Enterprise Computing Stage 6 (Year 11) – sample program of learning

Principles of cybersecurity

Contents

[About this resource 3](#_Toc158974585)

[Purpose of resource 3](#_Toc158974586)

[Target audience 3](#_Toc158974587)

[When and how to use 3](#_Toc158974588)

[Rationale 4](#_Toc158974589)

[Overview 5](#_Toc158974590)

[Outcomes 6](#_Toc158974591)

[Lesson sequence and details 8](#_Toc158974592)

[Week 1 8](#_Toc158974593)

[Weeks 2 and 3 19](#_Toc158974594)

[Week 4 29](#_Toc158974595)

[Week 5 41](#_Toc158974596)

[Week 6 51](#_Toc158974597)

[Week 7 60](#_Toc158974598)

[Week 8 66](#_Toc158974599)

[Week 9 73](#_Toc158974600)

[Week 10 81](#_Toc158974601)

[Overall program evaluation 87](#_Toc158974602)

[Capturing student voice when evaluating a program 87](#_Toc158974603)

[Additional information 89](#_Toc158974604)

[Further implementation support 89](#_Toc158974605)

[Assessment for learning 89](#_Toc158974606)

[Differentiation 90](#_Toc158974607)

[Support and alignment 91](#_Toc158974608)

[Evidence base 93](#_Toc158974609)

[References 95](#_Toc158974610)

# About this resource

## Purpose of resource

The resource is a sample program of learning for teaching Principles of cybersecurity in Year 11 during the Enterprise Computing 11–12 course.

## Target audience

This resource can be used by schoolteachers to support effective syllabus implementation of Enterprise Computing 11–12.

## When and how to use

This resource is designed for implementing 10 weeks or a term of learning on the Principles of cybersecurity. The resource can be adapted and contextualised to the school setting. Adjustments can be made to the program of learning to suit students in the teaching and learning cycle.

# Rationale

The NSW Department of Education publishes a range of curriculum support materials, including samples of lesson sequences, scope and sequences, assessment tasks, examinations, student and teacher resource booklets, and curriculum planning and curriculum evaluation templates. The samples are not exhaustive and do not represent the only way to complete or engage in each of these processes. Curriculum design and implementation is a dynamic and contextually-specific process. While the mandatory components of syllabus implementation must be met by all schools, it is important that the approach taken by teachers is reflective of their needs and faculty or school processes.

NESA defines [programming](https://educationstandards.nsw.edu.au/wps/portal/nesa/k-10/understanding-the-curriculum/programming) as the process of ‘selecting and sequencing learning experiences which enable students to engage with syllabus outcomes and develop subject specific skills and knowledge’ (NESA 2022). A program is developed collaboratively within a faculty. It differs from a unit in important ways, as outlined by NESA on their [Advice on units](https://educationstandards.nsw.edu.au/wps/portal/nesa/k-10/understanding-the-curriculum/programming/advice-on-units) page. A unit is a contextually-specific plan for the intended teaching and learning for a particular class for a particular period. The organisation of the content in a unit is flexible and it may vary according to the school, the teacher, the class and the learning space. They should be working documents that reflect the thoughtful planning and reflection that takes place during the teaching and learning cycle. There are mandatory components of programming and unit development, and this template provides one option for the delivery of these requirements. The NESA and department guidelines that have influenced this template are elaborated upon at the end of the document.

This resource has been developed to assist teachers in NSW Department of Education schools to create learning that is contextualised to their classroom. It can be used as a basis for the teacher’s own program, assessment, or scope and sequence, or be used as an example of how the new curriculum could be implemented. The resource has suggested timeframes that may need to be adjusted by the teacher to meet the needs of their students.

# Overview

**Description**: this program of learning 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 while 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.

**Duration**: this program of learning is designed to be completed over a period of approximately 10 weeks in 60-minute lesson sequences but can be adapted to suit the school context.

**Explicit teaching**: suggested learning intentions and success criteria are available for some lessons provided. Learning intentions and success criteria are most effective when they are contextualised to meet the needs of students in the class. The examples provided in this document are generalised to demonstrate how learning intentions and success criteria could be created.

# Outcomes

A student:

* describes how systems are used in a range of enterprises **EC-11-01**
* describes how data is safely and securely collected, stored and manipulated when developing enterprise computing systems **EC-11-03**
* describes how data is used in enterprise computing systems **EC-11-04**
* explains how innovative technologies have influenced enterprise computing systems **EC-11-06**
* explores the social, ethical and legal implications of the application of enterprise computing systems on the individual, society and the environment **EC-11-07**
* documents the management and evaluates the development of an enterprise solution **EC-11-09**

[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.

**Prior to planning for teaching and learning, please consider the following**:

**Engagement**

* How will I provide authentic, relevant learning opportunities for students to personally connect with lesson content?
* How will I support every student to grow in independence, confidence and self-regulation?
* How will I facilitate every student to have high expectations for themselves?
* How will I identify and provide the support each student needs to sustain their learning efforts?

**Representation**

* What are some different ways I can present content to enable every student to access and understand it?
* How will I identify and address language and/or cultural considerations that may limit access to content for students?
* How will I make lesson content and learning materials more accessible?
* How will I plan learning experiences that are relevant and challenging for the full range of students in the classroom?

**Expression**

* How will I provide multiple ways for students to respond and express what they know?
* What tools and resources can students use to demonstrate their understanding?
* How will I know every student has understood the concepts and language presented in each lesson?
* How will I monitor if every student has achieved the learning outcomes and learning growth?

# Lesson sequence and details

## Week 1

Table – lesson sequence and details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Outcomes and content | Teaching and learning activities | Evidence of learning | Differentiation and adjustments | Registration and evaluation notes |
| **Outcome**  **EC-11-07**  **Content**  Students:   * explore security vulnerabilities of social networking to both an individual and an enterprise   Including:   * account access * account behaviour * hosting platform security * identity theft * phishing. | **Learning intention**  Establish a pattern of thinking to analyse scenarios, ascertain facts, consider risks and make decisions.  **Success criteria**   * I can assess the risks to personal information online and know how to protect personal information. * I can keep accounts and devices safe, and know what to do if security is breached.   **Teaching and learning activities**  **Teacher**  Introduce the topic ‘principles of cybersecurity’ and outline the sequence of activities.  State the intent of activities is to analyse scenarios, ascertain facts, consider risks and make decisions.  Present social networking scenario and demonstrate how to interact with the [CyberFirst Navigators interactive video (0:30)](https://www.ncsc.gov.uk/training/cyberfirst/packages/en/index.html) noting the importance of recording decisions made (both actions and inaction).  **Students**  Students individually interact with and explore the [CyberFirst Navigators interactive video (0:30)](https://www.ncsc.gov.uk/training/cyberfirst/packages/en/index.html).  **Activity 1**: record decisions made (path taken) at each stage of the interactive video.  Record any additional relevant observations of actions by the characters.  **Teacher and students**  Identify actions (or inaction) that could be considered a risk.  **Students**  **Activity 2**: risks and consequences  Sort and match the risks taken by characters and the consequences.  **Teacher and students**  Discuss whether there is a best path through the interactive video storyline.  Identify the better option at each decision point. Through consensus, decide the best path through the scenario. | Students demonstrate making factual observations from the video scenes.  Students can identify characters’ actions that could be considered cybersecurity risks.  Consequences are correctly matched to identified security risks.  Students can assess 2 options presented in each scene and select the safer option. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  Teach key vocabulary and concepts prior to viewing videos, provide a transcript and use closed captions when viewing.  In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  Include multiple opportunities to respond and discuss, for example:   * verbally * individually * partner turn and talk * non-verbally * gesture * response cards. |  |
| **Content**  Students:   * investigate how an individual can contribute to maintaining the privacy of their own data | **Teaching and learning activities**  **Teacher**  Gather student feedback about what the term ‘social engineering’ might mean.  **Students**  Consider different ways that a hacker might use obtained information, for example:   * email account * social media account details * personal data.   **Activity 3**: What is social engineering?  **Activity 4**: identify which definitions are types of social engineering.  **Activity 5**: identify which examples of social engineering were experienced by characters in the film.  **Teacher**  Define personal information as stated in the Privacy Act 1988.  **Students**  **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).  **Activity 7**: cyber aware behaviours  Using the [6 behaviours (PDF 793 KB)](https://www.ncsc.gov.uk/static-assets/documents/cyberfirst-navigators/CyberFirst-Navigators-Lesson-1-resources.pdf), explain how these behaviours could have kept the characters’ personal information safe. | Students complete the ‘social engineering’ activity and are able to identify some forms of social engineering.  Students will be able to recall a usable and correct definition of personal information.  Students can:   * identify a range of cybersecurity risks and threats * explain how activities online might be subject to cyber threats * demonstrate ways to protect personal information to reduce the risk of being hacked. | Message abundancy may be useful when introducing new terminology. The word is spoken, written on the board and represented by visuals. |  |
| **Content**  Students:   * investigate how an individual can contribute to maintaining the privacy of their own data | **Teaching and learning activities**  **Teacher**  Ask students to recall the 6 Cyber Aware behaviours’ discussed last lesson.  **Students**  **Activity 8**: film scenes matching task  For the 6 scenes, use numbers to label ‘[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.  **Activity 9**: decide what actions can be taken to improve security of the characters’ data. | Students can recognise the 6 Cyber Aware behaviours and how applying these behaviours can improve the security of the character’s personal information (and their own personal information).  Students can explain the different ways to keep accounts and devices safe and demonstrate the skills needed to do so. | In creating or selecting scenarios, consider students’ own experiences and use of visuals.  **Extension**  Students consider which of the ways to protect accounts is the easiest and/or most effective, by ordering the 6 behaviours and explaining their decisions.  (Emphasise that all 6 behaviours covered are important and the more someone uses the behaviours, the safer their accounts and personal information are.) |  |
| **Content**  Students:   * research hardware and software strategies used to protect data   Including:   * password protection, encryption and permissions | **Teaching and learning activities**  **Teacher and students**  Referencing the scenario video, discuss examples of weak passwords.  **Activity 10**: discuss why ‘LiverpoolFC04’ is not a good password.  **Teacher**  **Activity 11:** describe how passwords are discovered.  Demonstrate the time required to hack a password of varying lengths and complexity, and show [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 [Have I Been Pwned](https://haveibeenpwned.com/).  **Teacher and students**  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.   **Teacher**  Demonstrate [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).  **Students**  Use strategies to generate a strong password.  **Teacher**  **Activity 12**: outline new strategies and technologies being developed to replace passwords.  **Teacher and students (optional)**  As a class discuss ‘How important are strong passwords?’ | Students can recognise the difference between weak and strong passwords.  Students will be able to generate a strong password.  Students can describe human behaviour that leads to insecure practices when creating and using passwords.  Students can determine if their username/password has been part of a data breach (pwned). | In creating or selecting scenarios, consider students’ own experiences and use of visuals. |  |
| **Content**  Students:   * investigate cybercrime threats to an enterprise   Including:   * employee action causing a vulnerability | **Teaching and learning activities**  **Teacher and students**  **Activity 13**: identify the cause(s) of the breach(es) in scenario (A) and categorise this as either a technical error or human error.  **Teacher**  **Activity 14**: summarise key aspects of the incident in scenario (A), including:   * risks * password hygiene * indicators of compromise.   **Students**  **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. | Students can identify causes of the breach(es) and correctly categorise as either technical errors or human errors.  Students recognise potential indicators of compromise from initial observations of change in account access and account behaviour.  Student explanations of security vulnerabilities demonstrate some technical understanding of account access and typical account behaviour.  Student explanations indicate how security vulnerabilities exist within social networking and how this potentially impacts the individual.  Students are able to explain how individuals can contribute to maintaining the privacy of their own data. |  |  |

## Weeks 2 and 3

Table – lesson sequence and details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Outcomes and content | Teaching and learning activities | Evidence of learning | Differentiation and adjustments | Registration and evaluation notes |
| **Outcomes**  **EC-11-04**  **EC-11-07**  **Content**  Students:   * explain privacy, trust and freedom of information with respect to people, systems and data. | **Learning intention**  Understand the value of data and the need to protect it.  **Success criteria**   * I can develop my understanding of common cyber attacks, including motive and method (techniques and tactics). * I can recognise the risks, impact and importance of mitigating potential damage.   **Teaching and learning activities**  **Teacher**  Teacher-led discussion on privacy, trust and freedom of information with respect to people, systems and data.  **Teacher and students**  **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 (1:31)](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.  **Students**  **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.   Determine what is a fair price for their personal data.  **Teacher and students**  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)?’ | Students can demonstrate their understanding of the value of data within different contexts.  Students will be able to describe common cyber attacks.  Students can define and distinguish between.  Students will be assessing and making judgements on various types of data and be able to assign relative value to personal data.  Students will have increased understanding of the value of personal information to various organisations.  Students will be able to explain how data, like date of birth and private address, can be used for identity theft. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  Message abundancy may be useful when introducing new terminology. The word is spoken, written on the board and represented by visuals.  Review key concepts and vocabulary before viewing video. Use closed captions and provide the transcript. Pause video to assess student understanding at appropriate points. |  |
| **Content**  Students:   * explain privacy, trust and freedom of information with respect to people, systems and data * describe privacy and security principles associated with access, storage and permissions used by enterprises to collect and interpret data. | **Teaching and learning activities**  **Teacher**  **Activity 20:** review these terms and add to the glossary:   * confidentiality * disclosure * privacy * public information * personal information * personally identifiable information (PII) * trust.   **Activity 21**: identify who is responsible for maintaining privacy and maintaining confidentiality.  **Teacher and students**  **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)’  **Activity 23**: evaluate the consequences of a violation of privacy, confidentiality and trust.  **Activity 24**: define data breach and provide some examples for the following incidents:   * Data breach * Neopets * Optus * Medibank.   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 of details of reported breaches in the media compared to breach data provided by the OAIC (as disclosed by affected organisations).  **Students**  **Activity 26**: describe possible consequences of a data breach. | Students are able to explain where and how there is a violation of privacy within a given scenario.  Students demonstrate an understanding of the relationship between privacy, confidentiality and trust in explanations they provide.  Students can describe and assess a range of consequences where privacy and confidentiality have been violated and there is an abuse of trust. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  Message abundancy may be useful when introducing new terminology. The word is spoken, written on the board and represented by visuals.  Review key concepts and vocabulary before viewing video. Use closed captions and provide the transcript. Pause video to assess student understanding at appropriate points.  **Extension**  Critically analyse the story and discuss 2 of the main issues raised.  Examine the [Office of the Australian Information Commissioner (OAIC) dataset in spreadsheet format (XLSX 38 KB)](https://live-production.wcms.abc-cdn.net.au/4403113143e5b8e0c4acd2644019c2c5) linked in the report and create a simple plot diagram (or other data visualisation). |  |
| **Content**  Students:   * investigate cybercrime threats to an enterprise   Including:   * hacking * phishing, including smishing * scamming * bots and botnets * employee action causing a vulnerability. | **Teaching and learning activities**  **Teacher**  Teacher-led discussion on investigating cybercrime threats to an enterprise.  **Activity 27**: define and compare the terms below:   * targeted cyber attack * un-targeted cyber attack * cybercrime * cybersecurity breach * cybersecurity incident * cyber threat * exploit * vulnerability.   **Activity 28**: outline the goals of protecting information.  **Students**  **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.   **Activity 30**: research activity  As a class outline common cyber attacks and cybercrime threats.  Assign cyber threats or attacks to students to research during the unit for later class discussion in various scenario exercises.  **Students**  For 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.  **Teacher**  As a class watch [Hacked Medical Devices: The Most Dangerous Examples (4:01)](https://www.youtube.com/watch?v=m49OreAs1WY).  Teacher-led discussion on other dimensions of cyber attacks and their impact beyond data breaches. | Students understand terms used in cybercrime treats.  Students can outline the goals of protecting information.  Students can describe an example of a cybersecurity breach in terms of a compromise.  Students can describe the vulnerability that enables an attack to proceed and correctly suggests strategies to mitigate risk(s) and prevent a data breach. | Provide worksheet with key terms to assist with vocabulary building and knowledge acquisition. |  |

## Week 4

Table –lesson sequence and details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Outcomes and content | Teaching and learning activities | Evidence of learning | Differentiation and adjustments | Registration and evaluation notes |
| **Outcomes**  **EC-11-04**  **EC-11-09**  **Content**  Students:   * describe the attributes of a cybersecurity breach   Including:   * confidentiality of information * integrity of information * availability of information * privacy implications * investigate vulnerabilities exploited by the threat actor involved in a breach, such as the impact on various elements   Including:   * data * people * processes * technology * investigate cybercrime threats to an enterprise   Including:   * employee action causing a vulnerability * investigate cyber risk management   Including:   * implementing a cybersecurity strategy with ongoing training * identifying and managing vulnerabilities * assessing the impact of a breach * controlling damage and loss. | **Learning intention**  Understand how the science and psychology of social engineering can underpin a cybersecurity breach.  **Success criteria**   * I can describe the attributes of a cybersecurity breach. * I can investigate vulnerabilities exploited by the threat actor involved in a breach. * I can identify employee action causing a vulnerability. * I can investigate cyber risk management.   **Teaching and learning activities**  **Teacher**  **Teacher-led discussion on the attributes of a cybersecurity breach.**  **Activity 31**: define and compare these related terms:   * adversary * cybercriminal * threat actor * adversarial mindset.   **Activity 32**: password data breach scenario (B)  Introduce password data breach scenario (B) and assign required groups and roles. Refer to scenario notes in teacher support resource document to facilitate moving through stages of the scenario, revealing additional information and prompting questions as required.  **Students**  In groups, define the problem and identify relevant facts from provided scenario text.  In an iterative process, combine and apply additional information (released in stages from teacher) to the scenario body of knowledge.  Use critical thinking to evaluate the situation and consider potential risks.  Apply adversarial mindset to imagine actions that would align with indicators of compromise.  Prepare a group response to share with the class.  **Teacher and students**  Share group responses and collaborate to build a better understanding of this scenario event and work towards an agreed response to the question.  **Teacher**  Summarise lessons learned. | Students are able to explain where and how there is a violation of privacy within the given scenario.  Students can describe the attributes of a cybersecurity breach.  Students can investigate vulnerabilities exploited by the threat actor involved in a breach.  Students can identify employee action causing a vulnerability.  Students can investigate cyber risk management. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  Some students may need support to work in a group.  Provide options for students to share roles if necessary.  During practical learning activities, use and emphasise target language required and encourage students to use this language in context.  Provide scaffolds and templates of documents based on student needs and the desired level of student independence.  Provide worksheet with key terms to assist with vocabulary building and knowledge acquisition. |  |
| **Content**  Students:   * assess cyber risk by implementing risk-management strategies using a risk matrix   Including:   * internal and external vulnerabilities * threat landscape * impact of exposure * likelihood of exploitation. | **Teaching and learning activities**  **Teacher**  **Activity 33**: phishing data breach scenario (C)  Introduce phishing data breach scenario (C) and assign required groups and roles.  Refer to scenario notes and discussion questions in teacher resource document to facilitate moving through stages of the scenario, revealing additional information and prompting questions as required.  **Students**  In groups, define the problem and identify relevant facts from provided scenario text.  In an iterative process, combine and apply additional information (released in stages from teacher) to the scenario body of knowledge.  Use critical thinking to evaluate the situation and consider potential risks.  Apply adversarial mindset to imagine actions that would align with indicators of compromise.  Prepare a group response to share with the class.  **Teacher and students**  Share group responses and collaborate to build a better understanding of this scenario event and work towards an agreed response to the question.  **Teacher**  Summarise lessons learned. | Students are able to explain how phishing emails can affect an enterprise.  Students can describe the attributes of a cybersecurity breach.  Students can investigate vulnerabilities exploited by the threat actor involved in a breach.  Students can identify internal and external vulnerabilities in a scenario.  Students can identify the threat landscape in a scenario.  Students can identify the impact of exposure in the scenario.  Students can identify the likelihood of exploitation in the scenario.  Students can investigate cyber risk management. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  Some students may need support to work in a group.  Provide options for students to share roles if necessary.  During practical learning activities, use and emphasise target language required and encourage students to use this language in context.  Provide scaffolds and templates of documents based on student needs and the desired level of student independence. |  |
| **Content**  Students:   * investigate vulnerabilities exploited by the threat actor involved in a breach, such as the impact on various elements   Including:   * people * processes * investigate cybercrime threats to an enterprise   Including:   * phishing, including smishing * scamming * employee action causing a vulnerability. | **Teaching and learning activities**  **Teacher**  As a class watch [Detecting and defending social engineering attacks (4:28)](https://www.youtube.com/watch?v=IQL8kaBReDQ).  **Activity 34:** outline how Cialdini’s 6 Principles of Influence are used in social engineering:   * reciprocity * scarcity (sense of urgency) * authority * consistency * liking * consensus (social proof or bandwagon).   Outline the System 1 and System 2 thinking theory and how fast and slow thinking shape perception and choice.  Outline the concept of a psychological ‘hot-state’ which prevents rational decision making and promotes more (visceral) impulsive decisions.  Outline the ‘Spock versus Homer’ analogy in terms of rational decision making.  **Teacher and students**  As a class watch [How phishing scammers manipulate your amygdala and oxytocin (11:00)](https://www.youtube.com/watch?v=9e6k_PtEXdM).  **Students**  **Activity 35**: manipulating your amygdala and oxytocin  Identify 4 main vectors of social engineering discussed in the video.  Identify emotional triggers used in the recorded conversation.  Explain how a scammer manipulates the target’s thinking and impedes their capacity for critical thinking. | Students can identify the principles of influence.  Students can explain how the principles of persuasion are used for successful social engineering attacks. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  Some students may need support to work in a group.  Provide options for students to share roles if necessary.  During practical learning activities, use and emphasise target language required and encourage students to use this language in context.  Provide scaffolds and templates of documents based on student needs and the desired level of student independence.  Provide worksheet with key terms to assist with vocabulary building and knowledge acquisition**.**  **Extension**  Attempt the [challenge social engineering tactics](https://www.linkedin.com/learning/cybersecurity-awareness-social-engineering-22875721/challenge-social-engineering-tactics) and check the [solution](https://www.linkedin.com/learning/cybersecurity-awareness-social-engineering-22875721/solution-social-engineering-tactics). |  |
| **Content:**  Students:   * investigate cybercrime threats to an enterprise   Including:   * phishing, including smishing. | **Teaching and learning activities**  **Teacher**  **Activity 36**: describe these social engineering attack vectors.  Describe these social engineering attack vectors:   * phishing * smishing * vishing * impersonation * spear phishing * whaling.   **Teacher and students**  As a class watch [SANS Security awareness: Email and Phishing (3:55)](https://www.youtube.com/watch?v=sEMrBKmUTPE).  **Activity 37**: identifying phishing attempts  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.   **Teacher**  **Activity 38**: combat social engineering attacks with critical thinking.  Guide students through first example.  **Students**  Complete questions based on the situation. They:   * describe how they would critically think about the situation * identify the principles of influence used * identify the emotional triggers used. | Students use the vocabulary of cybercrime accurately.  Students can identify phishing attempts.  Students can describe how they would critically think about the situation.  Students can identify the principles of influence used.  Students can identify the emotional triggers used. | Provide a glossary and allow students to translate vocabulary into home languages.  Provide visual and/or multimedia examples and check understanding of concepts. |  |

## Week 5

Table – lesson sequence and details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Outcomes and content | Teaching and learning activities | Evidence of learning | Differentiation and adjustments | Registration and evaluation notes |
| **Outcomes**  **EC-11-07**  **EC-11-09**  **Content**  Students:   * assess cyber risk by implementing risk-management strategies using a risk matrix   Including:   * internal and external vulnerabilities * threat landscape * impact of exposure * likelihood of exploitation. | **Learning intention**  Understand the importance of risk-management strategies by examining a scenario where vulnerabilities are exploited by a threat actor involved in a breach.  **Success criteria**   * I can assess cyber risk by implementing risk-management strategies using a risk matrix. * I can investigate vulnerabilities exploited by the threat actor involved in a breach.   **Teaching and learning activities**  **Teacher**  Teacher-led discussion on how to assess cyber risk by implementing risk-management strategies using a risk matrix. Including:   * internal and external vulnerabilities * threat landscape * impact of exposure * likelihood of exploitation.   **Activity 39**: define and review the terms below:   * risk * threat * vulnerabilities * likelihood * consequences * impact.   **Activity 40**: explain how impact can be evaluated in terms of (loss of):   * confidentiality * integrity * availability.   **Teacher and students**  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.  **Teacher**  **Activity 42**: describe the difference between risk assessment and risk management.  **Teacher and students**  Examine the [Guide to conducting cybersecurity risk assessment for critical information infrastructure (PDF 836KB)](https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf) document. 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.   (**Note**: key pages to examine are pages 10, 12, 14 and 16). | Students review and use key terminology correctly.  Students can recall and explain how impact can be evaluated in terms of (loss of):   * confidentiality * integrity * availability.   Students can recall how a cybersecurity risk assessment matrix is used.  Students can describe the difference between risk assessment and risk management. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  Provide a glossary and allow students to translate vocabulary into home languages.  Provide visual and/or multimedia examples and check understanding of concepts.  Ensure all students understand both technical and culturally-based terms.  The language required should be taught explicitly with opportunities for guided practice. |  |
| **Content:**  Students:   * investigate vulnerabilities exploited by the threat actor involved in a breach, such as the impact on various elements   Including:   * data * people * processes * technology. | **Teaching and learning activities**  **Teacher**  **Activity 43**: USB drop scenario (D)  As a class, read the USB drop scenario (D).  **Students**  Describe vulnerabilities a threat actor aims to exploit in this scenario.  Describe possible consequences (and their likelihood) of inserting an unknown USB drive into an organisation’s computer.  **Teacher**  Review 5 emotions that social engineers use against their targets across different social engineering attacks.  As a class watch [Security awareness episode 5: Removable media (1:22)](https://www.youtube.com/watch?v=FRxrHduwPjY).  **Students**  **Activity 44**: psychology of the USB drop  Identify 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.  **Teacher and students**  **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 these and similar social engineering attacks. | Students can perceive the correct steps in investigating vulnerabilities exploited by the threat actor involved in a breach in the USB drop scenario (D).  Students can correctly identify the relevant emotions a social engineer is hoping to exploit in this scenario.  Students can recall and discuss the risks of removable media. | In creating or selecting scenarios, consider students’ own experiences and use of visuals. Ensure all students understand both technical and culturally-based terms.  During practical learning activities, use and emphasise target language required and encourage students to use this language in context. |  |
| **Content:**  Students:   * investigate cyber risk management   Including:   * implementing a cybersecurity strategy with ongoing training * identifying and managing vulnerabilities * assessing the impact of a breach * controlling damage and loss. | **Teaching and learning activities**  **Teacher and students**  Teacher-led discussion on investigating cyber risk management.  **Activity 46**: human errors  Review previous scenarios and categorise and identify human errors and technical errors.  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.  **Teacher**  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.  **Teacher and students**  Review previous scenarios and discuss issues of changing the security behaviour of individuals or organisations.  **Students**  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? | Students can investigate cyber risk management.  Students can distinguish between human errors and technical errors.  Students will be actively engaged in class discussion and express ideas about the Swiss cheese model for cybersecurity.  Students can discuss issues of changing the security behaviour of individuals or organisations. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  **Extension**  Investigate the Generic Error-Modelling System (GEMS) and how it can be applied to cybersecurity to reduce human errors.  Watch (and importantly discuss) [Two views on Human Error (5:52)](https://www.youtube.com/watch?v=rHeukoWWtQ8) and [Was it technical failure or human error? (4:20)](https://www.youtube.com/watch?v=Ygx2AI2RtkI) to get another perspective on human error.  Discuss the statement ‘Only amateurs attack machines; professionals target people.’ (Bruce Schneier, Cryptographer).  View [Staff security awareness (11:26)](https://www.youtube.com/watch?v=2sh4BIaF6gg) and identify human errors made. |  |

## Week 6

Table – lesson sequence and details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Outcomes and content | Teaching and learning activities | Evidence of learning | Differentiation and adjustments | Registration and evaluation notes |
| **Outcomes**  **EC-11-04**  **EC-11-06**  **EC-11-07**  **Content**  Students:   * describe privacy and security principles associated with access, storage and permissions used by enterprises to collect and interpret data * describe the attributes of a cybersecurity breach   Including:   * confidentiality of information * integrity of information * availability of information * privacy implications * investigate vulnerabilities exploited by the threat actor involved in a breach, such as the impact on various elements   Including:   * data * people * processes * technology * investigate cybercrime threats to an enterprise   Including:   * employee action causing a vulnerability. | **Learning intention**  Establish a pattern of thinking to analyse scenarios, ascertain facts, consider risks and make decisions.  **Success criteria**   * I can describe privacy and security principles associated with access, storage and permissions. * I can describe the attributes of a cybersecurity breach. * I can investigate employee action causing a vulnerability in an enterprise.   **Teaching and learning activities**  **Teacher**  Introduce ‘insider threat’ incident scenario (E) and demonstrate accessing the data. Refer to activity notes in teacher resource document.  **Students**  **Activity 47**: insider threat scenario (E)  Work individually or in pairs.  Identify relevant data (evidence gathered from employee actions) and establish 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.  Construct timelines of events (employee actions) with available date/timestamps.  Prepare a narrative response to share with the class.  **Teacher and students**  Discuss findings and answer questions, for example:   * What is the employee trying to do? * Why are actions considered risky? * Is the employee a malicious insider or victim of human error?   Determine the appropriate action(s) to be taken.  **Teacher and students**  Gather student responses and summarise findings from scenario (E), including:   * list of relevant actions * timeline.   **Students**  Confirm alignment of their version of events and the incident.  **Teacher and students**  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?’ | Students can explain privacy and security principles associated with access, storage and permissions.  Students can describe the attributes of a cybersecurity breach.  Students can explain how employee action causing a vulnerability is a cybercrime threats to an enterprise.  Students can use critical thinking to evaluate the situation in a scenario and consider potential risks.  Students can apply adversarial mindset to devise strategies that would align with indicators of compromise.  Students can determine in a scenario:   * What is the employee trying to do? * Why are actions considered risky? * Is the employee a malicious insider or victim of human error? | This section is also for use in school when making adjustments to support all students to achieve in their learning.  Ensure students understand the meaning of ‘threat’ before introducing these other terms or concepts.  In creating or selecting scenarios, consider students’ own experiences and use of visuals. Ensure all students understand both technical and culturally-based terms.  During practical learning activities, use and emphasise target language required and encourage students to use this language in context.  When presenting data, consider the amount of text, text complexity and layout.  When demonstrating use of a data dashboard, zoom in and focus on one or 2 columns and one or 2 cells to make it easier for all students. |  |
| **Content:**  Students:   * research hardware and software strategies used to protect data   Including:   * physical security * biometrics * password protection, encryption and permissions * multi-factor authentication * back up and disaster recovery. | **Teaching and learning activities**  **Teacher**  **Activity 49**: in the table below, summarise different forms of authentication, different types of evidence a user provides, and highlight known weaknesses (or vulnerabilities), for example:   * passwords * biometrics * smart cards * federation and single-sign-on (SSO) * certificate-based authentication.   **Activity 50**: explain the principles of multi-factor authentication (MFA) and how this increases security.  **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.   **Students**  **Activity 52**: answer the following questions:   * Identify examples of organisations using multi-factor authentication. * Evaluate the advantages and disadvantages of organisations using multi-factor authentication apps in the workplace. * Explain whether mechanisms like Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) are identification or authentication access control processes. | Students can outline a diverse range of authentication processes or types and recall their known weaknesses.  Students can explain how and why the use of MFA provides greater security.  Students can recognise multiple types of authentication factors or multiple types of evidence and discern whether a combination is MFA or not.  Students can set up two-factor authentication (2FA) on at least one platform.  Students can identify platforms they use or know of that offer 2FA (or MFA) services for authentication.  Students can assess the costs and benefits to organisations of using 2FA (MFA), including with their workforce and with their customers.  Students can recognise what CAPTCHAs are (including any variations) and how they function.  Students can explain that CAPTCHAs verify that a person is human but do not verify their identity and therefore are not a form of authentication.  Students will be able to describe what threats CAPTCHAs protect against. | Provide a glossary and allow students to translate vocabulary into home languages.  Provide visual and/or multimedia examples and check understanding of concepts. |  |
| **Content:**  Students:   * describe privacy and security principles associated with access, storage and permissions used by enterprises to collect and interpret data. | **Teaching and learning activities**  **Teacher**  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.  **Activity 54**: define non-repudiation in relation to cybersecurity.  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.  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). | Students are able to use software tools to check hash values and digital signatures of files for integrity and authenticity.  Students can answer the questions:   * How can I trust this file? * How can I trust this email? * How can I trust this website? * How can I trust this download? | This section is also for use in school when making adjustments to support all students to achieve in their learning.  During practical learning activities, use and emphasise target language required and encourage students to use this language in context. |  |

## Week 7

Table – lesson sequence and details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Outcomes and content | Teaching and learning activities | Evidence of learning | Differentiation and adjustments | Registration and evaluation notes |
| **Outcomes**  **EC-11-01**  **EC-11-03**  **EC-11-05**  **Content**  Students:   * investigate vulnerabilities exploited by the threat actor involved in a breach, such as the impact on various elements   Including:   * data * people * processes * technology * investigate cybercrime threats to an enterprise   Including:   * hacking * employee action causing a vulnerability. | **Learning intention**  Understand the importance of hardware and software strategies used to prevent cybercrime.  **Success criteria**   * **I can examine cybercrime and take action with hardware and software strategies to minimise damage.** * I can identify hardware and software strategies used to protect data.   **Teaching and learning activities**  **Teacher**  Teacher-led discussion on investigating cybercrime threats to an enterprise.  **Activity 56**: lost luggage scenario (F)  Introduce lost luggage scenario (F) and assign required groups and roles.  Refer to scenario notes in teacher support resource document to facilitate moving through stages of the scenario, revealing additional information and prompting questions as required.  **Students**  In groups, define the problem and identify relevant facts from provided scenario text.  In an iterative process, combine and apply additional information (released in stages from teacher) to the scenario body of knowledge.  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. | Students can explain how hacking is a cybercrime threat to an enterprise.  Students can explain how employee action causing a vulnerability is a cybercrime threats to an enterprise.  Students can use critical thinking to evaluate the situation in a scenario and consider potential risks.  Students can apply adversarial mindset to devise strategies that would align with indicators of compromise. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  Provide visual and/or multimedia examples and check understanding of concepts.  The language required should be taught explicitly with opportunities for guided practice. |  |
| **Content:**  Students:   * research hardware and software strategies used to protect data   Including:   * isolation * physical security * biometrics * password protection, encryption and permissions * multi-factor authentication * back up and disaster recovery * firewalls * antivirus and anti-malware. | **Teaching and learning activities**  **Teacher**  **Activity 57:** analyse applicable cybersecurity concepts for the lost luggage scenario (F) for the following:   * authentication * authorisation * confidentiality * digital signatures * encryption * symmetric cipher * integrity * risk * policy * protocols * security practices (of organisation) * security measures   **Students**  With reference to this scenario, consider implementing a cybersecurity strategy with ongoing training.  **Activity 58**: identify vulnerabilities that could be exploited.  **Activity 59**: describe controls or other strategies that could be implemented to mitigate risk(s) of a breach. | Students can recall hardware and software strategies used to protect data.  Students learn, through the scenario, the cybersecurity concepts in a real-world scenario.  Students understand the concepts of digital signatures, encryption and symmetric ciphers.  Students can identify vulnerabilities that could be exploited.  Students can describe controls or other strategies that could be implemented to mitigate risk(s) of a breach assessing the impact of a breach. | In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  Some students may need support to work in a group.  Provide options for students to share roles if necessary.  Provide scaffolds and templates of documents based on student needs and the desired level of student independence.  Provide worksheet with key terms to assist with vocabulary building and knowledge acquisition. |  |
| **Content:**  Students:   * research hardware and software strategies used to protect data   Including:   * isolation * firewalls * antivirus and anti-malware. | **Teaching and learning activities**  **Teacher**  **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.   **Students**  **Activity 61**: identify strategies organisations can use or implement to uniquely identify users to a system.  Assess identification mechanisms and technologies for weaknesses.  **Activity 62**: identify hardware and software strategies used to protect data including:   * isolation * firewalls * antivirus * anti-malware. | Students can describe security controls used to ensure the goal of availability.  Students can identify strategies organisations can use or implement to uniquely identify users to a system.  Students can identify hardware and software strategies used to protect data, including:   * isolation * firewalls * antivirus * anti-malware. | Provide scaffolds and templates of documents based on student needs and the desired level of student independence.  Provide worksheet with key terms to assist with vocabulary building and knowledge acquisition. |  |

## Week 8

Table – lesson sequence and details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Outcomes and content | Teaching and learning activities | Evidence of learning | Differentiation and adjustments | Registration and evaluation notes |
| **Outcomes**  **EC-11-07**  **EC-11-09**  **Content**  Students:   * investigate vulnerabilities exploited by the threat actor involved in a breach, such as the impact on various elements   Including:   * data * people * processes * technology * investigate cybercrime threats to an enterprise   Including:   * hacking. | **Learning intention**  Understand through the use of a scenario, how a cybercrime can occur and investigate vulnerabilities that impact data, people, processes and technology.  **Success criteria**   * I can investigate vulnerabilities exploited by the threat actor involved in a breach. * I can assess the impact of data, people, processes and technology in a breach. * I can investigate hacking such as SQL injection in a breach.   **Teaching and learning activities**  **Teacher**  Teacher-led discussion on common vulnerabilities exploited in breaches and the potential impacts on data, people, processes and technology.  **Activity 63**:database input error scenario (F)  Introduce database input error scenario (F)and assign required groups and roles.  Refer to scenario notes in teacher resource document to facilitate moving through stages of the scenario, revealing additional information and prompting questions as required.  **Students**  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.  **Teacher and students**  Share group responses and collaborate to build a better understanding of this scenario event and work towards an agreed response to the question. | Students can investigate vulnerabilities exploited by a threat actor.  Students can understand database input errors.  Students can use critical thinking to evaluate the situation in a scenario and consider potential risks.  Students can apply adversarial mindset to devise strategies that would align with indicators of compromise. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  During practical learning activities, use and emphasise target language required and encourage students to use this language in context. |  |
| **Content**  Students:   * investigate cybercrime threats to an enterprise   Including:   * hacking. | **Teaching and learning activities**  **Teacher**  Recap findings from scenario (F), including:   * user input into online form * error messages * security logs.   **Activity 64**: explain the essential operations of SQL for storing, manipulating and retrieving data in databases.  **Activity 65**: explain how SQL commands are used in web page forms to collect and process user input.  SQL injection is the placement of malicious code in SQL statements via web page input.  As a class watch [What is SQL injection? (10:20)](https://www.youtube.com/watch?v=wX6tszfgYp4).  As a class examine how [SQL injection](https://owasp.org/Top10/A03_2021-Injection/) works and the link to findings in the scenario.  **Students**  **Activity 66**: describe the possible consequences of an [SQL injection attack](https://owasp.org/www-community/attacks/SQL_Injection) in terms of:   * Confidentiality * Authentication * Authorisation * Integrity.   **Teacher**  Demonstrate 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. | Students can investigate hacking by examining:   * user input into online form * error messages * security logs.   Students can explain the essential operations of SQL for storing, manipulating and retrieving data in databases.  Students can explain how SQL commands are used in web page forms to collect and process user input.  Students can explain how SQL injection works and the possible consequences in the scenario. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  Some students may need support to work in a group.  Provide options for students to share roles if necessary.  During practical learning activities, use and emphasise target language required and encourage students to use this language in context.  Provide scaffolds and templates of documents based on student needs and the desired level of student independence.  Provide worksheet with key terms to assist with vocabulary building and knowledge acquisition. |  |
| **Content:**  Students:   * investigate cybercrime threats to an enterprise   Including:   * hacking. | **Teaching and learning activities**  **Teacher**  Using a pre-prepared vulnerable web app (within a sandboxed environment), demonstrate how to apply SQL injection techniques.  **Students**  Within a suitable sandboxed environment, complete SQL injection activities.  **Activity 68**: describe known technical strategies to prevent SQL injection attacks. | Students demonstrate practical skills in using computer hardware and software to examine cybercrime threats. | During practical learning activities, use and emphasise target language required and encourage students to use this language in context. |  |

## Week 9

Table 8 – Week 9 lesson sequence and details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Outcomes and content | Teaching and learning activities | Evidence of learning | Differentiation and adjustments | Registration and evaluation notes |
| **Outcome**  **EC-11-07**  **Content**  Students:   * identify laws and legislation associated with cybersecurity. | **Learning intention**  Understand legal and regulatory structure for dealing with cybercrime in Australia.  **Success criteria**   * I can identify laws associated with cybersecurity. * I can identify legislation associated with cybersecurity.   **Teaching and learning activities**  Teacher-led discussion on identifying laws and legislation associated with cybersecurity.  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?’  As a class, watch [What is the difference between Ethics, Morality and the Law? (5:13)](https://www.youtube.com/watch?v=Xki2fRA0bY8) and facilitate a teacher-led class discussion.  **Teacher**  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.  **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.  As a class watch [Requesting access to your personal information (3:19)](https://www.youtube.com/watch?v=W8_Zl8f0hXc)  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).  **Students**  **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.  **Teacher and students**  **Activity 74**: outline federal and state laws and legislation associated with cybersecurity.  **Activity 75**: outline federal and state departments or bodies tasked with upholding identified laws.  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. | Students understand the need for privacy.  Students can examine and understand ethics.  Students can identify legal and regulatory structures for dealing with cybercrime in Australia. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  Some students may need support to work in a group.  Provide options for students to share roles if necessary.  During practical learning activities, use and emphasise target language required and encourage students to use this language in context.  Provide scaffolds and templates of documents based on student needs and the desired level of student independence.  Provide worksheet with key terms to assist with vocabulary building and knowledge acquisition. |  |
| **Content:**  Students:   * explain impacts of cybersecurity breaches on the individual, organisation and society   Including:   * financial loss * reputational damage * operational disruptions * legal and regulatory ramifications * identify laws and legislation associated with cybersecurity. | **Teaching and learning activities**  **Teacher**  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)  Teacher-led discussion on   * financial loss * reputational damage * operational disruptions * legal and regulatory ramifications.   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.  **Activity 77**: cyber operation against the power grid scenario (G)  Introduce the [Cyber operation against the power grid](https://cyberlaw.ccdcoe.org/wiki/Scenario_03:_Cyber_operation_against_the_power_gri) scenario.  As a class examine the [facts](https://cyberlaw.ccdcoe.org/wiki/Scenario_03:_Cyber_operation_against_the_power_grid#Facts) of the scenario. As appropriate, outline the [legal analysis](https://cyberlaw.ccdcoe.org/wiki/Scenario_03:_Cyber_operation_against_the_power_grid#Legal_analysis) provided in the resource.  **Teacher and students**  Discuss the provided facts of the scenario and determine agreed-upon answers to the questions, for example:   * did the operation result in actual physical damage or injury to individuals? * were any individuals associated with an outside state physically present in the domestic state’s territory without the latter’s consent?   Investigate examples of similar real-life occurrences (linked in resource) as required. | Students can apply contemporary legal, law enforcement and regulatory principles to cybercrime scenarios. | Provide students with different challenge options and/or negotiate the requirements of the task with appropriate adjustments.  Advanced students could be encouraged to research the legal arguments presented and evaluate against the related principle.  Work in teams or individually to complete the challenge.  **Extension**  Examine [Annex B: Australia's position on how international law applies to State conduct in cyberspace](https://www.internationalcybertech.gov.au/our-work/annexes/annex-b). |  |
| **Content:**  Students:   * explain impacts of cybersecurity breaches on the individual, organisation and society   Including:   * financial loss * reputational damage * operational disruptions * legal and regulatory ramifications * identify laws and legislation associated with cybersecurity. | **Teacher**  **Activity 78**: ransomware scenario (H)  As a class read the [Ransomware campaign](https://cyberlaw.ccdcoe.org/wiki/Scenario_14:_Ransomware_campaign) scenario. Examine the [facts](https://cyberlaw.ccdcoe.org/wiki/Scenario_14:_Ransomware_campaign#Facts) of the scenario.  As appropriate, outline the [legal analysis](https://cyberlaw.ccdcoe.org/wiki/Scenario_14:_Ransomware_campaign#Legal_analysis) provided in the resource.  Identify the questions to be resolved.  **Teacher students**  Discuss the provided facts of the scenario and determine agreed-upon answers to the questions, for example:   * can the ransomware attacks be attributed? * are the authors of the ransomware attack state organs or non-state organs exercising governmental authority? * is the ransomware a use of force?   Investigate [examples](https://cyberlaw.ccdcoe.org/wiki/Scenario_14:_Ransomware_campaign#Examples) of similar real-life occurrences as required. | Students can explain impacts of cybersecurity breaches on the individual, organisation and society.  Students can analyse a scenario based on ransomware.  Students can recall impacts of a cybersecurity breach such as:   * financial loss * reputational damage * operational disruptions * legal and regulatory ramifications.   Students can identify laws and legislation associated with cybersecurity. | Provide students with different challenge options and/or negotiate the requirements of the task with appropriate adjustments.  Advanced students could be encouraged to research the legal arguments presented and evaluate against the related principle.  Work in teams or individually to complete the challenge. |  |

## Week 10

Table 9 – Week 10 lesson sequence and details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Outcomes and content | Teaching and learning activities | Evidence of learning | Differentiation and adjustments | Registration and evaluation notes |
| **Outcomes**  **EC-11-01**  **EC-11-03**  **EC-11-06**  **Content**  Students:   * explore current and emerging cybercrime threats to an enterprise. | **Learning intention**  To explore current and emerging cybercrime threats to an enterprise.  **Success criteria**   * I can outline the impact of cybercrime threats. * I can examine current and emerging cybercrime threats to an enterprise. * I can discuss the impact or potential impact of current and emerging technologies.   **Teaching and learning activities**  **Teacher**  Teacher-led exploration of current and emerging cybercrime threats to an enterprise.  **Activity 79**: outline the impact of recently developed and emerging technologies on cybersecurity challenges, for example:   * cloud computing * hybrid workforce * virtualisation * internet of things (IoT) * embedded systems, such as autonomous cars.   **Activity 80**: outline emerging innovative cybersecurity solutions, for example:   * behaviour analytics * blockchain technology * deep learning * hardware authentication * quantum cryptography.   **Teacher and students**  **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, the class could [brainstorm](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/542) using strategies like [Think-Pair-Share](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/645) and bring ideas back to the larger group. | Students will be actively engaged in class discussion and expressing ideas about how various emerging technologies could potentially affect or change the way security challenges are addressed.  Indicators of student understanding will be demonstrated in their explanations of how a particular technology is employed, and further understanding will be evident as students propose logical consequences of a technology’s use. | Suggested adjusted activities. This section is also for use in school when making adjustments to support all students to achieve in their learning.  In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  Some students may need support to work in a group.  Provide options for students to share roles if necessary.  During practical learning activities, use and emphasise target language required and encourage students to use this language in context.  Provide scaffolds and templates of documents based on student needs and the desired level of student independence. |  |
| Students:   * investigate cybercrime threats to an enterprise   Including:   * hacking * phishing, including smishing * scamming * employee action causing a vulnerability. | **Teaching and learning activities**  **Teacher**  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.  **Teacher and students**  Complete some practice activities/challenges.  Research and document solutions to problems. | Students will be actively participating in some pre-event setup activities, familiarisation and preparation for a live capture the flag (jeopardy style) event.  Students will be able to set up a suitable computer workstation, including any necessary virtual machine images, ready to participate.  Students demonstrate working independently or collaboration skills if working in a small team. | In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  Some students may need support to work in a group.  Provide options for students to share roles if necessary. |  |
| Students:   * explore security vulnerabilities of social networking to both an individual and an enterprise   Including:   * account access * account behaviour * hosting platform security * identity theft * phishing * evil twins * investigate cyber risk management   Including:   * implementing a cybersecurity strategy with ongoing training. | **Teaching and learning activities**  **Teacher**  **Activity 82:** capture the flag  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.  **Students**  Participate in challenge. | Students will be actively participating in a capture the flag (jeopardy style) event and attempting to complete as many challenges as possible within the time allowed.  Students will demonstrate knowledge and understanding in completing practical exercises solving cybersecurity problems.  Students will understand one strategy that cybersecurity professionals use to test and develop their industry skills and knowledge. | This section is also for use in school when making adjustments to support all students to achieve in their learning.  In creating or selecting scenarios, consider students’ own experiences and use of visuals.  Ensure all students understand both technical and culturally-based terms.  Some students may need support to work in a group.  Provide options for students to share roles if necessary.  During practical learning activities, use and emphasise target language required and encourage students to use this language in context. |  |

# Overall program evaluation

Collating ongoing evaluations and reflecting on the strengths and areas for development within the program creates opportunities to enhance student outcomes. The following prompts can be used to support your evaluation of the program:

* Did the program assist all students to improve in their learning?
* How could the sequencing of the program be improved?
* What did the student evaluations of the program indicate? How can these be actioned to improve the program?
* The strategies and resources that were most effective for student learning were …
* Teaching strategies and resources that would benefit from review and refinement are …

## Capturing student voice when evaluating a program

Student voice is useful in the evaluation process for programs. The statements below could be useful as a starting point when asking students to provide feedback on their learning experiences. These statements are derived from some of the themes from [What works best 2020 update](https://education.nsw.gov.au/about-us/education-data-and-research/cese/publications/research-reports/what-works-best-2020-update) (CESE 2020b) and could be useful in teacher reflection on how these themes could be incorporated into a teaching program. The statements could also prompt student reflection on their metacognitive processes while learning.

**Please rate how much you agree with these statements**:

* My teacher had confidence that I could achieve and improve in my learning. (CESE 2020b Chapter 1: High expectations)
* I had a clear idea of what I was learning and why. (CESE 2020b Chapter 2: Explicit teaching)
* I used the feedback provided to improve my performance. (CESE 2020b Chapter 3: Effective feedback)
* I understood the feedback on the assessment task. (CESE 2020b Chapter 3: Effective feedback)
* I was able to predict the marks I achieved in the assessment tasks. (CESE 2020b Chapter 5: Assessment)
* The activities in the unit prepared me for the assessment task. (CESE 2020b Chapter 5: Assessment)
* I found the activities in the lessons interesting to me. (CESE 2020b Chapter 7: Wellbeing)
* I made valuable contributions to the class during this unit. (CESE 2020b Chapter 7: Wellbeing)
* I ask questions in class when I don’t understand yet. (CESE 2020b Chapter 7: Wellbeing)

**Optional open-ended prompts:**

* The lessons and/or activities that I most enjoyed were when we … because …
* When the learning was difficult, the strategy I used was …
* If I was giving advice to a student who was starting this unit, I would tell them to …
* If I was giving advice to a teacher who was teaching this unit, I would tell them to …

# Additional information

For additional support or advice, contact the TAS curriculum team by emailing [TAS@det.nsw.edu.au](mailto:TAS@det.nsw.edu.au).

## Further implementation support

Curriculum design and implementation is a dynamic and contextually-specific process. The department is committed to supporting teachers to meet the needs of all students. The advice below on assessment and planning for the needs of every student may be useful when considering the material presented in this sample program of learning.

## Assessment for learning

Possible formative assessment strategies that could be included:

* Learning intentions and success criteria assist educators to articulate the purpose of a learning task to make judgements about the quality of student learning. These help students focus on the task or activity taking place and what they are learning and provide a framework for reflection and feedback. [Online tools](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/622) can assist implementation of this formative assessment strategy.
* Eliciting evidence strategies allow teachers to determine the next steps in learning and assist teachers in evaluating the impact of teaching and learning activities. Strategies that may be added to a learning sequence to elicit evidence include all student response systems, [exit tickets](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/543), mini whiteboards (actual or [digital](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/575)), [hinge questions](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/560), [Kahoot](https://app.education.nsw.gov.au/digital-learning-selector/LearningTool/Card/621), [Socrative](https://app.education.nsw.gov.au/digital-learning-selector/LearningTool/Card/587), or quick quizzes to ensure that individual student progress can be monitored and the lesson sequence adjusted based on formative data collected.
* Feedback is designed to close the gap between current and desired performance by informing teacher and student behaviour (AITSL 2017). AITSL provides a [factsheet to support evidence-based feedback](https://www.aitsl.edu.au/teach/improve-practice/feedback#:~:text=FEEDBACK-,Factsheet,-A%20quick%20guide).
* [Peer feedback](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/549) is a structured process where students evaluate the work of their peers by providing valuable feedback in relation to learning intentions and success criteria. It can be supported by [online tools](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Browser?cache_id=1d29b).
* Self-regulated learning opportunities assist students in taking ownership of their own learning. A variety of strategies can be employed and some examples include reflection tasks, [Think-Pair-Share](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/645), [KWLH charts](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/562), [learning portfolios](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/583) and [learning logs](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/583).

The primary role of assessment is to establish where individuals are in their learning so that teaching can be differentiated and further learning progress can be monitored over time.

Feedback that focuses on improving tasks, processes and student self-regulation is the most effective. Students engaging with feedback can take many forms including formal, informal, formative, summative, interactive, demonstrable, visual, written, verbal and non-verbal (CESE 2020a).

## Differentiation

Differentiated learning can be enabled by differentiating the teaching approach to content, process, product and the learning environment. For more information on differentiation go to [Differentiating learning](https://education.nsw.gov.au/teaching-and-learning/professional-learning/teacher-quality-and-accreditation/strong-start-great-teachers/refining-practice/differentiating-learning) and [Differentiation](https://education.nsw.gov.au/campaigns/inclusive-practice-hub/primary-school/teaching-strategies/differentiation).

When using these resources in the classroom, it is important for teachers to consider the needs of all students in their class, including:

* **Aboriginal and Torres Strait Islander students**. Targeted [strategies](https://education.nsw.gov.au/teaching-and-learning/aec/aboriginal-education-in-nsw-public-schools) can be used to achieve outcomes for Aboriginal students in K-12 and increase knowledge and understanding of Aboriginal histories and cultures. Teachers should utilise students’ Personalised Learning Pathways to support individual student needs and goals.
* **EAL/D learners**. EAL/D learners will require explicit English language support and scaffolding, informed by the [EAL/D enhanced teaching and learning cycle](https://education.nsw.gov.au/teaching-and-learning/curriculum/literacy-and-numeracy/resources-for-schools/eald/enhanced-teaching-and-learning-cycle) and the student’s phase on the [EAL/D Learning Progression](https://education.nsw.gov.au/teaching-and-learning/curriculum/multicultural-education/english-as-an-additional-language-or-dialect/planning-eald-support/english-language-proficiency). In addition, teachers can access information about [supporting EAL/D learners](https://education.nsw.gov.au/teaching-and-learning/curriculum/multicultural-education/english-as-an-additional-language-or-dialect/planning-eald-support/english-language-proficiency) and [literacy and numeracy support specific to EAL/D learners](https://education.nsw.gov.au/teaching-and-learning/curriculum/literacy-and-numeracy/resources-for-schools/eald).
* **Students with additional learning needs**. Learning adjustments enable students with disability and additional learning and support needs to access syllabus outcomes and content on the same basis as their peers. Teachers can use a range of [adjustments](https://education.nsw.gov.au/teaching-and-learning/disability-learning-and-support/personalised-support-for-learning/adjustments-to-teaching-and-learning) to ensure a personalised approach to student learning. Subject specific curriculum considerations can be found on the [Inclusive Practice hub](https://education.nsw.gov.au/campaigns/inclusive-practice-hub).
* **High potential and gifted learners**. [Assessing and identifying high potential and gifted learners](https://education.nsw.gov.au/teaching-and-learning/high-potential-and-gifted-education/supporting-educators/assess-and-identify#Assessment1) will help teachers decide which students may benefit from extension and additional challenge. [Effective strategies and contributors to achievement](https://education.nsw.gov.au/teaching-and-learning/high-potential-and-gifted-education/supporting-educators/evaluate) for high potential and gifted learners help teachers to identify and target areas for growth and improvement. In addition, the [Differentiation Adjustment Tool](https://education.nsw.gov.au/teaching-and-learning/high-potential-and-gifted-education/supporting-educators/implement/differentiation-adjustment-strategies) can be used to support the specific learning needs of high potential and gifted students. The [High Potential and Gifted Education Professional Learning and Resource Hub](https://schoolsnsw.sharepoint.com/sites/HPGEHub/SitePages/Home.aspx) supports school leaders and teachers to effectively implement the High Potential and Gifted Education Policy in their unique contexts.

All students need to be challenged and engaged to develop their potential fully. A culture of high expectations needs to be supported by strategies that both challenge and support student learning needs, such as through appropriate curriculum differentiation (CESE 2020a:6).

## Support and alignment

**Resource evaluation and support:** all curriculum resources are prepared through a rigorous process. Resources are periodically reviewed as part of our ongoing evaluation plan to ensure currency, relevance and effectiveness. For additional support or advice, or to provide feedback, contact the TAS curriculum team by emailing [TAS@det.nsw.edu.au](mailto:TAS@det.nsw.edu.au).

**Differentiation:** further advice to support Aboriginal and Torres Strait Islander students, EALD students, students with a disability and/or additional needs and High Potential and gifted students can be found on the [Planning programming and assessing 7–12](https://education.nsw.gov.au/teaching-and-learning/curriculum/planning-programming-and-assessing-k-12/planning-programming-and-assessing-7-12) webpage. This includes the [Inclusion and differentiation 7–10 advice](https://education.nsw.gov.au/teaching-and-learning/curriculum/planning-programming-and-assessing-k-12/planning-programming-and-assessing-7-12/inclusion-and-differentiation-advice-7-10) webpage.

**Assessment:** further advice to support formative assessment is available on the [Planning programming and assessing 7–12](https://education.nsw.gov.au/teaching-and-learning/curriculum/planning-programming-and-assessing-k-12/planning-programming-and-assessing-7-12) webpage. This includes the [Classroom assessment advice 7–10](https://education.nsw.gov.au/teaching-and-learning/curriculum/planning-programming-and-assessing-k-12/planning-programming-and-assessing-7-12/classroom-assessment-advice-7-10-). For summative assessment tasks, the [Assessment task advice 7–10](https://education.nsw.gov.au/teaching-and-learning/curriculum/planning-programming-and-assessing-k-12/planning-programming-and-assessing-7-12/assessment-task-advice-7-10) webpage is available.

**Consulted with:** Curriculum and Reform and subject matter experts.

**Alignment to system priorities and/or needs:** [School Excellence Policy](https://education.nsw.gov.au/policy-library/policies/pd-2016-0468).

**Alignment to the School Excellence Framework:** this resource supports the [School Excellence Framework](https://education.nsw.gov.au/policy-library/policies/pd-2016-0468) elements of curriculum (curriculum provision) and effective classroom practice (lesson planning, explicit teaching).

**Alignment to Australian Professional Teaching Standards:** this resource supports teachers to address [Australian Professional Teaching Standards](https://educationstandards.nsw.edu.au/wps/portal/nesa/teacher-accreditation/meeting-requirements/the-standards/proficient-teacher) 1.1.2, 1.2.2, 1.3.2, 2.1.2, 2.2.2, 2.6.2, 3.2.2, 3.3.2, 3.4.2, 4.5.2, 6.2.2.

**Creation date:** 2024

# Evidence base

[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.

AITSL (Australian Institute for Teaching and School Leadership Limited) (n.d.) [Learning intentions and success criteria (PDF 251 KB)](https://www.aitsl.edu.au/docs/default-source/feedback/aitsl-learning-intentions-and-success-criteria-strategy.pdf?sfvrsn=382dec3c_2#:~:text=Learning%20Intentions%20are%20descriptions%20of,providing%20feedback%20and%20assessing%20achievement.), AITSL, accessed 14 February 2024.

AITSL (2017) ‘[Feedback Factsheet](https://www.aitsl.edu.au/teach/improve-practice/feedback#:~:text=FEEDBACK-,Factsheet,-A%20quick%20guide)’, AITSL, accessed 14 February 2024.

Brookhart S (2011) How to Assess Higher-Order Thinking Skills in Your Classroom, Hawker Brownlow Education, Victoria.

CESE (Centre for Education Statistics and Evaluation) (2020a) [*What works best: 2020 update*](https://education.nsw.gov.au/about-us/education-data-and-research/cese/publications/research-reports/what-works-best-2020-update), NSW Department of Education, accessed 14 February 2024.

CESE (2020b) [*What works best in practice*](https://education.nsw.gov.au/about-us/education-data-and-research/cese/publications/practical-guides-for-educators-/what-works-best-in-practice), NSW Department of Education, accessed 14 February 2024.

NESA (NSW Education Standards Authority) (2022) ‘[Advice on units](https://educationstandards.nsw.edu.au/wps/portal/nesa/k-10/understanding-the-curriculum/programming/advice-on-units)’, Programming*,* NESA website, accessed 14 February 2024.

NESA (2022) ‘[Proficient Teacher: Standard descriptors](https://educationstandards.nsw.edu.au/wps/portal/nesa/teacher-accreditation/meeting-requirements/the-standards/proficient-teacher)’, The Standards, NESA website, accessed 14 February 2024.

NESA (2022) ‘[Programming](https://educationstandards.nsw.edu.au/wps/portal/nesa/k-10/understanding-the-curriculum/programming)’, Understanding the curriculum, NESA website, accessed 14 February 2024.

Rosenshine B (2012) ‘[Principles of Instruction: Research-Based Strategies That All Teachers Should Know](https://eric.ed.gov/?id=EJ971753)’, American Educator, 36(1):12–19 accessed 14 February 2024.

Wiliam D (2013) ‘[Assessment: The bridge between teaching and learning](https://www.researchgate.net/publication/258423377_Assessment_The_bridge_between_teaching_and_learning)’, Voices from the Middle, 21(2):15–20, accessed 14 February 2024.

Wiliam D (2017) Embedded Formative Assessment, 2nd edn, Solution Tree Press, Bloomington, IN.

Wisniewski B, Zierer K and Hattie J (2020) ‘[The Power of Feedback Revisited: A Meta-Analysis of Educational Feedback Research](https://doi.org/10.3389/fpsyg.2019.03087)’, Frontiers In Psycholog*y*, 10:3087, doi:10.3389/fpsyg.2019.03087, accessed 14 February 2024.

# 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 (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 (n.d.) [*Cyber and Infrastructure Security Centre*](https://www.cisc.gov.au/) [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:_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 NetworkCommunications, 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.

Schneier B (15 October 2000) '[Crypto-Gram](https://www.schneier.com/crypto-gram/archives/2000/1015.html)', Schneier on Security Newsletter, accessed 12 February 2024.

Security Innovation (12 July2018) ['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:IC-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/).

[](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.