten information privacy principles.

3. When is a person or organisation required to complete and send a *Notifiable data breach incident report* to the OAIC?

4. Which of the following statements are correct regarding the General Data Protection Regulation (GDPR)? Select all that apply.

   ○ Any Australian company that has a branch in Europe must comply with the GDPR.

   ○ Australian companies only need to comply with state and federal laws.

   ○ The GDPR protects personal data for all European citizens, regardless of where they reside.

   ○ Australian companies selling goods in Europe can be fined for not complying with GDPR.

   ○ Companies based in the USA who store European citizens' data do not need to comply with the GDPR.

5. Which of the following terminology would be found in policies and procedures relating to cyber security? Select all that apply.

   ○ Data governance

   ○ Bring your own books (BYOB)

   ○ Document labelling

   ○ Person centred care

   ○ Encryption, and protocols for its uses

6. Notifications of updates can be an effective way to regularly reinforce key messages to staff.

   ○ True

   ○ False

7. Draw a line to match each term about data classification with its business impact level.

» Unofficial	» High business impact
» Protected	» Extreme business impact
» Secret	» No business impact
» Top secret	» Catastrophic business impact

Part B

Read the case study and answer the questions that follow.

Case study

Your business is being hacked regularly and a customer rings up to say he is able to access your business system with ease and has seen confidential information held on your system. He informs you that he was able to access the system by guessing or predicting passwords of staff members.

1. What type of hacker is this person?

○ White hat hacker

○ Black hat hacker

○ Grey hat hacker

○ Yellow hat hacker

3. Write a policy for your business for password protection, using the template below. Complete all sections and number each section and subheading.

	Title
	Purpose

	Scope (Who the policy applies to)
	Relevant legislation (What legislation is being adhered to? Include website address.)
	Policy statements (details of the policy inclusions)

	Supporting resources (any documents, both internal and external, that support the policy)
	Responsibility (Who in the organisation is responsible for the policy?)
	Promulgation (official communication of the policy's ratification)

5. Write a procedure for staff to follow in order to create and maintain a strong, secure password, using the template below. Complete all sections and number each section and subheading.

	Title (of procedure)
	Purpose (of procedure)
	Scope (Who does the procedure apply to?)
	Relevant legislation (What legislation is being adhered to?)

	Actionable steps (details of the procedure, including responsibilities)
	Supporting resources (any documents, both internal and external, that support the procedure)
	Responsibility (Who in the organisation is responsible for the procedure?)
	Promulgation (official communication of the procedure)

Topic 2 | Support effective cyber security practices at work

2A Review practices according to organisational policies and procedures

2B Arrange training, updates and maintain records

2C Present insights to mitigate impacts on workplace

2A Review practices according to organisational policies and procedures

As cyber threats change, reviewing cyber security policies and procedures is required to ensure controls, measures and practices within the workplace are adequate.

Many organisations have established cyber security policies and procedures that are aimed at keeping information secure and responding to any data security incidents. These policies and procedures need to be regularly reviewed to maintain constant cyber safety.

Reviewing current cyber security practices

Reviews should either be scheduled regularly or conducted as required after an incident or threat has been detected.

It is important for management to set the security posture of the organisation. Security posture refers to an organisation's cyber security strength: how well it can predict, prevent and respond to ever-changing cyber threats. Once the security posture has been established it then needs to be monitored and reviewed.

In order to review cyber security policies and procedures, organisations need to identify:

- information assets
- threats to these assets
- policies and procedures to protect assets
- security controls to protect assets.

Identifying information assets

The value of an information asset is measured by the impact the loss of this item would have on the organisation.

'Information assets' refers to data that your business relies on to carry out its business-as-usual operations.

Information assets and the sensitivity of these assets will vary depending on the type of business or service provided. For example, the type of information a medical clinic collects from its clients will be different from that of a retail business.

Information assets are classified according to the level of sensitivity and the security required for handling and storing this information.

A good data classification policy will highlight the sensitivity of the data, such as critical data, which should be protected via tight security controls.

Identifying threats to valuable assets

Potential threats to information assets need to be predicted, monitored and evaluated.

Knowing what kind of threats could affect your information assets is a daily practice that should be handled by the right personnel, including but not limited to the IT or security department and management.

A risk analysis is an effective way to identify the likelihood of threats occurring. A risk matrix tool (shown below) can be used to track potential threats that may arise and measure the impact this would have on the organisation's business activities.

A risk matrix is shown below.

		Consequences				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	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

1 – Very high, 2 – High, 3 – Moderate, 4 – Low (monitor)

The risk matrix provides a score against the probability of a risk occurring and the impact if the risk eventuated.

A threat matrix is similar to a risk matrix. It identifies assets susceptible to specific threats:

		Assets				
		Digital storage (at rest)	Cloud storage	Printed information	Firewalls	Corporate website
Threats	**Confidentiality attacks** (e.g. leaks, releasing confidential data)	High	Medium	High	Medium	High
	Integrity attacks (e.g. incorrect information, invoice amounts)	High	NA	Medium	NA	NA
	Availability attacks (e.g. physical theft of asset, server's availability)	Low	Medium	Low	High	High

It is important for organisations to keep abreast of the latest cyber crimes and threats that may affect their business. The Australian Cyber Security Centre (ASCS) reports on cyber threats daily and is an excellent resource for checking current cyber threats.

Policies and procedures to protect assets

Cyber security policies and procedures should provide clear steps for employees to follow, to keep information assets safe, to be alert to any possible threats and how to respond.

A review of an organisations policy might include the following areas that are covered under acceptable usage policies::

Passwords requirements	▪ How to store passwords ▪ Password strength
Email security	▪ Opening email attachments ▪ Junk mail policy ▪ Identifying and reporting suspicious emails

Handling sensitive data	▪ Sharing policy – Data classification – Identifying sensitive data – Destroying sensitive data
Technology handling	▪ Bring Your Own Devices (BYOD) policies ▪ Safely connecting BYOD procedures ▪ IT System updates and patching ▪ Removable devices policy and procedures
Social media	▪ Appropriate use of social media ▪ Appropriate social media accounts to access through company resources
Incident handling	▪ Incident response policy and procedures ▪ How to identify an incident ▪ Staff roles and responsibilities

Security controls to protect assets

Security controls are technical methods used to increase the security posture of an organisation.

ACSC has a list of eight essential security controls that companies should implement and have checked on a regular basis. A table outlining these security controls is provided below:

No.	Security control	Importance of this control
1	Application whitelisting	▪ A list of approved software applications ▪ Non-approved applications (including malicious code) are prevented from executing
2	Patch applications	▪ Patches are software and operating systems that systematically update security for applications ▪ Unpatched applications can be used to exploit IT systems
3	Patch operating systems	▪ Software updates that address security vulnerabilities within a program ▪ Security vulnerabilities in operating systems are common ways hackers gain initial access and search for sensitive information

No.	Security control	Importance of this control
4	Restrict administration privileges	▪ Restricting user access to critical or sensitive system resources and programs to bare minimum privileges necessary to perform the user's job role/function ▪ If these kinds of accounts are compromised, you are allowing hackers full reign.
5	Disable untrusted Microsoft Office macros	▪ Microsoft Office macros are mini applications that may be used to deliver malware
6	User application hardening	▪ Securing applications such as web browsers is critical as browsers are used to access sensitive information
7	Multi-factor authentication	▪ Verifying user identity using more than one method to access systems makes it harder for hackers to log in without authorisation
8	Daily backup of critical data	▪ Programs installed to automatically back up critical data allow you to restore critical data immediately following an incident

Example

Happy patch Tuesday

Patch Tuesday or Update Tuesday refers to the day Microsoft releases update packages for the Windows operating system and the Microsoft suite of applications. These packages patch recently detected vulnerabilities in applications. Applications should be patched according to the organisation's patch management policies and procedures.

Practice Task 4

Question 1

List two reasons why organisations should regularly review their cyber security policies and procedures.

Question 2

List four actions organisation needs to take when reviewing cyber security policies and procedures.

Question 3

Select true or false.

Employees should read and sign off their understanding on IT acceptable use policies before commencing employment.

» True » False

Question 4

Draw a line to match each term related to cyber security controls, to its definition.

» Application hardening	» An organisation's capability to protect its information, detect and react to cyber threats
» Application whitelist	» A management tool used to measure the likelihood of an event occurring and the impact
» Security posture	» A list of approved and authorised software applications used in an organisation
» Patch applications	» Securing applications such as web browsers
» Risk matrix	» Updates sent to users as weaknesses in software are detected

Question 5

Where can organisations in Australia find information about the latest cyber threats?

Question 6

List four parts of an organisation's cyber security policy that may need to be reviewed after a data security incident.

2B Arrange training, updates and maintain records

Organisations need to invest in training all staff to identify and handle cyber security incidents.

Good cyber security training should focus on the organisation's risks posture and the policies and procedures developed to safeguard against threats.

As with any training program there is a process to prepare, develop, deliver the training, and evaluate training outcomes.

The following nine strategies will assist you to plan and structure effective cyber awareness training.

1. Needs analysis

Firstly, it is necessary to identify the reason/s and define the purpose of the training.

This is done by conducting a needs analysis, which may include a survey or discussion with managers and/or staff to identify problems with cyber security, processes at work, responsibility and level of skills needed to identify and report threats, etc.

Results from the needs analysis will inform the content of the training.

2. The attendees

Knowing who will attend the training is important in order to tailor content. Keeping in mind the following learner variables will help you create the right balance of activities and input.

- **Digital literacy level.** Some attendees may find a computer daunting and others may be highly proficient.
- **Readiness to learn.** Motivation and willingness to learn is increased if people can see how the training will benefit their work role, rather than a mandatory work training punishable if they do not attend or pass.
- **Motivation to learn.** Similar to the previous step, sometimes a 'lunch and learn' with full catering may be required to provide the right incentive to learn.
- **Adult learners.** These people bring life experience and prior knowledge to training sessions, are goal oriented and often prefer to learn practically. Make sure you are familiar with some of their previous experience so you don't teach them things they already know and can engage them in activities more easily.
- **Methods of learning.** Everyone learns in their own way. Learners are often categorised as visual, kinaesthetic and/or auditory. Delivering training with a mixture of visuals, experiential activities, movement and oral activities will allow you to engage most learners.

3. Establish learning objectives

Learning objectives are the basis of any training session and make it easier for attendees to see the relevance, to understand and to focus during the training.

Learning objectives often start with a clear statement defining what the attendee will be able to do or know by the end of the session. For example: 'at the end of this training session, attendees will be able to detect possible cyber threats in emails'.

4. Structured training sessions

Structured training sessions keep your training efficient and on track. Always plan out your activities and think about what the participants will be doing at different stages of the training session. Allocate times beside each activity to keep the training moving and to make sure you spend the most time on the important issues.

Set an agenda you can stick to and share the training agenda with attendees before they arrive. This will keep the training on track and stop you from deviating too much from the objectives.

5. KISS presentations

A Keep It Simple, Stupid (KISS) presentation is a simple, effective model for delivering training using PowerPoint. Keeping slide presentations simple, by the use of simple graphics and emphasis on the key points, will strengthen the message to learners.

6. Training materials

Training materials generally fall into two main categories:

- trainer materials
- participant materials.

Trainer materials may include PowerPoint slides, policy and procedural information, activity sheets, answers to trivia quiz, etc.

A good model to keep in mind when generating session content is the 5E learning model, which describes the phases outlined below.

- **Engage** by establishing relevancy to workplace cyber awareness.
- **Explore** by presenting the session content, with practical tips relating back to policies and procedures.
- **Explain** to participants why topics are important for the organisation's cyber security goals.
- **Elaborate** by engaging participants in activities, getting them to practice tasks, etc.
- **Evaluate** by asking participants to outline the lessons learnt in the training sessions.

Participant materials may include an agenda, session overview with learning objectives, worksheets and supporting materials.

7. Make it fun

Keeping the lessons interactive and timely means that you use the learners' time wisely. Some participants may not be interested and have other important tasks to complete, so keep the training sessions fun with short, sharp but relevant activities that deliver maximum impact.

If topics are long in nature, consider breaking the information into bite-sized chunks that are easily understood, follow a logical pattern and include activities to reinforce the content or require attendees to practice skills.

8. Choice of venue

Having an appropriate location is important for any workplace training. Make sure the location is convenient, comfortable and the right size for the group activities planned. Make sure it also has the resources you need such as computer screens, whiteboards, paper, pens, good lighting, tea and coffee (if required), etc.

9. Conclusion and evaluation

When you have finished your training sessions, recap on the lessons learnt and always seek feedback. This may be informally, via a discussion at the end of the session, or more formally, by completing an online or paper-based survey. You can also seek further feedback anonymously on:

- the trainer/presenter
- the way the training was delivered
- specific activities
- the content and relevancy to job role
- the venue, comfort level, etc.

Common topics for training in cyber security

Cyber security is a common problem among all businesses and therefore there are some common topics used for training.

Although training will depend on each organisation's goals and experience with cyber threats and security, there are some common topics that often require input and training.

Some of these are explained below.

Identifying and reporting a cyber incident

With the increase in cyber attacks, it is critical that all organisations and employees are aware of their legal responsibility to report cyber incidents.

Since 22 February 2018, Mandatory Data Breach Notification (MDBN) laws mandate that all entities report cyber security breaches that are likely to cause harm.

The OAIC describes a data breach as harmful when 'personal information is accessed or disclosed without authorisation or is lost'.

Incident vs event

A cyber incident is defined as an unexpected occurrence, which interrupts a business process or system and has the potential to cause harm. A security incident can occur due to deliberate or malicious intent, though it could be unintended as well. It may be unexpected, unauthorised access to systems or disclosure of information.

A cyber event is a change in the daily operations of a network or system, indicating a possible breach of information security or failure of controls. It may be found to be an intentional act to cause harm.

The intent behind the disruption is an important factor to distinguish between an incident and an event. A cyber event or incident can be as a result of deliberate malicious intent, or accidental and unintentional. The root cause is usually identified during the analysis phase of incident response.

Organisations are required by law to have their own policies to identify what constitutes a reportable cyber incident or event in their workplace.

If in doubt, the best thing to do is to notify your department of anything suspicious or unusual.

Examples of cyber incident and events are shown below.

Cyber incidents	Cyber events
System administrator accidentally creates a new user.	System administrator intentionally creates a new user.
Client database accidentally ends up on Google Docs.	Client database is placed on Google Docs.
Backup process fails.	Backup process is tampered with.
Backup records are lost.	Backup records/systems are intentionally lost or deleted.
Accounts department unintentionally approves expenses without authorisation.	Accounts department intentionally approves expenses without authorisation.
General email is sent to the entire organisation from the CEO's email account.	General email is sent to the entire organisation from a fake CEO email account.

Incident reporting procedures

All workers in an organisation should know how to report a data breach, as it is a legal requirement according to the *Privacy Act 1988* (Cth).

If a person suspects or knows the organisation has been compromised, they can follow these steps:

1. Investigate the suspicious problem and notify IT department.
2. Talk with a staff member, manager or colleague.
3. Take notes such as screenshots, date and time, and record how you found the suspicious activity.
4. Report the incident, filling in an incident handling report.

Simulated activities for reporting incidents

Simulated activities are a useful way to train staff in following organisation procedures and to learn by doing.

First, create a life-like scenario and second, ask attendees to complete an activity based on the scenarios and following organisational procedures.

A simulated activity should include three components:

1. Action
2. Procedure
3. Context

A simulated activity for completing an incident report could include the following scenario outline:

- BizOps (fictitious company) has just moved to a new location due to its expansion into a new territory (3) and with staff recently trained in cyber awareness training, management is keen to put these new skills into action (2).
- The objective of this exercise is to assess any suspicious activity (1) in the new location by correctly identifying and reporting any suspicious behaviour believed to be an incident (2).

An example of an incident report is shown below.

Example

Sample of an incident report form

Incident summary	
Type of incident detected:	
Confidentiality attack	Information disclosure
Integrity attack/ deception attack	Unauthorised modifications, wrong data etc.
Availability attack	Denial of Service (DoS)
Other	
Incident location	Worksite 3, Building 2, workstation 23 (my work station)
Site	Melbourne Worksite 3
How was the incident detected	I saw red screen demanding bitcoin
Information on the incident	I think it is ransomware as the screen is asking me for money
How was the incident detected	I opened my email and saw an email addressed to me claiming I was a lucky winner during for free fuel due to my recent visit to the supermarket. I clicked on the link stating 'REDEEM YOUR FREE FUEL' and then I saw a red screen asking me for money

Scam phishing emails

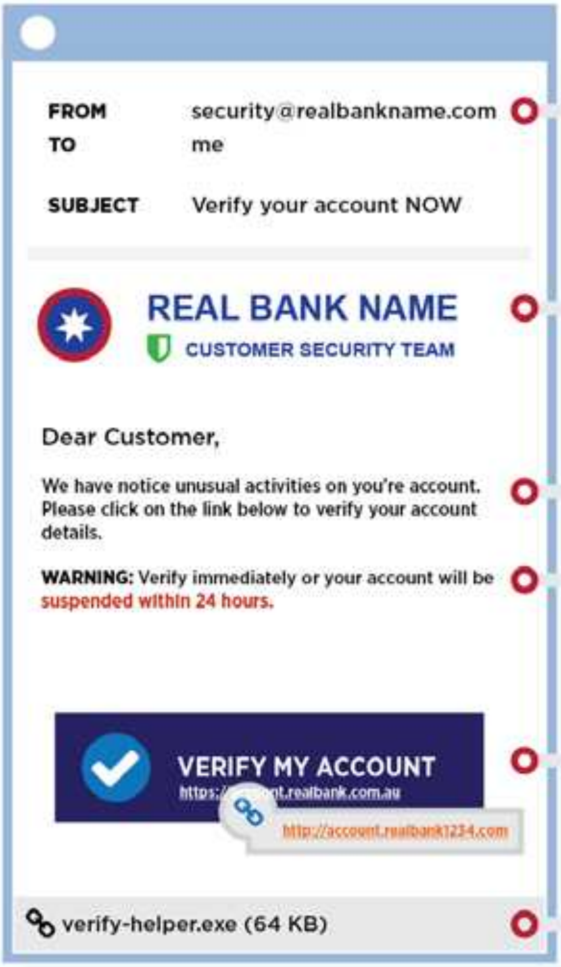
A phishing email originates from a sender who is disguised as a legitimate company or business, which sent to people in order to gain access to personal details, bank accounts and passwords.

Many organisations receive spam emails with varying degrees of malicious intent.

Phishing emails look genuine and are sometimes hard to detect, but there are signs to look for. Here is a list of warning signs of a phishing email:

- an unusual and unexpected email that claims to be from a trusted source such as your bank, telecommunications provider or any other entity you usually deal with
- it contains a generic template that does not address you personally, or has no unique identifier relating to you
- it contains typing errors and poor grammar
- the website address does not look genuine
- website links are unusual, hidden or have unusually short website addresses
- it includes an attachment such as a PDF, but in fact is likely to be a .exe file type (executable program); these can often be malware
- the imagery and branding are not 100 per cent accurate.

Some checks to look for to detect a scam email are shown in the following diagram:



FROM security@realbankname.com
TO me

SUBJECT Verify your account NOW

Dear Customer,

We have notice unusual activities on you're account. Please click on the link below to verify your account details.

WARNING: Verify immediately or your account will be suspended within 24 hours.

verify-helper.exe (64 KB)

ALWAYS check the 'from' email address, and be aware thet even this can be fabricated.

Scammers will make every attempt to make the email look legit.

If in doubt, check with the organisation directly.

May contain spelling mistakes and poor grammer.

Scammers may feign a sense of urgency or make threats to trick you into action.

ALWAYS check links in emails are real before clicking on them.

Hover on desktops or 'tap and hold' on mobile devices.

NEVER open or download anything unless you are 100% sure they are from a safe source, especially if they are an .EXE file.

For more information on phishing, please visit the ACCC: aspirelr.link/accc-phishing

Phishing attacks on business procedures

Phishing attacks are usually designed to send unsuspecting users links to access four main areas:

- **financial/payment services**, such as invoice payments, debts outstanding from the tax office
- **personal information**, such as retail purchases, parcel deliveries, order confirmations, etc.
- **communications**, such as information stored on cloud service providers, hijacking of social media accounts, etc.
- **technology based communications**, such as authentication required for fake services, including login requests, password resets, etc.

Phishing simulation activities

There are generally three ways to conduct phishing simulation activities:

- in-house generated activities
- free resources found online
- commercial products.

In-house generated activities

Fake or real phishing games can be generated from actual documents found in your workplace.

In-house generated activities may include printing A4 documents where colleagues are asked to look for signs that confirm if the document is real or fake. Results are explained, summarising key signs to look for when detecting a fake email.

Free resources found online

Many software providers offer free phishing quizzes in the hope to upgrade users to paid versions. These may be suitable for training purposes.

Commercial products

A range of virtualised software is available to train people in detecting fake emails. This includes a number of open-sourced software packages that can be used to simulate a phishing email, which can be sent to staff to test if they can identify it as a fake email.

IT staff need to install the open-sourced applications, which contain customised emails that appear to come from a CEO, banks and other trusted suppliers.

Some free open-sourced phishing simulators are listed below.

- **GoPhish**: aspirelr.link/go-phish
- **Lucy**: aspirelr.link/lucy-phish

Information updates and maintenance

Cyber security intelligence needs to be collected from a variety of sources so that mitigation strategies can be updated.

Information and cyber security intelligence can and should be gathered from many sources, such as employees, industry bodies, government officials, legislation, threat intelligence subscriptions etc. This information should be recorded via the correct procedures so that organisations are able to track the frequency of cyber threats and attacks and work to prevent them causing damage.

In a workplace, cyber security information must be forwarded to the right department (IT, security or management) to control the risk and decide if policies and procedures need to be updated.

Methods to combat cyber threats and maintain cyber safety at work should be freely available to employees and users of services.

Information available to employees may include updates on:

- how to back up your work
- new security software installed
- how to record a suspected cyber incident or unusual behaviour
- how to secure your devices such as your mobile phone, laptop and tablets before connecting to the corporate network
- knowing what encryption is and how to use it
- knowing how to set strong passwords.

If policies and procedures need to be updated urgently due to the detection of a cyber threat, then the updates should be disseminated to staff as quickly and efficiently as possible, using texts, email alerts, noticeboards, web page banners, newsletters, direct emails, impromptu staff meetings, etc.

Practice Task 5

Question 1

List four pieces of information you would need to know about participants, before planning a training session in cyber security.

Question 2

Number each step from 1 to 5 in the order you would follow to plan a cyber security training session.

○ Develop training materials

○ Conduct needs analysis

○ Establish learning objectives

○ Schedule training, agenda, venue etc.

○ Create an evaluation tool

Question 3

Which of the following statements relate to creating relevant cyber security training sessions? Select all that apply.

○ Training activities should always be fun and entertaining.

○ Simulated activities are a good way to engage adult learners.

○ Free commercial products are available for training people to identify phishing emails.

○ Adult learners learn by doing.

○ PowerPoint slides should contain all the information you need to convey.

Question 4

List four tips you might cover in a cyber security training session to assist staff to detect a phishing email.

2C Present insights to mitigate impacts on workplace

Feedback loops are essential for producing a cyber-aware workplace.

Once training has been conducted, it is time to assess the impact the training has had on cyber security practices in the workplace.

This may be measured by a reduction in cyber attacks, an increase in incident reporting by staff, less reliance on IT staff to retrieve lost data, etc.

Trainers responsible for facilitating cyber training and their support staff, have the responsibility to report findings to management. They can collect quantitative results and present these and overall feedback to management by using metrics and creating a baseline to measure improvement against.

Metrics

Metrics presented may include:

- a comparison of results between last training workshops
- a reduction of or increase in vulnerability and response times; the lower the response time the better
- an explanation of statistics, which show the value of cyber safety to the organisation in dollar terms or as an increase in assets.

Baselining

Baselining is the measurement of network activity against a previous measurement to identify differences.

Base lining is useful when managers want to measure performance of new techniques, personnel skills or strategies to measure improvement.

Results between time periods provide insights for managers into training needs, individual or department performances and opportunities for praise.

For example, in one business, this time last year, 20 per cent of IT requests were for retrieving lost data. This year only 10 per cent of IT service requests were data retrieval queries. Hence, the improved filing system and backup training sessions and procedures were judged as being successful.

Example

Baseline metric

BizOps Enterprises decides to use some metric information to start baselining their performance to improve their security posture. It does not know what to measure so is advised to start with the number of website security defects and the time taken to fix issues.

Initially BizOps finds that it takes longer than one month (32 days) to repair reported bugs in their website. Over a period of six months, the web department reduces the time it takes to fix website issues to just seven days, a significant reduction of 25 days.

A report outlining a reduction of days is sent to management and staff to communicate its impact.

Using a baseline helped BizOps management to improve on measurable activities. They soon started applying baselining to other departments.

Communication methods

Select communication methods based on the audience, the urgency and purpose of reporting and organisational policies and procedures.

Presenting technical information clearly and in a timely manner is important for decision-making.

Summarising the main points and succinctly explaining what the technical data shows and the impact on the business, is important.

Usually technical data can comprise a list of logs, codes or other sometimes, confusing technical documentation to an untrained eye. This level of detail may not be required or easy to understand for colleagues outside the IT or security departments.

A summary of what the data shows, it's impact on the business and the urgency of responses required will determine how the information is best reported.

Depending on who you need to report the information to, will also determine the method of communication.

Some communication methods are listed below.

Report format

- If reporting to managers or Board members, you may be required to present technical data in a written business report format, including sections for a title, content, executive summary, approach, findings, conclusions, recommendations, appendices.

- You may be required to present the data in a business presentation using PowerPoint slides with graphs and diagrams, emphasising key points and, if required, providing the technical data as an appendix or hand-out.

In-person meetings

- If technical data reveals an urgent cyber threat, you may need to schedule face-to-face meetings with different managers/teams/colleagues.
- For example, a phishing email has been detected and you notice someone has hacked into your customer database and is sending the email to all your customers. The worker who first detected the email contacted the IT department, and you were able to verify it is an email scam. Your IT manager asks you to inform the IT team of the issues urgently.
- You will need to alert the team, summarising the issue and its impact on the business, and discuss the means to control it.

Hands-on presentations

- Another method of communication is a hands-on demonstration or presentation.
- This could include an IT department/security personnel demonstrating to management the effects on a server when damaging attacks are undetected. It may also show the effects on the browser and how this will impact the organisation.

Practice Task 6

Question 1

Which of the following statements is correct? Select all that apply.

○ Cyber aware workplaces rely on feedback from multiple sources.

○ Metrics is a quantifiable measure used to track and assess business processes.

○ Trainers should always explain the technical data gathered.

○ Baselining is a strategy used to analyse computer network performance against future goals.

○ The purpose of cyber security training is to improve cyber awareness and safety.

Question 2

List three ways of communicating information on training results, to managers and colleagues.

Question 3

Which of the following statements related to communication methods is correct? Select all that apply.

○ The way you communicate information is not important when the matter is urgent, such as a cyber attack.

○ Select the communication method that best suits your audience.

○ Always refer to an organisation's communication policy when asked to present information.

○ Written business reports need to follow a set structure.

○ If you feel nervous presenting information to others, you can always email them.

Summary

- Reviewing practices according to organisational policies and procedures
  - Organisational policies and procedures need to be regularly updated in response to current cyber attacks/threats.
  - Procedures for password requirements; email security; handling sensitive data; technology handling; social media policies etc. should be covered in organisational procedures.
  - Risk and threat analysis tools are used by organisations to measure the likelihood and impact of cyber threats.
- Arranging training, updates and maintaining records
- Common topics covered in cyber security training include:
  - identifying and reporting an incident
  - how to detect a phishing email.
- Strategies to assist in structuring cyber awareness training begin with conducting a needs analysis; setting the purpose of training; understanding the audience (identifying the motivation and learning styles of participants); setting learning objectives; setting an agenda and sticking to it; using adult learning techniques; carrying out the simulation activities; evaluating the training exercise.
- Incident reporting procedures, which are required by law – *Privacy Act 1988* (Cth).
- How to use simulation activities to raise cyber awareness, by developing in-house simulations or using free commercial activities available online
- Outcomes of training should be evident in changes and improvements in workplace practices. These need to be measured, starting with a baseline and recording progress.
- Presenting insights to mitigate impacts in workplaces
- Different communication methods based on audience, urgency and organisational policies and procedures.

Learning Checkpoint 2

Support effective cyber security practices at work

Part A

1. List three training activities you could use to train staff to identify phishing scams.

2. Which procedures could be reviewed if an organisation's data was being breached? Select all that apply.

○ Storage and filing procedures

○ Password security

○ Access restrictions

○ Backup systems

○ Application whitelists

3. Explain what the 5E Learning model stands for and how you would use it when conducting training.

4. Which of the following would be contained within an IT acceptable use policy? Select all that apply.

   ○ How to use IT resources professionally and appropriately

   ○ How to operate meeting room tablets

   ○ Rules about sharing passwords

   ○ Examples of inappropriate use

5. How can the likelihood of risks to cyber security be analysed?

Part B

Read the case study and answer the questions that follow.

Case study

You work in a hardware business that has over 50 outlets around Australia. Part of your job role is to track and monitor staff cyber security awareness.

There have been various cyber trainings conducted over the last 12 months, but not very detailed notes were kept. Your manager is frustrated because he thinks the staff and the company are not benefiting from the training provided.

He has asked you to take over the training and to measure the performance of new techniques or strategies to reduce cyber attacks at work.

1. What are two methods you would use to measure the impact of the training on the organisation?

2. What are three ways you could provide updates on the latest cyber attacks in your workplace?

3. Write a text (no more than 50 words) you could send to staff to remind them to check for the latest cyber attack alerts. Your text should include:
   - a greeting
   - short message explaining reason for text
   - link to website
   - salutation.

Topic 3 | Review cyber security awareness in your work area

3A Review latest threats and trends

3B Review outcomes and suggest improvements

3C Communicate review outcomes and improvements

3A Review latest threats and trends

Threat intelligence is the accumulation of knowledge about the latest cyber threats and trends that may harm your organisation.

Threat intelligence can be best used by management and the IT or security departments to make decisions about how to mitigate and avoid harmful events.

Two reputable sources of threat intelligence are shown below.

Australian threat intelligence sources	
ACSC	Monitors cyber threats across the globe 24 hours a day, seven days a week to alert Australians early on what to do.
ACCC Scamwatch	A free service from ACCC to warn the Australian public how to identify, avoid and report scams.

Common threats affecting Australian organisations

Threats to Australian organisations are growing daily; however, there are some common ones to look for.

Many organisations are at risk due to the lack of knowledge, skills or planning to mitigate and respond to certain attacks. Knowledge of some of the common threats is essential.

Some common threats are shown below.

Common threats in Australia	
Malware	Software designed to cause harm to a computing system, operating system, network, device or host via a wide array of methods; can be viruses, trojans, worms, spyware, ransomware and other threats
Ransomware	A type of malware designed to crypto-lock and hold the operating system and its files for ransom unless a payment is paid
Distributed Denial of Service (DDoS)	An attack on the availability of a system where an attacker makes the target's system unavailable for regular use
Phishing	The practice of sending fraudulent emails designed to trick users into divulging personal information such as tax file numbers, bank login details and credit card numbers
Email scams	Fraudulent and deceptive acts using emails as the medium

Practice Task 7

Question 1

List two Australian organisations that source and distribute cyber threat information.

Question 2

Draw a line to match each term cyber threat to its definition.

- Distributed Denial of Service (DDoS)
- Ransomware
- Phishing
- Malware

- The practice of sending fraudulent emails designed to trick users to reveal personal information such as credit card details
- Software designed to cause harm to a computing system, in the forms of installing viruses, trojans, worms, spyware, ransomware and other forms
- A type of malware designed to crypto-lock and hold an operating system and its files for ransom unless a payment is paid
- An attack on a system that makes it unavailable for use

3B Review outcomes and suggest improvements

Reviewing cyber security is essential for improving an organisation's security posture.

Cyber security needs to be understood as a whole-of-business concern and not just a problem for the IT or security department. Therefore, any outcomes of a cyber threat review should be documented, actioned and communicated promptly.

A review of cyber security may:

- identify if any systems and processes need improving
- evaluate incidents before and after, and any lessons learnt
- require updates to cyber security incident response plans based on the lessons learnt, so you can improve your business response.

It is imperative that information is managed and executed by the relevant personnel. Suggested improvements need to be considered by mangers and other personnel. This may include:

- the Chief Executive Officer (CEO), who decides on the what cyber initiatives will be prioritised
- the Board, which advises on and monitors risk management and legal compliance
- the Chief Financial Officer (CFO), who manages resources for cyber initiatives
- the Chief Information Officer (CIO), Chief Information Security Officer (CISO) or Chief Technology Officer (CTO), who make decisions on how to implement suitable technology and initiate security controls.

Decisions need to be made in line with other industry benchmarks, such as the International Standard Organisation (ISO) standards, vendor standards and legislation.

Improvement resources

Industry organisations provide a good resource for all IT security personnel to update their professional knowledge and learn current strategies to mitigate risks.

All IT, security, computing, management and other personnel can improve their knowledge regarding cyber security and threats by staying up to date with the latest risks and belonging to industry organisations.

Some key industry bodies are listed below.

Professional improvement sources	
ACCC Scamwatch (Australian Competition and Consumer Commission)	Scamwatch is a free service to warn the Australian public how to identify, avoid and report scams.
AISA (Australian Information Security Association)	AISA is a not-for-profit organisation and charity focused on education, awareness within the information security sector by building the capacity of professionals in Australia.
AusCERT Australian Computer Emergency Response Team (CERT)	AusCERT is the premier Computer Emergency Response Team (CERT) in Australia and a leading CERT in the Asia/Pacific region. AusCERT operates within a worldwide network of information security experts to provide computer incident prevention, response and mitigation strategies for members and assistance to affected parties in Australia.
CAUDIT (Council of Australasian University Directors of Information Technology)	CAUDIT is an incorporated not-for-profit association owned by the Australasian universities and a number of major Australian research organisations. It supports CIOs and their teams through the provision of a broad range of services, fostering collaboration, leadership and good practice among its members. Services include benchmarking and professional development. Members are represented by the most senior IT person in their organisation – generally the CIO, Chief Digital Officer or Director of IT.

Practice Task 8

Question 1

Draw a line to match the job position to their role in reviewing cyber security outcomes.

» The Board	» Prioritises cyber initiatives taken in an organisation
» Chief Information Security Officer (CISO)	» Manages resources for cyber initiatives
» CEO	» Implements suitable technology and initiates security controls
» Chief Financial Officer (CFO)	» Monitors risk management and legal compliance

Question 2

According to ACCC's Scamwatch website, list three scams invented by cyber criminals during 2020.

Question 3

Research the AISA website and list three professional development activities they offer.

3C Communicate review outcomes and improvements

Communicating review outcomes should be done as soon as possible.

In order for cyber security to be a whole-of-workplace program, everyone needs to be kept informed of review outcomes and improvements made.

Once new cyber threats have been identified and the threat to the business has been assessed, a review of the cyber security strategy/plan should take place, and the outcomes documented, policies and procedures updated, and changes implemented.

It is imperative that the outcome of any review process is communicated as fast as possible to implement mitigation controls and avoid security breaches.

Improving internal policies and procedures

Review of cyber security should lead to improved policies and procedures.

Post-review

After compiling review information, follow the steps below to improve policies and procedures.

1. **Identify the priorities of the organisation.** Do not assume priorities are the same as in the last review, as modern businesses are dynamic and laws change often. Keep in mind that all policies and procedures must reflect current goals.
2. **Identify who will take responsibility.** Decide on the relevant staff responsible for implementing changes.
3. **Gather information.** Collate the information from the review, its implications, legal requirements, new techniques required etc.
4. **Draft policies and procedures.** Write or update policies and procedures.
5. **Present review outcomes and drafted policies and procedures to stakeholders.** With the previous steps in place:
   a) present the current situation or threat
   b) identify possible problems if nothing changes
   c) explain the legal and commercial implications if problems persist
   d) propose solutions in the form of draft policy and procedural improvements.

6. **Finalise, refine, rework policies and procedures.** Once stakeholders have approved changes, finalise new policies and procedures.
7. **Promulgate new policies and procedures to the organisation.** Announce the new policies and procedures and date of ratification.

'No matter how mature your business is regarding information security, you need to continuously improve and adapt your programs to a changing threat landscape. This means embedding awareness of good information security practices into the personal and professional lives of your employees, and staying abreast of developments in the area.' – *Stay Smart Online*

Example

Hackathons

The following is an example of how everyone can get involved by 'hacking' the business.

Staff and management
Internal IT security auditing
BizOps has decided to identify its vulnerabilities company-wide and has invited all departments and personnel to participate in a one-day challenge. It has proposed that all staff find work-arounds, also known as hacks, to current procedures and processes and simply document their workaround steps. BizOps stresses that it is just a challenge, and no one will be penalised if they find security flaws. In fact, BizOps is offering two awards for: ▪ the department/personnel who find the highest number of flaws ▪ the department/personnel who can reveal the highest number of sensitive information leaks. Due to the sensitivity of the challenge, BizOps emphasizes that: *'in the case where personal information can be sourced, it should not reveal the personal information'.* The purpose is to investigate and highlight how security can be comprised, by either insider or external attacks.

Practice Task 9

Question 1

Which of the following statements about reviews and outcomes are correct?
Select all that apply.

○ Reviews of cyber threats often result in updates to policies and procedures.

○ Reviews of cyber threats need to be communicated to staff as soon as possible.

○ Reviews of cyber security should take place regularly.

○ Reviews of cyber threats only relate to IT security personnel.

○ Outcomes of reviews need to be clearly documented.

Question 2

Number each step from 1 to 4 in the order you would present review outcomes.

○ Propose solutions in the form of draft policy and procedural improvements.

○ Present the current situation or threat.

○ Explain the legal and commercial implications if problems persist.

○ Identify possible problems if nothing changes.

Summary

- How to view the latest cyber threats and trends using threat intelligence:
  - use ACSC and ACCC websites and programs to view current threats.
- Common threats affecting Australian organisations include:
  - malware
  - ransomware
  - distributed denial of service
  - phishing
  - email scams.
- Review outcomes and suggested improvements can include:
  - scheduling reviews, documenting outcomes and communicating the outcomes
  - engaging stakeholders in monitoring and maintaining cyber security within an organisation.
- Improvement resources for required personnel include:
  - professional organisations offering online training, webinars, SMS alerts and conferences for people who need to keep their skills current and keep abreast of cyber threats.
- The types of outcomes that need to be communicated include:
  - the current situation or threat to business
  - possible problems if nothing changes
  - legal and commercial implications
  - solutions outlined in update policies and procedures.

Learning Checkpoint 3

Review cyber security awareness in your work area

1. Define ‘threat intelligence’.

2. List four common cyber threats in Australia and how they work.

3. List three professional development opportunities available to keep IT security workers abreast of cyber-attacks and threats.

4. List five services offered by the AusCERT Australian Computer Emergency Response Team (CERT).

5. Research the Australian Cyber security centre's (ACSC) website, and list three cybercrimes detected during COVID-19.