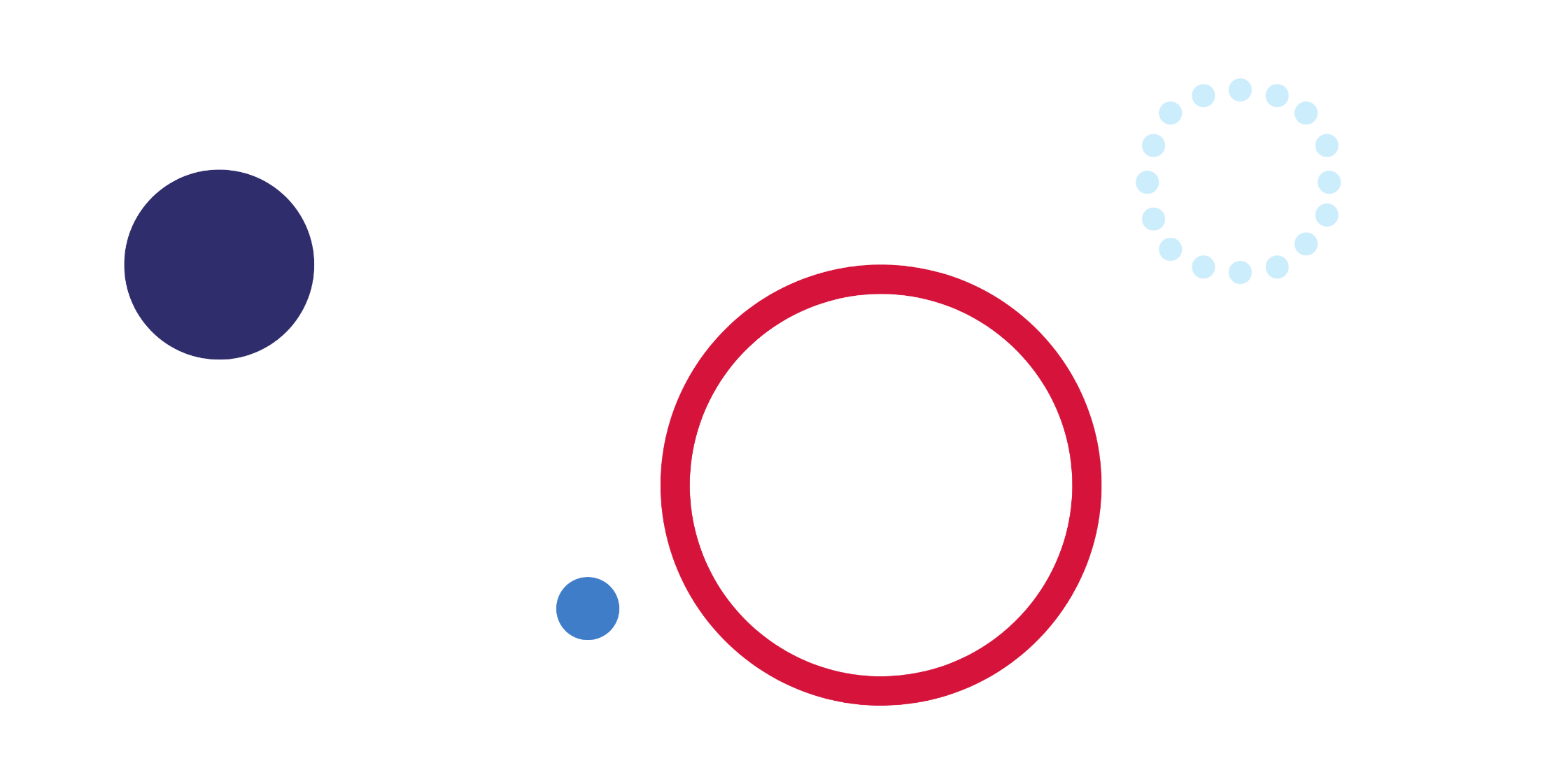
# iSTEM – Cyber security



Contents

[Cyber security 2](#_Toc126581724)

[Duration of learning 2](#_Toc126581725)

[Outcomes 2](#_Toc126581726)

[Rationale 3](#_Toc126581727)

[Aim 5](#_Toc126581728)

[Purpose and audience 5](#_Toc126581729)

[When and how to use this document 5](#_Toc126581730)

[Learning sequences 6](#_Toc126581731)

[Weeks 1 and 2 7](#_Toc126581732)

[Weeks 3 and 4 34](#_Toc126581733)

[Weeks 5 and 6 52](#_Toc126581734)

[Weeks 7 and 8 71](#_Toc126581735)

[Weeks 9 and 10 90](#_Toc126581736)

[Reflection and evaluation 107](#_Toc126581737)

[Additional information 108](#_Toc126581738)

[Assessment for learning 108](#_Toc126581739)

[Differentiation 109](#_Toc126581740)

[About this resource 110](#_Toc126581741)

[References 113](#_Toc126581742)

## Cyber security

Cyber security has emerged as one of the most important and rapidly evolving problems facing society. Research has indicated that the cyber security industry is facing [a skills shortage](https://www.austcyber.com/resources/sector-competitiveness-plan-2019/chapter3), with nearly 17,000 more cyber security workers needed by 2026. This provides an opportunity for students to develop lifelong skills in this rapidly expanding industry. Cyber security is a cross-disciplinary profession with many social, political, and legal implications. There are many different types of cyber security professionals and various pathways into these careers.

In this specialised topic, students develop skills and knowledge used in the cyber security professions by completing inquiry-based and problem-based learning tasks. Students engage with the cyber security industry and will gain insight into the nature of the profession and career pathways.

### Duration of learning

Indicative time – 25 hours.

### Outcomes

A student:

* **ST5-1** designs and develops creative, innovative, and enterprising solutions to a wide range of STEM-based problems
* **ST5-2** demonstrates critical thinking, creativity, problem solving, entrepreneurship and engineering design skills and decision-making techniques in a range of STEM contexts
* **ST5-3** applies engineering design processes to address real-world STEM-based problems
* **ST5-4** works independently and collaboratively to produce practical solutions to real-world scenarios
* **ST5-5** analyses a range of contexts and applies STEM principles and processes
* **ST5-6** selects and safely uses a range of technologies in the development, evaluation, and presentation of solutions to STEM-based problems
* **ST5-7** selects and applies project management strategies when developing and evaluating STEM-based design solutions
* **ST5-8** uses a range of techniques and technologies, to communicate design solutions and technical information for a range of audiences
* **ST5-9** collects, organises, and interprets data sets, using appropriate mathematical and statistical methods to inform and evaluate design decisions
* **ST5-10** analyses and evaluates the impact of STEM on society and describes the scope and pathways into employment.

Outcomes referred to in this document are from the [iSTEM course document](https://education.nsw.gov.au/teaching-and-learning/curriculum/department-approved-courses/istem#/asset2) © NSW Department of Education for and on behalf of the crown in the State of New South Wales (2021).

### Rationale

Australian businesses competing in a global economy will need more employees trained in science, technology, engineering, and mathematics (STEM). Research indicates that 75% of the fastest-growing occupations require STEM skills. Global accounting firm PwC (formerly known as PricewaterhouseCoopers) produced a report titled [‘A smart move’](https://www.pwc.com.au/publications/a-smart-move.html) where it found that shifting just 1% of the Australian workforce into STEM roles would add $57.4 billion to the gross domestic product (GDP) (net present value over 20 years).

iSTEM is a student-centred Stage 5 elective course that delivers science, technology, engineering, and mathematics education in an interdisciplinary, innovative, and integrated fashion. It was developed in direct response to industry’s urgent demand for young people skilled in science, technology, engineering, and mathematics.

The course was developed in collaboration with, and is supported by, industry, business, government, and universities, ensuring that students develop future-focused STEM skills. The course has a number of specialised topics, many of which are aligned with NSW State Government priority industries, identified in the [NSW Industry Development Framework](https://www.investment.nsw.gov.au/living-working-and-business/nsw-industry-development-framework/).

iSTEM develops enabling skills and knowledge that increasingly underpin many professions and trades, and the skills of a technologically enabled workforce. It provides students with learning opportunities to develop knowledge and skills to use the most up-to-date technologies including additive manufacturing (3D printing), laser cutters, augmented and virtual reality, drones, smart robotics and automation systems, artificial intelligence (AI), and a range of digital systems.

Students gain and apply knowledge, deepen their understanding, and develop collaborative, creative and critical thinking skills within authentic, real-world contexts. The course uses inquiry, problem and project-based learning approaches to solve problems and produce practical solutions utilising engineering design processes.

iSTEM is aligned to the concept of ‘[Industry 4.0](https://www.weforum.org/agenda/2019/01/why-companies-should-strive-for-industry-4-0/)’ which refers to a new and emerging phase in the industrial revolution that heavily focuses on interconnectivity, automation, machine learning, and real-time data.

iSTEM has been developed to meet the goals of National Federation Reform Council (NFRC) Education Council’s [National STEM School Education Strategy (2016-2026)](https://www.dese.gov.au/education-ministers-meeting/resources/national-stem-school-education-strategy), and supports the NSW Government’s [NSW Industry Development Framework](https://www.investment.nsw.gov.au/living-working-and-business/nsw-industry-development-framework/), the NSW Department of Education’s [Rural and Remote Education Strategy (2021-2024)](https://education.nsw.gov.au/about-us/strategies-and-reports/rural-and-remote-education-strategy-2021-24) and the [High Potential and Gifted Education policy](https://education.nsw.gov.au/policy-library/policies/pd-2004-0051).

### Aim

The aim of the course is to engage and encourage student interest and skills in STEM, appreciate the scope, impact and pathways into STEM careers, and learn how to work collaboratively, entrepreneurially, and innovatively to solve real-world problems.

### Purpose and audience

This teaching resource is for teachers delivering or planning to deliver the course. The learning sequence demonstrates how a combination of outcomes can be used to develop teaching and learning activities. It also suggests a range of resources to support teachers when planning and/or teaching the course.

### When and how to use this document

Use this resource when designing learning activities that align with the course outcomes and content. The activities and resources can be used directly or may be adapted based on teacher judgment and knowledge of their students. Consult the course document for further details on sequencing core, elective and specialised topics.

## Learning sequences

This sample learning sequence has been prepared by the NSW Department of Education. It has been developed as a guide for teachers to assist in the development of a teaching and learning program contextualised to an individual school's needs. The scope and depth of the content covered should relate to the school's context, expertise of the teachers delivering the course and the prior knowledge of the students. Plan learning activities that are inclusive and accommodate the needs of all students, in your classroom from the beginning. Some students may require more specific adjustments to allow them to participate on the same basis. Space is provided for adjustments and enhancements that are made to the learning sequence during its implementation, in order to meet the individual needs of students and to allow for differentiation of the iSTEM curriculum. For further advice, see [Additional information](#_Additional_information) in this document.

### Weeks 1 and 2

Table 1 – Cyber security weeks 1 and 2 learning sequence

|  |  |  |  |
| --- | --- | --- | --- |
| Outcomes and content | Teaching and learning | Evidence of learning | Adjustments and registration |
| **Week 1 – Introduction**  **The value of data**  **ST5-5**  Students:   * describe basic concepts of cyber security. | **Teacher**  Introduce the cyber security topic and outline the sequence of activities.  Define data and information, and elaborate on common usage of these terms.  Present 3 scenarios highlighting the value of data, for example:   * Aboriginal weather knowledge * agriculture relying on weather data to plan activities * financial data tracking market trends * consumer purchasing data.   **Students**  Explain the role of data and its value within each scenario.  **Teacher and students**  Consider:   * value of data * value in data * value from data.   Critically analyse the statement, ‘Data is the most valuable asset held by many organisations’.  Discuss, ‘What makes data valuable?’ | Students will be able to describe the difference between data and information, and outline how the terms are commonly used. Students should also be able to explain how the common usage of the term data is sometimes incorrectly used in place of information.  Students are able to explicitly identify data, data types, and explain its purpose within the given scenarios.  Students are actively engaged in the discussion about data and its value.  Students are able to recognise that data in different scenarios (contexts) can be used for a specific purpose and therefore has some inherent value. Some students may recognise that the same data applied to a different purpose or combined with other data may have further value (or additional value).  Students will be engaging in class discussion about the value of data and providing reasons for its value.  Students will recognise data as a valuable asset to organisations and a key reason to protect it. | For the 3 scenarios, consider how to present the examples of data for accessibility including visibility.  Consider a range of strategies and resources which can be used to support EAL/D student understanding and participation, for example:   * glossary of key terms * use visuals.   Provide extra response time during discussions. |
| **ST5-5**  Students:   * describe basic concepts of cyber security. | **Teacher**  Outline how data has different value in different contexts and diverse cultures.  **Teacher and students**  Explore the concept of trust within Aboriginal culture.  Discuss, ‘Can oral histories exist when trust is not present?’  Discuss the concept of trust in students’ own cultures and compare to the ideas of trust in (digital) technology contexts.  **Teacher**  Introduce the notion of protecting data.  Compare and contrast these terms:   * security * information security * cyber security.   **Extension**  Discuss, ‘How do humans behave with things of value?’ | Students are able to describe relevant examples of where and how data can have inherent value determined by its context and/or role in cultural activities.  Students recognise the value of data to the individual as well as to an organisation.  Students recognise ‘value’ as subjective by nature and influenced by culture.  Students can explain the relationship between data (or information) which has some intrinsic value, and the need to protect it.  Students can distinguish between security, information security, and cyber security, and describe the differences and similarities | Consider the varied cultural capital that students may bring into the classroom as a point of reference to connect to new learning. |
| **Ethics**  **ST5-5**  **Students:**   * **describe basic concepts of cyber security** * **distinguish between ethical and unethical behaviour** * **identify legal and ethical issues related to personal and organisational cyber security and evaluate the impact on stakeholders, including consumers, organisations and government.** | **Teacher and students**  **Discuss, ‘How do ethics influence my decisions?’**  **Discuss the relationship between** [ethics, morality and the law (5:13)](https://www.youtube.com/watch?v=Xki2fRA0bY8).  **Teacher**  **Present 3 scenarios with a technology context which highlight behaviours that are either ethical and/or unethical, for example:**   * **internet users getting targeted ads while browsing and using social media platforms** * **recommendation engines on streaming services** * **a social media post containing a (group) photo that has not been cleared for posting by an individual in the post.**   **Students**  Identify relevant people or organisations and their actions in the given scenarios.  Label and justify their actions (or behaviours) as ethical or unethical.  Explain the importance of trust in each scenario. | Students should be able to articulate the ethical values that guide or determine their choices and decisions.  Students should be able to distinguish between ethics, morals, and laws.  Students are able to explicitly identify ethical and unethical behaviours within the given scenarios. Students should be able to explain their reasoning and evaluate different opinions on ethics and ethical behaviour.  Students are actively engaged in the discussion about ethics and its value in society, and on individual choices. | 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. |
| **ST5-5**  Students:   * describe basic concepts of cyber security * distinguish between ethical and unethical behaviour * identify legal and ethical issues related to personal and organisational cyber security, and evaluate the impact on stakeholders, including consumers, organisations, and government. | **Teacher**  Outline any illegal actions or behaviour in the above scenarios.  For scenarios that are not illegal, pose the question, ‘What factors could make this scenario illegal?’  **Students**  Identify who owns the data in each of these scenarios, and who has the ethical responsibility and the legal responsibility to protect it.  **Teacher and students**  Discuss, ‘Can human behaviour be influenced by ownership or the value of data?’ For example, ‘If something has value, how do we respond differently?’  Evaluate, ‘What is the role of trust and [ethics in cyber security](https://dcencompass.com.au/blog/cybersecurity-ethics/)?’  **Teacher**  Present the question for further reflection during the unit,  ‘If trust is essential in cyber security, how can we verify trust to protect information?’  **Extension (optional)**  Discuss, ‘How can we evaluate value objectively?’ | Students are able to identify actions or behaviour from the scenarios that are illegal.  Students are able to describe additional factors or settings that, if introduced into the scenario, would cause issues of legality to be a concern.  Students can evaluate the influence of real or perceived value on human behaviour, and whether the idea of value is linked to ownership.  Students will be able to assess the importance of ethics. | ‘If…how…’ questions can be tricky for EAL/D students to understand. Break down the question form and practice responding.  Provide a summarised version of the [Cybersecurity Ethics](https://dcencompass.com.au/blog/cybersecurity-ethics/) webpage, highlighting key information and ideas. |
| **Privacy**  **ST5-5**  Students:   * describe basic concepts of cyber security * describe their online identity, profile, and data, and the need to protect it. | **Teacher and students**  Watch [Amazing mind reader reveals his 'gift' (2:28)](https://www.youtube.com/watch?v=F7pYHN9iC9I).  Discuss, ‘['What are some reasons to keep your data private](https://www.reputationdefender.com/blog/privacy/top-ten-reasons-keep-your-personal-information-private)?’  Discuss, ‘Who do you trust with your data?’  **Teacher**  Define relevant terms, for example:   * privacy * confidentiality * disclosure * anonymity * public information * personal (or private) information * [personally identifiable information (PII)](https://www.security.org/identity-theft/what-is-pii/) * persona (optional) * [identity theft](https://www.cyber.gov.au/acsc/view-all-content/threats/identity-theft).   Explain the differences and relationship between these commonly misused terms:   * privacy and confidentiality * privacy and anonymity * PII and social identity.   Outline issues with [sharing PII](https://www.cyber.gov.au/acsc/view-all-content/guidance/be-control-what-you-share) online, for example:   * identity theft * future employment. | Students will be able to identify everyday activities that generate data and whether or not it is collected by organisations.  Students will be actively engaged in discussion identifying categories of data, offering an opinion on what (personal) data should be kept private, and provide reasons to justify what data should be private.  Students can correctly recall definitions of privacy-related terms, and this will also be evident as they correctly use terms in their explanations of privacy-related scenarios.  Students are able to properly distinguish between similar (but sometimes misused) terms. More advanced responses will clarify how some terms are incorrectly used. | Teach key vocabulary and concepts prior to viewing videos, provide a transcript, and use closed captions when viewing.  To enable full class discussion, consider the length and complexity of the text and provide a summarised version of the [Top 10 reasons to keep your personal information private](https://www.reputationdefender.com/blog/privacy/top-ten-reasons-keep-your-personal-information-private) webpage, highlighting key information and ideas.  Provide a glossary and allow the use of bilingual dictionaries for uncommon terms. |
| **ST5-5**  Students:   * describe basic concepts of cyber security * describe their online identity, profile, and data, and the need to protect it. | **Students**  Draft a mock social or gamer identity, selecting information that they think is suitable to add to a public profile.  **Teacher and students**  Evaluate mock identities based on the type and value of data presented, for example:   * date of birth * address * terms and conditions of social platforms and ownership of posted photos. | Students will have drafted a mock social or gamer identity and it will only consist of examples of information suitable for public disclosure.  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. | Provide a model and deconstruct it with discussion of key features and language. Consider joint construction of a mock social/gamer identity before or instead of independent construction. |
| **Privacy**  **ST5-5**  Students:   * describe their online identity, profile and data, and the need to protect it. * describe basic concepts of cyber security. | **Teacher**  Present 3 scenarios containing issues related to privacy, for example:   * access to personal medical records * companies analysing spending habits * viewing history (either web or streaming service) * playlist history and suggestions.   **Students**  Determine within the scenarios whether there is a potential for violation of privacy and/or trust.  **Teacher**  Explain (where necessary) how confidentiality becomes an issue in the above scenarios.  **Teacher and students**  Evaluate the consequences of a violation of privacy, confidentiality, and trust.  Identify who is responsible for maintaining privacy and/or confidentiality.  Analyse each scenario and suggest simple options for protecting privacy and confidentiality where responsible parties failed.  **Extension (optional)**  What ethical issues are raised by increased anonymity? | Students are able to explicitly identify issues of privacy and assess whether there is a potential for privacy to be violated within the given scenarios.  Students are able to explain where and how there is a violation of privacy within a given scenario.  Students can explain their reasoning and should be able to respond to different opinions on privacy.  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.  Students can explain the relationship between ethics, trust, privacy, and confidentiality, and their developing understanding of how these concepts are central to the goal of protecting information.  Students will be able to discuss questions around trust, for example, ‘How can I trust this organisation?’ | (Add adjustments and registration). |
| **Weekly reflection** | **Teacher**  Explain purpose of a weekly reflection.  Demonstrate how to complete a weekly reflection using a procedural recount.  **Students**  Assess what they know, what they need to know, and how they might bridge any gap in understanding that exists.  Complete weekly reflections using a school-based template or learning platform. | Students will be able to record their key learning events or activities using a procedural recount.  Students will demonstrate the impact of these learning events or activities by making judgments about what has happened and what they still need to understand. | A procedural recount can be prepared on paper or digitally, including speech-to-text or voice recording.  Model and scaffold to support EAL/D students’ understanding of purpose, audience, language features, and structure. |
| **Week 2 – Protecting data of organisations**  **ST5-5**  Students:   * describe the interrelationship between confidentiality, integrity, and availability (the CIA Triad) and how it underpins privacy * implement access controls * describe basic concepts of cyber security. | **Teacher**  Introduce the role of a cyber security analyst and commence building an image of the role, responsibilities, skills, and knowledge required to:   * proactively defend systems * continuously improve security.   Outline the following goals of information security:   * protecting data/information assets * managing risk * establishing and maintaining trust.   Introduce the CIA Triad as an information security model security professionals and organisations use to develop policies and procedures to protect information and systems.  Outline goals of each component of the CIA Triad with examples:   * Confidentiality – protect data in transit, at rest, and in use * Integrity – trust data has not been tampered with * Availability – denial of service.   Explain the relationship between the 3 components and that how an organisation prioritises information security goals will affect the emphasis placed on each of the 3 components.  **Students**  Use a diagram of the CIA Triad to create a mind map of ‘How data can be protected?’  Explore how physical and logical access to data can be protected in physical and virtual settings. | Students start to build an image of what a cyber security analyst might do, and can describe in this early stage very general statements about the role and its responsibilities.  Students can identify the connections and link the goals of information security with these general roles and responsibilities. The learning of particular skills and knowledge will be acquired through progression in the unit.  Students can identify protecting, risk, and trust as key concepts.  Students can recall the CIA Triad is a model used to develop (and assess) information security policy and procedures.  Students can explain why trust is so important to cyber security, and how it is implicit in each component of the CIA Triad and one of the overarching goals of information security.  Students can define information assets to include information, technology, and systems.  Students will realise and be able to describe how the CIA Triad is a model that also represents the relationship between the 3 core components or goals, and that an organisations’ choices may lean on one or 2 goals more than the others.  Students will have created a mind map expressing their understanding of the connections between various terms and concepts. | Consider student needs and alternative options when using graphical organisers like mind maps.  Model how to complete whatever graphic organiser is used, as students may not be familiar with these learning tools. |
| **ST5-5**  Students:   * describe basic concepts of cyber security * implement access controls. | **Teacher**  Describe security controls used to ensure the goal of confidentiality (protecting data from unauthorised disclosure) such as:   * access controls * encryption.   **Student**  Add terms and descriptive text (and/or images) to mind map. | Students can identify a number of security controls and can describe their basic functions.  Students can then explain how a given security control is used to achieve the goal of confidentiality.  Students will have added extra words and descriptions to their mind map expressing their understanding of the connections between various terms and concepts. | Consider student needs and alternative options when using graphical organisers like the mind map. |
| **ST5-5**  **Students**   * **describe basic concepts of cyber security** * **implement access controls.** | **Teacher**  Describe security controls used to ensure the goal of integrity (protecting data from being altered without authorisation) such as:   * access controls * hashing * digital signatures * digital certificates.   Define authenticity and non-repudiation.  Demonstrate how to use **gpg** **tools** to verify the authenticity of a file.  Demonstrate how to use **sha256** **tools** to verify the integrity of a file.  **Students**  Add terms and descriptive text (and/or images) to mind map. | Students can identify a number of security controls and can describe their basic functions.  Students can then explain how a given security control is used to achieve the goal of integrity.  Students can recall the definitions of authenticity and repudiation.  Students are able to use software tools to check hash values and digital signatures of files for integrity and authenticity.  Students will have added extra words and descriptions to their mind map expressing their understanding of the connections between various terms and concepts.  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? | Terminology like ‘authenticity’ and ‘repudiation’ may require additional scaffolding for some students.  Provide a glossary and allow students to translate vocabulary into home languages.  Provide visual and/or multimedia examples and check understanding of concepts. |
| **ST5-5**  Students:   * describe basic concepts of cyber security * implement access controls. | **Teacher**  Describe security controls used to ensure the goal of availability (information and systems remain available to authorised users when needed) such as:   * redundancy and load balancing * backups * OS and application patching.   **Students**  Add terms and descriptive text (and/or images) to mind map. | Students can identify a number of security controls and can describe their basic functions.  Students can then explain how a given security control is used to achieve the goal of availability.  Students will have added extra words and descriptions to their mind map expressing their understanding of the connections between various terms and concepts. | Consider accessibility needs and alternative options when using graphical organisers like the mind map. |
| **Examining access controls and identification**  **ST5-5**  Students:   * describe basic concepts of cyber security * implement access controls * identify cyber security approaches * identify tools, controls, and technologies commonly used to protect people and organisations from a cyber-attack. | **Teacher**  Explain the 3 stages of the access control process and how they could be implemented in organisations (enterprises):   * identification * authentication * authorisation.   Present 3 scenarios where access controls would be used, for example:   * high school * bank * Service NSW.   **Students**  Explain using examples how access controls are used in these organisations.  **Teacher**  Outline mechanisms users can use or implement to uniquely identify themselves to a system, for example:   * usernames * access cards, including magnetic stripe cards, photo identification, RFID, NFC * biometrics, including fingerprint scan, eye scan, facial recognition.   **Students**  Assess identification mechanisms and technologies for weaknesses.  **Extension (optional)**  Investigate other biometric techniques used to uniquely identify individuals for access to systems, for example:   * hand geometry analysis * handwritten analysis * keystroke dynamics.   Compare the costs and efficiency of a range of biometric techniques. | Students can explain the function and requirement for each stage or process in access control. The explanation should demonstrate understanding of the subtle difference and relationship between all 3.  Students will be actively engaging with discussion around the chosen scenarios, and be able to explain how the 3 processes operate and why they are an essential requirement in a given scenario.  Students can describe a range of mechanisms which can be used to identify individuals to a system.  Students will be able to point out weaknesses in or strategies to circumvent a range of identification mechanisms. | Provide a glossary and allow students to translate vocabulary into home languages.  Provide visual and/or multimedia examples and check understanding of concepts.  Consider students at different levels of English language proficiency.  In creating or selecting scenarios, consider students’ own experiences and use of visuals. Ensure all students understand both technical and culturally-based terms. |
| **Authentication access controls**  **ST5-5**  Students:   * describe basic concepts of cyber security * implement access controls. | **Teacher**  Describe 3 authentication factors:   * something you know * something you are * something you have.   Present 3 (or more) scenarios illustrating authentication processes, for example:   * password to access a computer or network * using fingerprint to unlock a phone * entering a PIN at an ATM * answering secret questions * authentication token key fob or USB drive * SMS messages with one time use code or password (OTP).   **Students**  Classify provided examples of authentication processes according to 3 authentication factors above.  Analyse examples to identify strengths and weaknesses of each authentication process.  **Teacher and students**  Rank authentication factor and/or authentication processes in order of most secure to least secure. | Students can describe the factors with relevant examples.  Students will be actively engaging with discussion around the chosen scenarios and be able to identify the factor from the authentication process in each scenario.  Students can point out the strengths and weaknesses of a given authentication process.  Students will be able to indicate the relative merit of a range of given authentication processes in terms of security. | (Add adjustments and registration). |
| **ST5-5**  Students:   * describe basic concepts of cyber security * implement access controls. | **Teacher**  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) * password keys * certificate-based authentication.   Explain the principles of [multi-factor authentication](https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-multi-factor-authentication) (MFA) and how this increases security.  Present 3 scenarios each illustrating multiple authentication processes, for example:   * providing a password and answering a security question * providing a password and using a fingerprint scan.   **Students**  Evaluate each scenario to determine if it is using multifactor authentication (2 different factors) or not. | 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. | Teachers should consider a range of examples of authentication, including multi-sensory.  Provide a glossary and allow students to translate vocabulary into home languages.  Provide visual and/or multimedia examples and check understanding of concepts. |
| **ST5-5**  Students:   * describe basic concepts of cyber security * implement access controls. | **Teacher**  Demonstrate the setup and/or use of two-factor authentication (multi-factor authentication), for example:   * Authenticator app * Office 365 2FA * [Google accounts](https://www.cyber.gov.au/acsc/view-all-content/guidance/turning-two-factor-authentication-gmail) * website access.   **Students**  Set up and/or use two-factor authentication to use an online platform.  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 CAPTCHA are identification or authentication access control processes.  **Extension (optional)**  Investigate authentication protocols, for example:   * Kerberos * LDAP * OpenID * deprecated and/or insecure protocols. | 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 are able to 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. | (Add adjustments and registration). |
| **Weekly reflection** | **Teacher**  Monitor the progress of student reflections.  **Student**  Assess what they know, what they need to know, and how they might bridge any gap in understanding that exists. | Students will demonstrate the impact of these learning events or activities by making judgments about what has happened and what they still need to understand. | A procedural recount can be prepared on paper or digitally, including speech-to-text or voice recording. |

### Weeks 3 and 4

Table 2 – Cyber security weeks 3 and 4 learning sequence

|  |  |  |  |
| --- | --- | --- | --- |
| Outcomes and content | Teaching and learning | Evidence of learning | Adjustments and registration |
| **Week 3 – Secure passwords and human behaviour**  **ST5-5**  Students:   * Students implement access controls. | **Teacher and students**  Discuss, ‘How important are strong passwords and what amounts to a strong password?’  Discuss examples of [weak passwords](https://www.csoonline.com/article/3526408/most-common-passwords.html) and strong passwords.  **Teacher**  Demonstrate the [time required to hack a password](https://www.security.org/how-secure-is-my-password/) of varying lengths and complexity, for example:   * [password length matrix](https://www.hivesystems.io/blog/are-your-passwords-in-the-green) * password generator sites.   Define what is meant by human behaviour.  **Teacher and students**  Discuss elements of human behaviour which influence bad habits in password creation and use, for example:   * using [common passwords](https://nordpass.com/most-common-passwords-list/) * using patterns * using numbers and special characters only at the end * using character substitutions * using the same password on multiple sites.   **Teacher**  Demonstrate how to check if username/password has been [exposed in known data breaches](https://haveibeenpwned.com/Passwords).  Compare [passphrases](https://www.avg.com/en/signal/how-to-create-a-strong-password-that-you-wont-forget) with passwords.  Demonstrate [strategies](https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd) to generate a strong password or passphrase, for example:   * [three random words](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words) * [password strength checker](https://www2.open.ac.uk/openlearn/password_check/index.html).   Demonstrate how to use a [password manager](https://tech.co/password-managers/how-many-passwords-average-person).  Outline new strategies and technologies being developed to replace passwords.  **Students**  Use strategies to generate a strong password. | Students actively participate in class discussion and present logical reasoning to respond to the question.  Students can recognise the difference between weak and strong passwords.  Students will be able to generate a strong password.  Students will be able to use a password manager.  Students will know that browser-based password managers are less secure than desktop password manager applications.  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). | Consider accessibility needs and check for built-in features when using password generators and/or password manager software. |
| **Authorisation access controls**  **ST5-5**  Students:   * describe basic concepts of cyber security * implement access controls. | **Teacher**  Explain how the principle of least privilege:   * minimises the risk of potential damage from insider attacks * limits ability of external attackers to easily gain privileged access.   Explain how the principle of separation of duties reduces risk and enables stronger security.  **Students**  Describe a scenario where elevated privileges permit unauthorised activity.  **Teacher**  Demonstrate the use of access control lists on files and directories stored on a chosen operating system, for example:   * Windows server or domain-based client (NTFS) * Linux * MacOS.   **Students**  Set access control lists on files and directories. | Students can explain how the principles of least privilege and separation of duties can be implemented and how authorisation controls improve overall security posture.  Students’ description of a scenario where there is unauthorised activity will be based on credible circumstances reflecting issues organisations face.  Student can apply ACL permissions on a computing platform used in class. | (Add adjustments and registration) |
| **Threats and vulnerabilities**  **ST5-2, ST5-5**  Students:   * describe basic concepts of cyber security * identify cyber security approaches * analyse types of cyber security threats and how they are used to attack organisations, individuals, computer systems, and networks * complete a cyber risk assessment of an organisation and at home. | **Teacher**  Define following terms within the cyber security context:   * risk * threats * vulnerability * likelihood * impact.   Explain the relationship between risk, vulnerability, and threats using various representations, for example:   * threat + vulnerability = risk * risk = threat × vulnerability * risk = likelihood × impact * Venn diagrams.   Develop further insight of the cyber security analyst role with these additional responsibilities:   * leverage intelligence and threat detection * analyse and interpret data * identify and assess vulnerabilities * suggest preventative measures * respond to and recover from incidents. | Students can recall the definitions of relevant terms and use them in the correct context.  Students can explain multiple relationships between these 5 terms, and demonstrate an understanding beyond formulaic recall of the nuance between different representations. For example, the first representation shows that a threat and vulnerability combined will create a risk, while the second representation indicates that minimising either the threat or vulnerability will minimise the risk. Alternatively, reduce or remove the threat, and the risk is reduced or removed (that is, mathematically, multiply something by zero and the result is zero).  Students’ use of various representations supported with explanations will demonstrate their level of understanding.  Students continue to build an image of what a cyber security analyst might do and can describe additional information, including more statements about role and responsibility. Having additional knowledge about cyber concepts, they will also be able to provide relevant context to these activities. | (Add adjustments and registration). |
| **ST5-2, ST5-5**  Students:   * describe basic concepts of cyber security * analyse types of cyber security threats and how they are used to attack organisations, individuals, computer systems, and networks * complete a cyber risk assessment of an organisation and at home. | **Teacher**  Present 3 scenarios each illustrating threats, vulnerabilities, and potential risks, for example:   * not applying updates for operating system or software applications * clicking on unknown email links * downloading a torrent * browsing the web for cracked software.   **Students**  Identify the threat and vulnerability in each scenario.  Assess the likelihood and impact of each threat event occurring and/or the vulnerability being exploited.  **Teacher and students**  Discuss scenarios and student responses and evaluate the risk with a 5 × 5 risk matrix. | Students can assess the provided information in given scenarios and correctly identify any threat, vulnerability, and potential risk. Alternatively, students could demonstrate understanding by creating and describing hypothetical scenarios which illustrate threats, vulnerabilities, and risks, and explaining how and why the scenario shows this.  If the scenario lacks enough detail, this could also allow students to ask for clarification, and provide another pathway for them to demonstrate understanding.  Students will demonstrate further understanding by giving a considered assessment of likelihood and impact within given scenarios. This would also be an indicator of their understanding of the mechanics and human behaviour involved.  Students are able to describe the layout and function of a simple 5 × 5 risk matrix and apply it to a given scenario. | (Add adjustments and registration). |
| **Threats**  **ST5-2, ST5-5**  Students:   * describe basic concepts of cyber security * identify cyber security approaches * analyse types of cyber security threats and how they are used to attack organisations, individuals, computer systems, and networks * **explain how hardware technologies are targeted and exploited in a cyber-attack** * **explain how software applications are targeted and exploited in a cyber-attack** * **explain how critical infrastructure is targeted and exploited in a cyber-attack.** | **Teacher**  Define related threat language, for example:   * threat landscape * threat intelligence * threat hunting * threat actor.   Outline different types of threat actors (or adversaries) and their known motivations.  Outline some common cyber security threats, for example:   * incorrectly configured systems * threats against data * email related threats * malware * IoT threats * password attacks * supply chain threats.   **Students**  Analyse a [list of recent significant cyber incidents](https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents) and create a list of the types of critical infrastructure threat actors and adversaries target.  **Teacher**  List the 11 sectors and 22 asset classes as defined by the [Australian government](https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018).  Compare with [16 critical infrastructure sectors](https://www.cisa.gov/critical-infrastructure-sectors) as defined by United States government Cyber security and Infrastructure Agency (CISA).  **Students**  Explain the possible [impact of a cyber-attack](https://en.wikipedia.org/wiki/Stuxnet) on a specific sector or industry. | Students can recall definitions of threat terminology with enough detail to highlight distinguishing aspects.  Students can recognise a wide range of common cyber security threats and demonstrate understanding of how they function, what vulnerability they target and/or their likelihood and potential impact.  Students will produce a summary list of recent cyber incidents organised to show the identified target grouped by types of critical infrastructure.  Students can identify alignment between the types or categories identified by them and the list of 11 critical infrastructure sectors, and can place remaining incidents into one of the 11 categories.  Students will be able to infer and justify the potential impact of a form of cyber-attack on a sector/industry target. | Ensure students understand the meaning of ‘threat’ before introducing these other terms/concepts.  Ensure the [Significant Cyber Incidents](https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents) webpage text is accessible and comprehensible for EAL/D students  Provide a summarised version of the webpage content, highlighting key information and ideas. |
| **Weekly reflection** | **Students**  Complete weekly reflection identifying tasks undertaken, new knowledge, understanding or skills. | Students answer reflective questions, for example:  What did I learn about this week? | A procedural recount can be prepared on paper or digitally, including speech-to-text or voice recording. |
| **Week 4 – Industrial control systems**  **ST5-4, ST5-5, ST5-6**  Students:   * describe basic concepts of cyber security * identify cyber security approaches. | **Teacher**  Outline the history of industrial control systems (ICS) and their role in society.  Explain the significance of technology changes in the evolution of ICS security posture, for example:   * [air gap](https://gca.isa.org/blog/common-ics-cybersecurity-myth-1-the-air-gap) * internet of things (IoT).   Select the simulation platform appropriate to students needs and resourcing.  **Students**  Evaluate the impact of technological changes that increased the exposure to threats and vulnerabilities of the ICS infrastructure. | Students can explain the repercussions of ICS switching from predominantly operational technology (OT) focused, to informational technology (IT) focused.  Students can assess the increased exposure to cyber threats.  Students will complete the activities demonstrated by the teacher **using the selected platform.** | (Add adjustments and registration) |
| **ST5-4, ST5-6**  Students:   * Students describe basic concepts of cyber security. | **Teacher**  Outline the purpose of the model and function of individual components within the selected simulation platform, for example:   * ICS infrastructure – programmable hardware modelling a specific function (PLC) * hardware devices, such as clients, hosts/servers, and network medium * software.   Outline the sequence of activities to be completed, for example:   * manual control (air gap) * remote monitoring (connected) * surveillance * tampering/spoofing.   Demonstrate how to set up a testing lab to model a scenario.  Demonstrate how to set up a scenario-based learning environment to model a function of an ICS, for example:   * Cyber city (micro:bits) * virtual machines (images) * isolated computer network.   Demonstrate how to run necessary software and/or upload code to devices.  **Student**  Connect and/or configure devices as directed to represent the initial state of the ICS simulation. | Students can relate individual components within the selected simulated platform to components of the model ICS. | During practical learning activities, use and emphasise target language required and encourage students to use this language in context. |
| **Manual and automated control processes**  **ST5-4, ST5-5, ST5-6**  **Students:**   * **describe basic concepts of cyber security** * **identify cyber security approaches.** | **Teacher**  Present additional context to an ICS/PLC scenario where a programmable control process is required.  Demonstrate the code and/or software required to manually respond to changes in the ICS function.  **Students**  Modify code and/or configure software to manually respond to changes in the ICS function.  Test and confirm changes in process of the ICS function.  **Teacher**  Present additional context to the ICS/PLC scenario where an automated control process is now required.  Demonstrate the code and/or software required to automate the ICS process.  **Students**  Modify code and/or configure software to automate the ICS process.  Test and confirm changes in the function of ICS process. | Students can describe the ICS function and its purpose. | (Add adjustments and registration). |
| **Networked**  **ST5-4, ST5-5, ST5-6**  **Students:**   * describe how software and hardware communicate across a network * complete practical exercises solving cyber security problems. | **Teacher**  Explain the current state of the ICS simulation compared with the historical perspective of isolated (air gap) systems.  Present additional context to the ICS/PLC scenario where a remote monitoring (and control) process is required.  Demonstrate setup of additional devices and network, and procedures to connect to the network.  Demonstrate the code and/or software required to remotely monitor state and automated processes of the ICS function.  **Students**  Set up and configure additional devices to connect to the network.  Modify code and/or configure software to remotely monitor and control changes in the ICS function.  Test and confirm changes in the process of the ICS function.  **Teacher**  Explain relevant aspects of networking within the ICS simulation and how devices and nodes are communicating.  **Students**  Describe how software and hardware communicate across this network.  **Extension (optional)**  Explain any abstraction (elements that are ‘black-boxes’) of the simulation, issues with ‘sandboxing’, and potential limitations when compared to industrial/enterprise networks. | (Add evidence of learning). | (Add adjustments and registration). |
| **Weekly reflection** | **Teacher**  Monitor the progress of student reflections.  **Student**  Complete weekly reflection evaluating new knowledge, understanding or skills in relation to previous knowledge. | Students will demonstrate the impact of these learning events or activities by making judgments about what has happened and what they still need to understand. | Modelling of the reflective process may assist with the metacognitive aspects of this task. |

### Weeks 5 and 6

Table 3 – Cyber security weeks 5 and 6 learning sequence

|  |  |  |  |
| --- | --- | --- | --- |
| Outcomes and content | Teaching and learning | Evidence of learning | Adjustments and registration |
| **Week 5 – Covertly viewing commands**  **ST5-4, ST5-5**  Students:   * describe basic concepts of cyber security * analyse types of cyber security threats and how they are used to attack organisations, individuals, computer systems, and networks * complete practical exercises solving cyber security problems. | **Teacher**  Present additional context to a ICS/PLC scenario where a threat actor/adversarial node has access to the network.  Demonstrate setup of an ‘attack node’ and procedures to connect to the network.  Demonstrate the code and/or software required to covertly monitor ICS activity from attack node, including commands and state data.  **Students**  Set up and configure an attack node device(s) to connect to the network.  Modify and upload code and/or configure software to covertly monitor ICS activity from an attack node.  Test and confirm code operation and record details of any ICS activity, including commands and transmitted data. | Students can describe the progression of the scenario and what each component is doing at this stage.  Students can recognise the vulnerability of transmitting data on a network in plaintext.  Students have either produced functioning code, made modifications to a code base, or changed software configuration settings at the attack node and observed plaintext messages being transmitted and received across the network. | (Add adjustments and registration) |
| **Altering/injecting commands**  **ST5-5**  Students:   * describe basic concepts of cyber security * complete practical exercises solving cyber security problems. | **Teacher and students**  Define espionage and reconnaissance.  Discuss the implications of viewing transmitted ICS/PLC commands and data in plaintext, for example, confidentiality.  Discuss the implications of altering ICS/PLC commands, for example:   * intercepting * theft * modification – integrity, non-repudiation * disabling infrastructure – availability. | Students can recall the definitions of espionage and reconnaissance in relation to cyber security.  Students will be able to explain some implications of both viewing and modifying ICS/PLC commands. | (Add adjustments and registration) |
| **ST5-4, ST5-5**  Students:   * complete practical exercises solving cyber security problems. | **Teacher**  Demonstrate the code and/or software changes required to covertly modify ICS activity from the attack node, including commands, responses, and state data.  **Students**  Modify and upload code and/or configure software to covertly alter ICS activity from the attack node.  Test and confirm code operation, and record details of any changed ICS activity, including commands, responses, and transmitted data.  Confirm that the ICS infrastructure is disabled or inoperable. | Students can describe the progression of the scenario and what each component is doing at this stage.  Students can describe the exploit used and explain how it is working.  Students have either produced functioning code, made modifications to a code base, or changed software configuration settings at the attack node and injected modified messages to alter ICS activity.  Students have a record of their functioning code, noting the relevant changes, and records of the commands, responses, and transmitted data.  Students will be able to explain how and why the code has caused the observable changes, which should be that their code has disabled the ICS infrastructure. | (Add adjustments and registration). |
| **Implement basic encryption**  **ST5-4, ST5-5**  Students:   * apply encryption to secure data * use security mechanisms and tools to protect systems * complete practical exercises solving cyber security problems. | **Teacher**  Outline a brief history of cryptography and define relevant terms, for example:   * cryptography * encryption * decryption * cipher * ciphertext * key * algorithm.   Explain the difference between cryptography and encryption.  Describe the function of the Caesar cipher.  Outline the 3 essential elements required for all types of encryption:   * plaintext (clear text) * algorithm * key (encryption key). | Students can outline a brief history of cryptography, which indicates earliest known applications of cryptography and notes significant people or events along with the evolution of cryptography and use of encryption.  Students can recall definitions of relevant terms and use them in the correct context.  Students can distinguish between cryptography as a study or discipline and encryption as a process.  Students are able to describe how a Caesar cipher works, using either text and diagrams or a physical cipher wheel.  Students will be able to recall the 3 elements required for all encryption and identify the algorithm and key when presented with a type of encryption. | (Add adjustments and registration). |
| **ST5-4, ST5-5**  Students:   * complete practical exercises solving cyber security problems. | **Teacher**  Demonstrate the code and/or software changes required to encrypt commands and data and conceal ICS activity from the attack node using classic encryption, for example:   * Caesar cipher (historically defined as a shift of 3 characters) * another shift cipher.   **Students**  Modify and upload code and/or configure software to encrypt commands and data and conceal ICS activity from the attack node.  Test and confirm code operation, and record details of any changed output.  Confirm that the ICS infrastructure is operating correctly and does not respond to injected plaintext commands from the attack node**.** | Students can describe the progression of the scenario and what each component is doing at this stage.  Students can describe the encryption used and explain how it is working.  Students have either produced functioning code, made modifications to a code base, or changed software configuration settings to conceal ICS activity from the attack node.  Students have a record of their functioning code, noting the relevant changes, and records of the commands, responses, and transmitted data.  Students will be able to explain how and why the code has caused the observable changes, which should be that plaintext commands from the attack node are now ineffective on the ICS infrastructure. | (Add adjustments and registration). |
| **ST5-4, ST5-5**  Students:   * complete practical exercises solving cyber security problems. | **Teacher**  Explain the weakness of the Caesar cipher (or chosen shift cipher) and other types of substitution ciphers, for example:   * brute force attack * frequency analysis of characters.   Demonstrate code and/or software changes required to decrypt commands and data and reveal ICS activity at the attack node.  **Students**  Use knowledge of the key and algorithm, modify and upload code and/or configure software to decrypt commands and data and reveal ICS activity at the attack node.  Use the ability to encrypt commands with the same algorithm and key, modify and upload code and/or configure software to continue to covertly alter ICS activity from the attack node.  Test and confirm code operation, and record details of any changed ICS activity, including commands, responses, and transmitted data (in plaintext and ciphertext).  Confirm that the ICS infrastructure is disabled or inoperable (again).  **Teacher and students**  Discuss how to improve encryption of commands and responses to restore the confidentiality of ICS activity, for example:   * key length and algorithm * expected structure of commands (combination of metadata and frequency analysis) * other types of encryption. | [insert evidence of learning] | (Add adjustments and registration). |
| **More on encryption**  **ST5-4, ST5-5, ST5-6**  Students:   * describe how software and hardware communicate across a network * apply encryption to secure data * complete practical exercises solving cyber security problems. | **Teacher**  Outline other shift and substitution ciphers.  Review (and continue) the historical development of encryption algorithms, processes, and associated technology with a focus on modern encryption.  Explain the difference between symmetric and asymmetric encryption.  Demonstrate how to create a private and public key pair.  Teacher and students  Investigate steganography.  Evaluate the role of encryption and other cryptographic technologies in today’s society, assessing how well encryption is able to protect data.  **Students**  Describe examples of organisations, systems, or technology using encryption today. | Students can outline a range of encryption algorithms ordered from classical to modern encryption.  Students can describe how asymmetric encryption works.  Students will be able to generate their own public/private key pairs for secure transmission of data, for example:   * ssh-keygen * PuTTYgen.   Students use steganography to conceal data within images.  Students can provide examples of encryption used today, for example:   * protecting stored data on devices (data at rest) * secure network communications (data in motion).   Students can discuss the value of encryption in terms of:   * providing confidentiality * protecting integrity * ensuring availability. | (Add adjustments and registration). |
| **Weekly reflection** | **Teacher**  Monitor the progress of student reflections.  **Students**  Complete weekly reflection identifying tasks undertaken, new knowledge, understanding or skills. | Students answer reflective questions, for example:   * What did I learn about coding this week? | A procedural recount can be prepared on paper or digitally, including speech-to-text or voice recording. |
| **Week 6 – Threat modelling**  **ST5-5**  Students:   * describe basic concepts of cyber security * analyse types of cyber security threats and how they are used to attack organisations, individuals, computer systems, and networks * complete practical exercises solving cyber security problems. | **Teacher**  Outline the role of [threat modelling](https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/) to identify threats to a product or system in a structured way in order to improve its engineering.  Explain how threat modelling can be used to predict how a system or software design will handle real-world cyber security challenges.  List some threat modelling frameworks and/or tools.  Explain how the STRIDE threat modelling framework operates and its 4 simple questions.   * What are we working on? * What can go wrong? * What are we going to do? * Did we do a good job?   Elaborate on each letter of the mnemonic:   * S – spoofing * T – tampering * R – repudiation * I – information disclosure * D – denial of service * E – elevation of privilege.   Describe an example for each threat category (letter) of the framework.  **Students**  Identify the desired goal that is being violated in each example. | Students can recall the definition of threat modelling and outline some reasons why it is important in cyber security.  Students will also be able to explain why threat modelling is an important process to consider when starting to engineer or design a system.  Students will be able to recall the components of the STRIDE mnemonic, explain what each letter stands for, and the type of threat it represents.  Students can recall and correctly match the security control being breached to a range of scenarios. | (Add adjustments and registration) |
| **(Optional)**  **Threat modelling game**  **ST5-4, ST5-5**  Students:   * complete practical exercises solving cyber security problems. | **Teacher and students**  Ask, ‘What can we learn from playing games?’ For example:   * [strategies](https://www.schneier.com/academic/archives/1999/12/attack_trees.html) * effect of chance.   **Teacher**  Present the rules of [Elevation of privilege](https://www.microsoft.com/en-us/download/details.aspx?id=20303) and demonstrate how to set up and play.  **Teacher and students**  Play Elevation of privilege. At the conclusion of the game, discuss experiences and what was learnt. | Students are actively engaged in playing Elevation of privilege and can articulate the links between the game and threat modelling processes. | (Add adjustments and registration) |
| **ST5-4, ST5-5**  Students:   * complete practical exercises solving cyber security problems. | **Teacher**  Create a new scenario to threat model using STRIDE and its 4 questions. Alternatively, use the original ICS scenario. If using a new scenario, fully describe or demonstrate the operation of relevant systems within the scenario.  **Teacher and students**  Apply STRIDE where relevant to the chosen scenario.  Define the system and its boundaries. What are we working on?  Using experiences and knowledge from the ICS scenario, focus on answering the second and third question for the chosen scenario.   * What can go wrong? * What are we going to do?   **Students**  Record scenario details and answers. | Students complete threat modelling activities, identifying potential threats and developing solution(s) to resolve identified issues and weaknesses. | (Add adjustments and registration). |
| **Threat modelling**  **ST5-4, ST5-5**  Students:   * describe basic concepts of cyber security * analyse types of cyber security threats and how they are used to attack organisations, individuals, computer systems, and networks * apply encryption to secure data * use security mechanisms and tools to protect systems * complete practical exercises solving cyber security problems. | **Teacher and students**  Continue the threat modelling exercise from previous lesson.  **Teacher**  Provide opportunity for students to explore and apply ideas, designs, and code solutions to the selected scenario.  **Students**  Modify and upload code and/or configure software to enhance the security of the system.  Test and confirm code operation, and that the system is operating correctly.  Record details, including relevant messages or outputs from the system.  **Teacher and students**  Assess, ‘Did we do a good job?’ (question 4 in STRIDE).   * What counts as a good job? * How do we know we were successful? * How do we know we completed the job? * What if …?   **Students**  Record final scenario details and answers, including a summary of applied modifications. | Students complete threat modelling activities, presenting a modified solution with explanations of how they identified potential threats and how their solution resolves previously identified issues and weaknesses.  Students are actively engaged in class discussion, critically evaluating the threat modelling process they undertook and assessing the validity of the proposed solution. | (Add adjustments and registration). |
| **ST5-5**  Students:   * describe basic concepts of cyber security. | **Teacher**  Outline the historical mindset of cyber security, which focused on maintaining perimeter defences, and explain how changes in technology and the cyber threat landscape required a change from this mindset.  Describe the principle of defence in depth.  Explain the need for a resilient modern security posture to include these 3 equally important dimensions:   * prevention * detection * response.   Explain the concurrent nature of these dimensions. | (Add evidence of learning). | (Add adjustments and registration). |
| **Weekly reflection** | **Teacher**  Monitor the progress of student reflections.  **Students**  Complete weekly reflection evaluating new knowledge, understanding or skills in relation to previous knowledge. | Students answer reflective questions, for example:   * What did I learn about coding this week?   How is this learning activity like the operation of sensors in normal cars? | A procedural recount can be prepared on paper or digitally, including speech-to-text or voice recording. |

### Weeks 7 and 8

Table 4 – Cyber security weeks 7 and 8 learning sequence

|  |  |  |  |
| --- | --- | --- | --- |
| Outcomes and content | Teaching and learning | Evidence of learning | Adjustments and registration |
| **Week 7 – Vulnerabilities**  **ST5-4**  Students:   * describe basic concepts of cyber security * explain how hardware technologies are targeted and exploited in a cyber-attack * explain how software applications are targeted and exploited in a cyber-attack * develop an understanding of the cyber security industry. | **Teacher**  Define additional vulnerability terminology, for example:   * [Common Vulnerabilities and Exposures (CVE)](https://cve.mitre.org/) database * [CVSS](https://www.first.org/cvss) * [zero-day vulnerability](https://docs.tenable.com/cyber-exposure-studies/2021-threat-landscape-retrospective/Content/ZeroDayVulnerabilities.htm) * [zero-day exploit](https://www.cyber.gov.au/acsc/view-all-content/glossary/zero-day-0-day).   Outline 3 main types of vulnerability and their causes:   * operating system * software applications * configuration.   Outline strategies or methods to prevent attacks based on exploits of vulnerabilities, for example:   * patching * upgrade, replace, remove, or uninstall * upgrade firmware * change default passwords * reconfigure.   Identify other public repositories of vulnerabilities, alerts, and advisories.  **Students**  Examine a sample of vulnerabilities and recommend suitable actions. | Students can correctly apply relevant terminology.  Students can classify given vulnerabilities into one of the 3 categories and propose appropriate mitigation actions.  Students can identify the importance of rapid response to minimise the risks of exposure to known vulnerabilities. | (Add adjustments and registration) |
| **Secure coding**  **ST5-5**  Students:   * describe basic concepts of cyber security * identify tools, controls, and technologies commonly used to protect people and organisations from a cyber-attack * explain how software applications are targeted and exploited in a cyber-attack. | **Teacher**  Outline the principals of secure coding, for example:   * [secure by design](https://www.veracode.com/blog/managing-appsec/security-needs-shift-left-and-right) * secure by default * secure by communication * secure by implementation.   Outline secure coding best practices, for example:   * validate input * default deny * threat modelling * cryptographic practices * use effective quality assurance techniques.   **Teacher and students**  Explore a range of software testing practices, for example:   * software composition analysis (SCA) * static application security testing (SAST) * advanced fuzz testing (AFT) fuzzing.   Investigate version control software and processes. | Students can describe the principles and practices of secure coding:   * security by design * shift-left * trust boundaries * secure by default * defence in depth * robust error checking * trust no input * least privileges.   Students can describe what types of vulnerabilities are addressed through each testing practice, for example:   * SCA for CVE, known vulnerabilities * SAST for CWE, known software weaknesses * AFT for zero days.   Students can describe parts of the continuous security testing process. | (Add adjustments and registration) |
| **Vulnerability scanning**  **ST5-5**  Students:   * describe basic concepts of cyber security * identify tools, controls, and technologies commonly used to protect people and organisations from a cyber-attack * explain how hardware technologies are targeted and exploited in a cyber-attack * explain how software applications are targeted and exploited in a cyber-attack. | **Teacher**  Outline the process of a vulnerability assessment, including vulnerability scanning.  Describe the difference between vulnerability assessment and penetration testing.  Demonstrate how to use a network scanner for vulnerability scanning and network discovery, for example:   * nmap * Zenmap.   Use an isolated or virtual network.  Demonstrate how to use a vulnerability scanner, for example:   * Nessus * Nexpose * OpenVAS * Burp Suite.   **Teacher and students**  Investigate the use of a vulnerability scanner using an isolated or virtual network of VMs.  Generate report of vulnerabilities found on tested systems.  **Students**  Record details of practical activities. | Students can distinguish between vulnerability assessment and scanning.  Students can distinguish between vulnerability assessment and penetration testing (pentest).  Students are able to safely demonstrate how to use network scanning software to scan an isolated test network for vulnerabilities and network discovery.  Students are able to analyse and explain the output from the selected network scanning software.  Students can identify commonly used ports, and associated network protocol and services, for example:   * port 80 * http (web).   Students can explain what a port is, and the significance of open ports on systems.  Students can identify components of the vulnerability report, for example severity and type.  Students will have a record of activities performed and the resulting output. | (Add adjustments and registration) |
| **Weekly Reflection** | **Teacher**  Monitor the progress of student reflections.  **Student**  Complete weekly reflection identifying tasks undertaken, new knowledge, understanding or skills. | Students answer reflective questions, for example:   * What did I learn about this week? | A procedural recount can be prepared on paper or digitally, including speech-to-text or voice recording. |
| **Week 8 – Threat detection**  **ST5-5**  Students:   * describe basic concepts of cyber security * identify tools, controls, and technologies commonly used to protect people and organisations from a cyber-attack * explain how hardware technologies are targeted and exploited in a cyber-attack * explain how software applications are targeted and exploited in a cyber-attack. | **Teacher**  Present the average time to detect a breach or compromise on an organisation’s network.  Outline the historical development of threat detection technologies from intrusion detection systems (IDS) through to security information, event management (SIEM), and application of artificial intelligence.  Outline the functions of IDS and differentiate between host-based intrusion detection (HIDS) and network-based intrusion detection systems (NIDS).  Present examples of IDS tools, including:   * software applications * physical appliances * HIDS * NIDS.   Outline detection methods:   * signature-based * anomaly-based * specification-based detection.   Outline the functional differences of intrusion prevention systems (IPS) from an IDS.  Outline the function of security information and event management (SIEM) and [extended detection and response](https://www.paloaltonetworks.com/cyberpedia/what-is-xdr) (XDR) systems.  Outline the process of Security Event Correlation to enhance detection of intrusion.  Describe the concept, [benefits, and risks of a honeypot](https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/honeypots-and-deception/) as a cyber security strategy.  **Teacher and students**  Investigate IDS software (and/or IPS software tools) using practical activities where possible, for example:   * OSSEC (HIDS) * Advanced Intrusion Detection Environment (AIDE) (HIDS) * Fail2ban (HIDS) * Snort (NIDS) * Zeek (NIDS)   Investigate SIEM software using practical activities where possible, for example, Wazuh.  **Students**  Record details of practical activities.  Evaluate the benefits and risks of using honeypots as a cyber security strategy. | Students can explain through a historical narrative the iterative nature of attackers developing new methods to breach security and defenders continually adapting and developing new methods to correspondingly detect and prevent data breaches. | Model and scaffold to support students’ understanding of purpose, audience, language features and structure. |
| **Incident response**  **ST5-5**  Students:   * describe basic concepts of cyber security * identify tools, controls, and technologies commonly used to protect people and organisations from a cyber-attack * explain how hardware technologies are targeted and exploited in a cyber-attack * explain how software applications are targeted and exploited in a cyber-attack. | **Teacher**  Outline the 4 phases of the NIST incident response lifecycle:   * preparation * detection and analysis * containment, eradication, and recovery * post-incident activity.   Outline and [compare](https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide) the SANS incident response process, including:   * preparation * identification/scoping * containment/intelligence development * eradication/remediation * recovery * lessons learned.   Outline the [use of tabletop exercises](https://www.sans.org/blog/top-5-ics-incident-response-tabletops-and-how-to-run-them/) in incident response planning.  Explain the importance of [threat intelligence in incident response](https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/) to better understand the behaviour of an adversary, and the threats and the risks to an organisation, including:   * strategic level (who and why) * operational level (how and where) * tactic level (what).   Outline the 3 critical time frames, including:   * time to detect * time to contain * time to remediate.   Define terms:   * Indicators of Compromise (IoC) * Indicators of Attack (IoA).   **Students**  Create a table or summary of similarities and differences between NIST and SANS incident response processes.  Create a timeline diagram to demonstrate the 3 critical time frames. Label where IoA or IoC might occur in this timeline. | Students can recall the steps and sequence of either or both incident response lifecycles (frameworks).  Students will be able to note the minor differences between both lifecycles and recognise that they are similar and aim to achieve the same objective. | (Add adjustments and registration) |

**Note**: Three options, A, B, and C are provided. Please choose one based on availability of resources. Allow at least 2 lessons for any option.

Table 5 – Cyber security weeks 7 and 8 learning sequence (continued)

|  |  |  |  |
| --- | --- | --- | --- |
| Outcomes and content | Teaching and learning | Evidence of learning | Adjustments and registration |
| ****A: Digital forensics software tutorial****  Use EITHER:   * live-USB distributions * virtual machines * Windows Subsystem for Linux (WSL).   ****ST5-4, ST5-5****  Students:   * describe basic concepts of cyber security * identify tools, controls, and technologies commonly used to protect people and organisations from a cyber-attack * explain how hardware technologies are targeted and exploited in a cyber-attack * explain how software applications are targeted and exploited in a cyber-attack. | **Teacher and students**  Investigate digital forensics and incident response (DFIR) tools, for example:   * Autospy * SIFT Workstation (Digital Forensics and Incident Response Distribution) * The Sleuth Kit (TSK) * Volatility * Xplico * CAINE.   **Students**  Record details of practical activities in folio. | Students will be actively participating in some setup activities, familiarisation, and preparation for digital forensics software tutorial.  Students will be able to set up a suitable computer workstation, with either a live-USB or a virtual machine image, ready to participate.  Students demonstrate working independently or collaboration skills if working in a small team.  Students will have a record of actions, and observation and/or answers to questions. | Teacher to consider accessibility options when using the digital forensics software. |
| ****B: Data forensics case study****  Requires virtual machines.  ****ST5-2, ST5-4, ST5-5, ST5-6****  Students:   * **describe basic concepts of cyber security** * **identify tools, controls, and technologies commonly used to protect people and organisations from a cyber-attack** * **explain how hardware technologies are targeted and exploited in a cyber-attack** * **explain how software applications are targeted and exploited in a cyber-attack** * **develop an understanding of the cyber security industry.** | **Teacher**  Explain the risks and issues of acquiring digital forensic evidence, for example:   * order of volatility * acquire the evidence without altering or damaging the original * authenticate the image * analyse the data without modifying it * legal issues.   **Teacher and students**  Investigate digital forensics and incident response (DFIR) tools while performing activities for the data forensics case study, for example:   * The Sleuth Kit * Autospy * SIFT Workstation (Digital Forensics and Incident Response Distribution) * Volatility * Xplico.   **Students**  Record details of practical activities in folio. | Students can outline principals of acquiring evidence.  Students will be actively participating in some setup activities, familiarisation, and preparation for the data forensics case study.  Students will be able to setup a suitable computer workstation, including necessary virtual machine images, ready to participate.  Students will be actively following the narrative of the case study, completing the sequence of activities, and developing knowledge and skills in using the appropriate software.  Students demonstrate working independently or collaboration skills if working in a small team. | Teacher to consider accessibility options when using the digital forensics software.  Provide students with different challenge options and/or negotiate the requirements of the task with appropriate adjustments.  Advanced students could be encouraged to research advanced techniques and seek out additional tutorials.  Work in teams or individually to complete the challenge. |
| C: Data breach incident case study  Requires virtual machines.  ****ST5-2, ST5-4, ST5-5, ST5-6****  Students:   * describe basic concepts of cyber security * identify tools, controls, and technologies commonly used to protect people and organisations from a cyber-attack * explain how critical infrastructure is targeted and exploited in a cyber-attack * explain how hardware technologies are targeted and exploited in a cyber-attack * explain how software applications are targeted and exploited in a cyber-attack * develop an understanding of the cyber security industry. | **Teacher and students**  Investigate digital forensics and incident response (DFIR) tools while performing activities for the data breach incident case study, for example:   * The Sleuth Kit * Autospy * SIFT Workstation (Digital Forensics and Incident Response Distribution) * Volatility * Xplico.   **Students**  Record details of practical activities in folio. | Students will be actively participating in some setup activities, familiarisation, and preparation for the data breach incident case study.  Students will be able to setup a suitable computer workstation, including necessary virtual machine images, ready to participate.  Students will be actively following the narrative of the case study, completing the sequence of activities, and developing knowledge and skills in using the appropriate software.  Students demonstrate working independently or collaboration skills if working in a small team. | Teacher to consider accessibility options when using the digital forensics software.  Provide students with different challenge options and/or negotiate the requirements of the task with appropriate adjustments.  Advanced students could be encouraged to research advanced techniques and seek out additional tutorials.  Work in teams or individually to complete the challenge. |
| Weekly reflection | **Teacher**  Monitor the progress of student reflections.  **Students**  Complete weekly reflection evaluating new knowledge, understanding or skills in relation to previous knowledge. | Students will demonstrate the impact of these learning events or activities by making judgments about what has happened and what they still need to understand. | A procedural recount can be prepared on paper or digitally, including speech-to-text or voice recording. |

### Weeks 9 and 10

Table 6 – Cyber security weeks 9 and 10 learning sequence

|  |  |  |  |
| --- | --- | --- | --- |
| Outcomes and content | Teaching and learning | Evidence of learning | Adjustments and registration |
| **Week 9 – Red team/blue team**  **ST5-5**  Students:   * describe basic concepts of cyber security * develop an understanding of the cyber security industry * explain how hardware technologies are targeted and exploited in a cyber-attack * explain how software applications are targeted and exploited in a cyber-attack. | **Teacher**  Outline the [purpose of red teams and blue teams (12:16)](https://www.youtube.com/watch?v=jNY59pil8Tk) in cyber security.  Define typical red team operations.  Define typical blue team operations.  Identify metrics used by the 2 teams to demonstrate different goals.  **Student**  Explain how red team operations emulate adversaries for defensive purposes.  **Teacher and students**  Discuss the importance of offensive security operations and defensive security operations to improve an organisation’s overall cyber security posture.  **Teacher**  Describe the role of the purple team.  **Student**  Draw a Venn diagram to indicate the operations and activities that members of each team perform. | Students can outline the need for organisations to develop both offensive and defensive cyber capabilities.  Students can explain the purpose of red team and blue team operations.  Students can describe purple team operations where red and blue team members collaborate to improve the security posture of the organisation. | (Add adjustments and registration) |
| **MITRE ATT&CK framework**  **ST5-5, ST5-6, ST5-8, ST5-9**  Students:   * identify tools, controls, and technologies commonly used to protect people and organisations from a cyber-attack * explain how critical infrastructure is targeted and exploited in a cyber-attack * explain how hardware technologies are targeted and exploited in a cyber-attack * explain how software applications are targeted and exploited in a cyber-attack * develop an understanding of the cyber security industry * describe the contributions that cyber security professionals make to society. | **Teacher**  Identify attack frameworks used to examine an attacker’s behaviour throughout various stages of an attack:   * [MITRE ATT&CK](https://attack.mitre.org/) * [Lockheed Martin’s Cyber Kill Chain](https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html) * [Diamond Model of Intrusion Analysis](https://threatconnect.com/blog/tag/diamond-model-of-intrusion-analysis/) * [Unified Kill Chain](https://www.unifiedkillchain.com/)   Explain how an attack framework is used to analyse and better understand an organisation’s threat environment, including potential attacks and attack vectors.  Describe the organisation of the [MITRE ATT&CK Framework](https://attack.mitre.org/), including:   * table of ATT&CK techniques * tactics * methods * mitigating controls.   Explain the benefit of studying adversarial tactics and strategies.  Provide a printed copy of the MITRE ATT&CK framework for both the enterprise and ICS matrices.  **Students**  Compare and highlight differences (missing or extra techniques) between the matrices.  Using the online version of MITRE, search for and identify a group that has targeted the energy sector and record the techniques it has used.  **Teacher (optional)**  Describe the organisation of the Cyber Kill Chain analysis framework, including:   * 7 phases * reconstruction of intrusion.   **Extension (optional)**  **Teacher and students**  Interact with the MITRE ATT&CK framework and additional tools, for example:   * creating heat maps exercises * mapping the adversary * emulating the adversary.   Compare how various attack frameworks model attacker behaviour differently:   * categorise individual attack techniques * characteristics of an attack * activities of an attacker. | Students can recognise the main attack frameworks.  Students can explain how the different attack frameworks can give insight into adversarial behaviour.  Students will be able to navigate across columns and rows using paper or online versions to find tactics, techniques groups, and mitigations.  Students will be able to describe the relationship between gathering and analysing threat intelligence and planning defence.  Students can identify differences in the 3 matrices (enterprise, mobile, and ICS).  Students will successfully search for and identify a documented group that has attacked a given target, for example a target in the energy sector. Students will list documented techniques used by the group. | When presenting the MITRE ATT&CK framework, consider the amount of text, text complexity, and layout. The MITRE ATT&CK framework is quite large and goes over a screen width. It is a web-based table and would be difficult to navigate without guidance.  Zoom in and focus on one or 2 columns and one or 2 cells to make it easier for all students.  Printing on paper would require A3 sizing as a minimum.  Provide a differentiated task for students to help them manage this linguistically and visually complex framework. |
| **Industry bodies and career pathways**  **ST5-1, ST5-2, ST5-4, ST5-6, ST5-8, ST5-10**  Students:   * develop an understanding of the cyber security industry * investigate the nature of work and the pathways into the cyber security profession * engage in industry career development opportunities to gain a deeper knowledge of cyber security professions, develop skills, knowledge, and understanding of authentic, real-world problem-solving * describe the contributions that cyber security professionals make to society. | **Teacher**  Present government and industry bodies in the cyber security sector, for example:   * [Australian Cyber Security Centre (ACSC)](https://www.cyber.gov.au/) * [Digital.NSW](https://www.digital.nsw.gov.au/policy/cyber-security) * [Australian Information Security Association (AISA)](https://www.aisa.org.au/) * [AustCyber](https://www.austcyber.com/).   Present websites with cyber careers and skills frameworks, for example:   * [AustCyber education map](https://www.austcyber.com/resources/dashboards/education-map) * [National Initiative for Cybersecurity Education (NICE) workforce framework](https://www.austcyber.com/resources/dashboards/NICE-workforce-framework) * [AUCyber Explorer](https://www.aucyberexplorer.com.au/) * [Guide for women in cyber security](https://cybersecurityguide.org/resources/women-in-cybersecurity/) * [Cyber Seek](https://www.cyberseek.org/).   Outline certification options and pathways.  **Teacher and students**  Discuss personal attributes and aptitudes suitable to cyber security professionals.  **Students**  Investigate the nature of work undertaken and the pathways into cyber security professions. | Students can identify cyber security careers and pathways into the profession that match their aptitude and developing skillset. | (Add adjustments and registration). |
| **Weekly reflection** | **Teacher**  Monitor the progress of student reflections.  **Student**  Complete weekly reflection by identifying and evaluating new knowledge or skills considering previous knowledge. | Students answer reflective questions, for example:   * What did I learn about communication this week? | A procedural recount can be prepared on paper or digitally, including speech-to-text or voice recording. |
| **Week 10 – Emerging technology, AI, and ML**  **ST5-1, ST5-2, ST5-4, ST5-6, ST5-8, ST5-10**  Students:   * explain the effects of emerging technologies on current and future cyber security challenges and on professional skills and careers in the industry. | **Teacher**  Outline the impact of recently developed and emerging technologies on cyber security challenges, for example:   * cloud computing * hybrid workforce * virtualisation * internet of things (IoT) * embedded systems, such as autonomous cars.   Outline emerging innovative cyber security solutions, for example:   * behaviour analytics * blockchain technology * deep learning * hardware authentication * quantum cryptography.   **Teacher and students**  Discuss the impact or potential impact of recently developed and emerging technologies on cyber security challenges. To cover a wider range of technologies, the class could brainstorm 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 able to outline some cyber security challenges that align with the strengths of machine learning (ML) and its application, and have been shown to suitably address these challenges.  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. | (Add adjustments and registration) |
| **ST5-1, ST5-2, ST5-4, ST5-6, ST5-8, ST5-10**  Students explain the effects of emerging technologies on current and future cyber security challenges and on professional skills and careers in the industry. | **Teacher**  Outline how machine learning (ML) can be applied to address the challenges of security, for example:   * classification algorithms * pattern recognition * anomaly detection * synthetic data.   Outline how artificial intelligence (AI) can negatively impact an organisation, for example:   * limitations of AI * vulnerabilities of AI * attackers using AI.   **Teacher and students**  Discuss the skills and knowledge domains required by cyber security professionals. | Students will be able to outline some cyber security challenges that align with the strengths of ML and its application, and have been shown to suitably address these challenges.  Students will be able to outline the potential for AI to adversely impact organisations when relied upon for both defensive and offensive activities.  Students will be actively engaged in class discussion and expressing ideas about the range and type of skills required by cyber security professionals. | (Add adjustments and registration) |

**Note:** Three options, A, B, and C are provided. Please choose one based on availability of resources and whether a capture the flag event is scheduled during the term the unit is delivered. These options may be logically delivered prior to the Week 10 activities above, which relate to the effects of emerging technologies on current and future cyber security challenges.

Table 7 – Cyber security weeks 9 and 10 learning sequence (continued)

|  |  |  |  |
| --- | --- | --- | --- |
| ****Outcomes and content**** | ****Teaching and learning**** | ****Evidence of learning**** | ****Adjustments and registration**** |
| ****A: Capture the flag event (preparation day)****  ****ST5-1, ST5-2, ST5-3, ST5-4, ST5-6, ST5-8, ST5-9****  **Students:**   * **complete practical exercises solving cyber security problems** * **develop an understanding of the cyber security industry** * **investigate the nature of work and the pathways into the cyber security profession** * **work individually and collaboratively to apply an engineering design process to complete real-world problems and challenges to cyber security related scenarios** * **engage in industry career development opportunities to gain a deeper knowledge of cyber security professions, develop skills, knowledge and understanding of authentic, real-world problem-solving.** | **Teacher**  **Present benefits of typical capture the flag (CTF) events and activities, for example:**   * **learning** * **creative problem-solving** * **legally practising cyber security skills** * **identifying talent.**   **Demonstrate how to solve some CTF type problems.**  **Teacher and students**  **Complete some practise activities/challenges.**  **Research and document solutions to problems in folio.** | **CTF option**  **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.** | **(Add adjustments and registration).** |
| ****B: OWASP Juice Shop (local)****  **This option provides an opportunity for students to have a similar experience to CTF activities and develop similar critical thinking and problem-solving skills as an alternative to a live CTF event.**  ****ST5-1, ST5-2, ST5-3, ST5-4, ST5-6, ST5-8, ST5-9****  ****Students:****   * **complete practical exercises solving cyber security problems** * **work individually and collaboratively to apply an engineering design process to complete real-world problems and challenges to cyber** security related scenarios. | **Teacher**  **Outline OWASP and its role.**  **Present overview of OWASP Juice Shop activities, for example:**   * **learning web app vulnerabilities and exploits** * **legally practising cyber security skills** * **identifying talent.**   **Demonstrate how to use tools to complete some Juice Shop hacking challenges.**  **Teacher and students**  **Complete some practise activities/problems.**  **Research and document solutions to problems in folio.** | **OWASP Juice Shop option**  **Students will be actively participating in some setup activities, familiarisation, and preparation for the OWASP Juice Shop activity.**  **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.** | **(Add adjustments and registration).** |
| ****C: Class presentations (allow minimum of 2 days)****  **This option provides an opportunity for students to present solutions to tasks or challenges which may have been set by the teacher earlier in the unit.**  ****ST5-1, ST5-2, ST5-4, ST5-6, ST5-8****  **Students:**   * **develop an understanding of the cyber security industry** * **investigate the nature of work and the pathways into the cyber security profession** * **complete practical exercises solving cyber security problems** * **demonstrate innovation and entrepreneurial activity, and communicate solutions to problems involving cyber security.** | **Teacher**  **Organise students to present their solutions to challenges assigned earlier in the unit, for example:**   * **risk assessment** * **threat modelling** * **improved security design** * **vulnerability assessment (vulnerability scanning results).**   **Presentation format and medium may include:**   * **speech** * **poster presentation** * **folio** * **how-to tutorial** * **recorded video and/or animation.**   **Student**  Present solutions to assigned tasks or challenges**.** | **Students’ presentations and submitted work.** | **Provide clear instructions, guidelines, and models to indicate what is expected of students.**  **If a speech is required, ensure students are taught the structure of a speech and appropriate language features, and opportunities to practice and receive feedback.** |
| ****A: Capture the flag event****  ****B: OWASP Juice Shop (local)****  ****ST5-1, ST5-2, ST5-3, ST5-4, ST5-6, ST5-8, ST5-9****  **Students:**   * **complete practical exercises solving cyber security problems** * **develop an understanding of the cyber security industry** * **investigate the nature of work and the pathways into the cyber security profession** * **complete practical exercises solving cyber security problems** * **work individually and collaboratively to apply an engineering design process to complete real-world problems and challenges to cyber security related scenarios.** | **Teacher**  Ensure access to suitable technology, for example:   * computer lab or laptop trolley (options A and B) * computer with OWASP Juice Shop installed (option B only).   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.  **Student**  Participate in challenge. | **CTF option**  **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.**  **OWASP Juice Shop option**  **Students will be actively participating in a OWASP Juice Shop activity and attempting to complete as many challenges as possible within the time allowed.**  **Completion of challenges (or tasks within a challenge) will indicate understanding and learnt skills.** | **(Add adjustments and registration).** |
| ****Weekly reflection**** | **Teacher**  Assess the progress of student knowledge and skills from reflections.  **Student**  **Complete weekly reflection evaluating new knowledge, understanding or skills in relation to previous knowledge.** | **Students will demonstrate the impact of these learning events or activities by making judgments about what has happened and what they still need to understand.** | **A procedural recount can be prepared on paper or digitally, including speech-to-text or voice recording.** |

## Reflection and evaluation

**Reflecting on and evaluating learning activities should be an ongoing process that happens throughout the delivery of this topic. Teachers should document their evaluation of learning activities throughout the program. The space below is provided to reflect on and evaluate this overall unit of work.**

## Additional information

**Resource evaluation and support**: Please complete the following [feedback form](https://forms.office.com/Pages/ResponsePage.aspx?id=muagBYpBwUecJZOHJhv5kbKo2q_ZUXlHndJMnh2Wd8NUOUk0VTIzUDVVSlVFQVM5MkdOMkJGTjVKNCQlQCN0PWcu) to help us improve our resources and support.

The information below can be used to support teachers when using this teaching resource for iSTEM.

### 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#.Y9w1CT4W5as.link), [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.

[What works best update 2020](https://education.nsw.gov.au/about-us/educational-data/cese/publications/research-reports/what-works-best-2020-update) (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/secondary-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. In addition, the [Universal Design for Learning planning tool](https://education.nsw.gov.au/teaching-and-learning/learning-from-home/teaching-at-home/teaching-and-learning-resources/universal-design-for-learning) can be used to support the diverse learning needs of students using inclusive teaching and learning strategies. 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).

### About this resource

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 contact the Teaching and Learning Curriculum team by emailing [secondaryteachingandlearning@det.nsw.edu.au](mailto:secondaryteachingandlearning@det.nsw.edu.au).

**Alignment to system priorities and/or needs**:

This resource aligns to the School Excellence Framework elements of curriculum (curriculum provision) and effective classroom practice (lesson planning, explicit teaching).

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) 2.1.2, 2.3.2, 3.2.2, 7.2.2

This resource has been designed to support schools with successful implementation of new curriculum, specifically the NSW Department of Education approved elective course, iSTEM © 2021 NSW Department of Education for and on behalf of the Crown in right of the State of New South Wales.

The resource is produced to assist schools with promoting and implementing the course for the first time. As the course may be taught by teachers from a range of key learning areas, the resource is designed to support teachers from a variety of KLA expertise.

**Department approved elective course**: iSTEM

**Course outcomes**: ST5-1, ST5-2, ST5-3, ST5-4, ST5-5, ST5-6, ST5-7, ST5-8, ST5-9, ST5-10

**Author**: Curriculum Secondary Learners

**Publisher**: State of NSW, Department of Education

**Resource**: Teaching resource

**Related resources**: Further resources to support iSTEM can be found on the Department approved elective courses webpage including course document, sample scope and sequences, assessment materials and other learning sequences.

**Professional Learning**: Join the [Teaching and Learning 7-12 statewide staffroom](https://education.nsw.gov.au/teaching-and-learning/curriculum/statewide-staffrooms) for information regarding professional learning opportunities.

**Universal Design for Learning Tool**: [Universal Design for Learning planning tool](https://education.nsw.gov.au/teaching-and-learning/learning-from-home/teaching-at-home/teaching-and-learning-resources/universal-design-for-learning). Support the diverse learning needs of students using inclusive teaching and learning strategies.

**Consulted with**: Aboriginal Outcomes and Partnerships, Inclusion and Wellbeing, EAL/D.

**Reviewed by**: This resource was reviewed by Curriculum Secondary Learners and by subject matter experts in schools to ensure accuracy of content.

**Creation date**: 15th November 2022

**Rights**: © State of New South Wales, Department of Education

**Evidence Base**:

‘The long-term vision is for a curriculum that supports teachers to nurture wonder, ignite passion and provide every young person with knowledge, skills and attributes that will help prepare them for a lifetime of learning, meaningful adult employment and effective future citizenship’ (NESA 2020:xi).

The development of the course and the course document as part of department approved electives aims to respond to the goals articulated in NESA’s curriculum review. Consistent messages from the review include:

* ‘flexibility’ was the word most used by teachers to describe the systemic change they want
* teachers need more time to teach important knowledge and skills
* students want authentic learning with real-world application.

This teaching resource provides teachers with some examples of explicit and authentic learning experiences. The option to adjust these learning sequences leads to ‘increased local decision making in relation to the curriculum’ as this ‘is associated with higher levels of student performance’ (NESA 2020:52).

The suggested strategies for teaching and learning align with the principles of explicit teaching. ‘The evidence shows that students who experience explicit teaching practices perform better than students who do not. Explicit teaching reduces the cognitive burden of learning new and complex concepts and skills, and helps students develop deep understanding’ (CESE 2020a:11).

## References

**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.

Except as otherwise noted, all material is [© State of New South Wales (Department of Education), 2021](https://education.nsw.gov.au/about-us/copyright) and licensed under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/). All other material (third-party material) is used with permission or under licence. Where the copyright owner of third-party material has not licensed their material under a Creative Commons or similar licence, you should contact them directly for permission to reuse their material.

Creative commons logo


AISA (Australian Information Security Association) (n.d.) [*AISA*](https://aisa.org.au/) [website], accessed 2 February 2023.

AITSL (Australian Institute for Teaching and School Leadership (2017) ‘[Feedback Factsheet](https://www.aitsl.edu.au/teach/improve-practice/feedback#:~:text=FEEDBACK-,Factsheet,-A%20quick%20guide)’, AITSL, accessed 2 February 2023.

AustCyber (Australian Cyber Security Growth Network Limited) (n.d.)[*AUCyber Explorer*](https://www.aucyberexplorer.com.au/) [website], accessed 2 February 2023.

AustCyber (2019) ‘[SCP – Chapter 3 – The challenge: Australia needs to fill the workforce gap, remove startup barriers and strengthen research and development](https://www.austcyber.com/resources/sector-competitiveness-plan-2019/chapter3)’, Sector Competitiveness Plan 2019, AustCyber website, accessed 2 February 2023.

AustCyber (2023) [*AustCyber*](https://www.austcyber.com/) [website], accessed 2 February 2023.

AustCyber (2023) ‘[Education Map](https://www.austcyber.com/resources/dashboards/education-map)’, *Resources*, AustCyber website, accessed 2 February 2023.

AustCyber (2023) ['National Initiative for Cybersecurity Education (NICE) Workforce Framework'](https://www.austcyber.com/resources/dashboards/NICE-workforce-framework), *Resources*, AustCyber website, accessed 2 February 2023.

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 Blog*, accessed 2 February 2023.

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)’, *ReputationDefender: Privacy blog*, accessed 2 February 2023.

Chhillar S (2022) ‘[Common ICS Cybersecurity Myth #1: The Air Gap](https://gca.isa.org/blog/common-ics-cybersecurity-myth-1-the-air-gap)’, *Building a Resilient World: The ISAGCA (International Society of Automation Global Cybersecurity Alliance) blog*, accessed 2 February 2023.

Ciccone S (25 July 2017) ‘[Security Needs to Shift Left – and Right](https://www.veracode.com/blog/managing-appsec/security-needs-shift-left-and-right)’, *Veracode blog*, accessed 2 February 2023.

Commonwealth of Australia (2012) ‘[Implementing Multi-Factor Authentication](https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-multi-factor-authentication)’, *Publications*, ACSC (Australian Cyber Security Centre) website, accessed 2 February 2023.

Commonwealth of Australia (2015) [‘National STEM School Education Strategy’](https://www.dese.gov.au/education-ministers-meeting/resources/national-stem-school-education-strategy), Education Council, Australian Department of Education, Skills and Employment, accessed 2 February 2023.

Commonwealth of Australia (2020) ‘[Identity theft](https://www.cyber.gov.au/acsc/view-all-content/threats/identity-theft),’ *Threats*, ACSC website, accessed 2 February 2023.

Commonwealth of Australia (2020) ‘[Securing Google Accounts](https://www.cyber.gov.au/acsc/view-all-content/guidance/securing-google-accounts)’, Advice and g*uidance*, ACSC website, accessed 2 February 2023.

Commonwealth of Australia (2020) ['Zero day (0-day)'](https://www.cyber.gov.au/acsc/view-all-content/glossary/zero-day-0-day), *Glossary*, ACSC website, accessed 2 February 2023.

Commonwealth of Australia (2021) ‘[Personal Cyber Security: First Steps Guide](https://www.cyber.gov.au/acsc/view-all-content/guidance/personal-cyber-security-first-steps-guide)’, *Advice and Guidance*, ACSC website, accessed 2 February 2023

Commonwealth of Australia (2021) ‘[Security of Critical Infrastructure Act 2018](https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018)’, *Security coordination*, Department of Home Affairs website, accessed 2 February 2023.

(CSIS) Center for Strategic and International Studies (2023) ‘[Significant Cyber Incidents](https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents)’, *Strategic Technologies Program*, CSIS website, accessed 2 February 2023.

Cybersecurity Guide (2021) ‘[A guide for women in cybersecurity](https://cybersecurityguide.org/resources/women-in-cybersecurity/),’ *Women's Guide*, Cybersecurity Guide website, accessed 2 February 2023.

Cyberseek US (n.d.) [*CyberSeek*](https://www.cyberseek.org/) [website], accessed 2 February 2023.

FIRST (Forum of Incident Response and Security Teams) (2023) [*Common Vulnerability Scoring System SIG*](https://www.first.org/cvss/), FIRST website, accessed 2 February 2023.

Fruhlinger J and Martin JA (15 April 2021) ‘[The password hall of shame (and 10 tips for better password security)](https://www.csoonline.com/article/3526408/most-common-passwords.html)’, CSO Australia, accessed 2 February 2023.

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)’, *NIST* (*National Institute of Standards and Technology*)*: Taking Measure blog*, accessed 2 February 2023.

Girken E (3 January 2020) ‘[Incident Response Steps and Frameworks for SANS and NIST](https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide)’, *AT&T Cybersecurity blog*, accessed 2 February 2023.

Guillaume D (25 September 2012) [‘Amazing mind reader reveals his "gift" [video]’](https://www.youtube.com/watch?v=F7pYHN9iC9I), *Duval Guillaume*, YouTube, accessed 2 February 2023.

Hunt T (n.d.) [*Pwned Passwords*](https://haveibeenpwned.com/Passwords), Have I Been Pwned website, accessed 2 February 2023.

J and R Group Pty Ltd T/A DC Encompass (25 July 2021) ‘[Cybersecurity Ethics](https://dcencompass.com.au/blog/cybersecurity-ethics/)’, *DC Encompass blog*, accessed 2 February 2023.

Lockheed Martin Corporation (2023) ‘[The Cyber Kill Chain](https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)’, *Cyber*, Lockheed Martin website, accessed 2 February 2023.

Messer Studios LLC (3 February 2021) ['Honeypots and Deception – SY0-601 CompTIA Security+ : 2.1' [video]](https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/honeypots-and-deception/), Messer Studios LLC, Professor Messer website, accessed 2 February 2023.

Microsoft (2023) ‘[Elevation of Privilege (EoP) Threat Modeling Card Game](https://www.microsoft.com/en-us/download/details.aspx?id=20303)’, Microsoft Download Centre, Microsoft, accessed 2 February 2023.

National Cyber Security Centre (NCSC) (2021) ‘[Three random words](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words)’, *Top tips for staying secure online*, NCSC website, accessed 2 February 2023.

NESA (NSW Education Standards Authority) (2020) [*Nurturing Wonder and Igniting Passion, designs for a new school curriculum: NSW Curriculum Review* [PDF 1.12MB]](https://nswcurriculumreform.nesa.nsw.edu.au/pdfs/phase-3/final-report/NSW_Curriculum_Review_Final_Report.pdf), NESA, accessed 2 February 2023.

Neskey C (2 March 2022) ‘[Are Your Passwords in the Green?](https://www.hivesystems.io/blog/are-your-passwords-in-the-green)’, *Hive Systems Infographic blog*, accessed 2 February 2023.

Nord Security (2023) [*Top 200 most common passwords*](https://nordpass.com/most-common-passwords-list/), NordPass website, accessed 2 February 2023.

Palo Alto Networks (2023) ‘[What is XDR](https://www.paloaltonetworks.com/cyberpedia/what-is-xdr)’, *Cyberpedia*, Palo Alto Networks Cortex website, accessed 2 February 2023.

Parsons D (16 June 2021) ‘[Top 5 ICS Incident Response Tabletops and How to Run Them](https://www.sans.org/blog/top-5-ics-incident-response-tabletops-and-how-to-run-them/)’, *SANS Cyber Security Blog*, accessed 2 February 2023.

Pendergast A (24 August 2015) ‘[Diamond Model of Intrusion Analysis](https://threatconnect.com/blog/tag/diamond-model-of-intrusion-analysis/)’, *ThreatConnect blog*, accessed 16 June 2022.

Pols P (2021) [*The Unified Kill Chain*](https://www.unifiedkillchain.com/) [website], accessed 2 February 2023.

PurpleSec (24 September 2020) ['Red Team VS Blue Team: What's The Difference? | PurpleSec' [video]](https://www.youtube.com/watch?v=jNY59pil8Tk), PurpleSec, YouTube, accessed 2 February 2023.

PwC (PricewaterhouseCoopers) (2015) ‘[A smart move](https://www.pwc.com.au/publications/a-smart-move.html)’, PwC Australia, PwC, accessed 31 January 2023.

Rowe A (2021) ‘[Study Reveals Average Person Has 100 Passwords](https://tech.co/password-managers/how-many-passwords-average-person)’, *Password Managers*, Tech.co website, accessed 2 February 2023.

Schneier B (1999) ‘[Attack Trees](https://www.schneier.com/academic/archives/1999/12/attack_trees.html)’, *Academic*, Schneier on Security website, accessed 2 February 2023.

Security.org (2023) [*How Secure is My Password?*](https://www.security.org/how-secure-is-my-password/), Security.org, accessed 2 February 2023.

Shevchenko N (3 December 2018) ['Threat Modeling: 12 Available Methods'](https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/), *Carnegie Mellon University, Software Engineering Institute blog*, accessed 2 February 2023.

State of New South Wales (Customer Service NSW) (2023) ‘[Cyber Security](https://www.digital.nsw.gov.au/policy/cyber-security)’, *Policy*, Digital NSW website, accessed 2 February 2023.

State of New South Wales (Department of Education) and CESE (Centre for Education Statistics and Evaluation) (2020a) ‘[What works best: 2020 update](https://education.nsw.gov.au/about-us/educational-data/cese/publications/research-reports/what-works-best-2020-update)’, CESE, NSW Department of Education, accessed 2 February 2023.

State of New South Wales (Department of Education) and CESE (Centre for Education Statistics and Evaluation) (2020b) ‘[What works best in practice](https://education.nsw.gov.au/about-us/educational-data/cese/publications/practical-guides-for-educators-/what-works-best-in-practice)’, CESE, NSW Department of Education, accessed 2 February 2023.

State of New South Wales Investment NSW (2021) ‘[The NSW Industry Development Framework](https://www.investment.nsw.gov.au/living-working-and-business/nsw-industry-development-framework/)’, Living, working and business, Investment NSW website, accessed 2 February 2023.

Tassel L (16 January 2019) ‘[Why strive for Industry 4.0](https://www.weforum.org/agenda/2019/01/why-companies-should-strive-for-industry-4-0/)’, World Economic Forum Agenda articles, accessed 2 February 2023.

Tenable, Inc (2021) ‘[Zero-Day Vulnerabilities](https://docs.tenable.com/cyber-exposure-studies/2021-threat-landscape-retrospective/Content/ZeroDayVulnerabilities.htm)’, Vulnerability Landscape, Tenable Inc website, accessed 2 February 2023.

The Ethics Centre (15 April 2020) [‘What is the difference between Ethics, Morality and the Law?’ [video]](https://www.youtube.com/watch?v=Xki2fRA0bY8), *The Ethics Centre*, YouTube, accessed 2 February 2023.

The MITRE Corporation (2022) [*ATT&CK*](https://attack.mitre.org/) [website], accessed 2 February 2023.

The MITRE Corporation (2022) [*CVE (Common Vulnerabilities and Exposures)*](https://cve.mitre.org/index.html) [website], accessed 2 February 2023.

The Open University (n.d.) [*Password Strength Checker*](https://www2.open.ac.uk/openlearn/password_check/index.html), OpenLearn website, accessed 2 February 2023.

United States Government (2020) ‘[Critical Infrastructure Sectors](https://www.cisa.gov/critical-infrastructure-sectors)’, *Infrastructure Security*, Cybersecurity and Infrastructure Security Agency website, accessed 2 February 2023.

Vigderman A and Turner G (16 March 2022) ‘[What is Personally Identifiable Information (PII)?](https://www.security.org/identity-theft/what-is-pii/)’, ID Theft Protection Tips, Security.org, accessed 10 June 2022.

Walter J and Guerrero-Saade JA (2021) ‘[Hive Attacks | Analysis of the Human-Operated Ransomware Targeting Healthcare](https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/)’, *Crimeware*, SentinelLABS website, accessed 2 February 2023.

Wikipedia, the free encyclopedia (2022) [*Stuxnet*](https://en.wikipedia.org/wiki/Stuxnet), Wikipedia website, accessed 2 February 2023.