Enterprise Computing Stage 6 (Year 11) – teacher support resource

**Principles of cybersecurity**

# Teacher support resource

**Teacher note:** this resource has been designed to facilitate the ready conversion into a student booklet by removing the answers within the response windows. Teacher notes can be deleted before distributing to students.

Student name:

Class:

Teacher:

Contents

[Teacher support resource 1](#_Toc158973951)

[Unit overview 5](#_Toc158973952)

[Glossary 6](#_Toc158973953)

[NESA glossary keywords 9](#_Toc158973954)

[The design and production process 10](#_Toc158973955)

[Explore security vulnerabilities of social networking to both an individual and an enterprise 11](#_Toc158973956)

[Account access 11](#_Toc158973957)

[Account behaviour 11](#_Toc158973958)

[Hosting platform security 12](#_Toc158973959)

[Identity theft 12](#_Toc158973960)

[Phishing 13](#_Toc158973961)

[Evil twins 13](#_Toc158973962)

[Investigate how an individual can contribute to maintaining the privacy of their own data 17](#_Toc158973963)

[Explain privacy, trust and freedom of information with respect to people, systems and data 23](#_Toc158973964)

[Describe privacy and security principles associated with access, storage and permissions 27](#_Toc158973965)

[Investigate cybercrime threats to an enterprise 32](#_Toc158973966)

[Hacking 32](#_Toc158973967)

[Phishing, including smishing 32](#_Toc158973968)

[Scamming 32](#_Toc158973969)

[Bots and botnets 33](#_Toc158973970)

[Employee action causing a vulnerability 33](#_Toc158973971)

[Describe the attributes of a cybersecurity breach 38](#_Toc158973972)

[Confidentiality of information 38](#_Toc158973973)

[Integrity of information 38](#_Toc158973974)

[Availability of information 38](#_Toc158973975)

[Privacy implications 39](#_Toc158973976)

[Investigate vulnerabilities exploited by the threat actor involved in a breach, such as the impact on various elements 43](#_Toc158973977)

[Assess cyber risk by implementing risk-management strategies using a risk matrix 51](#_Toc158973978)

[Internal and external vulnerabilities 51](#_Toc158973979)

[Threat landscape 52](#_Toc158973980)

[Impact of exposure 52](#_Toc158973981)

[Likelihood of exploitation 52](#_Toc158973982)

[Investigate cyber risk management 59](#_Toc158973983)

[Implementing a cybersecurity strategy with ongoing training 59](#_Toc158973984)

[Identifying and managing vulnerabilities 59](#_Toc158973985)

[Assessing the impact of a breach 60](#_Toc158973986)

[Controlling damage and loss 60](#_Toc158973987)

[Describe privacy and security principles associated with access, storage and permissions used by enterprises to collect and interpret data 62](#_Toc158973988)

[Research hardware and software strategies used to protect data 65](#_Toc158973989)

[Investigate cybercrime threats to an enterprise 71](#_Toc158973990)

[Hacking 71](#_Toc158973991)

[Phishing, including smishing 71](#_Toc158973992)

[Scamming 71](#_Toc158973993)

[Bots and botnets 72](#_Toc158973994)

[Employee action causing a vulnerability 72](#_Toc158973995)

[Research hardware and software strategies used to protect data 74](#_Toc158973996)

[Investigate vulnerabilities exploited by the threat actor involved in a breach, such as the impact on various elements 78](#_Toc158973997)

[Identify laws and legislation associated with cybersecurity 85](#_Toc158973998)

[Explain impacts of cybersecurity breaches on the individual, organisation and society 89](#_Toc158973999)

[Financial loss 90](#_Toc158974000)

[Reputational damage 90](#_Toc158974001)

[Operational disruptions 90](#_Toc158974002)

[Legal and regulatory ramifications 91](#_Toc158974003)

[Explore current and emerging cybercrime threats to an enterprise 95](#_Toc158974004)

[Investigate cybercrime threats to an enterprise 100](#_Toc158974005)

[Implementing a cybersecurity strategy with ongoing training 100](#_Toc158974006)

[Identifying and managing vulnerabilities 100](#_Toc158974007)

[Assessing the impact of a breach 100](#_Toc158974008)

[Controlling damage and loss 101](#_Toc158974009)

[References 103](#_Toc158974010)

# Unit overview

In this unit students will develop a fundamental understanding of Principles of cybersecurity. The lessons and sequences are designed to allow students to investigate the current data and information security strategies of an enterprise, examine real and potential threats to the security of data and information, and recommend strategies to improve current practices.

Scenario-based learning is an active learning technique which offers a potential bridge between these goals, allowing learners to both achieve an understanding of core concepts whilst being asked to apply them to more complex and imprecise problems.

Weeks 1 to 6 see students learn about data and information security and its importance to an enterprise. Students investigate security strategies used by an enterprise to manage the storage, communication and disposal of data and information in their networked environment.

Weeks 7 to 10 see students explore threats to data and information, evaluate methods used by an enterprise to protect data and information, and consider potential consequences. Students apply systems thinking skills when investigating and recommending strategies to reduce threats to data and information, considering legal requirements and ethical issues faced by enterprises.

# Glossary

Many of the following words will gather more meaning to you as you work through this booklet.

Each time you see a new word in bold throughout this workbook you can add its definition in the table below in case you need to refer back later.

|  |  |
| --- | --- |
| Word | Definition |
| Anti-malware | Antimalware is a type of software program created to protect information technology (IT) systems and individual computers from malicious software, or malware. Antimalware programs scan a computer system to prevent, detect and remove malware. |
| Antivirus | Software designed to detect and destroy computer viruses. |
| Back up recovery | Backup and recovery is the process of duplicating data and storing it in a secure place in case of loss or damage, and then restoring that data to a location. |
| Botnets | A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, for example to send spam. |
| Bots | An autonomous program on the internet or another network that can interact with systems or users. |
| Cybercrime | Criminal activities carried out by means of computers or the internet. |
| Cybersecurity strategy | A cybersecurity strategy is an action plan detailing how a business will protect itself from cyber threats. An effective cybersecurity strategy provides a blueprint on what to prioritise in order have a safe and secure cyber environment. |
| Cybersecurity | The protection of information technology elements, including hardware and software, data or network services. |
| Disaster recovery | Disaster recovery is an organisation's plan to protect its IT systems and data from disasters and recover quickly to minimise downtime and losses. |
| Encryption | The process of converting information or data into a code, especially to prevent unauthorised access. |
| Firewall | A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organisation's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public internet. |
| Hacking | The gaining of unauthorised access to data in a system or computer. |
| Identity theft | The fraudulent practice of using another person's name and personal information in order to obtain credit, loans and so on. |
| Multi-factor authentication | Multi-factor Authentication (MFA) is an authentication method that requires the user to provide 2 or more verification factors to gain access to a resource such as an application or online account. |
| Phishing | The fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. |
| Privacy | A state in which one is not observed or disturbed by other people. |
| Risk matrix | A risk matrix is a matrix that is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity. This is a simple mechanism to increase visibility of risks and assist management decision making. |
| Security vulnerabilities | A security vulnerability is a weakness, flaw or error found within a security system that has the potential to be leveraged by a threat actor in order to compromise a secure network. |
| Smishing | The fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers. |
| Threat actor | An individual or group that poses a security threat to an individual or organisation. |
| Threat landscape | The threat landscape is the big picture of potential risks and dangers people may face online. It can include a range of cybersecurity risks (from malware attacks and stolen data to data breaches) that can harm individuals, organisations or enterprises. |

**Teacher note:** for students with an EAL/D background. The glossary can be provided complete so that they have additional time to understand the key terms with bilingual dictionaries. The glossary can be provided to students in their preferred communication mode.

# NESA glossary keywords

NESA keywords can be used in the syllabus and in the Higher School Certificate examination. Familiarisation with these keywords can assist in understanding how to write and respond to questions.

|  |  |
| --- | --- |
| Key term | Definition |
| Assess | Make a judgement of value, quality, outcomes, results or size. |
| Describe | Provide characteristics and features. |
| Explain | Relate cause and effect; make the relationships between things evident; provide why and/or how. |
| Identify  | Recognise and name. |
| Investigate | Plan, inquire into and draw conclusions about. |

[NESA: A Glossary of Key Words](https://educationstandards.nsw.edu.au/wps/portal/nesa/11-12/hsc/hsc-student-guide/glossary-keywords)

**Teacher Note:** explore and research are used in this topic and are not listed.

# The design and production process

Throughout your study of Enterprise Computing, you will learn about design processes and how to apply them. You will explore different types of design processes and learn how to apply them in your design project.

The design and production process:

* involves a sequence of organised steps which provide a solution to design needs and opportunities
* may take a few seconds or minutes, such as when you select what clothes to wear, or may take years as in the case with the design of a motor vehicle
* may involve one person or may involve many people
* may be simple or complex, depending on the task
* involves questioning (or evaluating) throughout the iterative process.

Figure 1 – flowchart of design and production process



# Explore security vulnerabilities of social networking to both an individual and an enterprise

## Account access

Account access is a critical security vulnerability in social networking, posing risks to both individuals and enterprises.

For individuals, weak passwords, password reuse or falling victim to phishing attacks can lead to unauthorised access to their personal profiles, potentially resulting in identity theft, privacy breaches and even financial harm.

Enterprises are also vulnerable, as employees may use company email addresses and passwords for personal social media accounts, potentially exposing sensitive corporate data in the event of a security breach.

Cybercriminals might target employees through social engineering techniques, exploiting their personal information to launch targeted attacks against the organisation, such as spear-phishing, with the aim of compromising business networks and stealing valuable data. Thus, robust security practices, including strong, unique passwords, two-factor authentication, and employee training, are crucial to mitigate these account access risks.

## Account behaviour

Account behaviour represents a significant security vulnerability in the context of social networking, affecting both individuals and enterprises.

For individuals, sharing personal information, location and daily activities on social media can expose them to threats like stalking, cyberbullying or physical harm. Moreover, oversharing can inadvertently reveal sensitive details that attackers can exploit for phishing and identity theft.

Enterprises, on the other hand, face risks related to employee behaviour on social media, as inappropriate or careless posts can damage the organisation's reputation, leak sensitive information or lead to legal repercussions. Additionally, social engineering attacks often leverage information gathered from social media to manipulate individuals within an enterprise, making account behaviour an area of concern for both personal and corporate security. It is crucial for users to be cautious about what they share and for organisations to establish clear social media usage policies and provide education and training to mitigate these risks.

## Hosting platform security

Hosting platform security is a critical aspect of social networking vulnerabilities that impacts both individuals and enterprises.

For individuals, when using social media, they rely on the security measures implemented by the hosting platforms to protect their personal data and privacy. Vulnerabilities in the platform's security, such as data breaches or account hacks, can expose users' personal information and sensitive content to threat actors, leading to identity theft, scams or harassment.

Enterprises, on the other hand, may leverage social networking platforms for marketing and customer engagement, which makes them dependent on the platform's security for safeguarding their brand image and customer interactions. If a hosting platform suffers a security breach or outage, it can disrupt business operations, damage reputation and compromise customer data.

Therefore, both individuals and enterprises must be aware of the security measures employed by hosting platforms and take additional steps, like enabling two-factor authentication and using strong, unique passwords to enhance their own security while using social networks.

## Identity theft

Identity theft is a significant security vulnerability in the realm of social networking, posing risks to both individuals and enterprises.

For individuals, the personal information shared on social media, such as full names and birth dates, can be exploited by threat actors to impersonate or steal their identities, potentially leading to financial fraud, reputation damage or unauthorised access to accounts.

In an enterprise context, employees' social media profiles may inadvertently provide cybercriminals with valuable information to launch targeted attacks against the organisation, including spear-phishing campaigns. Moreover, if an enterprise's social media presence is compromised, it can damage its reputation, mislead customers and facilitate further cyber attacks. Therefore, vigilant privacy settings and cautious sharing of personal information are essential for individuals, while employee awareness and stringent social media policies are critical for enterprises to mitigate the risks associated with identity theft.

## Phishing

Phishing represents a pervasive security vulnerability affecting both individuals and enterprises on social networking platforms.

For individuals, phishing attacks often involve deceptive messages or links appearing to be from trusted sources, tricking users into revealing their personal information, login credentials or financial data. This can lead to identity theft, financial loss or unauthorised account access.

Enterprises are susceptible to phishing as well, with cybercriminals targeting employees through social media to gain access to corporate networks or sensitive data. Employees may inadvertently click on malicious links or provide confidential information, potentially leading to data breaches, compromised networks or the spread of malware within the organisation. Vigilance, employee training and robust email filtering systems are essential to counter these social networking-based phishing threats for both individuals and enterprises.

## Evil twins

Evil twins are a security vulnerability that can impact both individuals and enterprises on social networking platforms. In this context, evil twins refer to fake or malicious accounts that impersonate a legitimate person or entity.

For individuals, encountering an evil twin can result in deception, as they may interact with a fraudulent account believing it to be a friend, family member or reputable organisation, potentially sharing personal information or falling victim to scams.

Enterprises can face threats from evil twins as well, as cybercriminals may create fake corporate profiles, impersonating the organisation and disseminating false information, damaging the brand's reputation, or engaging in social engineering attacks against employees or customers. Recognising and reporting these fraudulent accounts is crucial for both individuals and enterprises to mitigate the risks associated with evil twins on social networking platforms.

Students individually interact with and explore the [CyberFirst Navigators interactive video](https://www.ncsc.gov.uk/training/cyberfirst/packages/en/index.html).

**Activity 1:** social networking scenario (A)

Record decisions made during the interactive video and any additional relevant observations of actions by the characters.

|  |
| --- |
| **Sample answers:*** Olivia puts off (procrastinates) tasks requiring prompt action.
* Olivia ignores prompts to install important software updates.
* Luca trusted the online ad and tried purchasing cheap headphones through the link provided.
* Raheem has his location sharing set to on.
* Olivia trusted the private message sent from Luca’s account, thinking it was from Luca but not realising it was from cybercriminals.
* Raheem receives a similar private message from Luca’s account but appears to be aware of similar phishing scams, does not respond to it and later reports it.
* (depending on path selected) Olivia ignores prompt to set up two-step verification.
* Olivia does not check emails linked to online accounts regularly.
 |

**Activity 2:** risks and consequences

Describe the risks taken by characters and the consequences.

|  |
| --- |
| **Sample answer:**Olivia ignores prompts to install important software updates. Software updates provide security fixes to known vulnerabilities to prevent hackers (cybercriminals/threat actors) from exploiting the user.Olivia uses the same password for all online accounts. If one account is compromised (or breached) then cybercriminals will try the same password on associated accounts hoping to gain access to other online accounts and/or devices.Olivia does not appear to have changed her password for some time. If any enterprise that Olivia has a user account with has a data breach, then the password is potentially compromised and should be changed.Luca uses a password which is reasonably easy to guess based on known personal information.Luca was a victim of a phishing scam (on social media) which allowed cybercriminals to access his accounts and subsequently change his passwords and send similar phishing messages (with similar phishing links) to his contacts but appearing to be from him.Olivia ignores prompt to set up 2-step verification. The risk of not using 2-step verification (or MFA) is that a hacker only needs one form of authentication (or one piece of evidence to verify identity). |

**Activity 3:** What is social engineering?

|  |
| --- |
| **Sample answer:**A range of tactics to manipulate, influence or deceive a victim in order to gain control over a computer system or to steal personal and financial information. |

Consider different ways that a hacker might use obtained information, for example:

* email account
* social media account details
* personal data.

**Activity 4:** identify which definitions are types of social engineering.

|  |
| --- |
| **Sample answer:*** phishing
* blagging
* pharming
* shoulder surfing
* spear-phishing
* smishing
 |

**Activity 5:** identify which examples of social engineering were experienced by characters in the film.

|  |
| --- |
| **Sample answer:*** phishing/smishing
* spear-phishing.
 |

# Investigate how an individual can contribute to maintaining the privacy of their own data

**Activity 6:** investigate how an individual can contribute to maintaining the [privacy of their own data](https://www.oaic.gov.au/privacy/your-privacy-rights/ways-to-protect-your-privacy/tips-to-protect-your-privacy).

Identify the 10 concepts in the article.

|  |
| --- |
| **Sample answer:**1. Know your rights.
2. Read privacy policies and collection notices.
3. Always ask why, how and who.
4. Check your credit report.
5. Protect yourself online.
6. Be aware of your mobile security.
7. Use security software.
8. Be careful what you share on social media.
9. Don’t leave your personal information lying around.
10. Beware of scams.
 |

**Activity 7:** cyber aware behaviours

Six behaviours for safe online behaviour are as follows.

1. Use a strong and different password for email accounts.
2. Create strong passwords for all accounts.
3. Turn on Multi-Factor Authentication (MFA or 2FA).
4. Use a password manager.
5. Back up data.
6. Update devices.

Using the 6 behaviours, explain how these behaviours could have kept the characters’ personal information safe?

|  |
| --- |
| **Sample answers:**Luca would benefit from creating a strong and different password for email accounts.Olivia would benefit from updating devices, turning on Multi-Factor Authentication and using a password manager. |

**Activity 8:** film scenes matching task

For the 6 scenes, identify ‘[Cyber Aware behaviours’](https://www.ncsc.gov.uk/static-assets/documents/cyberfirst-navigators/CyberFirst-Navigators-Lesson-2-resources.pdf) that would have helped the characters in each scene.

|  |  |
| --- | --- |
| Scene | Identify behaviour |
| **Scene 1** | 6. Update devices. |
| **Scene 2** | 2. Create strong passwords for all accounts.4. Use a password manager. |
| **Scene 3** | 3. Turn on Multi-Factor Authentication (MFA or 2FA).**Note:** in the UK the term used is 2-step verification (2SV). |
| **Scene 4** | 5. Back up data. |
| **Scene 5** | Checking emails regularly for suspicious activity on connected accounts. |
| **Scene 6** | 1. Use a strong and different password for email accounts.4. Use a password manager. |

**Activity 9:** decide what actions can be taken to improve the security of the characters’ data.

|  |
| --- |
| **Sample answers:**Actions might include any of the 6 behaviours with some justification. |

**Activity 10:** discuss why ‘LiverpoolFC04’ is not a good password.

|  |
| --- |
| **Sample answer:**Luca’s password is very simple, made up of information people know about him or information he has freely posted online. LiverpoolFC is apparently the football club he supports and ‘04’ is the year he was born, which would make it easy to guess.The password is 13 characters long and if it consisted of random characters it might be more difficult to guess or crack. A longer password containing more random characters or even random words would be better. |

**Activity 11:** describe how passwords are discovered.

|  |
| --- |
| **Sample answers:**They can be stolen, guessed or brute-forced.People are inclined to be lazy and form bad habits using common (bad) passwords (and worse, reusing them) and storing them where other people may find them.Known compromised passwords are collected and posted online (sometimes via the dark web) and word lists containing compromised passwords and dictionary terms are compiled for use in password cracking tools. |

****As a class watch [Diving into hash algorithms](https://www.linkedin.com/learning/learning-cryptography-and-network-security-2/challenge-password-strength-tests) (1:09) and examine the [Hive Systems Password Table](https://www.hivesystems.io/blog/are-your-passwords-in-the-green).

Demonstrate how to check if an email or a password has previously been exposed in known data breaches at [haveibeenpwned](https://haveibeenpwned.com/).

Discuss elements of human behaviour which influence bad habits in password creation and use, for example:

* using common passwords
* using patterns
* using numbers and special characters only at the end
* using character substitutions
* using the same password on multiple sites.

****Examine [strategies](https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd) to generate a [strong password or passphrase](https://www.avg.com/en/signal/how-to-create-a-strong-password-that-you-wont-forget), for example, [Three random words](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words). Apply this knowledge and use these strategies to generate a strong password for one of your accounts.

**Activity 12:** outline new strategies and technologies being developed to replace passwords.

|  |
| --- |
| **Sample answer:**Passkeys are built on the WebAuthentication (or "WebAuthn") standard, which uses public key cryptography. During the account registration process, the operating system creates a unique cryptographic key pair to associate with an account for that app or website. These keys are generated by the device, securely and uniquely, for every account. The passkey is stored on your phone.A cryptographic private key is stored on the device, and the corresponding public key uploaded to a server, for example, providers like Google, Apple, Microsoft, Paypal or Ebay. The server never learns what the private key is.Biometrics – using your unique fingerprint, iris or face to verify your identity. |

As a class, discuss how important strong passwords are.

**Activity 13:** identify the cause(s) of the breach(es) in scenario (A) and categorise this as either a technical error or human error.

|  |
| --- |
| **Sample answer:**Luca had a weak password and also fell victim to credential harvesting (or possibly phishing) by clicking on a link on social media. (human error)Olivia did not apply software updates as required; she did not use different passwords for different accounts. She trusted a message she thought came from Luca. (human error)(depending on the path selected) Olivia did not set up MFA which could have mitigated the phishing risk. (human error) |

**Activity 14:** summarise key aspects of the incident in scenario (A), including:

* risks
* password hygiene
* indicators of compromise.

|  |  |
| --- | --- |
| Key aspects | Summary of key aspects |
| **Risks** | * Olivia trusted a message she thought came from Luca.
 |
| **Password hygiene** | * Luca had a weak password and fell victim to credential harvesting.
* Olivia did not set up MFA which could have mitigated the risk of someone stealing her password.
* Olivia did not use different passwords for different accounts.
 |
| **Indicators of compromise** | * Luca could not get into his account.
* Raheem received messages from Luca’s account after he knew Luca couldn’t access it.
* Olivia could not get into her email account.
 |

**Activity 15:** explain security vulnerabilities of social networking to individuals as highlighted in the scenario video. Including:

* account access
* account behaviour
* hosting platform security
* identity theft
* phishing.

|  |
| --- |
| **Sample answer:**Social networking platforms can give attackers a platform to impersonate trusted people. If a friend’s account is compromised and you are unaware, you may still trust messages, requests or links within messages on the assumption they are from a friend or trusted source.Social networking platforms make it very easy to share and pass on just about anything – and that includes malware. Additionally, the same type of human error that causes people to click on links sent to them in emails is exponentially greater on social media platforms because people are more likely to consider themselves among friends.Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you may become. Even when using high-security settings, friends or websites may inadvertently leak your information. Information on social networking/media platforms could give hints to your frequently used passwords.Scammers use information and photos easily found online to create fake X, Facebook, Instagram and LinkedIn accounts and then use these fake social media profiles to scam others out of money or to tarnish your firm’s reputation.Social networking phishing uses platforms like Facebook or X to steal personal data or gain control of a person’s social media account. An example is a post that offers free vouchers and giveaways by clicking on a link that goes to a malicious website.Vulnerable third-party apps or plugins. |

# Explain privacy, trust and freedom of information with respect to people, systems and data

Privacy, trust and freedom of information are interconnected concepts that pertain to the rights and responsibilities associated with the protection and management of people, systems and data. Let's explore each concept in more detail.

**Privacy**

Privacy refers to an individual's right to control their personal information and how it is collected, used, stored and shared. It encompasses the protection of sensitive data from unauthorised access and it is essential for maintaining personal autonomy and dignity.

|  |  |  |
| --- | --- | --- |
| People | Systems | Data |
| Individuals have the right to keep their personal information private, which includes aspects like personal identifiers, health records, financial data and communication. | Organisations (enterprises) that manage systems which store personal information are required by law to implement practices/processes that ensure the privacy of individuals' personal information. | Protecting data privacy requires safeguarding sensitive information through encryption, access controls and consent-based data sharing practices. |

**Trust**

Trust is the foundation of any relationship, especially in the digital realm. It involves the reliance on the integrity, security, and ethical behaviour of individuals, organisations and systems. Trust is essential for fostering cooperation, collaboration, and information exchange, as well as ensuring the safe handling of personal data.

|  |  |  |
| --- | --- | --- |
| People | Systems | Data |
| Trust among individuals is built on honesty, transparency and ethical conduct. Respecting privacy and maintaining promises are key aspects of building trust. | Trust in systems involves ensuring their reliability, security and protection against data breaches.Users should have confidence that their data is handled responsibly. | Trust in data management involves accurate reporting, data integrity and adherence to privacy regulations.Users should trust that their data is not manipulated or misused. |

**Freedom of information**

Freedom of information refers to the right to access information held by public bodies and organisations. It ensures transparency and accountability while allowing individuals to make informed decisions. Balancing freedom of information with privacy considerations is essential to strike a fair and ethical balance.

|  |  |  |
| --- | --- | --- |
| People | Systems | Data |
| Individuals have the right to access information that pertains to them, ensuring accuracy and control over their personal data. | Organisations must provide access to relevant information for their users, while also protecting sensitive data from unauthorised access. | Ensuring data transparency means providing individuals with the ability to access, correct and delete their personal data as required by privacy regulations. |

**Activity 16:** activate prior knowledge about data and information using a [KWHL chart](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Browser?cache_id=94866).

As a class watch [Data to go](https://www.youtube.com/watch?v=sq-0tjv4_BA) [(1:32)](https://www.youtube.com/watch?v=sq-0tjv4_BA) to introduce the concepts of valuing and protecting data.

**Activity 17:** [brainstorm](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Browser?cache_id=ee9ac) ‘How private is your personal information?’

****As a class watch [What Is Privacy? (3:11)](https://www.youtube.com/watch?v=zsboDBMq6vo) to promote thinking around types of personal information and where it is generated (or provided), stored and accessed by others.

**Activity 18:** identify attributes of their personal data that could be of value to someone else and rank the relative value of these attributes, for example:

* contact details
* health information
* playlist history.

|  |
| --- |
| **Sample answer:**Online shopping history including the store you shop at, exchanging messages on social media, google searches and location. Including profile, political interests, contacts, health, financial data, psychometrics, email, tagged photos, ID and habits. |

Determine what is a fair price for someone’s personal data.

|  |
| --- |
| **Sample answer:**Determining a fair price for personal data is a complex matter involving ethical, legal and economic considerations. Different types of data have varying levels of sensitivity. The more sensitive the data, the higher the price should be. The purpose of data use needs to be considered. Is it for research or marketing? If the data is being used for research that benefits society, the fair price may be different compared to data used for targeted advertising.After considering these points students could consider estimating actual dollar values for comparison against published values of similar data. |

As a class view several sources on the monetised value of personal data which demonstrate some variance in value.

* [Data Calculator](https://calc.datum.org/)
* [How Much is Your Data Worth? The Complete Breakdown for 2024](https://www.invisibly.com/learn-blog/how-much-is-data-worth/)
* [How much is your data worth to tech companies?](https://theconversation.com/how-much-is-your-data-worth-to-tech-companies-lawmakers-want-to-tell-you-but-its-not-that-easy-to-calculate-119716)
* [What your data is actually worth](https://www.datapods.app/blogs/what-your-data-is-actually-worth)

**Activity 19:** discuss ‘How do we put a price on our privacy and should we value it more than companies or cybercriminals?’

|  |
| --- |
| **Sample answer:**The intention of this question is to elicit thinking and responses around the price of privacy. It could be delivered as a class debate. |

# Describe privacy and security principles associated with access, storage and permissions

**Activity 20:** define the following terms.

Confidentiality

|  |
| --- |
| **Sample answer:**Confidentiality is the principle of ensuring that sensitive information is not disclosed to unauthorised individuals or entities, preserving its secrecy and restricting access only to authorised parties. |

Disclosure

|  |
| --- |
| **Sample answer:**Disclosure refers to the act of revealing or making information known, often in the context of sharing details that were previously confidential or private. |

Privacy

|  |
| --- |
| **Sample answer:**Privacy is the right of individuals to control and safeguard their personal information, preventing its unauthorised access, use or disclosure by others. |

Public information

|  |
| --- |
| **Sample answer:**Public information refers to data, facts or knowledge that is freely available and accessible to the general public without restrictions on its dissemination or use. |

Personal information

|  |
| --- |
| **Sample answer:**Personal information is data that relates to an identifiable individual, including details such as name, contact information and other specifics that can be used to distinguish or trace an individual's identity. |

Personally Identifiable Information (PII)

|  |
| --- |
| **Sample answer:**PII is any information that can be used to distinguish or trace an individual's identity, such as names or biometric data, often requiring protection due to its potential privacy implications. |

Trust

|  |
| --- |
| **Sample answer:**Trust is the reliance or confidence in the integrity, reliability and ethical conduct of individuals, organisations or systems, forming the basis for positive expectations and cooperation. |

**Activity 21:** identify who is responsible for maintaining privacy and confidentiality.

|  |
| --- |
| **Sample answer:**The responsibility for maintaining privacy and confidentiality typically falls on both individuals and organisations. Individuals are responsible for safeguarding their own personal information, such as using secure passwords and being cautious about sharing sensitive details.Organisations, especially those handling personal or sensitive data, have a duty to implement robust security measures, establish privacy policies, and comply with relevant regulations to ensure the confidentiality and protection of the information they handle.Additionally, regulatory bodies or government entities may set and enforce standards to promote privacy and confidentiality in specific sectors. |

**Activity 22:** discuss ‘[What are some reasons to keep your data private?](https://www.reputationdefender.com/blog/privacy/top-ten-reasons-keep-your-personal-information-private)’

|  |
| --- |
| **Sample answers:*** prevent identity theft
* protect your financial information
* avoid being robbed
* protect your employability
* maintain your business’s reputation
* protect your freedom of thought
* gain admission to the university of your choice
* keep your insurance
* defend yourself in legal proceedings
* protect yourself from threats that don’t exist yet.
 |

**Activity 23:** evaluate the consequences of a violation of privacy, confidentiality and trust.

|  |
| --- |
| **Sample answer:** Violations of privacy, confidentiality and trust can have profound and far-reaching consequences impacting individuals, organisations and society as a whole.Students may be prompted to consider the consequences of each and how they erode trust throughout society. They may consider the degree to which our post-truth world is a product of these consequences. |

**Activity 24:** define data breach and provide some examples for the following incidents:

Data breach

|  |
| --- |
| **Sample answer:**A data breach is an incident in which unauthorised individuals gain access to sensitive and confidential information, potentially leading to its exposure, theft or misuse, often resulting in harm to individuals or organisations. |

Neopets data breach

|  |
| --- |
| **Sample answer:**The Neopets data breach refers to a security incident where unauthorised individuals gained access to user account information on the popular virtual pet website Neopets, potentially compromising user credentials and personal data. |

Optus data breach

|  |
| --- |
| **Sample answer:** The Optus data breach was a cyber attack that exposed the personal information of up to 10 million customers including names, phone numbers, email addresses and in some cases, home addresses, drivers' licenses and passport numbers.The breach occurred through an unprotected and publicly exposed Application Programming Interface (API) that did not require user authentication. The attackers demanded a ransom of US$1 million in cryptocurrency but later withdrew it and claimed to have deleted the data.A 19-year-old man was arrested for threatening some of the affected customers with financial crimes. The government and Optus advised customers to be vigilant of scams and identity theft. Optus was responsible for the digital equivalent of ‘leaving the window open’. |

Medibank data breach

|  |
| --- |
| **Sample answer:** Millions of Medibank customers may have had their information stolen, with the company revealing hackers accessed the personal data of all customers across its Medibank, ahm Health Insurance and OSHC brands.The data included first names and surnames, addresses, dates of birth, Medicare numbers, policy numbers, phone numbers, claims made to the insurer, where customers received medical services and the codes relating to their diagnosis and procedures.A single compromised password was enough to access Medibank’s customer data. |

****As a class read [the most detailed portrait yet of data breaches in Australia](https://www.abc.net.au/news/2023-03-28/detailed-portrait-data-breaches-oaic-disclosures/102131586), noting the numerical data provided in the story.

**Activity 25:** outline the issue presented on details of reported breaches in the media compared to breach data provided by the Office of the Australian Information Commissioner (OAIC) (as disclosed by affected organisations).

|  |
| --- |
| **Sample answer:**Multiple significant breaches remain unreported with the possibility of many more. The OAIC’s disclosure log is not a complete record of the breaches affecting Australians.This is partly because to be eligible for disclosure under the *Privacy Act 1988*, a data breach has to put the affected individuals ‘at likely risk of serious harm’ and the companies that have been breached decide on what that risk is. |

**Activity 26:** describe possible consequences of a data breach.

|  |
| --- |
| **Sample answer:**A massive erosion of trust. Students could apply a 5 Whys analysis to this initial consequence and consider why that is important. |

# Investigate cybercrime threats to an enterprise

Effective cybersecurity strategies to counter threats include employee training and awareness programs, the implementation of strong access controls and monitoring systems, patch management to address vulnerabilities and incident response plans to handle security breaches. Regular security assessments and audits are also essential for identifying and mitigating risks in an enterprise's digital environment.

## Hacking

**Threat:** hacking involves unauthorised access to computer systems, networks, or devices to steal, alter or disrupt data. Attackers use various techniques, including exploiting vulnerabilities, password cracking and SQL injection.

**Impact:** hacking can lead to data breaches, financial losses, service disruptions and reputational damage. Sensitive information, trade secrets and customer data are often targeted.

## Phishing, including smishing

**Threat:** phishing is a deceptive technique in which attackers impersonate trustworthy entities through email or messaging to trick individuals into revealing sensitive information or clicking on malicious links. Smishing is a similar tactic but carried out via SMS.

**Impact:** phishing and smishing attacks can result in data breaches, identity theft, financial fraud and malware infections. They often exploit human vulnerabilities, making employee awareness and training essential.

## Scamming

**Threat:** scams involve fraudulent schemes and social engineering tactics to deceive individuals or employees into making financial transactions, providing personal information or taking harmful actions.

**Impact:** scams can lead to financial losses, the compromise of personal or business information and damage to an organisation's reputation. Common scams include investment fraud, lottery scams and tech support scams.

## Bots and botnets

**Threat:** bots are automated programs that can perform tasks on the internet. Botnets are networks of compromised devices controlled by an attacker, often used for malicious purposes such as Distributed Denial of Service (DDoS) attacks, spam or credential stuffing.

**Impact:** botnets can disrupt services, steal sensitive data and propagate malware. Organisations may find their networks overwhelmed by DDoS attacks, affecting operational continuity.

## Employee action causing a vulnerability

**Threat:** employees can inadvertently introduce vulnerabilities by falling victim to phishing attacks, misconfiguring systems or violating security policies. Insider threats also pose a risk.

**Impact:** employee actions can lead to data breaches, unauthorised access and operational disruptions. Insider threats can be particularly challenging to detect and mitigate, as they involve trusted individuals with access to sensitive information.

**Activity 27:** define and compare the terms below.

Targeted cyber attack

|  |
| --- |
| **Sample answer:**A targeted cyber attack, also known as an advanced persistent threat (APT), is a sophisticated and focused assault in which adversaries use advanced techniques to compromise specific individuals, organisations or systems for the purpose of unauthorised access, data theft or espionage. |

Un-targeted cyber attack

|  |
| --- |
| **Sample answer:**An un-targeted cyber attack refers to a broad and indiscriminate assault on computer systems, networks or individuals. Typically using automated methods or malware without specifically selecting a particular target and often seeking widespread exploitation rather than a tailored approach. |

Cybercrime

|  |
| --- |
| **Sample answer:**Cybercrime refers to criminal activities conducted using computer networks, digital technologies or the internet, encompassing a range of illicit actions such as hacking, identity theft, fraud and the distribution of malicious software. |

Cybersecurity breach

|  |
| --- |
| **Sample answer:**A cybersecurity breach is the unauthorised access, disclosure or compromise of sensitive information, computer systems or networks, often resulting in potential harm, data loss or exploitation by malicious actors. |

Cybersecurity incident

|  |
| --- |
| **Sample answer:**A cybersecurity incident is an event that compromises the confidentiality, integrity or availability of information systems, networks or data, requiring investigation and potential remediation to mitigate the impact of the security breach. |

Cyber threat

|  |
| --- |
| **Sample answer:**A cyber threat is a potential danger or malicious activity in the digital realm, ranging from vulnerabilities and exploits to sophisticated attacks, with the intent to compromise the security of computer systems, networks or data. |

Exploit

|  |
| --- |
| **Sample answer:**An exploit is a piece of software or a sequence of commands designed to take advantage of vulnerabilities or weaknesses in computer systems, applications or networks to gain unauthorised access or perform malicious actions. |

Vulnerability

|  |
| --- |
| **Sample answer:**A vulnerability is a weakness or flaw in a computer system, network or application that could be exploited by a threat actor, potentially leading to unauthorised access, data breaches or other security compromises. |

**Activity 28:** outline the goals of protecting information.

|  |
| --- |
| **Sample answer:*** Confidentiality – protecting data from unauthorised disclosure.
* Integrity – protecting data from being altered without authorisation.
* Availability – information and systems remain available to authorised users when needed.
 |

**Activity 29:** using a [recent cyber breach](https://www.webberinsurance.com.au/data-breaches-list) as an example, describe a cybersecurity breach in terms of a compromise of:

* confidentiality of information
* integrity of information
* availability of information
* privacy implications.

|  |
| --- |
| **Sample answer:**The [Webber Insurance](https://www.webberinsurance.com.au/data-breaches-list) website lists major cyber breaches in Australia since 2018. Scanning the annual lists for ‘leak’, ‘leaking’, ‘exposes’ or ‘exposed’ will identify examples where there has been compromised confidentiality and privacy implications.Scanning the annual lists for ‘ransomware’, ‘locked’ or ‘outage’ will identify examples where availability of data or systems has been compromised (or attacked). Examples of ransomware attacks where data is encrypted would also be examples of compromised integrity.**Note:** many articles in the list are freely available but some articles may be behind a paywall.The [IT Security Guru](https://www.itsecurityguru.org/2016/11/29/2017-year-data-integrity-breach/) website lists published data integrity breaches including:2008 – Hackers infiltrate the Brazilian governments systems and inflate the logging quotas to disrupt logging industry.2010 – Hackers use the Stuxnet Worm to make minor changes in Iran’s nuclear power programme in an attempt to destroy it.2013 – A Syrian group hacked into the Associated Press’ Twitter account and tweeted that President Obama had been injured in explosions at the White House – the single tweet caused a 147-point drop in the Dow.2015 – JP Morgan Chase was breached with subsequent attempts at market manipulation.2016 – Both the World Anti-Doping Agency and Democratic National Committee are breached with hackers manipulating their data to embarrass the organisations.Searching for ‘data integrity breach’ will find other recent examples. |

**Activity 30:** research activity

**Teacher note:** as a class identify common cyber attacks and cybercrime threats, for example:

Malware, phishing, spoofing, identity-based attacks, code injection, supply chain attacks, insider threats, malicious, negligent and compromised.

Assign cyber threats or attacks to students to research during the unit for later class discussion in various scenario exercises.

You will be assigned a common cyber attack or cybercrime threat. For the assigned threat or attack, begin research and describe the vulnerability that enables the attack to proceed and strategies to mitigate risk(s) and prevent a data breach.

|  |
| --- |
| **Sample answer:** |

****As a class watch [Hacked Medical Devices: The Most Dangerous Examples (4:01)](https://www.youtube.com/watch?v=m49OreAs1WY).

Discuss another dimension of the impact of cyber attacks beyond data breaches.

# Describe the attributes of a cybersecurity breach

## Confidentiality of information

The confidentiality of information is one of the critical attributes of a cybersecurity breach. When a breach occurs, it often results in the unauthorised access, exposure or theft of sensitive and confidential data. This can encompass a wide range of information, including personal records, financial data, trade secrets, intellectual property and more. Breaches compromise the confidentiality of this data by making it accessible to threat actors, who can use it for malicious purposes, such as identity theft, fraud or corporate espionage. Protecting the confidentiality of information is a fundamental aspect of cybersecurity, and breaches that undermine this attribute can lead to severe consequences, including legal and regulatory issues, financial losses and reputational damage for individuals and organisations.

## Integrity of information

The integrity of information is another vital attribute affected by a cybersecurity breach. Breaches can compromise the accuracy and reliability of data by introducing unauthorised changes, alterations or deletions. This can lead to significant distortions in the quality of information, potentially resulting in incorrect decisions or actions. In a cybersecurity breach, integrity is often compromised through the insertion of malware, unauthorised edits to databases or data manipulation. Ensuring data integrity is essential in maintaining trust in digital systems, and breaches that undermine this attribute can have far-reaching consequences, especially in sectors where data accuracy is crucial, such as finance, healthcare and critical infrastructure.

## Availability of information

The availability of information is a key attribute affected by a cybersecurity breach. Breaches can disrupt the accessibility of data and services by causing downtime, system crashes, or denial-of-service attacks, rendering information or resources inaccessible to authorised users. This lack of availability can lead to business interruptions, financial losses and inconvenience to individuals and organisations alike. Cyber attacks that focus on compromising the availability of information can range from distributed denial of service (DDoS) attacks that overwhelm servers to ransomware incidents that encrypt data and demand a ransom for its release. Ensuring the availability of critical data and systems is a fundamental aspect of cybersecurity, and breaches that undermine this attribute can be highly disruptive and damaging.

## Privacy implications

Privacy implications are a significant attribute of a cybersecurity breach. When a breach occurs, it often leads to the unauthorised exposure of personal or sensitive information, resulting in a violation of individuals' privacy. Breached data can include personal identifiers, financial records, healthcare information and more, and its exposure can lead to identity theft, fraud or other malicious activities that infringe on an individual's right to privacy. Organisations that suffer breaches may also inadvertently disclose their customers' private data, leading to legal consequences, regulatory fines and damage to their reputation. Safeguarding privacy is a fundamental aspect of cybersecurity, and breaches that impact this attribute can have severe consequences for both individuals and businesses in terms of legal liabilities and loss of trust.

**Activity 31:** define and compare these related terms.

Adversary

|  |
| --- |
| **Sample answer:**An adversary typically refers to a threat actor or malicious entity seeking to exploit vulnerabilities and compromise the security of computer systems or networks. |

Cybercriminal

|  |
| --- |
| **Sample answer:**A cybercriminal is an individual or group that engages in illegal activities and conducts malicious actions using computer systems, networks or digital technologies with the intent to compromise security, commit fraud, steal sensitive information or engage in other illicit activities in the cyberspace. |

Threat actor

|  |
| --- |
| **Sample answer:**A threat actor refers to an individual, group, organisation or entity that carries out activities, whether intentionally or unintentionally, that pose a potential risk or threat to the security of computer systems, networks or information. Threat actors can include hackers, cybercriminals, hacktivists, nation-states or insiders with malicious intent. |

Adversarial mindset

|  |
| --- |
| **Sample answer:**An adversarial mindset refers to a strategic approach that involves thinking like a potential adversary or opponent to proactively identify and address vulnerabilities, threats and weaknesses in a system or organisation. This mindset is crucial as it allows security professionals to anticipate and understand the tactics, techniques and procedures that threat actors might employ, enabling the development of effective defence strategies and measures to enhance overall security posture. |

**Activity 32:** password data breach scenario (B)

As a class read the following text:

Yesterday, a teacher notified the IT helpdesk that some course grades have been changed in the system. All the students in one course had their grades changed to reflect much better scores than they actually earned.

Initial investigation shows that someone logged on using the teacher’s login information and manually changed the grades.

Additionally, the logs indicate that several reports were also downloaded from other systems, including some that contained private information (like private contact details) about the school’s employees.

In groups, define the problem and identify relevant facts from the provided scenario text.

In an iterative process, combine and apply the additional information below to the scenario body of knowledge.

Logs indicate that the login occurred from the school’s wi-fi network after school hours.

Reports have surfaced about students offering to change additional grades for money. No names have yet been revealed.

Use critical thinking to evaluate the situation and consider potential risks.

Apply an adversarial mindset to imagine actions that would align with indicators of compromise.

Prepare a group response to share with the class.

Share group responses and collaborate to build a better understanding of this scenario event and work towards an agreed response to the question.

**Activity 33:** phishing data breach scenario (C)

As a class read the following text:

An employee in your organisation received an urgent email purportedly from a high-ranking executive, requesting them to share their Office 365 login credentials due to a supposed IT emergency. Believing the message was legitimate, the employee provided their credentials.

Assign required groups and roles.

In groups, define the problem and identify relevant facts from the provided scenario text.

In an iterative process, combine and apply additional information below to the scenario body of knowledge.

The attacker gained access to the employee's Office 365 account and began sending phishing emails from their account to other employees, further compromising sensitive data. What would you do to respond?

Add the following additional information.

The organisation has policies in place to verify the authenticity of urgent requests for sensitive information.

Use critical thinking to evaluate the situation and consider potential risks.

What actions should be taken immediately upon discovering the social engineering attack?

Apply an adversarial mindset to imagine actions that would align with indicators of compromise. Use these questions to help understand the situation and prepare a group response to share with the class.

**Discussion questions:**

How can the enterprise determine the scope and impact of the attack?

How can the enterprise identify the extent of compromised accounts and the data accessed by the attacker?

What steps should be taken to recover control of compromised accounts and mitigate further damage?

What additional layers of authentication and authorisation be implemented to prevent unauthorised access to critical systems?

How can the enterprise improve internal security awareness and training to prevent future social engineering attacks?

Share group responses and collaborate to build a better understanding of this scenario event and work towards an agreed response to the question.

# Investigate vulnerabilities exploited by the threat actor involved in a breach, such as the impact on various elements

This table provides an overview of common vulnerabilities exploited in breaches and the potential impacts on data, people, processes, and technology. It underscores the importance of proactive cybersecurity measures to mitigate these vulnerabilities and safeguard critical elements of an organisation.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vulnerability exploited | Impact on data | Impact on people | Impact on processes | Impact on technology |
| Weak passwords | Data may be easily accessed or stolen, leading to data breaches and leaks. | Individuals' accounts may be compromised, leading to identity theft or fraud. | Authentication and access controls need review and strengthening. | Weak passwords can lead to unauthorised access to systems and networks. |
| Phishing attacks | Sensitive data may be compromised, revealing confidential information. | Individuals may fall victim to scams, leading to financial loss. | Business processes may be disrupted as staff respond to phishing incidents. | Email security and user education measures need to be enhanced to prevent phishing attacks. |
| Unpatched software | Vulnerable systems can be exploited, leading to data breaches and unauthorised access. | Users may unknowingly install malicious software or face disruptions due to system crashes. | Patch management and vulnerability assessments need to be improved. | Regular system updates and security patches need to be applied promptly to mitigate vulnerabilities. |
| Insider threats | Insider misuse can result in unauthorised access to data and data leaks. | Employees may unknowingly compromise sensitive data or be manipulated to act against the organisation. | Incident response plans and monitoring procedures should be reviewed and enhanced to detect and prevent insider threats. | Access controls need to be implemented and monitored to detect and prevent insider threats. |
| Third-party risks | Third-party security breaches can lead to data leaks. | Exposure of sensitive data or loss of trust. | Vendor risk assessments and due diligence required for third-party security. | Robust vendor management processes and contracts need to be in place. |

****As a class watch [Detecting and Defending Social Engineering Attacks (4:28)](https://www.youtube.com/watch?v=IQL8kaBReDQ).

**Activity 34:** Cialdini’s Principles of Influence

In the table below, outline how Cialdini’s 6 Principles of Influence are used in social engineering.

|  |  |
| --- | --- |
| Cialdini’s 6 Principles of Influence | Outline of principle |
| Reciprocity | Social engineers initiate by offering a small favour, information or assistance, creating a sense of indebtedness in the target. |
| Scarcity (sense of urgency) | Social engineers create a perception of limited availability or urgency to motivate immediate compliance. |
| Authority | Social engineers impersonate figures of authority or use symbols of authority to manipulate targets. |
| Consistency | Social engineers encourage targets to commit to small actions or beliefs, making it more likely for them to comply with larger requests later. |
| Liking | Social engineers build rapport and connections, exploiting the natural human tendency to comply with those they like. |
| Consensus (social proof or bandwagon)  | Social engineers use the influence of others to persuade targets, creating a perception that many people are already complying. |

****Outline the System 1 and System 2 thinking theory and how fast and slow thinking shape perception and choice.

|  |
| --- |
| **Sample answer:**System 1 is fast and automatic thinking which relies on intuition and heuristics for quick judgments, often leading to cognitive biases and errors. It is efficient for routine tasks and immediate responses.System 2 involves slow, deliberate thinking, requiring conscious effort and analytical reasoning. It engages in critical evaluation, problem-solving and decision making in complex situations. The interplay between fast and slow thinking influences perception and choice. System 1 shapes initial perceptions rapidly based on past experiences, while System 2 intervenes to adjust or critically assess those perceptions. |

****Outline the concept of a psychological ‘hot-state’ which prevents rational decision making and promotes more (visceral) impulsive decisions.

|  |
| --- |
| **Sample answer:**The concept of a psychological ‘hot-state’ refers to a heightened emotional and impulsive state of mind that hinders rational decision making. In this state, emotions such as excitement, stress or anger are intensified, impacting cognitive processes and making individuals more susceptible to impulsive decisions.In a ‘hot-state’, individuals may prioritise immediate emotional gratification over careful consideration of consequences, leading to impulsive actions. This heightened emotional arousal can reduce cognitive control, distort risk perception and compromise the ability to think critically.The psychological ‘hot-state’ can be triggered by various factors, including emotional stimuli or stressful situations, influencing individuals to make decisions driven more by immediate feelings than rational thought, ultimately shaping impulsive choices. |

****Outline the ‘Spock versus Homer’ analogy in terms of rational decision making.

|  |
| --- |
| **Sample answer:**Spock personality trait/behaviour is a rational, logical decision-making approach.Homer personality trait/behaviour is an emotionally driven, impulsive approach.The analogy highlights the importance of finding a balance between the 2 extremes. While Spock's logical reasoning minimises emotional biases, Homer's emotional decision making may bring a human touch and spontaneity to certain situations. The analogy encourages individuals to be aware of their decision-making tendencies, striving for a middle ground that incorporates both rational analysis and emotional intelligence, ultimately leading to well-informed and balanced choices. |

****As a class watch [How phishing scammers manipulate your amygdala and oxytocin (11:00)](https://www.youtube.com/watch?v=9e6k_PtEXdM).

**Activity 35:** manipulating your amygdala and oxytocin

Identify 4 main vectors of social engineering discussed in the video.

|  |
| --- |
| **Sample answer:*** phishing
* vishing
* smishing
* impersonation.
 |

****Identify emotional triggers used in the recorded conversation.

|  |
| --- |
| **Sample answers:*** fear
* happiness.
 |

****Explain how a scammer manipulates the target’s thinking and impedes their capacity for critical thinking.

|  |
| --- |
| **Sample answer:**The scammer makes the target feel like he is trusted and this releases oxytocin.The scammer stimulates responses before the brain can kick in (Amygdala).Logic centres or parts of the brain shut down when strong emotions like fear are triggered. |

**Activity 36:** describe these social engineering attack vectors.

Phishing

|  |
| --- |
| **Sample answer:**Phishing is a social engineering attack vector where threat actors use deceptive emails, messages or websites to trick individuals into disclosing sensitive information, such as usernames, passwords or financial details. |

Smishing

|  |
| --- |
| **Sample answer:**Smishing is a social engineering attack vector that involves the use of fraudulent text messages or SMS to trick individuals into divulging sensitive information, clicking on malicious links or downloading malicious attachments. |

Vishing

|  |
| --- |
| **Sample answer:**Vishing is a social engineering attack vector in which attackers use voice communication, typically over the phone, to manipulate individuals into revealing sensitive information such as passwords or financial details. |

Impersonation

|  |
| --- |
| **Sample answer:**Impersonation is a social engineering attack vector where malicious actors mimic trusted entities or individuals, often through email or other communication channels, to deceive targets into disclosing sensitive information or performing actions against their best interests. |

Spear-phishing

|  |
| --- |
| **Sample answer:**Spear-phishing is a targeted social engineering attack vector where cybercriminals tailor deceptive messages to specific individuals or organisations, leveraging personalised information to increase the likelihood of successful phishing attempts. |

Whaling

|  |
| --- |
| **Sample answer:**Whaling is a social engineering attack vector that specifically targets high-profile individuals, such as executives or senior management, using sophisticated and personalised tactics to deceive them into divulging sensitive information or initiating financial transactions. |

****As a class watch [SANS Security Awareness: Email and phishing (3:55)](https://www.youtube.com/watch?v=sEMrBKmUTPE).

**Activity 37:** identifying phishing attempts

As a class examine examples of [phishing emails](https://www.cde.state.co.us/dataprivacyandsecurity/socialengineeringeducation) and describe the errors that have been highlighted.

As a class discuss how organisations and their employees can reduce the likelihood or impact of phishing, for example:

* training
* technical measures
* multi-factor authentication
* information sharing and reporting across organisations
* critical thinking.

**Activity 38:** combat social engineering attacks with critical thinking.

Read the following text:

You get a call from the ‘Help Desk’. The person calling explains that there is a problem with your computer. They ask for your username and password to access your machine to be able to investigate and remediate the problem.

Describe how you would critically think about the situation.

|  |
| --- |
| **Sample answer:**Providing your login credentials to the caller is a liability. A password is your authentication, and as soon as even one other person knows it, it can no longer prove your identity. Any activity done on your machine, with your password, is traced back to you. Do you really want to be responsible for the actions of another? |

What are the principles of influence used?

|  |
| --- |
| **Sample answer:**Reciprocity and authority. |

What are the emotional triggers used?

|  |
| --- |
| **Sample answer:**Fear and trust. |

# Assess cyber risk by implementing risk-management strategies using a risk matrix

Assessing cyber risk using a risk matrix involves evaluating various factors related to internal and external vulnerabilities, the threat landscape, the impact of exposure and the likelihood of exploitation. A risk matrix typically uses a grid to categorise risks based on their potential impact and likelihood, creating a visual representation that helps prioritise and manage these risks.

Figure 2 – risk assessment matrix



‘[Risk assessment matrix](https://en.wikipedia.org/wiki/File%3AIC-Risk-Assessment-Matrix-Template.jpg)’ by [Wikimedia Commons](https://commons.wikimedia.org/wiki/Main_Page) is licensed under [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/).

## Internal and external vulnerabilities

* Identify internal and external vulnerabilities.
* List internal vulnerabilities, which are weaknesses within an organisation, such as unpatched software, weak access controls or insider threats.
* Identify external vulnerabilities, including vulnerabilities in third-party software, supply chain weaknesses or exposure to external threats like malware and phishing.

## Threat landscape

* Understand the threat landscape.
* Analyse the current threat landscape by examining the types of threats (for example ransomware, DDoS attacks), their sources (hacktivists, nation-states, cybercriminals) and their methods (social engineering, zero-day exploits).
* Consider emerging threats and trends, such as new attack techniques or industry-specific risks.

## Impact of exposure

* Assess the impact of exposure.
* Define the potential impact of a cyber incident on your organisation. Consider financial losses, reputational damage, legal consequences, operational disruptions and the compromise of sensitive data.
* Assign impact values to each risk, such as low, medium or high based on the severity of the potential consequences.

## Likelihood of exploitation

* Determine the likelihood of exploitation.
* Evaluate the likelihood of each risk being exploited. This assessment should consider the presence of security controls, the organisation's historical exposure to similar threats and the effectiveness of security measures.
* Assign likelihood values, such as rare, occasional or frequent to each risk based on the probability of occurrence.

**Activity 39:** define and review the terms below:

Risk

|  |
| --- |
| **Sample answer:**Risk refers to the likelihood and potential impact of harm or damage resulting from threats or vulnerabilities to an organisation's information systems and data. |

Threat

|  |
| --- |
| **Sample answer:**A threat is a potential danger that can exploit vulnerabilities in a system or its components, posing a risk of harm to the confidentiality, integrity or availability of data and resources. |

Vulnerabilities

|  |
| --- |
| **Sample answer:**Vulnerabilities are weaknesses or flaws in a system's design, implementation or configuration that could be exploited by attackers to compromise the security and integrity of the system. |

Likelihood

|  |
| --- |
| **Sample answer:**Likelihood refers to the probability or chance that a specific threat will exploit a vulnerability, leading to a security incident or breach. |

Consequences

|  |
| --- |
| **Sample answer:**Consequences refer to the negative outcomes or impacts that may result from a security incident, including harm to data integrity, confidentiality breaches, system disruptions and potential financial or reputational losses for an organisation. |

Impact

|  |
| --- |
| **Sample answer:**Impact refers to the magnitude of harm or disruption that may occur because of a security incident, encompassing consequences such as financial losses, damage to reputation or compromise of data integrity and confidentiality. |

**Activity 40:** explain how impact can be evaluated in terms of (loss of):

* confidentiality
* integrity
* availability.

|  |
| --- |
| **Sample answer:**Evaluating the impact of a security incident involves assessing the extent of the loss of confidentiality, integrity and availability. This analysis helps organisations understand the severity of the breach, prioritise response efforts and implement appropriate measures to mitigate the consequences and prevent future occurrences. |

****As a class watch [Risk and How to use a Risk Matrix (5:28)](https://www.youtube.com/watch?v=-E-jfcoR2W0).

**Activity 41:** describe how a cybersecurity risk assessment matrix is used.

|  |
| --- |
| **Sample answer:**A cybersecurity risk assessment matrix is used as a tool to systematically evaluate and prioritise potential risks within an organisation's digital environment. The matrix typically consists of 2 main dimensions: the likelihood of a specific risk occurring and the potential impact it may have. Each identified risk is assigned a rating within this matrix based on these criteria. The risk assessment matrix aids in visualising and categorising risks, allowing organisations to focus their resources on addressing high-impact, high-likelihood risks first. It serves as a valuable guide for decision making, resource allocation and the development of risk mitigation strategies, helping organisations enhance their cybersecurity posture by prioritising efforts based on the probability of various cyber threats. |

**Activity 42:** describe the difference between risk assessment and risk management.

|  |
| --- |
| **Sample answer:**Risk assessment involves identifying, evaluating and quantifying potential risks within a system or organisation, considering the likelihood and impact of various threats. Risk management encompasses the processes of developing strategies to mitigate, transfer, accept or avoid identified risks, aiming to control and optimise the overall risk exposure in alignment with organisational objectives. |

****Examine the [Guide to conducting cybersecurity risk assessment for critical information infrastructure (PDF 836 KB)](https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf) document. Note that key pages to examine are pages 10, 12, 14 and 16.

Focus on these steps and tasks:

* risk identification
* identify assets
* construct risk scenarios
* risk analysis
* determine likelihood
* determine impact
* risk evaluation
* determine and prioritise risk.

**Activity 43:** USB drop scenario (D)

Read the following text:

Meet Jimmy. Jimmy is an employee in your company. He Does Things With Computers (official title). Last Wednesday, as Jimmy got out of his car after parking in the company-owned parking lot, he saw something on the ground.

That ‘something’ was a 512 GB USB flash drive!

Jimmy picks up the drive, whistling along to himself as he enters the office and settles down in his cubicle. At which point he plugs in his new, free USB flash drive. Without knowing it, Jimmy has just allowed a targeted malware into your company’s network.

****Describe vulnerabilities a threat actor aims to exploit in this scenario.

|  |
| --- |
| **Sample answers:**The main vulnerability being exploited is human nature and, specifically, curiosity.* For someone who wants to use the USB – the USB should look new, clean and unlabelled.
* For someone curious about the person who owns it – the USB may have the label ‘personal’ or ‘photos’.
* For someone who has a personal business interest – the USB may have the label ‘finance’, ‘clients’ or ‘confidential’.
* For someone generally curious – the label may be something ambiguous or simply left blank. Then, the individual might project their own idea of what could be on there and be driven by curiosity to find out.
* Other vulnerabilities could include a lack of staff awareness training and policies to guide how staff should respond to this situation.
 |

****Describe possible consequences (and their likelihood) of inserting an unknown USB drive into an organisation’s computer.

|  |
| --- |
| **Sample answers:**Malware and viruses: the USB drive may contain malicious software, such as viruses, Trojans or ransomware. If executed, these could infect the organisation's systems and compromise data integrity and confidentiality. Malware is commonly spread through infected USB drives.Unauthorised access: the USB drive might carry software designed to exploit vulnerabilities or gain unauthorised access to the organisation's network. This could lead to data breaches, unauthorised system access and potential theft of sensitive information.  |

****Review 5 emotions that social engineers use against their targets across different social engineering attacks.

|  |
| --- |
| **Sample answer:**Social engineers exploit a range of emotions to manipulate their targets in various social engineering attacks. Fear is leveraged to create urgency, prompting impulsive actions.Curiosity is exploited through enticing content, leading individuals to click on malicious links.Trust is established by impersonating reputable figures or entities, fostering compliance with deceitful requests.Urgency is manufactured to sidestep scrutiny, compelling rapid, unquestioning responses. Greed is targeted by promising financial rewards, enticing individuals to disclose sensitive information or undertake compromising actions.  |

****As a class watch [Security Awareness Episode 5: Removable Media (1:22)](https://www.youtube.com/watch?v=FRxrHduwPjY).

**Activity 44:** psychology of the USB drop

****As a class discuss the relevant emotions a social engineer is hoping to exploit in this scenario.

Read [The Psychology of a Cyber Attack: USB Drop Simulation](https://www.assentriskmanagement.co.uk/the-psychology-of-a-cyber-attack-usb-drop-simulation/) and describe possible factors for someone to pick up an unknown USB and plug it into a computer.

|  |
| --- |
| **Sample answer:**One factor is they are curious as to what is on it. Humans are naturally curious creatures, so it’s only natural that one might wonder what a USB stick contains. But what would be the drive behind this curiosity? They might be interested to see what personal stuff the owner has on there – such as photos. They also might be curious to see if any sensitive data is on there – humans have a natural drive to discover the unknown.Another factor is they have a personal interest in who it belongs to. Someone might be interested to find information they can use against the person – if it is someone they dislike, or to see if they have anything to hide. Perhaps, they might believe it contains information about another company – a rival for example. |

**Activity 45:** removeable media risks

As a class watch the [Removable Media Security Video (2:31)](https://www.youtube.com/watch?v=OGbhLAaELmw).

As a class discuss the risk(s) of this action considering its impact on various elements of the organisation, including:

* data
* people
* processes
* technology.

****Describe how an organisation can protect against removable media vulnerability and similar social engineering attacks.

|  |
| --- |
| **Sample answers:**To safeguard against removable media vulnerabilities and mitigate the risks of social engineering attacks, organisations should implement a multi-faceted security strategy.They should establish comprehensive security policies that strictly regulate the use of removable media devices, outlining procedures for their authorised usage and restricting access to sensitive systems.Employ robust endpoint protection solutions capable of detecting and blocking malicious software that may be introduced via removable media.Conduct regular security awareness training for employees, emphasising the risks associated with unknown USB drives and promoting a culture of scepticism towards unsolicited emails or messages prompting media insertion.Implement device control measures to restrict unauthorised devices from connecting to organisational systems. |

# Investigate cyber risk management

A well-rounded cyber risk management strategy combines proactive measures for risk identification and vulnerability management with reactive measures for incident response and damage control. It is important to note that cybersecurity is an ever-evolving field and organisations should adapt their strategies and training programs to keep up with emerging threats and vulnerabilities. Regular risk assessments and ongoing training are key components of a resilient cybersecurity posture.

## Implementing a cybersecurity strategy with ongoing training

**Strategy development:** effective cyber risk management begins with the development of a robust cybersecurity strategy. This strategy should encompass goals, priorities and a roadmap for protecting digital assets and data.

**Ongoing training:** employees are often the first line of defence against cyber threats. Regular training and awareness programs help them recognise and respond to potential risks. Training should cover topics like safe online practices, recognising phishing attempts and understanding the organisation's cybersecurity policies.

## Identifying and managing vulnerabilities

**Risk assessment:** organisations must regularly assess their systems and networks to identify vulnerabilities. This includes vulnerability scanning, penetration testing and vulnerability management.

**Patch management:** after identifying vulnerabilities, it is crucial to promptly apply security patches and updates to mitigate known risks. Establish a process for tracking and applying patches to all systems.

## Assessing the impact of a breach

**Incident response plan:** part of risk management involves preparing for the possibility of a breach. Develop an incident response plan that outlines the steps to take in the event of a cybersecurity incident. This plan includes roles and responsibilities, communication protocols and legal compliance considerations.

**Impact assessment:** in the event of a breach, assess its impact on the organisation. This involves understanding the extent of data exposure, financial losses, operational disruptions and reputational damage.

## Controlling damage and loss

**Mitigation measures:** implement measures to control damage and limit further losses during and after a breach. This includes isolating affected systems, stopping unauthorised access and removing malware.

**Communication:** maintain clear and open communication with affected parties, including customers, employees and regulatory bodies. Timely and transparent communication can help manage reputational damage.

**Activity 46:** human errors

Categorise in the table below human errors and technical errors from previous scenarios.

|  |  |
| --- | --- |
| Human errors | Technical errors |
| * Clicking unknown links.
 | * Poor access control.
 |
| * Ignoring software updates.
 |  |
| * Weak and/or old passwords.
 |  |
| * Inserting unknown USB drives/media.
 |  |

****Read [Human Errors in Cyber Security – a Swiss Cheese of Failures](https://securityandpeople.com/2017/07/human-errors-in-cyber-security-a-swiss-cheese-of-failures/) and further categorise the human errors according to the 7 error definitions provided.

Share and discuss answers with the class.

****As a class view the [Swiss cheese model for cybersecurity](https://www.linkedin.com/pulse/swiss-cheese-model-cybersecurity-hicham-faik/) and explain how it aligns with the Defence in Depth mindset and encourages use of multiple controls and defences within organisations to protect against threats.

Review previous scenarios and discuss issues of changing the security behaviour of individuals or organisations.

****As a class watch the [Role of Human Error in Cybersecurity (3:08)](https://www.youtube.com/watch?v=AYduljAMYxI) and consider the following approaches to changing the security behaviour of individuals or organisations.

As a class discuss and decide, should they:

* make users aware of how the underlying technology works? Or make their choices as simple as possible?
* use peer learning and social influence? Or rules?
* use risk-assessment mindsets? Or simple heuristics?

# Describe privacy and security principles associated with access, storage and permissions used by enterprises to collect and interpret data

**Activity 47:** insider threat scenario (E)

Read the following text:

A DevOps engineer, responsible for managing software on your organisation's cloud infrastructure and holding a position of trust, engages in malicious activity. This engineer, motivated by personal gain, decides to leak sensitive company information.

Leveraging their extensive access privileges, they intentionally expose company credentials on the internet. As a result, an outsider discovers the exposed credentials and sends an email to the CISO notifying them of this security breach.

Work individually or in pairs.

Identify relevant data (evidence gathered from employee actions) and establish a set of facts within provided scenario.

Use critical thinking to evaluate data and consider potential risks.

Apply adversarial mindset to devise strategies that would align with indicators of compromise.

Prepare a narrative response to share with the class.

****Discuss findings with the class and answer the following questions.

What is the employee trying to do?

|  |
| --- |
| **Sample answer:**The employee is trying to engage in malicious activity to leak sensitive enterprise information. |

****What are the risks of this employee’s actions?

|  |
| --- |
| **Sample answer:**The enterprise credentials are exposed on the internet. |

****Is the employee a malicious insider or victim of human error?

|  |
| --- |
| **Sample answer:**The employee is a malicious insider as they are within an enterprise and they are intentionally and knowingly posing a threat to the security of the enterprise. Malicious insiders have authorised access to the enterprise's systems, networks or sensitive information due to their legitimate affiliation with the enterprise. |

Determine appropriate action(s) to be taken.

**Discussion questions:**

Who within the organisation needs to be immediately informed about the incident?

How should the organisation identify the extent of data exposure and the specific information that has been compromised?

What steps should be taken to change company credentials and secure them?

Should access to critical servers be temporarily shut down or limited?

What procedures can be put in place to prevent insider threats like this in the future?

What steps can the organisation take to bounce back from a security breach and reduce the risks associated with exposed data?

Are there policies and training programs in place to address insider threats and the handling of sensitive data?

What is the process for monitoring privileged users' activities and identifying suspicious behaviour?

Confirm alignment of their version of events and the incident.

****As a class watch [Everything You Need to Know About Insider Threats...in 2 Minutes (2:22)](https://www.youtube.com/watch?v=QXnNkSeT6dM).

**Activity 48:** discuss ‘How can organisations protect against this threat?'’

|  |
| --- |
| **Sample answers:*** User education and awareness: implement ongoing training programs to educate employees about the risks associated with insider threats, emphasising the importance of security policies, data protection and recognising suspicious activities.
* Access controls: enforce the principle of least privilege, ensuring that employees have the minimum level of access required to perform their duties. Regularly review and update user permissions based on job roles.
* Monitoring and auditing: implement robust monitoring systems to track user activities, especially those involving sensitive data or critical systems. Regularly audit access logs for unusual behaviour or deviations from normal patterns.
* Endpoint security: utilise endpoint security solutions to monitor and control activities on individual devices. This can include the use of antivirus software, endpoint detection and response (EDR) tools and application control mechanisms.
* Incident response plan: develop and regularly update an incident response plan specifically addressing insider threats. This plan should include procedures for investigating and responding to suspected incidents promptly.
* Background checks: conduct thorough background checks during the hiring process and periodically review employee records. This can help identify potential red flags in an individual's history or behaviour.
 |

# Research hardware and software strategies used to protect data

**Activity 49:** in the table below summarise different forms of authentication, different types of evidence a user provides, and highlight known weaknesses or vulnerabilities.

|  |  |  |
| --- | --- | --- |
| Different forms of authentication | Different types of evidence a user provides | Known weaknesses or vulnerabilities |
| Passwords | This authentication evidence is based on ‘what the user knows’. | Can be guessed or stolen. |
| Biometrics | Biometrics authentication relies on the unique biological characteristics of an individual.Facial recognition, fingerprint scanners and speaker recognition.This authentication evidence is based on ‘what the user is’. | Requires hardware to process physical attributes. No known weaknesses or vulnerabilities if implemented well. |
| Smart cards | A smart card is a physical card that has an embedded integrated chip that acts as a security token.This token-based authentication relies on ‘what the user has’.Smart cards may provide strong security authentication for single sign-on (SSO) within organisations. | Can be lost or stolen. |
| Federation and single-sign-on (SSO) | Can either be based on password or biometric. | If the authentication method is compromised the attacker has access to all things. |
| Certificate-based authentication | Identity is established using electronic documents known as digital certificates. Digital certificates contain identification data generated by cryptographic processes. | Certificates expire and users rely on verified certificates. |

**Activity 50:** explain the principles of multi-factor authentication (MFA) and how this increases security.

|  |
| --- |
| **Sample answer:**MFA is a robust security measure that enhances the protection of digital accounts and systems by requiring users to provide multiple forms of identification before gaining access. The fundamental principles of MFA revolve around the use of 2 or more independent factors to authenticate a user. These factors typically fall into 3 categories: something you know (like a password or PIN), something you have (such as a smartphone or a security token) and something you are (biometric data like fingerprints or facial recognition). By combining these factors, MFA significantly strengthens the security posture of an authentication system. Even if one factor is compromised, an unauthorised user would still need the additional factor(s) to gain access, making unauthorised access much more difficult. MFA mitigates the risks associated with password-based authentication, as passwords alone are susceptible to various attacks like phishing or brute-force attempts. This layered approach ensures a higher level of security and helps safeguard sensitive information and resources from unauthorised access. |

**Activity 51:** evaluate 2 examples, each illustrating multiple authentication processes, for example:

* providing a password and answering a security question
* providing a password and using a fingerprint scan.

|  |  |
| --- | --- |
| Examples | Illustrate the multiple authentication processes |
| Providing a password and answering a security question | This example is not MFA because both forms of evidence are things that the user knows.MFA requires at least 2 different types of evidence. |
| Providing a password and using a fingerprint scan | This example is MFA because one form is evidence is something the user knows and the other form of evidence is something the user is. |

**Activity 52:** answer the following questions.

Identify examples of organisations using multi-factor authentication.

|  |
| --- |
| **Sample answers:*** technology companies
* financial institutions
* social media platforms
* healthcare organisations
* government agencies.
 |

****Evaluate the advantages and disadvantages of organisations using multi-factor authentication (MFA) apps in the workplace.

|  |
| --- |
| **Sample answer:**The adoption of MFA apps in the workplace offers notable advantages, including enhanced security by mitigating the risk of unauthorised access and reducing the effectiveness of phishing attacks. These apps provide adaptability and user convenience, as they can be integrated with various devices and systems, offering a user-friendly experience.However, the implementation of MFA apps may face challenges related to initial setup complexity, dependency on mobile devices, potential integration issues with legacy systems, associated costs and potential user resistance. |

****Explain whether mechanisms like Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) are identification or authentication access control processes.

|  |
| --- |
| **Sample answer:**Mechanisms like CAPTCHA primarily serve as identification processes rather than authentication in access control. CAPTCHA is designed to verify that the user attempting access is human, aiming to distinguish between automated bots and genuine users. It focuses on confirming the user's ability to solve visual or auditory challenges rather than verifying their specific identity or credentials. While CAPTCHA adds an extra layer to user identification, authenticating users typically involves confirming their claimed identity through the use of passwords, biometrics, or other credentials. In this context, CAPTCHA contributes to the overall access control process by ensuring that the entity seeking access is a human user, preventing automated bots from maliciously interacting with web applications. |

As a class discuss security controls used to ensure the goal of integrity (protecting data from being altered without authorisation) such as:

* access controls
* hashing
* [digital signatures](https://www.dock.io/post/digital-signatures)
* digital certificates.

**Activity 53:** define authenticity in relation to cybersecurity.

|  |
| --- |
| **Sample answer:**In cybersecurity, authenticity refers to the quality of being genuine, valid, and trustworthy. It is a measure of the legitimacy and origin of digital entities, such as users, data or communication channels. Ensuring authenticity is crucial for verifying the identity of users, confirming the integrity of data and validating the source of information or communication. Authentication mechanisms, such as passwords, biometrics or cryptographic protocols, are employed to establish the authenticity of users, while digital signatures and cryptographic hashes are used to verify the authenticity and integrity of data or messages. |

**Activity 54:** define non-repudiation in relation to cybersecurity.

|  |
| --- |
| **Sample answer:**Non-repudiation is a cybersecurity concept that ensures an entity cannot deny the authenticity or origin of a communication, action, or transaction. It is a measure designed to prevent individuals from later disowning their involvement in a particular event or interaction. In the context of digital communication, non-repudiation is often achieved using cryptographic techniques, such as digital signatures which provide proof of the originator's identity and ensure that the sender cannot deny sending a particular message. This concept is critical in legal and contractual scenarios where establishing the authenticity of digital interactions is essential for accountability, dispute resolution and maintaining the overall trustworthiness of digital transactions. |

****As a class watch the [overview of cryptography (4:47)](https://www.linkedin.com/learning/ssl-tls-for-beginners-securing-network-communications/cryptography-overview) in securing network communications.

****As a class watch [Symmetric and asymmetric encrypting (6:13)](https://www.linkedin.com/learning/ssl-tls-for-beginners-securing-network-communications/symmetric-and-asymmetric-encrypting) and read about [Asymmetric Keys](https://learn.microsoft.com/en-us/windows/win32/seccrypto/public-private-key-pairs).

**Activity 55:** explain the difference between symmetric and asymmetric encryption.

|  |
| --- |
| **Sample answer:**Symmetric and asymmetric encryption are 2 fundamental approaches to secure communication in cybersecurity. In symmetric encryption, a single shared key is used for both encryption and decryption processes. While this method is efficient, it poses challenges in secure key distribution and requires a high level of trust among communicating parties. On the other hand, asymmetric encryption involves a pair of public and private keys. The public key is used for encryption and the private key is used for decryption. This approach addresses the key distribution challenge but is computationally more intensive. Asymmetric encryption is often employed for secure key exchange and digital signatures, while symmetric encryption is utilised for bulk data encryption in a more resource-efficient manner. |

****As a class watch [Signing and verifying data using GPG (8:30)](https://www.youtube.com/watch?v=4bbyMEuTW7Y) to understand how to use cryptographic tools to verify the authenticity of a file.

Teacher-led demonstration on how to use cryptographic tools to verify the integrity of a file, for example:

* SHA-256
* [obtain a digital certificate and create a digital signature](https://support.microsoft.com/en-au/office/obtain-a-digital-certificate-and-create-a-digital-signature-e3d9d813-3305-4164-a820-2e063d86e512)
* [creating digital signatures and certificates](https://support.microsoft.com/en-au/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-22bd163e8e96)
* [using a hash generator](https://www.linkedin.com/learning/learning-cryptography-and-network-security-2/looking-deeper-into-message-digests).

# Investigate cybercrime threats to an enterprise

Effective cybersecurity strategies to counter threats include employee training and awareness programs, the implementation of strong access controls and monitoring systems, patch management to address vulnerabilities, and incident response plans to handle security breaches. Regular security assessments and audits are also essential for identifying and mitigating risks in an enterprise's digital environment.

## Hacking

**Threat:** hacking involves unauthorised access to computer systems, networks, or devices to steal, alter or disrupt data. Attackers use various techniques, including exploiting vulnerabilities, password cracking and SQL injection.

**Impact:** hacking can lead to data breaches, financial losses, service disruptions and reputational damage. Sensitive information, trade secrets and customer data are often targeted.

## Phishing, including smishing

**Threat:** phishing is a deceptive technique in which attackers impersonate trustworthy entities through email or messaging to trick individuals into revealing sensitive information or clicking on malicious links. Smishing is a similar tactic but carried out via SMS.

**Impact:** phishing and smishing attacks can result in data breaches, identity theft, financial fraud and malware infections. They often exploit human vulnerabilities, making employee awareness and training essential.

## Scamming

**Threat:** scams involve fraudulent schemes and social engineering tactics to deceive individuals or employees into making financial transactions, providing personal information or taking harmful actions.

**Impact:** scams can lead to financial losses, the compromise of personal or business information, and damage to an organisation's reputation. Common scams include investment fraud, lottery scams and tech support scams.

## Bots and botnets

**Threat:** bots are automated programs that can perform tasks on the internet. Botnets are networks of compromised devices controlled by an attacker, often used for malicious purposes such as Distributed Denial of Service (DDoS) attacks, spam or credential stuffing.

**Impact:** botnets can disrupt services, steal sensitive data and propagate malware. Organisations may find their networks overwhelmed by DDoS attacks, affecting operational continuity.

## Employee action causing a vulnerability

**Threat:** employees can inadvertently introduce vulnerabilities by falling victim to phishing attacks, misconfiguring systems or violating security policies. Insider threats also pose a risk.

**Impact:** employee actions can lead to data breaches, unauthorised access and operational disruptions. Insider threats can be particularly challenging to detect and mitigate, as they involve trusted individuals with access to sensitive information.

**Activity 56:** lost luggage scenario (F)

Read the following scenario text:

Bob’s manager Alice is traveling abroad to give a sales presentation. Bob receives an email with the following message: ‘Bob, I just arrived and the airline lost my luggage. Would you please send me the technical specifications for our new product? Thanks, Alice.’ What should Bob do?

Assign required groups and roles.

In groups, define the problem and identify relevant facts from provided scenario text.

In an iterative process combine and apply additional information to the scenario body of knowledge.

**Discussion questions:**

What concerns arise when considering the security of communications involving intellectual property. What will be protected? What are the adversary’s motivations and goals? What are the adversary’s capabilities? What do we trust?

What if it is someone impersonating Alice?

How sensitive is the information in the technical specifications? Who might be interested in obtaining the presentation?

If Alice’s identity is verified, what techniques enable a timely resolution of the problem?

Does the company have existing processes like secure (encrypted) corporate email?

Use critical thinking to evaluate the situation and consider potential risks.

Apply adversarial mindset to devise strategies that would align with indicators of compromise.

Prepare a group response to share with the class.

# Research hardware and software strategies used to protect data

**Activity 57:** analyse applicable cybersecurity concepts for the lost luggage scenario (F) for the following:

|  |  |
| --- | --- |
| Cybersecurity concept | Analysis of scenario (F) |
| Authentication | Is the communication really from Bob’s boss Alice? How can we verify the authenticity of the communication and its sender?If the company used a secure e-mail system, Bob could check if the email came from Alice’s company email server and included a valid digital signature. |
| Confidentiality | If Alice wanted confidentiality, she would encrypt the message.Possible options could include using encrypted email, such as PGP. Using a secure cloud-based file-sharing application. Send the specifications by a trusted courier (if time permits). |
| Digital signatures | Digital signatures enable authentication of Alice as sender of the message. |
| Encryption | Encryption protects the confidentiality (but not necessarily integrity) of the sales presentation that Bob would send to Alice. Consider advantages and disadvantages of symmetric or asymmetric encryption. |
| Integrity | Hash functions support integrity of transmissions, facilitating the detection of any message modification.Message integrity, ensuring that Alice’s message arrived without modification, can be provided as part of the digital signature process, which provides authentication. |
| Cryptography | A cryptographic hash function creates a digest (fixed-length tag) that is generated from Alice’s message. The cryptographic aspect of ‘cryptographic hash’ indicates that it is not possible to modify the message and produce the same tag, nor to find any 2 different messages that produce the same tag. Any modification to the message would result in a detectable change to the hash tag. |
| Risk | What are the risks, likelihood and impact of sensitive information being disclosed to unauthorised people?Clear guidelines reduce risk. |
| Security practices (of organisation) | Is this sort of problem unexpected due to carefully designed plans for handling company assets? Why was the sensitive material placed in a potentially vulnerable location? Security measures must be sufficiently robust to adapt to unexpected events.It is essential that Bob recognise the potential vulnerabilities inherent in this scenario. Bob might try first to contact a company official or security officer to ask for guidance. Regardless, he should report the incident. |
| Security measures | Security measures must be sufficiently robust to adapt to unexpected events.Securing the sending and receiving devices is another important consideration, both to protect the unencrypted product specifications and the secret keys needed for security in transit. For example, it is important to guard against possible malware that might compromise their mobile computing devices. |

With reference to this scenario, consider implementing a cybersecurity strategy with ongoing training.

**Activity 58:** identify vulnerabilities that could be exploited.

|  |
| --- |
| **Sample answers:*** Staff awareness and lack of knowledge of procedures.
* No secure enterprise or corporate email system in place.
* Devices are not configured with appropriate security settings and controls.
 |

**Activity 59:** describe controls or other strategies that could be implemented to mitigate risk(s) of a breach.

|  |
| --- |
| **Sample answer:**The enterprise must ensure they have security access controls in place.They could mitigate risks by using the following controls or strategies:* permissions and access control lists (ACLs)
* encryption on email communication
* digital certificates and digital signatures
* staff training to increase awareness and technical proficiency
* review of policies and practices to ensure staff know what they should do in certain circumstances
 |

**Activity 60:** describe security controls used to ensure the goal of availability (information and systems remain available to authorised users when needed) such as:

* backups
* operating system (OS) and application patching.

|  |
| --- |
| **Sample answer:*** Data backups can help restore systems quickly in the event of theft or loss. Backups and full disaster recovery plans also help a company regain availability soon after a cyber incident.
* Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Fixing vulnerabilities reduces the risk of cyber attacks from known exploits.
 |

**Activity 61:** identify strategies organisations can use or implement to uniquely identify users to a system.

|  |
| --- |
| **Sample answers:*** usernames
* access cards, including magnetic stripe cards, photo identification, RFID and NFC
* biometrics, including fingerprint scan, eye scan and facial recognition.
 |

**Activity 62:** identify hardware and software strategies used to protect data.

|  |
| --- |
| **Sample answers:*** isolation
* firewalls
* antivirus
* anti-malware.
 |

# Investigate vulnerabilities exploited by the threat actor involved in a breach, such as the impact on various elements

This table provides an overview of common vulnerabilities exploited in breaches and the potential impacts on data, people, processes and technology. It underscores the importance of proactive cybersecurity measures to mitigate these vulnerabilities and safeguard critical elements of an organisation.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vulnerability exploited | Impact on data | Impact on people | Impact on processes | Impact on technology |
| Weak passwords | Data may be easily accessed or stolen, leading to data breaches and leaks. | Individuals' accounts may be compromised, leading to identity theft or fraud. | Authentication and access controls need review and strengthening. | Weak passwords can lead to unauthorised access to systems and networks. |
| Phishing attacks | Sensitive data may be compromised, revealing confidential information. | Individuals may fall victim to scams, leading to financial loss. | Business processes may be disrupted as staff respond to phishing incidents. | Email security and user education measures need to be enhanced to prevent phishing attacks. |
| Unpatched software | Vulnerable systems can be exploited, leading to data breaches and unauthorised access. | Users may unknowingly install malicious software or face disruptions due to system crashes. | Patch management and vulnerability assessments need to be improved. | Regular system updates and security patches need to be applied promptly to mitigate vulnerabilities. |
| Insider threats | Insider misuse can result in unauthorised access to data and data leaks. | Employees may unknowingly compromise sensitive data or be manipulated to act against the organisation. | Incident response plans and monitoring procedures should be reviewed and enhanced to detect and prevent insider threats. | Access controls need to be implemented and monitored to detect and prevent insider threats. |
| Third-party risks | Third-party security breaches can lead to data leaks. | Exposure of sensitive data or loss of trust. | Vendor risk assessments and due diligence required for third-party security. | Robust vendor management processes and contracts need to be in place. |

**Activity 63:** database input error scenario (F)

As a class read the following text:

When a user Mike O’Brien registered a new account for an online shopping site, he was required to provide his username, address and first and last name. Immediately after Mike submitted his request, you as the security engineer receive a database input error message in the logs. What might you infer from this error message?

Assign required groups and roles.

In groups, define the problem and identify relevant facts from provided scenario text.

Use critical thinking to evaluate the situation and consider potential risks.

Apply adversarial mindset to devise strategies that would align with indicators of compromise.

Prepare a group response to share with the class.

Share group responses and collaborate to build a better understanding of this scenario event and work towards an agreed response to the question.

Recap findings from scenario (F) including:

|  |  |
| --- | --- |
| Database issue | Discussion points |
| User input into online form | Because the error was a ‘database input error’, we may infer that the error was detected by a database program upon attempting to make an input into a database. |
| Error messages | Let us assume that the error was not caused by a straightforward programming error triggered by any user input (such an error would be less likely to cause interesting security issues) nor by the user failing to follow instructions such as entering all required information (in which case the program should respond with helpful feedback to the user). |
| Security logs | We shall assume that the log files record normal operating events and error conditions. It seems likely that the error logged was caused by something that the user entered.  |

**Activity 64:** explain the essential operations of SQL for storing, manipulating and retrieving data in databases.

|  |
| --- |
| **Sample answer:**SQL plays a pivotal role in handling data within databases through its essential operations. The core functions involve data definition, manipulation and retrieval.First, data definition involves creating and modifying the structure of a database, defining tables, specifying data types and establishing relationships between tables. The manipulation operations, which include INSERT, UPDATE, and DELETE statements, allow users to add, modify or remove data from the database, ensuring the integrity and accuracy of stored information.Additionally, SQL's SELECT statement facilitates data retrieval by enabling users to extract specific information from one or more tables based on specified criteria. Clauses such as WHERE, JOIN, and GROUP BY provide the flexibility to filter, combine and aggregate data as needed. The overall versatility of SQL in managing databases makes it a powerful tool for storing, manipulating and retrieving data, providing a comprehensive solution for interacting with structured information efficiently and securely. |

**Activity 65:** explain how SQL commands are used in web page forms to collect and process user input.

|  |
| --- |
| **Sample answer:**SQL commands are embedded in web page forms to collect and process user input by facilitating the communication between the front-end interface and the database, allowing for the seamless insertion, updating or retrieval of data based on the information entered by users. |

****SQL injection is the placement of malicious code in SQL statements via web page input. As a class watch [What is SQL injection?](https://www.youtube.com/watch?v=wX6tszfgYp4) (10:20).

As a class examine how [SQL injection](https://owasp.org/Top10/A03_2021-Injection/) works and the link to findings in the scenario.

**Activity 66:** describe the possible consequences of an [SQL injection attack](https://owasp.org/www-community/attacks/SQL_Injection) in terms of:

Confidentiality

|  |
| --- |
| **Sample answer:**In terms of confidentiality, an SQL injection attack can have severe consequences by allowing unauthorised access to sensitive information stored in a database. Attackers can exploit vulnerabilities to view, modify or extract confidential data, such as personal user details, financial records or business information. This breach of confidentiality poses a significant threat to individuals and organisations, leading to potential privacy violations, identity theft or unauthorised disclosure of sensitive data. |

Authentication

|  |
| --- |
| **Sample answer:**In terms of authentication, an SQL injection attack can compromise user credentials and authentication mechanisms, leading to unauthorised access to systems and sensitive accounts. By injecting malicious SQL code into login forms or authentication processes, attackers can bypass authentication checks potentially gaining elevated privileges or impersonating legitimate users. This can result in unauthorised access to confidential data, manipulation of system configurations or even complete compromise of the affected application.  |

Authorisation

|  |
| --- |
| **Sample answer:**In terms of authorisation, an SQL injection attack can have serious consequences by enabling attackers to manipulate or bypass access control mechanisms within a database or application. By injecting malicious SQL code, attackers may exploit vulnerabilities to gain unauthorised access to specific data, modify user roles or escalate their privileges. This can result in unauthorised actions, such as data manipulation, deletion or the exposure of sensitive information. |

Integrity

|  |
| --- |
| **Sample answer:**In terms of integrity, an SQL injection attack poses a significant threat by allowing unauthorised modification or tampering of data stored in a database. Attackers can inject malicious SQL code to alter records, manipulate critical information or even delete entire datasets. This compromise of data integrity can have severe consequences, leading to misinformation, financial loss and damage to an organisation's reputation. |

As a class discuss the impact of injection attacks using example(s) of past cybersecurity breach(es), for example:

* Heartland Payment Systems 2007–2008 (US)
* British Telecom firm, TalkTalk 2016
* CVE-2023-34362 – MOVEit Transfer Zero-Day SQL Injection Vulnerability Actively Exploited in the Wild

**Activity 67:** describe techniques for [testing for SQL injection](https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection.html) vulnerabilities.

|  |
| --- |
| **Sample answer:**To test for SQL injection vulnerabilities, you can employ both manual and automated techniques. Manually, testers should validate input fields by attempting to input special characters, such as quotes and semicolons. They can also execute error-based tests by intentionally injecting SQL errors and observing application responses. Automated tools can automate the process, scanning for vulnerabilities by injecting payloads and analysing responses.Testing stored procedures and functions, implementing positive security models, regular expression validation and leveraging web application firewalls are crucial for comprehensive SQL injection testing.Testing should always be performed in a controlled, ethical manner, and keeping software updated is essential to address potential security vulnerabilities. |

**Teacher note:** students would benefit from a practical experience. Using a pre-prepared vulnerable web app (within a sandboxed environment) the teacher could demonstrate how to apply SQL injection techniques.

Students with access to a suitable sandboxed environment could complete SQL injection activities.

**Activity 68:** describe known technical strategies to prevent SQL injection attacks.

|  |
| --- |
| **Sample answer:**Input validation is crucial, ensuring that user inputs are thoroughly checked for conformity with expected patterns and rejecting any input that may be indicative of an attack.Parameterised queries and prepared statements should be used to separate SQL code from user input, preventing malicious code injection.Employing least privilege principles by granting the minimum necessary permissions to database accounts can limit the impact of an injection attack.Web application firewalls (WAFs) can be deployed to filter and monitor HTTP traffic, identifying and blocking potential SQL injection attempts.Regularly updating and patching the underlying database and web application software is also essential to address known vulnerabilities. |

# Identify laws and legislation associated with cybersecurity

In Australia, several laws and regulations are associated with cybersecurity and data protection. Some of the key ones include:

*Privacy Act 1988*: the *Privacy Act 1988* establishes the Australian Privacy Principles (APPs), which govern the handling of personal information by Australian government agencies and many private sector organisations. It includes provisions related to data security and breach notification requirements.

Notifiable Data Breaches (NDB) Scheme: an amendment to the *Privacy Act 1988*, the NDB scheme mandates that organisations covered by the *Privacy Act 1988* notify affected individuals and the Australian Information Commissioner of eligible data breaches.

*My Health Records Act 2012*: this legislation pertains to the security and privacy of electronic health records in Australia, outlining measures to protect patient data.

Telecommunications Act 1997: this Act includes provisions related to the security and integrity of telecommunications networks, with a focus on protecting against unauthorised access and interference.

Defence Trade Controls Act 2012: this legislation governs the export of defence and strategic goods and technology, including cybersecurity-related items.

Criminal Code Act 1995: this Act includes provisions related to cybercrime, such as unauthorised access, data interference and unauthorised modification of data.

Cyber Security Strategy: while not legislation, Australia has released multiple national cybersecurity strategies to outline the government's approach to cybersecurity and the protection of critical infrastructure.

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018: this controversial legislation grants certain powers to law enforcement and intelligence agencies for accessing encrypted communications. It has raised privacy and security concerns.

****As a class view the [Cyber and Infrastructure Security Centre](https://www.cisc.gov.au/) website and the [Collective Cyber Defence for Critical Infrastructure](https://ci-isac.com.au/) website. These websites guide Australian industries to meet cybersecurity principles.

**Activity 69:** discuss ‘How do ethics influence my decisions?’

|  |
| --- |
| **Sample answer:**Ethics can significantly shape decisions by providing a moral framework that guides choices based on principles of fairness, integrity and social responsibility.Considering the ethical implications ensures that decisions align with values and contribute to positive outcomes, fostering trust and accountability in both personal and professional contexts. |

****As a class watch [Ethics, Morality and the Law (5:13)](https://www.youtube.com/watch?v=Xki2fRA0bY8) and facilitate a teacher-led class discussion.

****As a class watch [What is privacy? (1:21)](https://www.youtube.com/watch?v=wmCE_CkV58I).

**Activity 70:** describe the *Privacy Act 1988* and its role in protecting the privacy of individuals.

|  |
| --- |
| **Sample answer:**The *Privacy Act 1988* in Australia is a comprehensive legal framework designed to safeguard the privacy of individuals by regulating the collection, handling and disclosure of their personal information by organisations and government entities. The Act establishes principles for the fair and responsible handling of personal data, providing individuals with rights of access, correction and redress while promoting transparency and accountability in the management of personal information. |

**Activity 71:** ****describe the *Freedom of Information Act 1982* and its role in ensuring open, transparent and accountable government in relation to the handling of personal and non-personal information.

|  |
| --- |
| **Sample answer:**The *Freedom of Information Act 1982* in Australia promotes open, transparent and accountable government by providing individuals with the right to access government documents, including both personal and non-personal information, held by federal agencies. This legislation aims to enhance public scrutiny, facilitate informed decision-making, and foster a culture of transparency within government entities by allowing citizens to request and obtain information about government activities and decision-making processes. |

****As a class watch [Requesting access to your personal information (3:19)](https://www.youtube.com/watch?v=W8_Zl8f0hXc) and facilitate a teacher-led discussion on the role of the *NSW Privacy and Personal Information Protection Act 1998* (PPIP Act), *Freedom of Information Act 1989* (NSW) and the *Government Information (Public Access) Act 2009* (GIPA Act).

**Activity 72:** create a [mind map](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Browser?cache_id=ee9ac) to illustrate the operation of these laws to protect personal information.

**Activity 73:** ****explain how privacy and freedom of information laws are fundamental to building trust, transparency and accountability in decision-making between community, business and government agencies and the provision of services.

|  |
| --- |
| **Sample answer:**Privacy and freedom of information laws are fundamental in building trust among the community, business and government agencies by ensuring that individuals have control over their personal information and by fostering transparency and accountability in decision-making processes. These laws establish clear guidelines for responsible data handling, empower individuals with access rights and create a framework that encourages open communication, ultimately contributing to a more trustworthy and accountable relationship between stakeholders in the provision of services. |

**Activity 74:** outline federal and state laws and legislation associated with cybersecurity.

|  |
| --- |
| **Sample answers:*** *Cybercrime Act 2001*
* *Crimes Act 1914*
* *Customs Act 1901*
* *Commonwealth Criminal Code Act 1995*
* *Privacy Act 1988*
* *Security of Critical Infrastructure Act 2018*
* *Telecommunications and Other Legislation Amendment Act 2018* (TOLA Act)
* Telecommunications Sector Security Reforms
 |

**Activity 75:** outline federal and state departments or bodies tasked with upholding identified laws.

|  |
| --- |
| **Sample answers:*** Department of Home Affairs
* Attorney General’s Department
* Office of the Australian Information Commissioner
* Australian Signals Directorate (ASD)
* Australian Cyber Security Centre (ACSC)
* Critical Infrastructure Centre
 |

****As a class view the case study ‘[Jin and Bella – small business owners](https://www.police.vic.gov.au/cybercrime-strategy-2022-2027/cybercrime-case-studies)’.

**Activity 76:** discuss the impact of cybercrime on people’s lives.

|  |
| --- |
| **Sample answer:**Cybercrime can significantly impact people's lives by compromising personal and financial information, leading to identity theft, financial loss and emotional distress.The increasing frequency and sophistication of cyber attacks result in the need for strong cybersecurity measures to mitigate these risks and safeguard individuals from the far-reaching consequences of digital criminal activities. |

# Explain impacts of cybersecurity breaches on the individual, organisation and society

As a class view [The Australian Energy Sector Cyber Security Framework (AESCSF)](https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources).

The Australian Energy Sector Cyber Security Framework (AESCSF) has been developed through collaboration with industry and government stakeholders, including the Australian Energy Market Operator (AEMO), Australian Cyber Security Centre (ACSC), Cyber and Infrastructure Security Centre (CISC) and representatives from Australian energy organisations.

The AESCSF is a set of guidelines and recommendations to enhance the cybersecurity practices and resilience of organisations operating in the Australian energy sector. The AESCSF is designed to help energy sector entities, including electricity generators, distributors and utilities, improve their cybersecurity posture and protect critical infrastructure from cyber threats.

Key features of the AESCSF include:

**Risk management:** the framework emphasises the importance of identifying and mitigating cybersecurity risks through risk assessments and risk management practices tailored to the energy sector's specific needs.

**Security controls:** it provides a set of security controls and guidelines to protect critical assets and infrastructure, focusing on measures like access controls, network security, incident response, and employee training.

**Information sharing:** the AESCSF encourages information sharing and collaboration among organisations within the energy sector to strengthen collective cybersecurity defences.

**Compliance:** it aligns with various national and international cybersecurity standards, regulations and best practices, ensuring that organisations adhere to relevant compliance requirements.

**Continuous improvement:** the framework promotes a culture of continuous improvement by encouraging organisations to assess their cybersecurity maturity, set improvement goals and monitor progress.

**Incident response:** it provides guidance on developing robust incident response plans to effectively respond to and recover from cyber incidents.

**Supply chain security:** the AESCSF addresses supply chain security, emphasising the need to secure the technology and services provided by third-party vendors.

## Financial loss

**Individual:** individuals can suffer direct financial losses in the aftermath of a cyber breach, such as unauthorised credit card charges, theft of personal funds or identity theft leading to fraudulent transactions.

**Organisation:** organisations may face significant financial losses due to costs associated with breach response, including incident investigation, system repairs, legal fees and potential regulatory fines. Additionally, they may lose revenue due to downtime, customer churn or damage to business relationships.

**Society:** in the broader societal context, financial losses can accumulate on a large scale. This can affect the economy as a whole when multiple organisations experience cyber breaches, leading to decreased investor confidence and reduced economic growth.

## Reputational damage

**Individual:** while individuals may not have a ‘reputation’ in the corporate sense, they can still suffer reputational damage if their personal information is exposed or misused, leading to a loss of trust in online services or brands.

**Organisation:** reputational damage is a significant consequence of breaches. When a company's data security is compromised, it can result in a loss of customer trust and confidence. This can lead to reduced customer loyalty, negative media coverage and a tarnished brand image.

**Society:** a widespread loss of trust in online services and institutions can erode societal confidence in the digital economy, impacting how individuals and businesses conduct their affairs online and potentially hindering innovation and growth.

## Operational disruptions

**Individual:** cyber breaches can lead to personal disruptions, such as identity theft, the loss of digital assets and inconvenience associated with recovering compromised accounts or information.

**Organisation:** operational disruptions, including system downtime, data loss and compromised critical infrastructure, can significantly impact an organisation's ability to conduct business efficiently. This can result in lost productivity and delays in delivering products or services.

**Society:** widespread operational disruptions can affect critical infrastructure sectors (for example energy, healthcare, transportation) and disrupt public services, potentially leading to safety concerns and hindrances to daily life.

## Legal and regulatory ramifications

**Individual:** individuals may have legal recourse against organisations that fail to protect their personal data. Data breach victims can potentially file lawsuits for damages or seek compensation for the misuse of their data.

**Organisation:** organisations that suffer data breaches can face legal actions, regulatory fines and penalties for non-compliance with data protection laws. Compliance failures can also lead to further audits and scrutiny.

**Society:** legal and regulatory actions against organisations that experience breaches help reinforce the importance of cybersecurity and data protection. They set precedents and encourage businesses to take cybersecurity more seriously, ultimately benefiting society by promoting better security practices.

**The Security of Critical Infrastructure Act 2018 or SOCI Act**

The *Security of Critical Infrastructure Act 2018* is a piece of legislation in Australia.

It was enacted to address the protection of critical infrastructure, particularly in the context of national security and cybersecurity. The Act provides a legal framework for the identification, management and protection of assets and systems that are deemed essential to the functioning of the nation and could be vulnerable to security risks, including cyber threats.

Some key provisions and objectives of the *Security of Critical Infrastructure Act 2018* in Australia include:

**Identification of critical infrastructure:** the Act outlines a process for identifying and designating specific assets and systems as ‘critical infrastructure’. This encompasses sectors such as energy, telecommunications, transportation and water.

**Security obligations:** it imposes security obligations on the owners and operators of critical infrastructure, including the requirement to report incidents and vulnerabilities that could compromise security.

**Collaboration:** the Act promotes collaboration between government agencies, owners and operators of critical infrastructure and law enforcement agencies to enhance the security and resilience of these assets.

**Government intervention:** in certain circumstances, the government can intervene to mitigate security risks and the Act provides for emergency powers to address significant threats.

**Penalties and enforcement:** the Act specifies penalties for non-compliance and outlines enforcement mechanisms to ensure adherence to security obligations.

****As a class view the [*Security of Critical Infrastructure Act 2018*](https://www.legislation.gov.au/Details/C2022C00160) which is part of the broader Australian Government’s efforts to strengthen the resilience and security of the nation's critical infrastructure. This Act is important in recognising the increasing need for cybersecurity in safeguarding key assets.

**Activity 77:** cyber operation against the power grid scenario (G)

As a class read [Cyber operation against the power grid](https://cyberlaw.ccdcoe.org/wiki/Scenario_03%3A_Cyber_operation_against_the_power_grid).

As a class examine the [facts](https://cyberlaw.ccdcoe.org/wiki/Scenario_03%3A_Cyber_operation_against_the_power_grid#Facts) of the scenario. As appropriate, outline the [legal analysis](https://cyberlaw.ccdcoe.org/wiki/Scenario_03%3A_Cyber_operation_against_the_power_grid#Legal_analysis) provided in the resource.

Discuss the provided facts of the scenario and determine agreed answers to the questions.

Did the operation result in actual physical damage or injury to individuals?

|  |
| --- |
| **Sample answer:**As a consequence of the operation, many households are left without electricity for days, resulting in significant inconvenience for the local residents as well as some economic damage to company X and other actors in State A’s territory, including the State itself. However, the power cuts are limited to residential areas and no physical damage or personal injury is reported from any of the affected areas. |

Were any individuals associated with an outside state physically present in the domestic state’s territory without the latter’s consent?

|  |
| --- |
| **Sample answer:**Once the computers are integrated in the ICS, the hackers are able to remotely monitor the activities in the technical control centre and to assume control over the infrastructure of company X without the staff knowing.Given the facts of the scenario, individuals from an outside State were not physically present. |

Did the operation occasion a loss of functionality of cyber infrastructure?

|  |
| --- |
| **Sample answer:**Cyber operations causing temporary, though significant loss of functionality could be characterised as violations of sovereignty. The operation was limited to physically non-destructive effects and its impact on the electrical distribution grid was fully reversible. A State organ conducting cyber operations against a target State or entities, or persons located there while physically present in the target State's territory, violates the target State's sovereignty.Causation of a loss of functionality of cyber infrastructure constitutes ‘damage’ and thus a breach of sovereignty; no consensus has been achieved on the precise threshold for a loss of functionality. |

**Activity 78:** ransomware scenario (H)

As a class read the [Ransomware campaign](https://cyberlaw.ccdcoe.org/wiki/Scenario_14%3A_Ransomware_campaign) scenario. Examine the [facts](https://cyberlaw.ccdcoe.org/wiki/Scenario_14%3A_Ransomware_campaign#Facts) of the scenario.

As appropriate, outline the [legal analysis](https://cyberlaw.ccdcoe.org/wiki/Scenario_14%3A_Ransomware_campaign#Legal_analysis) provided in the resource.

****Discuss the provided facts of the scenario and determine agreed answers to the questions.

Can the ransomware attacks be attributed?

|  |
| --- |
| **Sample answer:**Legal attribution is one of the elements of an international wrongful act and consists of the attachment ‘of a given action or omission to a State’. As a rule, the conduct of State organs is attributable to the State in question; by contrast, the conduct of non-State actors or third States’ organs can only be attributed to the State under specific circumstances. |

****Are the authors of the ransomware attack state organs or non-state organs exercising governmental authority?

|  |
| --- |
| **Sample answer:**It is not clear that the hackers are a State organ of State B, nor that they are exercising governmental authority on behalf of State B. There is no evidence to suggest that the hackers were operating under the instructions or effective control of State B. Likewise, there is insufficient evidence to indicate that State B adequately acknowledged and adopted the behaviour of the hackers as its own. |

****Is the ransomware a use of force?

|  |
| --- |
| **Sample answer:**It is unlikely that the ransomware attacks amount to a use of force. Crucially, the ransomware attacks’ overall severity was significant. While the disruption in municipal functions caused only inconvenience for citizens and municipal agencies, the harm that resulted from the disruption to medical services was significant.The consequences of the ransomware attacks did not follow immediately from the cyber activities. There is no indication that the attacks had a military character. The reconnaissance and network probing activities of the hackers were qualitatively similar to espionage activities, which are not per se regulated under international law and thus not presumptively judged to be uses of force. Severity is subject to a *de minimis* rule. It is likely that the severity of the ransomware attacks was not sufficient to meet that de minimis. |

# Explore current and emerging cybercrime threats to an enterprise

Cybercrime threats to enterprises are constantly evolving as threat actors become more sophisticated and innovative. Here are some current and emerging cybercrime threats that organisations need to be aware of:

**Ransomware attacks**

Ransomware continues to be a significant threat. Attackers encrypt an organisation's data and demand a ransom for decryption. Recent trends show that ransomware groups are increasingly targeting high-profile organisations, conducting double-extortion attacks (stealing data before encrypting it) and demanding larger ransoms.

**Supply chain attacks**

Cybercriminals are targeting the supply chain to compromise software and hardware before it reaches the enterprise. This includes software supply chain attacks like SolarWinds and hardware-level attacks on components.

**Zero-day exploits**

Attackers are exploiting previously unknown vulnerabilities (zero-days) to gain access to systems and data. These exploits are valuable on the dark web and cybercriminals often use them before security patches are available.

**Business Email Compromise (BEC)**

BEC attacks involve spoofing or compromising email accounts to trick employees into making financial transfers or divulging sensitive information. These attacks are highly targeted and often difficult to detect.

**Cloud security threats**

As more organisations migrate to the cloud, attackers are focusing on cloud-based infrastructure. Misconfigured cloud resources, insecure APIs and poor access controls are common vulnerabilities.

**Phishing and social engineering**

Phishing remains a prevalent threat. Cybercriminals are using more sophisticated and convincing phishing tactics to trick employees into revealing sensitive information or executing malicious code.

**IoT and OT attacks**

Internet of Things (IoT) and Operational Technology (OT) devices are often vulnerable and targeted by attackers. These devices can be used as entry points into corporate networks or disrupted to cause operational failures.

**AI and machine learning attacks**

Attackers are using artificial intelligence and machine learning to enhance their tactics, such as crafting more convincing deepfake videos for social engineering attacks or automated, intelligent malware.

**Deepfake threats**

Deepfake technology is being used to manipulate video and audio content for fraudulent purposes, including impersonating executives for financial scams or spreading disinformation.

**Cyber-physical attacks**

Cyber-physical attacks target critical infrastructure, such as power grids, water supply systems and transportation networks. These attacks can have severe real-world consequences.

**Emerging technologies threats**

****As new technologies like 5G, quantum computing and blockchain evolve, new security threats may arise. Quantum computing, for example, could potentially break current encryption standards.

**Activity 79:** outline the impact of recently developed and emerging technologies on cybersecurity challenges.

Cloud computing

|  |
| --- |
| **Sample answer:**The widespread adoption of cloud computing introduces both opportunities and challenges to cybersecurity, as centralised management enhances security measures but shared environments, third-party dependencies and evolving technologies demand continuous adaptation to address emerging threats. |

Hybrid workforce

|  |
| --- |
| **Sample answer:**The hybrid workforce model, combining remote and on-site work, presents new cybersecurity challenges by expanding the attack surface, requiring robust measures to secure both traditional and remote endpoints and necessitating enhanced vigilance against evolving threats in diverse work environments. |

Virtualisation

|  |
| --- |
| **Sample answer:**Virtualisation introduces cybersecurity challenges by expanding the attack surface, creating new vulnerabilities in virtualised environments and requiring specialised security measures to mitigate risks associated with hypervisors and inter-VM communication. |

Internet of things (IoT)

|  |
| --- |
| **Sample answer:**The proliferation of Internet of Things (IoT) devices introduces extensive cybersecurity challenges, including concerns about data privacy, insufficient device security measures and the potential for widespread network vulnerabilities, necessitating robust strategies to address the evolving threats in this interconnected landscape. |

Embedded systems, such as autonomous cars.

|  |
| --- |
| **Sample answer:**The advent of autonomous cars amplifies cybersecurity challenges as the integration of complex software and connectivity features increases the risk of cyber attacks, emphasising the need for stringent measures to secure vehicular systems and protect passenger safety. |

**Activity 80:** outline emerging innovative cybersecurity solutions in the space below.

Behaviour analytics

|  |
| --- |
| **Sample answer:**Behaviour analytics is an emerging and innovative cybersecurity solution that leverages advanced analytics and machine learning to proactively identify and mitigate security threats by analysing patterns of user behaviour, offering a dynamic and adaptive approach to cybersecurity defence. |

Blockchain technology

|  |
| --- |
| **Sample answer:**Blockchain technology is an emerging and innovative cybersecurity solution that provides a decentralised and tamper-resistant ledger, enhancing data integrity, transparency and authentication across digital transactions, thereby minimising various cyber threats. |

Deep learning

|  |
| --- |
| **Sample answer:**Deep learning, as an emerging and innovative cybersecurity solution, utilises neural networks and advanced algorithms to analyse vast datasets, enabling the detection of complex patterns and anomalies, thus enhancing threat detection and response capabilities in the evolving landscape of cybersecurity. |

Hardware authentication

|  |
| --- |
| **Sample answer:**Hardware authentication is an emerging and innovative cybersecurity solution that leverages physical devices such as security tokens or biometric sensors to enhance identity verification and access control, providing an extra layer of protection against unauthorised access and cyber threats. |

Quantum cryptography

|  |
| --- |
| **Sample answer:**Quantum cryptography is an emerging and innovative cybersecurity solution that leverages the principles of quantum mechanics to secure communication channels. It offers theoretically unbreakable encryption using quantum key distribution, thereby addressing the challenges posed by classical cryptographic methods in the face of quantum computing advancements. |

**Activity 81:** as a class discuss the impact or potential impact of recently developed and emerging technologies on cybersecurity challenges.

To cover a wider range of technologies, as a class [brainstorm](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/542#.ZC4skSv0RLg.link) using strategies like [Think-Pair-Share](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/645#.ZCFIk74Z-24.link) and bring ideas back to the larger group.

# Investigate cybercrime threats to an enterprise

A well-rounded cyber risk management strategy combines proactive measures for risk identification and vulnerability management with reactive measures for incident response and damage control. It's important to note that cybersecurity is an ever-evolving field, and organisations should adapt their strategies and training programs to keep up with emerging threats and vulnerabilities. Regular risk assessments and ongoing training are key components of a resilient cybersecurity posture.

## Implementing a cybersecurity strategy with ongoing training

**Strategy development:** effective cyber risk management begins with the development of a robust cybersecurity strategy. This strategy should encompass goals, priorities and a roadmap for protecting digital assets and data.

**Ongoing training:** employees are often the first line of defence against cyber threats. Regular training and awareness programs help them recognise and respond to potential risks. Training should cover topics like safe online practices, recognising phishing attempts and understanding the organisation's cybersecurity policies.

## Identifying and managing vulnerabilities

**Risk assessment:** organisations must regularly assess their systems and networks to identify vulnerabilities. This includes vulnerability scanning, penetration testing and vulnerability management.

**Patch management:** after identifying vulnerabilities, it is crucial to promptly apply security patches and updates to mitigate known risks. Establish a process for tracking and applying patches to all systems.

## Assessing the impact of a breach

**Incident response plan:** part of risk management involves preparing for the possibility of a breach. Develop an incident response plan that outlines the steps to take in the event of a cybersecurity incident. This plan includes roles and responsibilities, communication protocols and legal compliance considerations.

**Impact assessment:** in the event of a breach, assess its impact on the organisation. This involves understanding the extent of data exposure, financial losses, operational disruptions and reputational damage.

## Controlling damage and loss

**Mitigation measures:** implement measures to control damage and limit further losses during and after a breach. This includes isolating affected systems, stopping unauthorised access and removing malware.

**Communication:** maintain clear and open communication with affected parties, including customers, employees and regulatory bodies. Timely and transparent communication can help manage reputational damage.

**Activity 82:** capture the flag (CTF)

Present benefits of typical capture the flag (CTF) events and activities, for example:

* learning
* creative problem-solving
* legally practising cybersecurity skills
* identifying talent.

Demonstrate how to solve some CTF type problems.

Complete some practice activities/challenges.

Research and document solutions to problems in the space below.

|  |
| --- |
| **Sample answer:**An example of a solution could be describing the strategy of examining source code of the target web page to search for vulnerabilities like misconfigurations and comments that unintentionally reveal security issues. |

Ensure access to suitable technology, for example:

* computer lab
* laptop trolley
* online platforms.

Demonstrate how to connect to the relevant challenge.

Facilitate self-directed learning and monitor the progress of individuals and/or groups of students.

Provide guidance to assist students with challenging tasks and/or suggest strategies and techniques to solve questions.

**Teacher note:** students may be provided with the comprehensive set of resources from [The Grok Academy – Schools Cyber Security Challenges](https://groklearning.com/a/cyber/). There are a range of activities that can assist students in understanding cybersecurity concepts and to inform students of career opportunities in the field.

# References

This resource contains NSW Curriculum and syllabus content. The NSW Curriculum is developed by the NSW Education Standards Authority. This content is prepared by NESA for and on behalf of the Crown in right of the State of New South Wales. The material is protected by Crown copyright.

Please refer to the NESA Copyright Disclaimer for more information <https://educationstandards.nsw.edu.au/wps/portal/nesa/mini-footer/copyright>.

NESA holds the only official and up-to-date versions of the NSW Curriculum and syllabus documents. Please visit the NSW Education Standards Authority (NESA) website <https://educationstandards.nsw.edu.au> and the NSW Curriculum website <https://curriculum.nsw.edu.au>.

[Enterprise Computing 11–12 Syllabus](https://curriculum.nsw.edu.au/learning-areas/tas/enterprise-computing-11-12-2022/overview) © NSW Education Standards Authority (NESA) for and on behalf of the Crown in right of the State of New South Wales, 2022.

Appuhamy R (9 June 2018) ‘[Risk and How to use a Risk Matrix [video]](https://youtu.be/-E-jfcoR2W0?si=FD-heaISpnZx3Q3Z)’, *Let’s Learn Public Health*, YouTube, accessed 30 January 2024.

Ashcraft A, Sharkey K, Coulter D, Batchelor D, Satran, M (8 January 2021) ‘[Asymmetric Keys](https://learn.microsoft.com/en-us/windows/win32/seccrypto/public-private-key-pairs)’, Microsoft Learn website, accessed 31 January 2024.

Australian Energy Market Operator (2022) ‘[AESCSF framework and resources](https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources)’, *Cyber Security,* AEMO (Australian Energy Market Operator) website, accessed 30 January 2024.

Belcic I (19 December 2022) ‘[Password Ideas: How to Create a Strong Password](https://www.avg.com/en/signal/how-to-create-a-strong-password-that-you-wont-forget)’, *AVG Signal*, accessed 30 January 2024.

Bock L (4 January 2021) '[Diving into hash algorithms](https://www.linkedin.com/learning-login/share?forceAccount=false&redirect=https%3A%2F%2Fwww.linkedin.com%2Flearning%2Flearning-cryptography-and-network-security-2%2Fdiving-into-hash-algorithms%3Ftrk%3Dshare_video_url%26shareId%3DsUwd%252BZ2NRNiv%252BWq%252FMIfMGA%253D%253D)’ [video], *Learning Cryptography and Network Security,* LinkedIn Learning, accessed 30 January 2024.

Bridges J (26 October 2016) ‘[Top 10 reasons to keep your personal information private](https://www.reputationdefender.com/blog/privacy/top-ten-reasons-keep-your-personal-information-private)’, *Norton: Reputation Defender*, accessed 30 January 2024.

CI-ISAC (n.d.) [*Collective Cyber Defence for Critical Infrastructure*](https://ci-isac.com.au/index.html) [website], accessed 30 January 2024.

Cifas (5 July 2016) ‘[Data to Go’ [video]](https://youtu.be/sq-0tjv4_BA?si=cxPVPBuKx1c9rBfL), *Cifas*, YouTube, accessed 30 January 2024.

Clover Infotech (30 August 2022) ['Role of Human Error in Cybersecurity' [video]](https://youtu.be/AYduljAMYxI?si=GvNx6_jT6iJM5u9x), Clover Infotech, YouTube, accessed 30 January 2024.

Colorado Department of Education (21 January 2020) [*Social Engineering Education*](https://www.cde.state.co.us/dataprivacyandsecurity/socialengineeringeducation), Colorado Department of Education website, accessed 30 January 2024.

Commonwealth of Australia (n.d.) [*Cyber and Infrastructure Security Centre*](https://www.cisc.gov.au/) [website], accessed 30 January 2024.

Commonwealth of Australia (19 January 2024) [*Security of Critical Infrastructure Act 2018* and superseded version](https://www.legislation.gov.au/C2018A00029/2022-04-02/text), Federal Register of Legislation website, accessed 30 January 2024.

Commonwealth of Australia (23 November 2023) [*Tips to protect your privacy*](https://www.oaic.gov.au/privacy/your-privacy-rights/ways-to-protect-your-privacy/tips-to-protect-your-privacy) The Office of the Australian Information Commissioner website, accessed 30 January 2024.

Commonwealth of Australia (4 August 2014) [‘What is privacy?’ [video]](https://youtu.be/wmCE_CkV58I?si=6FGUKt0BQfE7XghP), *OAICgov*, YouTube, accessed 30 January 2024.

Commonwealth of Australia (28 April 2022) [‘Requesting access to your personal information. Information for complainants [video]](https://youtu.be/W8_Zl8f0hXc?si=N2okBacdiRIVPx6Z), *OAICgov*, YouTube, accessed 30 January 2024.

CSA Singapore (February 2021) [*Guide To Conducting Cybersecurity Risk Assessment For Critical Information Infrastructure* (PDF 836 KB)](https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf), CSA Singapore website, accessed 30 January 2024.

Datum (n.d.) [*Data Calculator*](https://calc.datum.org/)*,* Datum website, accessed 30 January 2024.

DFIR Science (29 December 2016) ‘[Linux Intro: Signing and verifying data using GPG [video]](https://youtu.be/4bbyMEuTW7Y?si=HAKq0RWewW_Ch4_c)’, *DFIRScience,* YouTube, accessed 31 January 2024.

Dock Labs AG (8 December 2023) [*A Beginner’s Guide to Digital Signatures for Verifiable Credentials*](https://www.dock.io/post/digital-signatures), dock website, accessed 31 January 2024.

Faik H (10 October 2022) [*Swiss cheese Model for Cybersecurity*](https://www.linkedin.com/pulse/swiss-cheese-model-cybersecurity-hicham-faik/), LinkedIn website, accessed 31 January 2024.

Feel J, Piper G and Liddy M (28 March 2023) ‘[This is the most detailed portrait yet of data breaches in Australia](https://www.abc.net.au/news/2023-03-28/detailed-portrait-data-breaches-oaic-disclosures/102131586)’, *Story Lab – ABC NEWS*, accessed 30 January 2024.

Fraser-Knight E (4 July 2019) ‘[The Psychology of a Cyber Attack: USB Drop Simulation](https://www.assentriskmanagement.co.uk/the-psychology-of-a-cyber-attack-usb-drop-simulation/)’, *Assent*, accessed 30 January 2024.

Garcia M (4 October 2017) ‘[Easy Ways to Build a Better P@$5w0rd](https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd)’, *National Institute of Standards and Technology (U.S. Department of Commerce)*, accessed 30 January 2024.

Gjaere E A (31 July 2017) ‘[Human Errors in Cyber Security — A Swiss Cheese of Failures](https://securityandpeople.com/2017/07/human-errors-in-cyber-security-a-swiss-cheese-of-failures/)’, *Security and People blog*, accessed 31 January 2024.

Grok Academy Limited (n.d.) [*Schools Cyber Security Challenges*](https://groklearning.com/a/cyber/), Grok learning website, accessed 30 January 2024.

Hadnagy C (25 August 2018) ['How phishing scammers manipulate your amygdala and oxytocin' [video]](https://youtu.be/9e6k_PtEXdM?si=GKKzi_TgnwoJiwhM), *TEDx Talks*, YouTube, accessed 30 January 2024.

Hunt T (n.d.) [*Have I been pwned?*](https://haveibeenpwned.com/), Superlative Enterprises Pty Ltd website, accessed 30 January 2024.

International cyber law: interactive toolkit contributors (3 February 2023) ‘[Scenario 03: Cyber operation against the power grid’](https://cyberlaw.ccdcoe.org/wiki/Scenario_03%3A_Cyber_operation_against_the_power_grid), *The Cyber Law Toolkit*, International cyber law: interactive toolkit website, accessed 30 January 2024.

Invisibly (13 July 2021) ‘[How Much is Your Data Worth? The Complete Breakdown for 2024](https://www.invisibly.com/learn-blog/how-much-is-data-worth/)’, *Learn blog,* accessed 30 January 2024.

Kaduu (21 January 2020) ['Removable Media Security Video' [video]](https://youtu.be/OGbhLAaELmw?si=QSWw1ueAxyO0O9pg), *Kaduu – Dark Web Monitoring*, YouTube, accessed 30 January 2024.

Lachance D (21 February 2019) ['Cryptography Overview' [video]](https://www.linkedin.com/learning-login/share?forceAccount=false&redirect=https%3A%2F%2Fwww.linkedin.com%2Flearning%2Fssl-tls-for-beginners-securing-network-communications%2Fcryptography-overview%3Ftrk%3Dshare_video_url%26shareId%3D%252B%252Fw3FOtKQkqYlLjZSYAUDw%253D%253D), *SSL/TLS for Beginners: Securing Network Communications*, LinkedIn Learning, accessed 31 January 2024.

Lachance D (21 February 2019) ['Symmetric and asymmetric encrypting' [video]](https://www.linkedin.com/learning-login/share?forceAccount=false&redirect=https%3A%2F%2Fwww.linkedin.com%2Flearning%2Fssl-tls-for-beginners-securing-network-communications%2Fsymmetric-and-asymmetric-encrypting%3Ftrk%3Dshare_video_url%26shareId%3Dd61kAr8JRbGSG82xKxEuXg%253D%253D), *SSL/TLS for Beginners: Securing Network Communications*, LinkedIn Learning, accessed 31 January 2024.

Lengen S (11 July 2019) ‘[How much is your data worth to tech companies?](https://theconversation.com/how-much-is-your-data-worth-to-tech-companies-lawmakers-want-to-tell-you-but-its-not-that-easy-to-calculate-119716)’, *The Conversation*, accessed 30 January 2024.

Microsoft (n.d.) [*Digital signatures and certificates*](https://support.microsoft.com/en-au/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-22bd163e8e96), Microsoft Support website, accessed 31 January 2024.

Microsoft (n.d.) [*Obtain a digital certificate and create a digital signature*](https://support.microsoft.com/en-au/office/obtain-a-digital-certificate-and-create-a-digital-signature-e3d9d813-3305-4164-a820-2e063d86e512), Microsoft Support website, accessed 31 January 2024.

National Cyber Security Centre (n.d.) ['CyberFirst Navigators: How to stay secure online video' [video]](https://www.ncsc.gov.uk/training/cyberfirst/packages/en/index.html), National Cyber Security website, accessed 30 January 2024.

National Cyber Security Centre (7 October 2022) [*Cyber First: Lesson 1 Resource* [PDF 793 KB]](https://www.ncsc.gov.uk/static-assets/documents/cyberfirst-navigators/CyberFirst-Navigators-Lesson-1-resources.pdf), National Cyber Security Centre, accessed 30 January 2024.

National Cyber Security Centre (7 October 2022) [Cyber First: Lesson 2 Resource [PDF 778 KB]](https://www.ncsc.gov.uk/static-assets/documents/cyberfirst-navigators/CyberFirst-Navigators-Lesson-2-resources.pdf), National Cyber Security Centre, accessed 30 January 2024.

National Cyber Security Centre (7 October 2022) ‘[Three random words](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words)’, *Top tips for staying secure online*, National Cyber Security Centre, accessed 30 January 2024.

Neskey C (April 2018) ‘[Are Your Passwords in the Green?](https://www.hivesystems.io/blog/are-your-passwords-in-the-green)’, *Hive Systems*, accessed 30 January 2024.

OWASP Foundation, Inc (n.d.) ‘[SQL Injection](https://owasp.org/www-community/attacks/SQL_Injection)’, *OWASP Community Pages: Attacks*, OWASP website, accessed 31 January 2024.

OWASP Foundation, Inc (n.d.) [‘Testing for SQL Injection](https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection.html)’,*Input Validation Testing,*OWASP website, accessed 31 January 2024.

PortSwigger (22 May 2020) [What is SQL injection? [video]](https://youtu.be/wX6tszfgYp4?si=cUTJHTpbQHDDN182), *Web Security Academy*, YouTube accessed 30 January 2024.

Privacy International (12 May 2015) ['What Is Privacy?' [video]](https://youtu.be/zsboDBMq6vo?si=12jzUQzXoz97WSib), *Privacy International*, YouTube, accessed 30 January 2024.

SANS Institute (19 March 2020) ['Detecting and Defending Social Engineering Attacks' [video]](https://youtu.be/IQL8kaBReDQ?si=hqGXwnvGNrzfFNzQ), *SANS Institute*, YouTube, accessed 30 January 2024.

SANS Offensive Operations (20 March 2020) ['SANS Security Awareness: Email and Phishing' [video]](https://youtu.be/sEMrBKmUTPE?si=m68cMMHQn6q5w-xB), *Sans Offensive Operations*, YouTube, accessed 30 January 2024.

Security Innovation (12 July 2018) ['Everything You Need to Know About Insider Threats... In 2 Minutes' [video]](https://youtu.be/QXnNkSeT6dM?si=jZYtbdpjjaW75ZpM), *Security Innovation*, YouTube, accessed 31 January 2024.

State Government of Victoria (30 March 2023) ‘[Cybercrime case studies](https://www.police.vic.gov.au/cybercrime-strategy-2022-2027/cybercrime-case-studies)’, *Cybercrime Strategy 2022–2027*, Victoria Police website, accessed 31 January 2024.

StaySafeOnline (30 June 2020) ['Security Awareness Episode 5: Removable Media' [video]](https://youtu.be/FRxrHduwPjY?si=EwDvk_SBVwFZkGbi), *StaySafeOnline.org*, YouTube, accessed 30 January 2024.

Stein L (31 October 2023) ‘[What your data is actually worth](https://www.datapods.app/blogs/what-your-data-is-actually-worth)’, *Datapods*, accessed 30 January 2024.

The Ethics Centre (15 April 2020) ['What is the difference between Ethics, Morality and the Law?' [video]](https://youtu.be/Xki2fRA0bY8?si=gRDwwrLGpmJGc127), *The Ethics* Centre, YouTube, accessed 30 January 2024.

The Gurus (29 November 2016) ‘[The Year of the Data Integrity Breach](https://www.itsecurityguru.org/2016/11/29/2017-year-data-integrity-breach/)’, IT Security Guru Editor’s news, accessed 30 January 2024.

The Open Worldwide Application Security Project (OWASP) Top 10 team (2021) [*Injection*](https://owasp.org/Top10/A03_2021-Injection/), OWASP website, accessed 31 January 2024.

Webber Insurance Services (2022) [*The Complete List of Data Breaches in Australia for 2018–2024*](https://www.webberinsurance.com.au/data-breaches-list), Webber Insurance Services website, accessed 31 January 2024.

Wikipedia: The Free Encyclopedia (20 October 2017) [*File:IC-Risk-Assessment-Matrix-Template.jpg*](https://en.wikipedia.org/wiki/File%3AIC-Risk-Assessment-Matrix-Template.jpg), Wikipedia website, accessed 30 January 2024.

**© State of New South Wales (Department of Education), 2024**

The copyright material published in this resource is subject to the Copyright Act 1968 (Cth) and is owned by the NSW Department of Education or, where indicated, by a party other than the NSW Department of Education (third-party material).

Copyright material available in this resource and owned by the NSW Department of Education is licensed under a [Creative Commons Attribution 4.0 International (CC BY 4.0) license](https://creativecommons.org/licenses/by/4.0/).



This license allows you to share and adapt the material for any purpose, even commercially.

Attribution should be given to © State of New South Wales (Department of Education), 2024.

Material in this resource not available under a Creative Commons license:

* the NSW Department of Education logo, other logos and trademark-protected material
* material owned by a third party that has been reproduced with permission. You will need to obtain permission from the third party to reuse its material.

**Links to third-party material and websites**

Please note that the provided (reading/viewing material/list/links/texts) are a suggestion only and implies no endorsement, by the New South Wales Department of Education, of any author, publisher, or book title. School principals and teachers are best placed to assess the suitability of resources that would complement the curriculum and reflect the needs and interests of their students.

If you use the links provided in this document to access a third-party's website, you acknowledge that the terms of use, including licence terms set out on the third-party's website apply to the use which may be made of the materials on that third-party website or where permitted by the Copyright Act 1968 (Cth). The department accepts no responsibility for content on third-party websites.