MODULE 2:
CYBERSECURITY & DATA PROTECTION

Cybersecurity and data protection are essential for any organization that collects, processes, or stores personal or sensitive information. In this chapter, we will explore some of the key concepts and challenges.

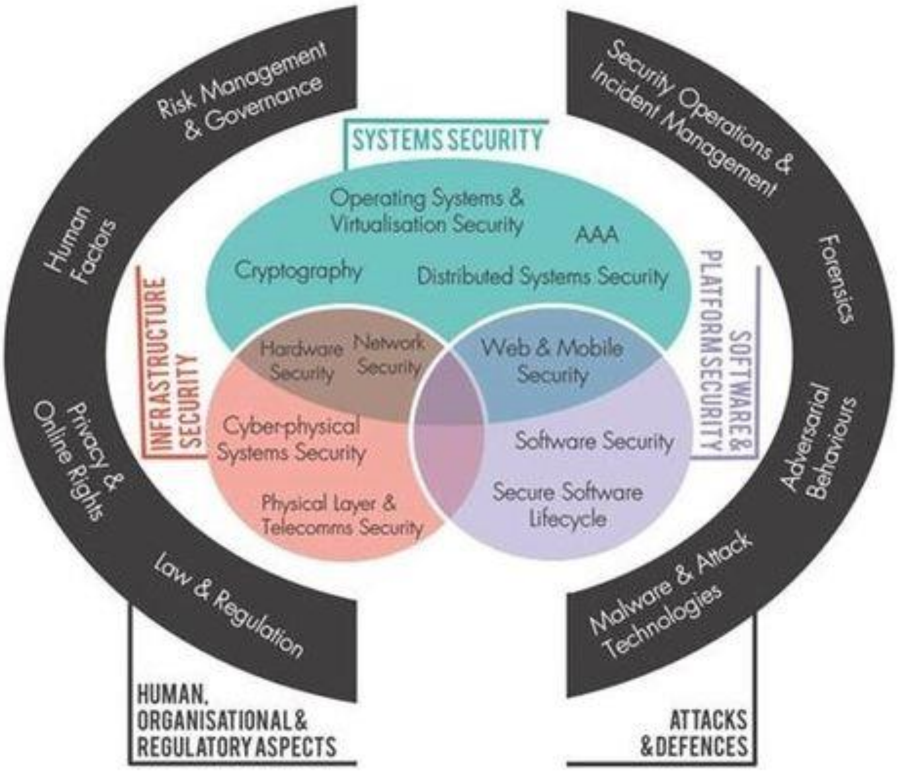
Data breach notification and communication: How to prepare for and respond to data breaches, and how to communicate effectively with stakeholders, regulators, and the public about the incident and its consequences.

Cybersecurity training and ethical hacking: How to educate and empower employees and users about cybersecurity best practices, and how to use ethical hacking techniques to test and improve the security of systems and networks.

This module provides a concise overview of these topics, as well as practical examples and recommendations on how to implement them in your organization. By reading this chapter, you will gain a better understanding of the current trends and challenges in cybersecurity and data protection, as well as the best practices and standards that can help you achieve a high level of compliance and performance.

2.1 CYBERSECURITY BODY OF KNOWLEDGE (CYBOK)

The CyBOK is an international project aimed at codifying best cyber security knowledge and practice.


Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
AAA
Cryptography
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Web & Mobile Security
Cyber-physical Systems Security
Physical Layer & Telecomms Security
Software Security
Secure Software Lifecycle
SOFTWARE & PLATFORM SECURITY
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

CyBOK provides the means to fill the rising demand for skilled cybersecurity professionals by defining a common body of knowledge that encompasses various domains within the field. It covers topics such as security management, human factors, software security, network security, and cryptography, among others. The knowledge areas defined in CyBOK serve as the building blocks for developing cybersecurity expertise.

The CyBOK framework is focusses on thirteen fundamental knowledge areas:

1. **Access Control and Identity Management** - covers the principles and practices involved in managing access to systems, networks, and resources, as well as establishing and maintaining user identities.
2. **Cybersecurity Architecture** - addresses the design and implementation of secure systems and networks, considering factors such as threat modelling, security controls, and risk management.
3. **Cybersecurity Governance and Management** - explores the organizational aspects of cybersecurity, including governance

frameworks, policies, regulations, risk assessment, and incident response planning.

4. **Digital Forensics and Incident Response** - focuses on the techniques and methodologies employed in the investigation and analysis of cyber incidents, as well as the appropriate response measures.
5. **Human Factors in Cybersecurity** - recognizes the critical role of human behaviour and psychology in cybersecurity, covering topics such as security awareness, training, and usability considerations.
6. **Information Assurance** - encompasses the principles and practices of safeguarding information assets, ensuring data integrity, confidentiality, availability, and non-repudiation.
7. **Malware and Software Vulnerability Analysis** - delves into the identification, analysis, and mitigation of software vulnerabilities and malware threats.
8. **Network Security** - explores the concepts, protocols, and technologies used to secure computer networks, including network architecture, encryption, intrusion detection, and firewall implementation.
9. **Operating Systems Security** - focuses on securing operating systems, including access control, secure configuration, patch management, and secure administration practices.
10. **Privacy and Online Trust** - covers the legal, ethical, and technical aspects of protecting individual privacy in the digital realm, as well as establishing trust in online interactions.
11. **Resilience and System Recovery** - addresses the strategies and techniques for ensuring system resilience, business continuity planning, and disaster recovery.
12. **Secure Systems Engineering** - emphasizes secure software development practices, secure coding techniques, and secure software lifecycle management.
13. **Software Security Assurance** - explores methods for assuring the security of software systems, including secure testing, code reviews, and vulnerability assessment.

The CyBOK framework provides a holistic approach to cybersecurity, covering technical, managerial, and human factors. It serves as a valuable resource for professionals seeking to broaden their knowledge, educators designing cybersecurity curricula, and policymakers shaping cybersecurity policies.

In summary, the Cybersecurity Body of Knowledge (CyBOK) is a comprehensive guide that defines the essential knowledge areas within the field of cybersecurity. It covers a wide range of topics and disciplines, providing a structured framework to understand, develop, and apply cybersecurity expertise. By promoting a common understanding of cybersecurity principles, CyBOK contributes to the advancement of the field, addressing the critical need for skilled cybersecurity professionals in today's interconnected world

2.2. CYBERSECURITY & DATA PROTECTION

Australian laws, such as the Privacy Act of 1988 and the Notifiable Data Breaches (NDB) scheme, mandate the protection of personal data. Organizations are obliged to establish robust cybersecurity policies and practices to safeguard sensitive information, thus ensuring compliance with legal requirements and ethical responsibilities alike.

Cybersecurity & Data Protection is therefore the practice of safeguarding your devices, accounts and data from cyber threats such as scams and malware.

As a general guide to train organisation staff to resist social engineering attacks, these are considered basic cybersecurity best practices:

- Turn on automatic updates for your software, apps and operating systems to fix any vulnerabilities that cybercriminals can exploit.
- Use strong passwords and authentication methods for your accounts, such as multi-factor authentication or biometrics, to prevent unauthorized access.
- Avoid clicking on pop-ups, unknown emails and links that may contain malware or phishing attempts to steal your information or money.
- Always connect to secure Wi-Fi networks that are encrypted and password-protected and avoid using public Wi-Fi for sensitive activities such as online banking or shopping.
- Encrypt your data, especially when it is stored or transmitted over the internet or other networks, to prevent cybercriminals from reading or modifying it.
- Collaborate and share information with other organisations, security agencies and law enforcement to improve your cyber resilience and awareness of potential threats.
- Manage your assets, such as software and data, by using centralised systems and configuration management to ensure visibility and control of your critical resources.
- Implement protective measures and controls for your cyber risks, such as firewalls, antivirus software and backup systems, based on the Australian Signals Directorate's (ASD) Strategies to mitigate targeted cyber intrusions or equivalent.
- Use detection systems and processes to monitor your devices and networks for any signs of cyberattacks, such as unusual activity or anomalies, and use data analytics to integrate sources of threats in real time.
- Plan for response and recovery in case of a cyber incident, by having a clear strategy, roles and responsibilities, communication channels and contingency plans.

This advice notwithstanding, you should always tailor your approach to your specific context, needs and risks. You should also keep yourself updated on the latest trends and developments in cyber security, as cyber threats are constantly evolving and becoming more sophisticated.

Australian laws, such as the Privacy Act of 1988 and the Notifiable Data Breaches (NDB) scheme, mandate the protection of personal data. Organizations are obliged to establish robust cybersecurity policies and practices to safeguard sensitive information, thus ensuring compliance with legal requirements and ethical responsibilities alike.

CYBERSECURITY POLICIES

Cybersecurity policies are considered essential for protecting the digital assets and interests of individuals, organizations and nations from cyber threats and attacks.

When formulating cybersecurity policies, the following points should be covered:

- Be based on a comprehensive risk assessment and a clear understanding of the cyber threat landscape, as well as the legal, ethical and social implications of cyber activities.
- Aim to achieve a balance between security, privacy, accessibility and innovation, while respecting the rights and responsibilities of all stakeholders in the cyberspace.
- Promote the adoption of best practices and standards for cyber resilience, such as zero trust and attack surface management, which can help prevent, detect and mitigate cyber risks.
- Address the challenges and opportunities posed by emerging technologies, such as artificial intelligence, cloud computing and quantum computing, which can enhance or undermine cyber security.
- Be aligned with national and international laws and regulations, as well as with the norms and values of the global community, to foster cooperation and trust among cyber actors.
- Be regularly reviewed and updated to reflect the dynamic nature of cyber threats and technologies, as well as the evolving needs and expectations of the cyber society.

These policies, often informed by industry best practices and regulatory mandates, guide organizations in implementing a multi-layered defence strategy to protect critical assets and sensitive data.

Such policies should *specifically* include:

- Acceptable Use Policy.
- Security Awareness and Training Policy.
- Change Management Policy.

- Incident Response Policy.
- Remote Access Policy.
- Vendor Management Policy.
- Password Creation and Management Policy.
- Network Security Policy.

THE PRIVACY ACT & DATA PROTECTION

The **Privacy Act of 1988** is a cornerstone of data protection in Australia. It lays the foundation for safeguarding personal information, ensuring that organizations collect, use, and disclose data in a responsible and ethical manner. The Act sets out strict guidelines that organizations must follow, with serious consequences for violations. This legal framework serves as a reminder of the ethical duty organizations must respect the privacy of individuals and safeguard their personal information.

The Privacy Act covers the following:

- Know why your personal information is being collected, how it will be used and who it will be disclosed to.
- Have the option of not identifying yourself, or of using a pseudonym in certain circumstances.
- Ask for access to your personal information (including your health information)

THE NOTIFIABLE DATA BREACHES SCHEME

The **Notifiable Data Breaches (NDB) scheme** is a legal requirement for organisations and agencies that are covered by the Privacy Act 1988 to report data breaches that are likely to cause serious harm to the individuals whose personal information is involved.

A data breach occurs when personal information is lost, accessed or disclosed without authorisation. For example, when a device with customer information is stolen, a database with personal information is hacked, or personal information is mistakenly given to the wrong person.

The notification to individuals must include recommendations about the steps they should take in response to the data breach. The notification to the Office of the Australian Information Commissioner (OAIC) must be done using the online Notifiable Data Breach form.

The NDB scheme aims to protect the privacy and security of personal information and to enhance public confidence in how organisations handle personal information.

The NDB scheme also provides guidance and support for organisations and agencies on how to prevent, prepare for and respond to data breaches, drawing on research and best practice.

ETHICAL & LEGAL CONSIDERATIONS

Ethical and legal considerations in cybersecurity and data protection are essential to ensure the privacy, security and trust of individuals, organisations and society.

You should be aware of and comply with the relevant laws and regulations that apply to your jurisdiction, sector and activities, such as the **Privacy Act 1988 (Cth)** in Australia, which sets out 13 Australian Privacy Principles for handling personal information.

You should also follow the international standards and best practices for data privacy and security, such as ISO 27701, which relates to the way an organisation collects personal data and prevents unauthorised use or disclosure.

You should respect the confidentiality, integrity and availability of the data you collect, use, store and disclose, and only do so for legitimate purposes and with consent or authorisation from the data subjects or owners.

You should employ reasonable protection efforts in your use of technology to communicate with clients, colleagues and stakeholders, and prevent unauthorized disclosure of sensitive information.

You should act ethically and responsibly when dealing with data, especially when using artificial intelligence or machine learning, which present some extraordinary challenges in terms of law, ethics and technical advancement.

You should consider the potential impact of your actions on individuals, organisations and society, and balance the benefits and risks of data use and sharing.

You should be transparent and accountable for your data practices and report any breaches or incidents promptly and appropriately.

CONFIDENTIALITY, INTEGRITY, & AVAILABILITY

Confidentiality, integrity, and availability (CIA) are the three main objectives of cybersecurity that aim to protect data and information from unauthorized access, use, and disclosure.

Confidentiality ensures that only authorized users and processes can access or modify data. This can be achieved by using encryption, authentication, access control, and other security measures.

Integrity ensures that data is maintained in a correct state, and nobody can improperly modify it, either accidentally or maliciously. This can be achieved by using checksums, digital signatures, audit trails, and other security measures.

Availability ensures that authorized users can access data whenever they need to do so. This can be achieved by using backup systems, redundancy, load balancing, and other security measures.

Cybersecurity and data protection are broader topics that cover the legal, ethical, and technical aspects of ensuring the CIA of data in various contexts and domains.

The best advice on the topic of CIA in cybersecurity and data protection is to follow the relevant standards, guidelines, and best practices that apply to your specific industry, sector, or organization. Some examples are ISO/IEC 27001, NIST SP 800-53, GDPR, HIPAA, etc. .

THE EVOLVING THREAT LANDSCAPE

The evolving threat landscape is a perpetual top priority for security and risk management leaders, according to a Gartner survey.

The COVID-19 pandemic has created new challenges and opportunities for cyberattackers, who exploit vulnerabilities in remote work environments, digital meeting solutions, and unpatched systems.

Cyber resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

A **Defence in Depth (DiD)** architecture is an approach to cybersecurity that uses a series of layered defensive mechanisms to protect valuable data and information.

Artificial intelligence (AI) models are becoming effective at enhancing the capabilities of both defenders and attackers in the cyber domain, requiring adaptive strategies to safeguard sensitive data and protect against potential breaches.

Security best practices include using strong passwords, enabling multi-factor authentication, updating software and firmware, encrypting data, backing up data, avoiding phishing emails, and educating users on cyber hygiene.

COLLABORATIVE APPROACH

Recognize that cybersecurity risks are global and require a coordinated, collaborative approach. Cyberattacks can affect any country, sector, or organization, and have severe economic and social consequences. Therefore, we need to ensure that risks to cybersecurity, data protection, privacy, and online safety are addressed at all levels and by all stakeholders.

Share knowledge, build capacity and expertise, and assess cybersecurity risks at the country level. To cope with the evolving nature and complexity of cyber threats, we need to foster a culture of learning and innovation among cybersecurity and data protection professionals. We also need to conduct regular risk assessments to identify the most critical assets and vulnerabilities and prioritize the appropriate measures to protect them.

Provide incentives for the private sector to invest in digital infrastructure and technology. The private sector plays a vital role in developing and deploying secure and resilient digital solutions for various domains, such as health, transport, energy, etc. Therefore, we need to create a favourable environment for private sector participation, such as by providing tax breaks, subsidies, grants, or public-private partnerships.

Unite data protection and cybersecurity skills. Data breaches can have multiple impacts on an organization's reputation, operations, finances, and legal compliance. Therefore, we need to ensure that both data protection and cybersecurity specialists work together to prevent and respond to data breaches, by combining their skills in areas such as encryption, authentication, access control, incident response, etc.

THE HUMAN ELEMENT

The human element is a crucial factor in cybersecurity and data protection, as humans are both the primary source of risks and the target of attacks.

According to ISACA, humans represent a mystery to be deciphered by security/cybersecurity experts because their behaviours, attitudes, beliefs, rituals and decisions constitute a little-understood universe for executives and their heads of security.

The human factor in information security can be seen as the weakest link in the chain or as the reliable and resilient factor of the system, depending on how organizations approach the challenge of educating and empowering their employees.

Harvard Business Review suggests that better cybersecurity starts with fixing employees' bad habits, such as using weak passwords, clicking on suspicious links, or sharing sensitive information online.

The human element of cybersecurity also involves ethical, legal, and social aspects, such as privacy, consent, accountability, and responsibility.

To address the human element of cybersecurity and data protection, organizations need to adopt a holistic approach that combines technical, organizational, and behavioural measures, such as encryption, policies, training, and awareness.

Some points include:

- Keeping software up to date.
- Avoiding opening suspicious emails.
- Keeping hardware up to date.
- Using a secure file-sharing solution to encrypt data.
- Using anti-virus and anti-malware.
- Using a VPN to privatize your connections.
- Check links before you click.
- Don't be lazy with your passwords.

2.3. DATA BREACH NOTIFICATION & COMMUNICATION

Data breaches have become an unfortunate reality, posing significant threats to individuals' privacy and organizations' sensitive information. In response, data breach notification and communication policies have emerged as vital tools to address these challenges.

These policies establish clear guidelines for organizations to follow when a breach occurs, ensuring affected individuals and relevant authorities are promptly informed. Ethical and legal considerations underscore the importance of transparent and timely communication during data breaches, fostering trust, accountability, and responsible data handling.

TRANSPARENCY, TRUST, & ACCOUNTABILITY

Transparency, trust and accountability are essential principles for managing data breaches involving personal information.

Data breach notifications are required by law under the Privacy Act 1988 (Cth) when a breach is likely to result in serious harm to affected individuals and remedial action cannot prevent or mitigate the harm.

Data breach notifications should inform the affected individuals and the Office of the Australian Information Commissioner (OAIC) of the following: *what happened, what information was involved, what are the risks and impacts, what are the steps taken or planned to address the breach, and what are the options for individuals to protect themselves*.

Data breach notifications must be timely, clear, concise and easy to understand. They should also be honest, respectful and empathetic. It is not uncommon for organisations to wait weeks or months before notifying those affected. Meanwhile their personal information is being sold on the dark web.

Data breach notifications can help reduce the potential harm to individuals, restore trust and confidence in the organisation, and demonstrate compliance with legal obligations and ethical standards.

Such notifications should be part of a broader data breach response plan that includes preparation, containment, assessment, notification, review and evaluation stages.

Data breach response plans must be aligned with best practices and guidance from relevant authorities, such as the OAIC, the Data Protection Commissioner and industry bodies.

THE MODERN DATA LANDSCAPE

The ubiquity of digital systems has led to an unprecedented accumulation of personal and sensitive data. From financial records and healthcare information to personal preferences and online behaviours, data has become an asset, making it an attractive target for cybercriminals.

The modern data landscape is dynamic, with data being collected, stored, processed, and shared across multiple platforms, devices, and jurisdictions.

Data breaches are therefore a serious threat to the privacy and security of personal information, and can have significant legal, reputational, and financial consequences for organisations and individuals.

As mentioned, data breach notification and communication should follow the best practices outlined by the Office of the Australian Information Commissioner (OAIC) in its Data Breach Preparation and Response Guide, as well as any applicable laws or regulations in the relevant jurisdictions.

Some of the best practices for data breach notification and communication are:

- Notify the OAIC and affected individuals as soon as practicable after becoming aware of a data breach that is likely to result in serious harm, unless remedial action can prevent or mitigate the risk of harm.
- Use multiple communication channels to ensure that all affected individuals are notified, such as email, phone, SMS, website, social media, or postal mail.
- Use plain language that is clear, concise, and accurate, and avoid technical jargon or legal terms that may confuse or mislead the recipients.
- Provide a comprehensive explanation of what happened, what information was involved, what actions have been taken to contain and resolve the breach, what steps are being taken to prevent future breaches, and what assistance or support is available to the affected individuals.
- Use effective headlines that capture the attention and convey the urgency of the message, such as "Important: Data Breach Notification" or "Urgent: Action Required Following Data Breach".
- Inform the affected individuals about the next steps they should take to protect themselves from potential harm, such as changing passwords, monitoring accounts, contacting credit reporting agencies, or seeking legal advice.

Data breach notification and communication should be tailored to the specific circumstances and context of each breach, considering factors such as the nature and extent of the breach, the type and sensitivity of the information involved, the potential harm to the affected individuals, and the expectations and preferences of the recipients.

Data breach notification policies are a structured framework that organizations must adhere to when a data breach occurs. These policies outline the necessary steps for identifying, mitigating, and communicating the breach to the affected individuals and relevant authorities.

Have a written data breach response plan that outlines the roles and responsibilities of the data breach response team, the steps to contain, assess, notify and review the breach, and the communication strategies for internal and external stakeholders.

Consider the safety and privacy of the individuals whose personal information has been compromised and avoid disclosing any confidential or sensitive information that could put them at further risk.

Comply with the requirements of the Privacy Act 1988 (Cth) and the Notifiable Data Breaches (NDB) scheme, which mandate notification to the affected individuals and the Office of the Australian Information Commissioner (OAIC) if a data breach is likely to result in serious harm.

Provide clear and timely information to the affected individuals about the nature and extent of the breach, the steps taken to mitigate the harm, the actions they can take to protect themselves, and the contact details for further assistance.

Review the incident and identify the causes and contributing factors of the breach and implement measures to prevent or reduce the likelihood of future breaches.

TIMELINESS THE ETHICAL IMPERATIVE

Ethical data breach notification policies stress the urgency of timely communication. Delayed notification can exacerbate the impact of a breach, allowing cybercriminals more time to exploit compromised data.

Timeliness is an ethical imperative in data breach notification because it can reduce or prevent the harm to the affected individuals and restore the trust in the organisation that handles their personal information.

The Privacy Act 1988 (Cth) requires organisations to notify individuals and the Commissioner of eligible data breaches as soon as practicable after becoming aware of them unless an exception applies.

An eligible data breach occurs when there is any unauthorised access, disclosure or loss of personal information that is likely to result in serious harm to any of the individuals to whom the information relates.

To determine whether a data breach is likely to result in serious harm, organisations should consider the nature and sensitivity of the personal information involved, the circumstances of the breach, and the potential consequences for the individuals.

Timely notification and communication can help individuals to take steps to protect themselves from the harm, such as changing passwords, monitoring accounts, or contacting their financial institutions.

Timely notification and communication can also demonstrate that the organisation is taking the data breach seriously, is committed to protecting the privacy of its customers or clients and is transparent and accountable for its actions.

To achieve timeliness in data breach notification and communication, organisations should have a data breach response plan that outlines the roles and responsibilities of staff, the steps to contain, assess, notify and review a data breach, and the communication strategies and channels to use.

Organisations should also train their staff on how to identify and report a data breach, and regularly review and update their data breach response plan to ensure its effectiveness.

BALANCING LEGAL COMPLIANCE & ETHICAL VALUES

Data breach notification policies often align with legal requirements imposed by data protection regulations. However, ethical considerations go beyond legal mandates, emphasizing the moral responsibility of organizations to safeguard individuals' data and rights.

Balancing legal compliance and ethical values in data breach notification and communication is a complex and challenging task that requires careful consideration of various factors, such as:

- The applicable laws and regulations in different jurisdictions that may impose different obligations and standards for data breach notification and communication, such as the type, timing, content, and format of the notification.
- The ethical values and expectations of the stakeholders that may go beyond the legal requirements and demand more transparency, accountability, and responsiveness from the organization.
- The potential risks and benefits of disclosing or withholding certain information about the data breach, such as the cause, scope, severity, and consequences of the breach, as well as the remedial measures taken or planned by the organization.

Based on research and best practice, some of the general principles and guidelines for balancing legal compliance and ethical values in data breach notification and communication are:

- Be proactive and prepared - develop a data breach response plan that outlines the roles, responsibilities, procedures, and resources for data breach notification and communication. Conduct regular training and testing to ensure that the plan is effective and up to date.

- Be timely and accurate - notify the affected stakeholders as soon as possible after discovering a data breach, without unreasonable delay. Provide accurate and information about the data breach, without speculation or exaggeration. Update the information as new facts emerge or circumstances change.
- Be clear and concise - use plain and simple language that is easy to understand by the intended audience. Avoid technical jargon or legal terms that may confuse or mislead the stakeholders. Use appropriate channels and formats to communicate the information, such as email, phone call, letter, website, social media, etc.
- Be respectful and empathetic - acknowledge the impact and harm caused by the data breach to the stakeholders. Express sincere apology and regret for the incident. Demonstrate genuine concern and care for the stakeholders' well-being and security. Offer assistance and support to help them cope with the aftermath of the data breach.
- Be honest and accountable - admit responsibility and liability for the data breach, if applicable. Explain the root cause and contributing factors of the data breach. Disclose the actions taken or planned to investigate, contain, recover, and prevent future breaches. Cooperate with relevant authorities and regulators in their inquiries or investigations. Accept feedback and criticism from the stakeholders and address their questions or concerns.

RESILIENT DEFENCES & RESPONSIBLE PRACTICES

Offensive cyber security training involves teaching students how to perform penetration testing, ethical hacking and other techniques to identify and exploit vulnerabilities in systems and networks.

This type of training can have many benefits, such as improving the security posture of organizations, enhancing the skills and knowledge of cyber security professionals, and contributing to the advancement of cyber security research and innovation.

However, such training also poses significant ethical risks, such as misuse or abuse of the acquired skills, violation of privacy or confidentiality, damage to systems or data, or harm to individuals or society at large.

Therefore, you should follow some ethical principles for designing responsible offensive cyber security training, such as:

- **Principle 1: Respect for autonomy**. You should respect the autonomy of your students and other stakeholders by informing them about the objectives, methods, risks and benefits of the training, and obtaining their consent before engaging in any offensive cyber security activities.

- **Principle 2: Beneficence and non-maleficence**. You should aim to maximize the benefits and minimize the harms of the training for your students and other stakeholders by ensuring that the training is relevant, proportionate, necessary and effective.
- **Principle 3: Justice**. You should ensure that the training is fair and equitable for your students and other stakeholders by avoiding discrimination, bias, favouritism or exploitation, and providing equal opportunities for participation and learning.
- **Principle 4: Accountability**. You should be accountable for your actions and decisions in the training by adhering to relevant laws, regulations, standards and codes of conduct, and being transparent, honest and responsible for the outcomes and impacts of the training.
- **Principle 5: Education**. You should educate your students and other stakeholders about the ethical implications of offensive cyber security by raising their awareness, fostering their critical thinking, and encouraging their ethical reasoning and decision-making.

In addition to these principles, you should also follow some good practices for cyber resilience that can help you protect your assets, detect threats, respond to incidents and recover from disruptions. Some of these practices are:

- Developing a cybersecurity strategy and governance framework that aligns with your organizational goals and objectives and involves board engagement and oversight.
- Implementing a cyber risk management process that identifies, assesses, treats and monitors cyber risks, including those related to third parties such as vendors or partners.
- Collaborating and sharing information with other organizations, security agencies and law enforcement entities to enhance your situational awareness, threat intelligence and incident response capabilities.
- Managing your assets effectively by maintaining an inventory of your critical internal and external assets (e.g., software and data), and ensuring their visibility, availability and integrity.
- Implementing protective measures and controls based on the Australian Signals Directorate's (ASD) Strategies to mitigate targeted cyber intrusions (or equivalent), as well as additional controls such as encryption for data in transit.
- Using detection systems and processes that enable continuous monitoring of your systems and networks, and leverage data analytics to integrate sources of threats in real time.

Elevating the human element in cybersecurity means strengthening the awareness, skills and behaviours of the people who interact with digital systems and data.

According to a report by Verizon, human errors and actions accounted for 82% of all cyberattacks in 2022. Therefore, it is crucial to train and educate employees on how to prevent and respond to cyber threats.

Some best practices for elevating the human element in cybersecurity are:

- Offering continuous training opportunities for all staff members, from the CEO to the receptionist, on their role in protecting the organization from cyber risks.
- Deploying advanced email protections, such as spam filters, phishing simulations and email encryption, to reduce the chances of falling victim to malicious messages.
- Revisiting the approach to password security, such as enforcing strong and unique passwords, using password managers and changing passwords regularly.
- Updating multifactor authentication controls, such as using biometric or token-based verification methods, to add an extra layer of security for accessing sensitive data or systems.
- Using insider threat protection technology, such as user behaviour analytics or data loss prevention tools, to monitor and detect abnormal or suspicious activities by authorized users.

CONTINUOUS IMPROVEMENT & LEARNING

Continuous Improvement & Learning (CIL) is a key aspect of data breach notification and communication, as it helps organisations to prevent, prepare for and respond to data breaches effectively.

CIL involves reviewing and learning from data breach incidents, identifying the root causes, implementing prevention plans, and updating policies and procedures accordingly.

CIL also involves communicating the lessons learned and the actions taken to relevant stakeholders, such as affected individuals, regulators, partners, and employees.

CIL can help organisations to reduce the risk of harm to individuals, comply with the Privacy Act 1988 (Cth) and the Notifiable Data Breaches (NDB) scheme, and maintain trust and reputation as data custodians.

Some sources of information and guidance on CIL for data breach notification and communication are:

- Data breach preparation and response - Office of the Australian Information Commissioner
- Part 3: Responding to data breaches – four key steps | OAIC
- Data Breach Response: The Continuous Improvement Cycle - Tanner De Witt Solicitors

2.4 ETHICAL HACKING

A PROACTIVE APPROACH TO SECURITY

Ethical hacking is the use of hacking skills and techniques with good intentions and with the full consent and approval of the target.

Ethical hackers help organizations identify and fix vulnerabilities in their IT systems, networks, and applications before malicious hackers can exploit them.

Ethical hacking is a valued component of cybersecurity, but it is different from cybersecurity. Cybersecurity is a broader term that encompasses all the policies, practices, and tools that protect IT environments from cyber threats. Ethical hacking is a proactive approach that involves system testing to find and address weaknesses.

Ethical hacking requires a high level of technical skills, ethical standards, and legal compliance. Ethical hackers must follow certain principles, such as obtaining the target's consent, defining the scope of their activities, reporting their findings, and respecting the target's privacy and security.

It can benefit organizations in various ways, such as improving their security posture, enhancing their reputation, complying with regulations, and saving costs.

Ethical hacking can also benefit society by raising awareness of cyber risks, promoting ethical values, and contributing to cyber resilience.

THE RESPONSIBILITY OF RESPONSIBLE HACKING

Responsible hacking is the practice of using hacking skills for ethical, legal or beneficial purposes, such as testing the security of systems, finding vulnerabilities, or exposing wrongdoing.

Responsible hacking requires adhering to certain principles and standards, such as obtaining consent, respecting privacy, avoiding harm, reporting findings, and complying with laws and regulations.

Responsible hacking also entails being aware of the risks and consequences of hacking activities, such as legal liability, reputational damage, or retaliation from malicious actors.

As an IT professional, you should advise your clients or employers on how to implement responsible hacking practices in their cybersecurity training and ethical hacking programs.

Some of the best practices for responsible hacking include:

- Establishing clear policies and procedures for ethical hacking activities, such as defining the scope, objectives, methods, and reporting mechanisms.
- Obtaining written authorization from the owners or operators of the systems to be hacked and ensuring that the hacking activities do not violate any contractual or legal obligations.
- Conducting regular security assessments and audits to identify and remediate vulnerabilities, and using only approved tools and techniques that minimize the impact on the systems.
- Educating and training staff on ethical hacking skills and principles and ensuring that they follow the code of conduct and professional standards of the industry.
- Collaborating with other stakeholders, such as law enforcement agencies, regulators, or industry associations, to share information, best practices, and lessons learned.

Some of the sources that you can refer to for more information on responsible hacking are:

- Cybersecurity Laws and Regulations Report 2023 Australia, which covers common issues in cybersecurity laws and regulations in Australia.
- Cybersecurity. Who is responsible? which discusses the roles and responsibilities of different actors in cybersecurity.
- Who is Liable when Business Emails are Hacked? which explains the legal implications of hacking business emails in Australia.

MITIGATING LEGAL & REPUTATIONAL RISKS

Ethical hacking is a valuable practice that can help organizations improve their cybersecurity posture and prevent malicious attacks.

However, ethical hackers also face legal and reputational risks if they do not follow certain principles and guidelines.

Some of the best practices for mitigating legal and reputational risks in ethical hacking are:

- Obtain written consent from the client or the target organization before conducting any penetration testing or vulnerability assessment. This consent should specify the scope, duration, and objectives of the ethical hacking activity, as well as the roles and responsibilities of both parties.
- Follow the principle of least privilege and only access the minimum amount of data and systems necessary to perform the ethical hacking task. Avoid accessing, modifying, or deleting any sensitive or personal information that is not relevant to the security assessment.

- Report any findings or incidents to the client or the target organization in a timely and transparent manner. Provide clear and actionable recommendations on how to address the identified vulnerabilities or threats. Do not disclose any information to third parties without prior authorization.
- Adhere to the relevant laws, regulations, standards, and codes of ethics that apply to the ethical hacking domain. Respect the privacy, confidentiality, and intellectual property rights of the client or the target organization and their stakeholders.
- Maintain a high level of professionalism and integrity throughout the ethical hacking process. Do not engage in any malicious, fraudulent, or illegal activities that could harm the client or the target organization or their reputation.