7907ICT
IT & Cybersecurity Governance, Policy, Ethics & Law

COURSE NOTES

David Tuffley PhD
Senior Lecturer, School of ICT

A comprehensive introduction to the broad areas of IT (Information Technology) & Cybersecurity Governance, Policy, Ethics & Law. It is a course primarily for IT professionals with an emphasis on cybersecurity but may also be of interest to professionals from related disciplines.

The Learning@Griffith course site has all course material including a link to the Course Profile where you will find definitive information on all aspects of this course.

CONTENTS

INTRODUCTION TO COURSE

1.1 HELLO & WELCOME

American statesman Benjamin Franklin famously said that an *ounce of prevention is worth pound of cure*. He was reportedly talking about fire safety, and indeed it is true that preventing fires is worth putting effort into, just as important as being able to put them out.

More than two centuries later, the principle is alive and well and being applied to a wide range of sectors, not least of which is cybersecurity governance and with IT more generally. Given that the statistical probably of a data breach in an escalating risk environment is quite high, the *emphasis must be put on proactively minimizing the risk*. It is no less important than knowing what to do when a breach occurs.

It could be argued that with proactive risk management, the number of actual breaches will fall significantly when they are prevented before becoming a threat.

This course focusses on *both* the proactive and reactive aspects of IT and cybersecurity governance, and the related policies, ethical and legal considerations.

ACKNOWLEDGEMENT OF SOURCES

Material for these notes has been drawn from a wide variety of sources, principally from various Australian Government agencies, the Software Engineering Institute, Carnegie Mellon Univ. Pittsburgh, Centre for Risk Studies, Cambridge University, and the Office of the Australian Information Commissioner.

1.2 HOW SHOULD YOU APPROACH THIS COURSE?

The course is arranged in modules that we recommend you do each week, without skipping weeks with the intention of catching up later. Good time management is key ingredient if professional practice and we strongly encourage it in this course.

The first thing to do is download the self-contained course notes in PDF for online consumption. A printed copy is also available from Amazon for a fee, but you do not necessarily need to have the printed book, only if you want it.

Go through each module, listening / watching the material and read the content as well as stay up to date with any assessment tasks mentioned there.

For in-person students and those enrolled in the online synchronous offering, try to attend the online lectures and in-person workshops each week. These are recorded for your later viewing if the timing of the scheduled event is awkward.

You will get the most from this course if you invest your time and effort in making the learning journey.

For students enrolled in the fully asynchronous mode, you have no deadlines apart from the Trimester start and finish dates. It's important that you manage your time well and work your way through the content for a satisfaction finish. You are encouraged to interact with the other students on the forums provided.

MODULE 1:
IT GOVERNANCE FRAMEWORKS

IT governance frameworks are the rules and guidelines that help organizations manage their IT resources and processes effectively. They help align IT goals with business objectives, ensure compliance with laws and regulations, and protect data from unauthorized access or loss. Some examples of IT governance frameworks are COBIT, ITIL, ISO 27001, and NIST.

IT compliance and regulatory standards are the requirements that organizations must follow to meet the expectations of external stakeholders, such as customers, auditors, or government agencies. They help ensure quality, security, privacy, and accountability of IT services and products. Some examples of IT compliance and regulatory standards are GDPR, HIPAA (Health Insurance Portability and Accountability), PCI DSS, and SOX.

Data retention and deletion are the policies and practices that decide how long and where organizations store their data, and when and how they dispose of it. They help balance the needs of data availability, performance, cost, and risk. Some examples of data retention and deletion factors are legal obligations, business value, storage capacity, and backup frequency.

In this module workshop, you will learn how to apply IT governance frameworks to your organization, how to comply with IT standards and regulations, and how to design and implement data retention and deletion policies. You will also learn how to assess the benefits and challenges of IT governance, compliance, and data management in different scenarios.

1.1. IT GOVERNANCE FRAMEWORKS

There are several IT governance frameworks available, each with its own strengths, weaknesses, and applicability. Some of the most common frameworks are:

- **COBIT**. This is a comprehensive framework that covers 37 IT processes, each with detailed objectives, practices, inputs, outputs, activities, and metrics. COBIT helps organizations achieve effective IT governance and management by linking IT goals to business goals, ensuring IT resources are optimized, and managing IT risks and performance.
- **AS8015-2005**. This is a simple and concise framework developed in Australia that defines six principles for good IT governance: establish clearly understood responsibilities for IT; plan IT to best support the organization; acquire IT validly; ensure that IT performs well; ensure that IT conforms with formal rules; and respect human factors in IT.
- **ISO/IEC 38500**. This is an international standard that provides high-level guidance on the principles, roles, and responsibilities for effective IT

governance. ISO/IEC 38500 helps organizations evaluate, direct, and monitor their use of IT to achieve their business objectives and fulfill their legal and ethical obligations.

- **ITIL**. This is a widely adopted framework that focuses on the delivery and management of quality IT services that meet the needs and expectations of customers and stakeholders. ITIL covers the entire service lifecycle from strategy to design, transition, operation, and improvement. ITIL helps organizations improve their service efficiency, effectiveness, reliability, and value.

Choosing the right IT governance framework depends on various factors such as the size, complexity, culture, industry, and maturity of the organization. It is also possible to adopt a hybrid or customized approach that combines elements from different frameworks to suit the specific needs and context of the organization.

IT governance frameworks are not static or one-size-fits-all solutions. They require regular review and adaptation to keep up with the changing business environment and technology landscape. They also require strong leadership commitment, stakeholder involvement, clear communication, and continuous improvement to ensure successful implementation and outcomes.

COBIT ORCHESTRATING CONTROL & ASSURANCE

COBIT is a comprehensive framework for the governance and management of enterprise information and technology (I&T (Information Technology)). It helps organizations align their I&T goals with their business objectives, optimize their I&T resources and processes, and ensure effective control and assurance over their I&T activities.

COBIT consists of seven enablers: principles, policies and frameworks; processes; organizational structures; culture, ethics and behaviour; information; services, infrastructure and applications; and people, skills and competencies.

COBIT & IT GOVERNANCE FRAMEWORKS

IT governance frameworks are essential for ensuring that I&T supports the achievement of enterprise goals, delivers value to stakeholders, manages risks and complies with external requirements.

COBIT provides a holistic and integrated approach to IT governance that covers all aspects of I&T from strategy to operations.

COBIT also provides a common language and terminology for I&T governance that can be understood by all stakeholders, including business executives, IT managers, auditors and regulators.

HOW COBIT CONTROLS AND ASSURES

One of the key benefits of COBIT is that it enables organizations to establish and maintain a system of internal control and assurance over their I&T activities.

COBIT defines control as "the means of managing risk to ensure that enterprise objectives will be achieved" and assurance as "the provision of objective evidence that the design and operation of the system of internal control meets the agreed-upon requirements".

COBIT provides guidance on how to design, implement, monitor, evaluate and improve the system of internal control and assurance using the following processes:

MEA01: Managed Performance and Conformance Monitoring.

This process collects, validates, and evaluates enterprise and alignment goals and metrics, monitors that processes and practices are performing against agreed performance and conformance goals and metrics, provides systematic and timely reporting, and provides transparency of performance and conformance and drives achievement of goals.

MEA02: Managed System of Internal Control.

This process continuously monitors and evaluates the control environment, including self-assessments and self-awareness, enables management to identify control deficiencies and inefficiencies and to initiate improvement actions, plans, organizes and maintains standards for internal control assessment and process control effectiveness, obtains transparency for key stakeholders on the adequacy of the system of internal controls.

MEA03: Managed Compliance with External Requirements

This process evaluates that I&T processes and I&T-supported business processes are compliant with laws, regulations and contractual requirements, obtains assurance that the requirements have been identified and complied with; integrates IT compliance with overall enterprise compliance, ensures that the enterprise is compliant with all applicable external requirements.

MEA04: Managed Assurance

This process plans, scopes and executes assurance initiatives to comply with internal requirements, laws, regulations and strategic objectives, enables management to deliver adequate and sustainable assurance in the enterprise by performing independent assurance reviews and activities, enables the organization to design and develop efficient and effective assurance initiatives.

ITIL ELEVATING SERVICE MANAGEMENT

ITIL is a library of best practices used in IT Service Management (ITSM). ITSM is the process of designing, delivering, managing and improving IT services that meet

the needs and expectations of customers and stakeholders. ITSM covers a wide range of activities, such as incident management, change management, problem management, service level management, service design, service transition, service operation and continual service improvement.

ITIL provides a comprehensive and consistent framework for ITSM that is aligned with business goals and customer value. ITIL helps organizations to:

- Improve customer satisfaction by delivering reliable and high-quality IT services.
- Enhance IT services delivered using best practice procedures.
- Reduce costs and risks by optimizing the use of resources and avoiding service disruptions.
- Increase agility and innovation by enabling faster and more effective changes to IT services.
- Support digital transformation by integrating ITSM with other frameworks such as DevOps, Agile and SRE.

ELEVATING SERVICE MANAGEMENT WITH ITIL

To elevate service management with ITIL, you need to adopt a holistic and value-driven approach that encompasses the entire service lifecycle. You need to understand the needs and expectations of your customers and stakeholders, and design, deliver, manage, and improve IT services that create value for them. You need to establish clear and measurable service levels, and ensure that they are properly assessed, monitored and managed against these targets.

Collaborate with other teams and departments across the organization, and leverage the capabilities of people, processes, information and technology. You need to foster a culture of continual improvement that seeks feedback, learns from mistakes, identifies opportunities and implements changes.

Here are some practical steps you can take to elevate service management with ITIL:

Assess the current state of your ITSM practices and identify gaps and areas for improvement.

Define a vision and strategy for your ITSM that aligns with your organizational goals and customer value propositions.

Implement the ITIL Service Value System (SVS) that consists of five components: *guiding principles, governance, service value chain, practices, and continual improvement*.

Use the SVS to plan, engage, design, transition, obtain/build, deliver/support and improve your IT services.

Apply the seven guiding principles of ITIL to guide your decisions and actions: focus on value, start where you are, progress iteratively with feedback, collaborate and promote visibility, think and work holistically, keep it simple and practical, optimize and automate.

Establish a Service Management Office (SMO) that provides a central point for consistency and governance in organizational best practice.

Monitor and measure your service performance using relevant metrics and indicators.

Report and communicate your service achievements and challenges to your customers and stakeholders.

Review and evaluate your service outcomes and feedback using various methods such as surveys, audits, reviews, benchmarks etc.

Identify and prioritize improvement initiatives using techniques such as SWOT analysis, gap analysis, root cause analysis etc.

Implement improvement actions using methods such as PDCA cycle (plan-do-check-act), CSI approach (what is the vision? where are we now? where do we want to be? how do we get there? did we get there? how do we keep the momentum going?) etc.

ISO/IEC 38500 THE GOVERNING STANDARD

Advice on ISO/IEC 38500 The Governing Standard. ISO/IEC 38500 is an international standard for the corporate governance of information technology (IT), and provides guidance to those persons advising, informing or assisting directors on the effective and acceptable use of IT within the organization. It is based on six principles and a model for good governance of IT.

PRINCIPLES

The six principles of ISO/IEC 38500 are:

Responsibility. Assigning roles and responsibilities for the use of IT.

Strategy. Aligning the use of IT with the organizational objectives.

Acquisition. Procuring IT solutions and services to meet the organizational needs.

Performance. Measuring and evaluating the contribution of IT to the organization

Conformance. Ensuring compliance with laws, regulations, and policies.

Human Behaviour. Considering the human aspects of IT use.

MODEL

The model of ISO/IEC 38500 has four main elements:

Governing Body. The individual or group of individuals responsible and accountable for the performance and conformance of the organization

Evaluation. The process of assessing the current and future use of IT

Direction. The process of deciding on the objectives and policies for the use of IT

Monitoring. The process of verifying that the use of IT meets the objectives and policies.

The governing body should evaluate, direct, and monitor the use of IT in a continuous cycle, considering the six principles and the stakeholders' interests.

BENEFITS

The benefits of applying ISO/IEC 38500 include:

- Improving the alignment of IT with the organizational strategy.
- Enhancing the delivery of value from IT investments.
- Reducing risks related to IT projects and operations.
- Increasing transparency and accountability for IT decisions and outcomes.
- Fostering a culture of trust and collaboration among IT stakeholders.
- Supporting continuous improvement and innovation in IT.

UNIFYING BUSINESS & TECHNOLOGY

IT governance is a process that enables the IT staff to better manage risk and operate at its most efficient to the benefit of the organization. It is part of the corporate governance, which is a collection of processes that are designed to keep the entire corporation effective and efficient.

IT governance aims to:

- Ensure business value is generated by information and technology.
- Oversee the performance of IT managers.
- Assess risks associated with the IT department and mitigate them as needed.

THE SIGNIFICANCE OF IT GOVERNANCE

IT governance is important because it helps the organization to align its IT priorities, decisions and investments with its strategic goals and stakeholder requirements. It also helps the organization to comply with legal, contractual and policy obligations that impact IT. Furthermore, it supports the continuous improvement and optimization of IT services and resources.

IMPLEMENTING IT GOVERNANCE

There are different frameworks and standards that can guide the implementation of IT governance in an organization. Some of the most common ones are:

- **COBIT**. This is a comprehensive framework that covers 37 IT processes, with each process having a set of objectives, inputs, outputs, activities, roles, and responsibilities. It also provides maturity models, performance indicators and best practices for each process.
- **AS8015-2005**. This is a technical standard developed in Australia that defines six principles for good IT governance: establish clearly understood responsibilities for IT; plan IT to best support the organization; acquire IT validly; ensure that IT performs well, whenever required; ensure IT conforms with formal rules; ensure respect for human factors.
- **ISO/IEC 38500**. This is an international standard that provides a high-level framework for effective governance of IT. It defines six principles for good IT governance: responsibility; strategy; acquisition; performance; conformance; human behaviour.

These frameworks and standards can be adapted to suit the specific needs and context of each organization. However, some common steps for implementing IT governance are:

- Define the scope and objectives of IT governance.
- Establish the roles and responsibilities of IT governance stakeholders.
- Identify the key IT processes and activities that need to be governed.
- Define the policies, procedures, guidelines, and standards that govern IT.
- Establish the mechanisms and tools for monitoring, reporting, and evaluating IT performance and compliance.
- Implement continuous improvement initiatives to enhance IT value and maturity.

GUIDELINES FOR DECISION-MAKING

Guidelines for decision-making in IT governance frameworks, based on research and best practice:

- What is IT governance and why is it important?
- What are the key principles of IT governance?
- What are the common IT governance frameworks and how do they support decision-making?
- How to define the roles and responsibilities of decision-makers in IT governance?
- How to ensure transparency, accountability, and compliance in IT governance decisions?

WHAT IS IT GOVERNANCE AND WHY IS IT IMPORTANT?

IT governance is the process of defining the structures and processes that enable the organization to effectively oversee, direct and control its IT resources and processes. It involves evaluating stakeholder requirements, setting direction, prioritizing investments, monitoring performance, and ensuring compliance with legal, contractual and policy requirements that impact IT.

IT governance is important because it helps the organization to:

- Achieve its strategic goals and objectives by aligning IT with the business needs and expectations.
- Optimize the value of IT by delivering benefits to the organization and its stakeholders.
- Manage the risks associated with IT by identifying, assessing, and mitigating them.
- Enhance the performance of IT by improving the quality, efficiency, and effectiveness of IT services.
- Foster a culture of continuous improvement by learning from feedback and best practices.

ENSURING COMPLIANCE IN IT GOVERNANCE DECISIONS

Another key aspect of effective decision-making in IT governance is to ensure that the decisions are transparent, accountable and compliant with the relevant legal, contractual and policy requirements that impact IT.

Some of the ways to ensure transparency, accountability and compliance in IT governance decisions are:

- Documenting and communicating the IT governance framework, including the principles, rules, processes, roles, responsibilities and authorities that guide decision-making.
- Establishing and maintaining a repository of IT governance decisions, including the rationale, criteria, evidence, alternatives and impacts of each decision.
- Implementing and monitoring a set of KPIs and metrics that measure the performance and outcomes of IT governance decisions.
- Conducting regular audits and reviews of IT governance decisions to verify their validity, effectiveness and efficiency.
- Reporting and disclosing IT governance decisions to relevant stakeholders, such as senior management, board of directors, regulators, customers and suppliers
- Establishing and enforcing a mechanism for escalating, resolving and learning from issues, disputes and complaints related to IT governance decisions.

By following these steps, organizations can enhance the trust, confidence and satisfaction of their stakeholders regarding their IT governance decisions.

RISK MANAGEMENT & MITIGATION

Risk management and mitigation is the process of identifying, analysing, evaluating, and treating the potential threats and vulnerabilities that could affect the performance, security, reliability, and compliance of IT systems and processes.

It also involves monitoring and reviewing the risk situation and taking corrective actions as needed.

Risk management and mitigation is important because it helps organizations to:

- Protect their assets, data, reputation, and stakeholders from harm or loss.
- Ensure the continuity and availability of their IT services and operations.
- Achieve their strategic objectives and deliver value to their customers.
- Comply with legal, regulatory, contractual, and ethical obligations.
- Enhance their decision-making and innovation capabilities.
- Reduce costs and optimize resources.

Implementing Risk Management & Mitigation?

To implement a successful risk management and mitigation strategy, organizations should follow these steps:

- Establish a risk management framework that defines the scope, objectives, roles, responsibilities, policies, procedures, tools, and metrics for managing and mitigating risks.
- Conduct a risk assessment that identifies and prioritizes the sources and impacts of risks for each IT system and process.
- Develop a risk treatment plan that specifies the actions, resources, timelines, and owners for reducing or eliminating the risks or their consequences.
- Implement the risk treatment plan by executing the actions and allocating the resources as planned.
- Monitor and review the risk situation by measuring the performance, effectiveness, and efficiency of the risk treatment actions and reporting the results and progress.
- Update the risk management framework, assessment, treatment plan, and actions as needed to reflect changes in the internal or external environment or feedback from stakeholders.

ETHICAL & LEGAL COMPLIANCE

An IT governance framework is a set of policies, processes, roles and responsibilities that guide the creation, use and management of information technology (IT) assets and services in an organisation. It helps to ensure that IT supports the organisation's strategy, objectives and performance, while also managing the risks, costs and benefits of IT.

An IT governance framework should be aligned with the organisation's overall governance framework, which provides a holistic overview of how the organisation creates and manages its enterprise-wide information assets (records, information and data).

Ethical and legal compliance is important for several reasons:

- It helps to build trust and reputation among stakeholders, which can enhance customer loyalty, employee engagement, partner collaboration and social responsibility.
- It helps to avoid or minimise legal liabilities, fines, sanctions or lawsuits that can result from violating laws, regulations or standards that apply to the organisation's IT activities.
- It helps to prevent or mitigate ethical issues or dilemmas that can arise from the use or misuse of IT, such as privacy breaches, data misuse, cyberattacks, bias or discrimination.
- It helps to foster a culture of ethics and integrity in the organisation, which can encourage innovation, creativity and excellence in IT.

ACHIEVING ETHICAL & LEGAL COMPLIANCE

Some general steps that can be followed are:

Identify and understand the legal, regulatory and ethical requirements that apply to the organisation's IT activities. These may include laws and regulations related to data protection, cybersecurity, intellectual property, consumer rights, human rights or environmental protection. They may also include ethical principles or codes of conduct that reflect the organisation's values or industry standards.

Assess and document the current state of compliance in the organisation's IT governance framework. This may involve conducting audits, reviews or surveys to evaluate how well the organisation's IT policies, processes and practices comply with the relevant requirements. It may also involve identifying any gaps, weaknesses or risks that need to be addressed.

Develop and implement a plan to improve compliance in the organisation's IT governance framework. This may involve updating or creating new IT policies, processes or practices that align with the relevant requirements. It may also involve providing training, guidance or support to staff or stakeholders on how to comply with the requirements. It may also involve monitoring, measuring or reporting on the progress or outcomes of compliance efforts.

Review and update the compliance plan regularly. This may involve revisiting the legal, regulatory or ethical requirements periodically to ensure they are up-to-date and relevant. It may also involve evaluating the effectiveness or impact of compliance efforts on the organisation's performance or stakeholder satisfaction.

It may also involve seeking feedback or input from staff or stakeholders on how to improve compliance.

1.2. IT COMPLIANCE & REGULATORY STANDARDS

Today's business environment is becoming more complex, and organizations must negotiate the web of regulations and standards.

IT compliance and regulatory standards ensure that organizations adhere to a set of guidelines, laws, and best practices.

Organizations must define and implement policies that not only facilitate compliance but also engender ethical conduct, responsible innovation, and safeguards against risks.

THE REGULATORY FRAMEWORK

The regulatory framework for IT and cybersecurity compliance and regulatory standards is the set of laws, rules, guidelines and best practices that govern how businesses use, store, process and transmit information technology (IT).

The framework varies depending on the type and nature of the data involved, such as personal data, health data, financial data or government data. The framework also depends on the geographic location of the business and its customers, as different regions and countries have different regulations.

IT and Cybersecurity compliance standards include:

GDPR: The General Data Protection Regulation (GDPR) is a set of IT regulations that the European Union (EU) enforces. It protects the security and privacy of data belonging to EU citizens and residents. It applies to any business that operates with such data, even if it is not located in the EU.

Under the GDPR it is legal to process someone's data provided:

1. The data subject has given consent to the processing of his or her personal data,
2. Contractual obligations with a data subject have been fulfilled,
3. The data subject has complied with a data controller's legal obligations,
4. The vital interests of a data subject are protected,
5. The processing is done in the public interest or official authority,
6. The processing is done in the legitimate interests of a data controller unless precedence is taken by the interests of the data subject.

For informed consent to be used as the lawful basis for processing, that consent must have been explicitly given for the data concerned. That consent must be a "specific, freely given, plainly worded, and unambiguous affirmation" given by the data subject. It is not acceptable to have consent given by default on a web-form, nor to bundle multiple types of processing into the one affirmation.

Under GDPR, data subjects must have the option to withdraw consent at any time. And it must not be harder to do so than it was to opt in. In the case of

children less than 16 years, consent must be given by the child's verified parent or custodian.

Data controllers must meet the principles of data protection by *design* and by *default*, which means data protection measures are designed into the business processes. This includes the pseudonymising of personal data as soon as possible.

When data is collected, data subjects must be unambiguously informed about the extent of the data collection, what is the legal basis for the proposed processing of personal data, how long the data will be retained, whether that data will be communicated to a third-party inside or outside the EU and must disclosure of any automated decision-making that is made on a solely algorithmic basis.

Anti-Money Laundering (AML) & Know Your Customer (KYC). The Office of the Australian Information Commissioner (OAIC) prescribe the legal framework applicable to the prevention of money laundering and associated Know Your Customer.

They refer to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, and the *Anti-Money Laundering and Counter-Terrorism Financing Rules* which aim to prevent the practice and the financing of terrorism. They impose certain obligations on "reporting entities" which include the financial sector, gambling sector, remittance (money transfer) services, bullion dealers and other professionals or businesses that provide services with the potential for money laundering. These obligations include collecting and verifying certain 'know your customer' (KYC) information about a customer's identity before providing those services.

Entities that are required to comply with the *AML/CTF Act* are likewise required to comply with the *Privacy Act 1988* to safeguard the personal information collected for the purposes of compliance with their AML/CTF Act obligations.

The *Australian Transaction Reports and Analysis Centre (AUSTRAC)* is the Australian Government agency responsible for ensuring compliance with the AML/CTF Act.

*Privacy obligations of small business 'reporting entities'. S*mall businesses (annual turnover of $3 million or less) are generally not covered by the Privacy Act. However, small businesses that are reporting entities for the purposes of AML/CTF Act are required to comply with the Privacy Act when handling personal information collected for the purposes of meeting their obligations under the AML/CTF Act. This includes those small businesses exempt from obligations under the Privacy Act.

If a small business is brought into the Privacy Act because they are reporting entities under the AML/CTF Act and then are later exempted from reporting obligations due to rules issued by AUSTRAC under the AML/CTF Act, the small business is still a reporting entity within the meaning of the Privacy Act.

Therefore, in relation to activities it carried on for the purpose of complying with the AML/CTF Act or AML/CTF Rules, the small business continues to have all the Privacy Act obligations it had before the exemption was granted.

PCI DSS: The Payment Card Industry Data Security Standard (PCI DSS) governs the security of financial card data, such as credit card or debit card information. It applies to any business that stores, processes or transmits such data.

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) is an IT compliance standard for the health care industry. It regulates how medical organizations protect the sensitive information of their patients. It applies to any business that deals with health data.

NIST SP 800-171: The National Institute of Standards and Technology (NIST) Special Publication 800-171 is a set of IT security requirements for businesses that work with federal or state agencies. It ensures that government data is protected from unauthorized access or disclosure.

These are the most used IT compliance standards which includes cybersecurity. There are more that may apply to your business depending on your industry, location and data.

IMPLEMENTING STANDARDS

To follow the regulatory framework for IT compliance and regulatory standards, you need to:

Identify the IT compliance standards that apply to your business. You can do this by researching the laws and regulations of your industry and location, consulting with legal experts or using online resources.

Assess your current level of compliance. You can do this by conducting an IT security audit, using tools or services that measure your compliance status or hiring external auditors.

Implement security measures to meet the compliance requirements. You can do this by adopting security policies and procedures, using secure software and hardware, training your staff on security best practices or outsourcing security tasks to professionals.

Monitor and maintain your compliance status. You can do this by regularly reviewing your security policies and procedures, updating your software and hardware, testing your security systems or reporting your compliance activities.

Following standards can help protect business from security threats, legal penalties and reputational damage. It can also help you improve your customer trust and satisfaction.

IT COMPLIANCE POLICIES

IT compliance policies matter for several reasons:

They help the organization meet its legal and contractual obligations, such as the Sarbanes-Oxley Act (SOX) for financial reporting, the Gramm-Leach-Bliley Act (GLBA) for financial data protection, or the Payment Card Industry Data Security Standard (PCI DSS) for credit card transactions .

They enhance the organization's reputation and trustworthiness among its customers, partners, and regulators, by demonstrating its commitment to data security and privacy.

They reduce the likelihood and impact of cyberattacks, data breaches, and other incidents that could compromise the organization's data and systems, by implementing preventive and corrective measures.

They improve the efficiency and effectiveness of the organization's IT operations, by streamlining processes, reducing errors, and optimizing resources.

CREATING IT COMPLIANCE POLICIES

To create effective IT compliance policies, an organization should follow these steps:

1. **Identify the applicable laws, regulations, and standards** that affect its IT activities, such as SOX, GLBA, PCI DSS, HIPAA, GDPR, ISO 27001, NIST 800-53, etc.
2. **Assess the current state of its IT compliance posture**, by conducting audits, gap analyses, risk assessments, and maturity assessments.
3. **Define the desired state of its IT compliance posture**, by setting goals, objectives, and metrics for each compliance area.
4. **Develop the IT compliance policies** that outline the roles, responsibilities, procedures, controls, and tools for achieving compliance in each area.
5. **Implement the IT compliance policies** across the organization, by communicating them to all stakeholders, providing training and awareness programs, enforcing them through monitoring and reporting mechanisms, and reviewing them periodically for improvement.

RISK MANAGEMENT & MITIGATION

IT compliance and regulatory standards govern how organizations use, protect, and share information and technology. These standards may come from different sources, such as laws, regulations, industry codes, contracts, or ethical principles.

IT compliance and regulatory standards include:

The General Data Protection Regulation (GDPR), which is a European Union law that protects the privacy and rights of individuals in relation to their personal data.

The Payment Card Industry Data Security Standard (PCI DSS), which is a set of security requirements for organizations that process, store, or transmit credit card information.

The ISO/IEC 27000 series, which is a family of international standards for information security management systems.

MANAGING RISK IN IT COMPLIANCE AND REGULATORY STANDARDS?

Managing and mitigating risks in IT compliance and regulatory standards involves a systematic process of identifying, analysing, evaluating, treating, monitoring, and reviewing the risks. Some of the steps involved in this process are:

Establishing a governance framework for IT compliance and regulatory standards. This involves defining the roles, responsibilities, policies, procedures, and controls for ensuring that the organization meets its obligations and objectives in relation to information and technology.

Conducting a risk assessment for IT compliance and regulatory standards. This involves identifying the sources and causes of potential risks, estimating their likelihood and impact, and prioritizing them based on their severity.

Implementing risk treatment strategies for IT compliance and regulatory standards. This involves selecting and applying appropriate measures to avoid, reduce, transfer, or accept the risks. Some examples of risk treatment strategies are:

Implementing technical safeguards such as encryption, firewalls, antivirus software, or backup systems to protect information and technology from unauthorized access or damage.

Implementing administrative safeguards such as training, awareness, policies, procedures, or audits to ensure that staff follow the rules and requirements for information and technology.

Implementing legal safeguards such as contracts, agreements, or insurance to transfer or share the responsibility or liability for information and technology with other parties.

Monitoring and reviewing the effectiveness of risk management activities for IT compliance and regulatory standards. This involves measuring and reporting on the performance and outcomes of the risk management process, identifying any gaps or weaknesses, and adjusting or improvements as needed.

ETHICAL CONSIDERATIONS IN EMERGING TECHNOLOGIES

Emerging technologies such as artificial intelligence, cloud computing, big data, and cybersecurity have enormous potential to transform various domains of human activity.

ETHICAL DILEMMAS AND PRINCIPLES IN DATA RETENTION AND DELETION

Data retention and deletion involve ethical dilemmas that require careful balancing of competing values and interests. Some of the common ethical dilemmas are:

How long should data be retained? Retaining data for too long can increase the risk of data breaches, misuse, or abuse, while deleting data too soon can limit the potential benefits of data analysis or reuse.

How should data be deleted? Deleting data securely and completely can prevent unauthorized access or recovery, while retaining some traces of data can facilitate auditing or verification.

Who should decide on data retention and deletion? Data controllers and processors may have different incentives or preferences for data retention and deletion than data subjects or stakeholders, who may have different levels of awareness or consent.

What are the trade-offs between data retention and deletion? Data retention and deletion may involve trade-offs between efficiency and effectiveness, innovation and protection, individual and collective interests, or short-term and long-term goals.

ADDRESSING ETHICAL DILEMMAS

To address these ethical dilemmas, some ethical principles can guide the decision-making process. Some of the widely accepted ethical principles are:

Respect for human dignity. Data retention and deletion should respect the inherent worth and dignity of every human being, regardless of their characteristics or circumstances.

Fairness and justice. Data retention and deletion should ensure equal treatment and opportunity for all data subjects and stakeholders, without discrimination or bias.

Beneficence and non-maleficence. Data retention and deletion should maximize the benefits and minimize the harms for data subjects, stakeholders, and society at large.

Autonomy and consent. Data retention and deletion should respect the choices and preferences of data subjects, who should be informed and empowered to exercise their rights over their data.

Transparency and accountability. Data retention and deletion should be clear, consistent, and explainable to data subjects, stakeholders, and regulators, who should be able to monitor and evaluate their compliance and outcomes.

CASE STUDY: SUSPICIOUS BEHAVIOUR LINKED TO LARGE-SCALE IDENTITY FRAUD OPERATION

A bank teller submitted a report to AUSTRAC* detailing suspicious banking transactions. This report assisted authorities investigating a syndicate allegedly involved in large-scale identity fraud.

The report described over-the-counter transactions in which two people were involved – the account owner and the main suspect. The suspect was not connected to the account but controlled the transactions and would not allow the account owner to speak.

The pair transferred approximately AUD541,000 from a bank account in Jordan to an Australian account. They then withdrew approximately AUD394,000 from the Australian account in the form of a bank cheque. When the teller requested the account owner undertake this withdrawal, the suspect became agitated and aggressive. The pair also transferred approximately AUD147,000 from the Australian account to a third-party account.

These transactions left the account owner with an account balance of just AUD1,000. AUSTRAC information allowed authorities to link the suspect in this matter with the movement of funds to Jordan, the United Arab Emirates and Peru. Authorities continued their investigations and ultimately commenced proceeds of crime action against the suspect and members of the syndicate, and restrained approximately AUD1.6 million in assets, including real estate and cash.

***AUSTRAC** or the *Australian Transaction Reports and Analysis Centre* is an Australian government financial intelligence agency that monitors financial transactions to detect money laundering, organised crime, tax evasion, welfare fraud and terrorism.

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.

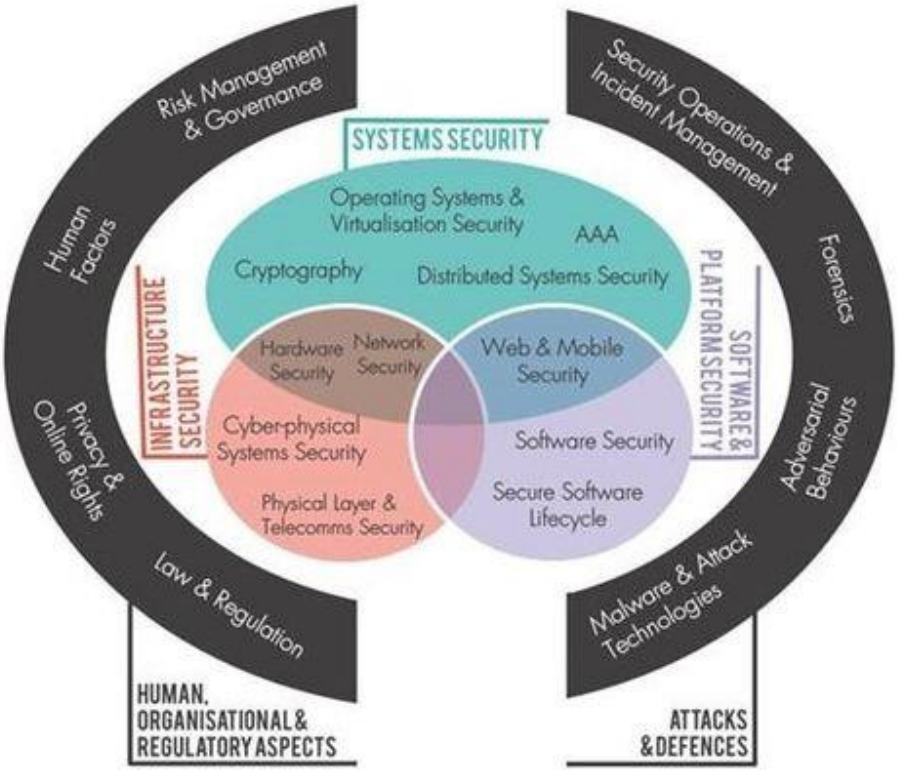
Data breach notification and communication: How to prepare for and respond to data breaches, and how to communicate effectively with stakeholders, regulators, and the public about the incident and its consequences.

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.



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

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.

MODULE 3:
DATA BREACH PREPARATION & RESPONSE

From 25 May 2018 Australian businesses of any size may need to comply with the GDPR if they have an establishment in the European Union (EU), if they offer goods and services in the EU, or if they monitor the behaviours of individuals in the EU.

The GDPR includes requirements that resemble those in the Privacy Act 1988, and additional measures that similarly aim to foster transparent information handling practices and business accountability around data handling.

In the lead-up to the commencement of the GDPR requirements, businesses should confirm whether they are covered by the GDPR, and if so, take steps to implement any necessary changes to ensure compliance.

3.1 PART 1 (OAIC)

Data breaches & the Australian Privacy Act

Key points:

- A data breach is an unauthorised access or disclosure of personal information, or loss of personal information.
- Data breaches can have serious consequences, so it is important that entities have robust systems and procedures in place to identify and respond effectively.
- Entities that are regulated by the Privacy Act should be familiar with the requirements of the NDB scheme, which are an extension of their information governance and security obligations.
- A data breach incident may also trigger reporting obligations outside of the Privacy Act.

WHAT IS A DATA BREACH?

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure or is lost.

Personal information is information about an identified individual, or an individual who is reasonably identifiable. Entities should be aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result.

A data breach may be the result of malicious action (by an external or insider party), human error, or a failure in information handling or associated security systems.

Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information.
- unauthorised access to personal information by an employee.
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person.
- disclosure of an individual's personal information to a scammer, because of inadequate identity verification procedures.

CONFIDENTIALITY BREACH

Technically, confidentiality is breached every time some who does not need to know, comes to know something. It is not just when the consequences make themselves felt. Breaches of this kind can occur in writing, by oral transmission or by electronic means including eavesdropping.

AVAILABILITY BREACH

A breach of availability can occur through Denial-of-Service attacks where the web server is deluged with requests, or when millions of spam emails overwhelm servers, or a virus spread on a network.

The latter point is a rather formal argument, based on the literal meaning of the word 'breach'. While it is normal to use the term for incidents affecting confidentiality and leading to unwanted disclosure of information, *temporary unavailability of systems or services is not normally defined as a breach*. People prefer to call this an 'incident' (based on terms used in the ITIL framework).

INTEGRITY BREACH

Whenever the integrity of information or its means of storage are violated. It could be through transmission errors, by intentional manipulation, by unintentional handling errors or by the corruption of file content or structure due to electrical, magnetic or other failures.

CONSEQUENCES OF A DATA BREACH

Data breaches can cause harm in multiple ways.

Individuals whose personal information is involved may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.

Examples of such harm include:

- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- family violence

- physical harm or intimidation
- extortion

A data breach can also negatively impact an entity's reputation for privacy protection, and as a result undercut an entity's commercial interests. As shown in the OAIC's long-running national community attitudes to privacy survey, privacy protection contributes to an individual's trust in an entity. 2 If an entity is perceived to be handling personal information contrary to community expectations, individuals may seek out alternative products and services.

An entity can reduce the reputational impact of a data breach by effectively minimising the risk of harm to affected individuals, and by demonstrating accountability in their data breach response. This involves being transparent when a data breach, which is likely to cause serious harm to affected individuals, occurs. Transparency enables individuals to take steps to reduce their risk of harm. It also demonstrates that an entity takes their responsibility to protect personal information seriously, which is integral to building and maintaining trust in an entity's personal information handling capability.

THE AUSTRALIAN PRIVACY PRINCIPLES

The Privacy Act contains 13 Australian Privacy Principles (APPs) listed below that set out entities' obligations for the management of personal information. The APPs are *principles*-based and technologically *neutral*; they outline principles for how personal information is handled and these may be applied across different technologies and uses of personal information over time.

1. APP 1 — Open and transparent management of personal information
2. APP 2 — Anonymity and pseudonymity
3. APP 3 — Collection of solicited personal information.
4. APP 4 — Dealing with unsolicited personal information.
5. APP 5 — Notification of the collection of personal information.
6. APP 6 — Use or disclosure of personal information.
7. APP 7 — Direct marketing.
8. APP 8 — Cross-border disclosure of personal information.
9. APP 9 — Adoption, use or disclosure of government related identifiers.
10. APP 10 — Quality of personal information.
11. APP 11 — Security of personal information.
12. APP 12 — Access to personal information.
13. APP 13 — Correction of personal information

Compliance with the APPs will reduce the risk of a data breach occurring because they ensure that privacy risks are either reduced or removed during the process of personal information handling, including collection, storage, use, disclosure, and destruction of personal information. For example, APP 3 restricts the collection of personal information. APPs 4.3 and 11.2 outline requirements to destroy or de-identify information if it is unsolicited or no longer needed by the entity.

Compliance with these requirements reduces the amount of data that may be exposed because of a breach.

Compliance with the requirement to secure personal information in APP 11 is key to minimising the risk of a data breach.3 APP 11 requires entities to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. The type of steps that are reasonable to protect information will depend on the circumstances of the entity and the risks associated with personal information handled by the entity.

In addition, APP 1 requires entities to take reasonable steps to establish and maintain practices, procedures, and systems to ensure compliance with the APPs.5

THE NOTIFIABLE DATA BREACHES (NDB) SCHEME

This topic was discussed in some detail in Module 2 – mentioned again here for full disclosure.

The NDB scheme in Part IIIC of the Privacy Act requires entities to notify affected individuals and the Commissioner of certain data breaches.

The NDB scheme requires entities to notify individuals and the Commissioner about 'eligible data breaches'. Such a breach occurs when the following criteria are met:

- There is unauthorised access to, or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

Entities must also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

OTHER OBLIGATIONS

Entities may have other obligations outside of those contained in the Privacy Act that relate to personal information protection and responding to a data breach. These may include other data protection obligations under state-based or international data protection laws. Australian businesses may need to comply with the European Union's (EU's) General Data Protection Regulation (GDPR) if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU.

For data breaches affecting certain categories of information, other mandatory or voluntary reporting schemes may exist. For example, entities might consider reporting certain breaches to:

- the entity's financial services provider
- police or law enforcement bodies
- the Australian Securities & Investments Commission (ASIC)
- the Australian Prudential Regulation Authority (APRA)
- the Australian Taxation Office (ATO)
- the Australian Transaction Reports and Analysis Centre (AUSTRAC)
- the Australian Cyber Security Centre (ACSC)
- the Australian Digital Health Agency (ADHA)
- the Department of Health
- State or Territory Privacy and Information Commissioners
- professional associations and regulatory bodies
- insurance providers.

Some entities may have additional obligations to report to the Commissioner under the National Cancer Screening Register Act 2016 (NCSR Act) or have different reporting obligations under the My Health Records Act 2012 (My Health Records Act).

Under the NCSR Act, current and former contracted service providers of the National Cancer Screening Register must notify the Secretary of the Department of Health (the Secretary) and the Commissioner if they become aware of unauthorised recording, use or disclosure of personal information included in the Register. The Secretary must also notify the Commissioner of certain data breaches, including potential breaches, in connection with the National Cancer Screening Register. The Secretary must also consult the Information Commissioner about notifying individuals who may be affected. Separately, entities with NCSR Act obligations must consider whether the incident also requires notification under the NDB scheme, as the two schemes operate concurrently. Where the test for both schemes have been met, the entity may make a joint notification to the Commissioner.

WHY DO YOU NEED A DATA BREACH RESPONSE PLAN?

All entities should have a data breach response plan. Your actions in the first 24 hours after discovering a data breach are often crucial to the success of your response. A quick response can substantially decrease the impact on the affected individuals.

High profile data breaches, both in Australia and overseas, highlight the significant disruption caused by a breach of personal information. Research suggests that the cost to an organisation for a data breach can be significant. Implementing a data breach response plan can assist in mitigating these costs.

Having a data breach response plan is part of establishing robust and effective privacy procedures. And having clear roles and responsibilities is part of good privacy governance. A data breach response plan can also help you:

- Meet your obligations under the Privacy Act — an entity must take reasonable steps to protect the personal information that it holds; those reasonable steps may include having a data response plan.
- Protect an important business asset — the personal information of your customers and clients as well as your reputation.
- Deal with adverse media or stakeholder attention from a breach or suspected breach
- Instil public confidence in your capacity to protect personal information by properly responding to the breach.

3.2 PART 2 (OAIC)

PREPARING A DATA BREACH RESPONSE PLAN

Key points

- A quick response to a data breach, based on an up-to-date data breach response plan, is critical to effectively managing a breach
- your data breach response plan should outline your entity's strategy for containing, assessing and managing the incident from start to finish
- this part will provide practical guidance to help you develop a comprehensive and effective data breach response plan.

WHY DO YOU NEED A DATA BREACH RESPONSE PLAN?

All entities should have a data breach response plan. A data breach response plan enables an entity to respond quickly to a data breach. By responding quickly, an entity can substantially decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result.

A data breach response plan can help you:

MEET YOUR OBLIGATIONS UNDER THE PRIVACY ACT

Under the Privacy Act, an entity must take reasonable steps to protect the personal information that it holds. A data breach response plan focussed on reducing the impact of a breach can be one of these reasonable steps.

LIMIT THE CONSEQUENCES OF A DATA BREACH

A quick response can reduce the likelihood of affected individuals suffering harm. It can also lessen financial or reputational damage to the entity that experienced the breach.

PRESERVE AND BUILD PUBLIC TRUST

An effective data breach response can support consumer and public confidence in an entity's respect for individual privacy, and the entity's ability to manage personal information in accordance with community expectations.

WHAT IS A DATA BREACH RESPONSE PLAN?

A data breach response plan is a framework that sets out the roles and responsibilities involved in managing a data breach. It also describes the steps an entity will take if a data breach occurs.

Your data breach response plan should be in writing to ensure that your staff clearly understand what needs to happen in the event of a data breach. It is also

important for staff to be aware of where they can access the data breach response plan on short notice.

You will need to regularly review and test your plan to make sure it is up to date and that your staff know what actions they are expected to take. You can test your plan by, for example, responding to a hypothetical data breach and reviewing how your response could be made more effective.

How regularly you test your plan will depend on your circumstances, including the size of your entity, the nature of your operations, the possible adverse consequences to an individual if a breach occurs, and the amount and sensitivity of the information you hold. It may be appropriate in some instances that a review of the plan coincides with the introduction of new products, services, system enhancements, or such other events which involve the handling of personal information.

WHAT SHOULD THE PLAN COVER?

The more comprehensive your data breach response plan is, the better prepared your entity will be to effectively reduce the risks and potential damage that can result.

Information that your plan should cover includes:

A CLEAR EXPLANATION OF WHAT CONSTITUTES A DATA BREACH

This will assist your staff in identifying a data breach should one occur (see What is a data breach? section above). You may also want to include potential examples of a data breach which are tailored to reflect your business activities.

A STRATEGY FOR CONTAINING, ASSESSING AND MANAGING DATA BREACHES

This strategy should include the actions your staff, and your response team, will take in the event of a data breach or a suspected data breach. Consider:

- potential strategies for containing and remediating data breaches
- ensuring you have the capability to implement those strategies as a matter of priority (e.g., having staff available to deal with the breach – see Response team membership section below). Your plan should reflect the capabilities of your staff to adequately assess data breaches and their impact, especially when breaches are not escalated to a response team.
- legislative or contractual requirements (such as the requirements of the NDB scheme if they apply to your entity)
- a clear and immediate communications strategy that allows for the prompt notification of affected individuals and other relevant entities. In particular:
  - who is responsible for implementing the communications strategy.

- determining when affected individuals must be notified (refer to Identifying eligible data breaches for further information about mandatory data breach notification requirements under the NDB scheme)
- how affected individuals will be contacted and managed.
- criteria for determining which external stakeholders should be contacted (for example, law enforcement and cyber security agencies, regulators such as the OAIC, and the media)
- who is responsible for liaising with external stakeholders.

THE ROLES AND RESPONSIBILITIES OF STAFF

Your plan should outline the responsibilities of staff members when there is a data breach, or a suspected data breach. Consider:

- who staff should inform immediately if they suspect a data breach
- the circumstances in which a line manager can handle a data breach, and when a data breach must be escalated to the response team. The following factors may determine when a data breach is escalated to the response team:
  - the number of people affected by the breach or suspected breach
  - whether there is a risk of serious harm to affected individuals now or in the future
  - whether the data breach or suspected data breach may indicate a systemic problem with your entity's practices or procedures
  - other issues relevant to your circumstances, such as the value of the data to you or issues of reputational risk.
- who is responsible for deciding whether the breach should be escalated to the response team. One option is for each senior manager to hold responsibility for deciding when to escalate a data breach to the response team. Another option is to have a dedicated role, such as the privacy contact officer.

DOCUMENTATION

Your plan should consider how your entity will record data breach incidents, including those that are not escalated to the response team. This will assist you in ensuring you have documentation of how your entity has met regulatory requirements.

RESPONSE TEAM MEMBERSHIP

Your data breach response team is responsible for carrying out the actions that can reduce the potential impact of a data breach. It is important that the staff that make up the response team, as well as their roles and responsibilities, are clearly established and documented before a data breach occurs. Otherwise, your response to the breach may be unnecessarily delayed.

Who is in your data breach response team will depend on the circumstances of your entity and the nature of the breach. Different skill sets and staff may be needed to respond to one breach compared to another. In some cases, you may need to include external experts in your team, for example legal advice, data forensics, or media management. You should identify the types of expertise you may need and ensure that this expertise will be available on short notice. You might consider creating a core team and adding other members as they are required.

You should keep a current list of response team members and clearly detail their roles, responsibilities, and authorities, as well as their contact details (possibly attached to the data breach response plan). You should ensure these contact details remain updated, particularly in the event of organisational changes. Each role on the response team should have a second point of contact in case the first person is not available.

TYPICAL DATA BREACH RESPONSE TEAM ROLES AND SKILLS

Your data breach response team may include:

- **Team leader** — who is responsible for leading the response team and reporting to senior management.
- **Project manager** — to coordinate the team and provide support to its members.
- **Senior member of staff** with overall accountability for privacy and/or key privacy officer — to bring privacy expertise to the team.
- **Legal support** — to identify legal obligations and provide advice.
- **Risk management support** — to assess the risks from the breach.
- **Information and Communication Technology (ICT) support/forensics support** — this role can help establish the cause and impact of a data breach that involved ICT systems.
- **Information and records management expertise** – to assist in reviewing security and monitoring controls related to the breach (for example, access, authentication, encryption, audit logs) and to provide advice on recording the response to the data breach.
- **Human resources (HR) support** — if the breach was due to the actions of a staff member.
- **Media/communications expertise** — to assist in communicating with affected individuals and dealing with the media and external stakeholders.

If you hold an insurance policy for data breaches, that insurer may have a pre-established panel of external service providers in many of the roles listed above. You may want to consult with your insurer as to the identity of that panel so they can be included in any response team. Alternatively, the insurer may have a hotline available to assist in the event of a data breach, and that could be noted in the response plan.

Which individuals carry out the roles outlined in your response team will depend on your circumstances. For example, in smaller entities it may not be necessary to include steps related to escalating the data breach to the response team, as this may be an automatic process. Depending on the size of your entity or the size of the breach, a single person may perform multiple roles. In smaller entities the owner/principal of the entity could potentially be the person who needs to respond to and act on that breach.

It is important that the response team has the authority to take the steps outlined in the response plan without needing to seek permission, as this will enable a faster response to the breach. The role of team leader should be carefully considered, as they should have sufficient ability and authority to effectively manage the various sections within the entity whose input is required and to report to senior management. It may be your senior member of staff with overall accountability for privacy, a senior lawyer (if you have an internal legal function) or another senior manager. If the breach is serious, it may be a senior executive.

ACTIONS THE RESPONSE TEAM SHOULD TAKE

A data breach response plan should also set out (or refer to) the actions the response team is expected to take when a data breach is discovered. Part 3 of this Guide provides a general framework for responding to a data breach, and Part 4 outlines the requirements of the NDB scheme, which may apply to your entity if they have personal information security obligations under the Privacy Act.

The response team will need to consider what information needs to be reported to senior management and at what point. This reporting structure should form part of the plan.

The data breach response plan should outline how staff will record how they have become aware of a data breach and the actions taken in response. Keeping records on data breaches and suspected breaches will help you manage the breach and identify risks that could make a breach more likely to occur.

OTHER CONSIDERATIONS

In developing your plan, you could also consider:

- when and how the response team could practice a response to a breach to test procedures and refine them
- whether your plan for dealing with personal information data breaches could link into or be incorporated into already existing processes, such as a disaster recovery plan, a cyber security/ICT incident response plan, a crisis management plan or an existing data breach response plan involving other types of information (e.g., commercially confidential information)
- whether senior management should be directly involved in the planning for dealing with data breaches and in responding to serious data breaches

- any reporting obligations under laws other than the Privacy Act or to other entities
- whether you have an insurance policy for data breaches that includes steps you must follow.

DATA BREACH RESPONSE PLAN QUICKCHECKLIST

Use this list to check whether your response plan addresses relevant issues.

Information to be included	Yes/No	Comments
What a data breach is and how staff can identify one		
Clear escalation procedures and reporting lines for suspected data breaches		
Members of the data breach response team, including roles, reporting lines and responsibilities		
Details of any external expertise that should be engaged circumstances		
How the plan will apply to various types of data breaches and varying risk profiles with consideration of possible remedial		
An approach for conducting assessments		
Processes that outline when and how individuals are notified		
Circumstances in which law enforcement, regulators (such as the OAIC), or other entities may need to be contacted		
Processes for responding to incidents that involve another entity		
A record-keeping policy to ensure that breaches are		
Requirements under agreements with third parties such as insurance policies or service agreements		
A strategy identifying and addressing any weaknesses in data handling that contributed to the breach		
Regular reviewing and testing of the plan		
A system for a post-breach review and assessment of the data breach response and the effectiveness of the data breach response		

3.3 PART 3 (OAIC)

RESPONDING TO DATA BREACHES — FOUR KEY STEPS

Key points

- Each data breach response needs to be tailored to the circumstances of the incident.
- In general, a data breach response should follow four key steps: contain, assess, notify and review.

OVERVIEW

Data breaches can be caused or exacerbated by a variety of factors, involve different types of personal information, and give rise to a range of actual or potential harms to individuals and entities.

As such, there is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

Generally, the actions taken following a data breach should follow four key steps:

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

Step 3: Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.

Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

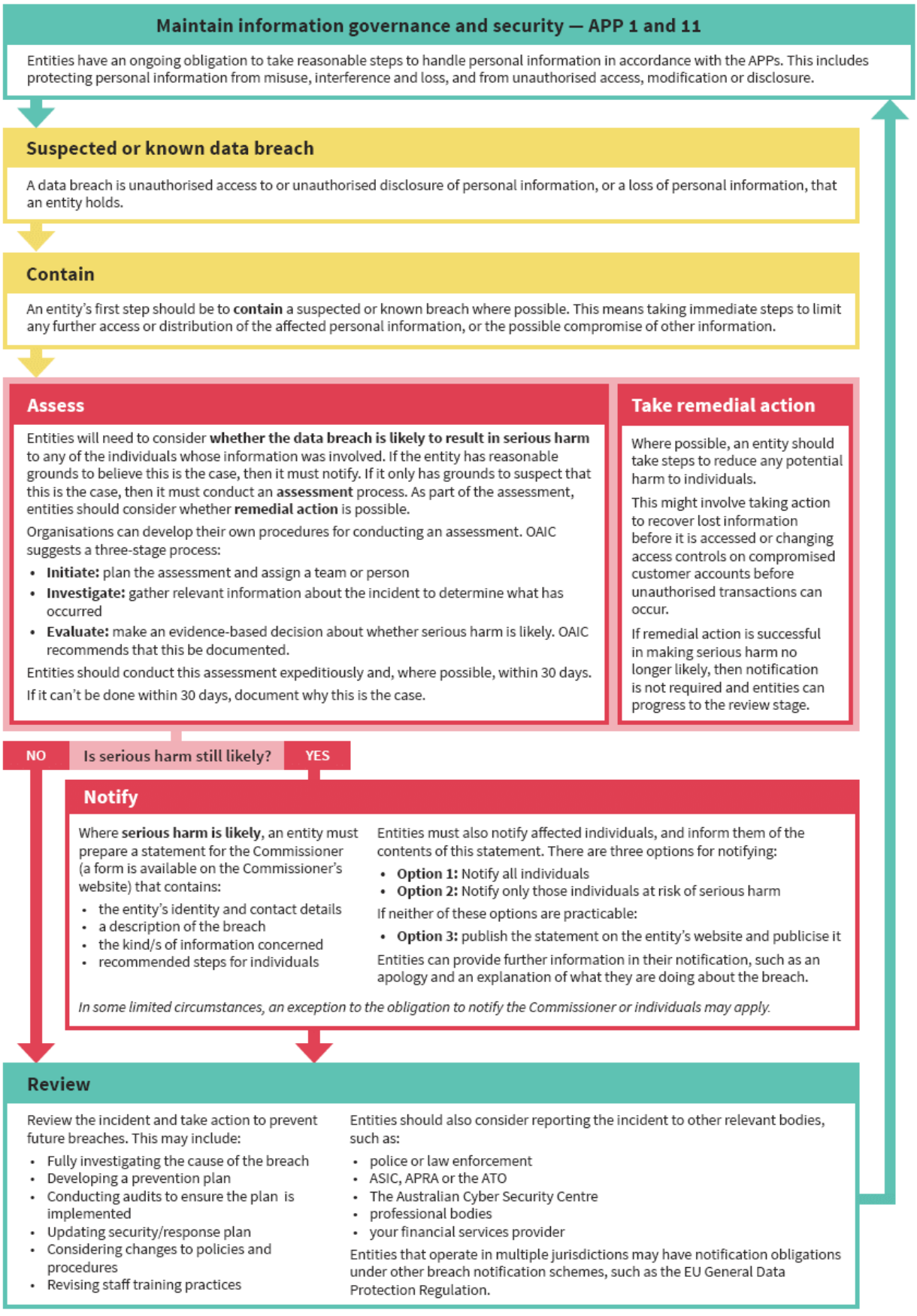
At any time, entities should take remedial action, where possible, to limit the impact of the breach on affected individuals. If remedial action is successful in preventing a likely risk of serious harm to individuals, the NDB scheme notification obligations may not apply.

In general, entities should:

- take each data breach or suspected data breach seriously and move immediately to contain, assess and remediate the incident. Breaches that may initially seem immaterial may be significant when their full implications are assessed

- undertake steps 1 (Contain), 2 (Assess), and 3 (Notify) either simultaneously or in quick succession. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs
- determine how to respond on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, an entity may take additional steps that are specific to the nature of the breach.

The following diagram summarises the data breach response process. The parts of this process that are required by the NDB scheme are coloured red. The NDB scheme is explained in detail in Part 4 of this guide.


Maintain information governance and security — APP 1 and 11
Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
Suspected or known data breach
A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.
Contain
An entity's first step should be to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.
Assess
Entities will need to consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an assessment process. As part of the assessment, entities should consider whether remedial action is possible.
Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:
Initiate: plan the assessment and assign a team or person
Investigate: gather relevant information about the incident to determine what has occurred
Evaluate: make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.
Entities should conduct this assessment expeditiously and, where possible, within 30 days.
If it can't be done within 30 days, document why this is the case.
Take remedial action
Where possible, an entity should take steps to reduce any potential harm to individuals.
This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.
If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.
NO
Is serious harm still likely?
YES
Notify
Where serious harm is likely, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:
the entity's identity and contact details
a description of the breach
the kind/s of information concerned
recommended steps for individuals
Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:
Option 1: Notify all individuals
Option 2: Notify only those individuals at risk of serious harm
If neither of these options are practicable:
Option 3: publish the statement on the entity's website and publicise it
Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.
In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.
Review
Review the incident and take action to prevent future breaches. This may include:
Fully investigating the cause of the breach
Developing a prevention plan
Conducting audits to ensure the plan is implemented
Updating security/response plan
Considering changes to policies and procedures
Revising staff training practices
Entities should also consider reporting the incident to other relevant bodies, such as:
police or law enforcement
ASIC, APRA or the ATO
The Australian Cyber Security Centre
professional bodies
your financial services provider
Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

STEP 1: CONTAIN

Once an entity has discovered or suspects that a data breach has occurred, it should immediately take action to limit the breach.

For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security.

Addressing the following questions may help you identify strategies to contain a data breach:

- How did the data breach occur?
- Is the personal information still being shared, disclosed, or lost without authorisation?
- Who has access to the personal information?
- What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

At this point, an entity may suspect an eligible data breach under the NDB scheme has occurred, which would trigger assessment obligations. Or the entity may believe the data breach is an eligible data breach, which requires them to notify individuals as soon as practicable.

During this preliminary stage, be careful not to destroy evidence that may be valuable in identifying the cause of the breach, or that would enable the entity to address all risks posed to affected individuals or the entity.

STEP 2: ASSESS

An assessment of the data breach can help an entity understand the risks posed by a data breach and how these risks can be addressed. It should be conducted as expeditiously as possible.

Gather and evaluate as much information about the data breach as possible. By creating a complete picture of the data breach, an entity can ensure they understand the risk of harm to affected individuals and identify and take all appropriate steps to limit the impact of a data breach.

This assessment should also assist entities in deciding whether affected individuals must be notified.

In your assessment of a data breach, consider:

- the type or types of personal information involved in the data breach
- the circumstances of the data breach, including its cause and extent
- the nature of the harm to affected individuals, and if this harm can be removed through remedial action.

All entities should consider whether remedial action can be taken to reduce any potential harm to individuals. This might also take place during Step 1: Contain, such as by recovering lost information before it is accessed.

Entities subject to the NDB scheme are required to assess 'suspected' eligible data breaches and take reasonable steps to complete this assessment within 30 days (see Assessing a suspected data breach). Criteria for assessing a data breach, including the risk of harm and remedial action, is explored in Identifying eligible data breaches.

STEP 3: NOTIFY

Notification can be an important mitigation strategy that has the potential to benefit both the entity and the individuals affected by a data breach. The challenge is to determine when notification is appropriate. Sometimes, notifying individuals can cause undue stress or harm. For example, notifying individuals about a data breach that poses very little or no risk of harm can cause unnecessary anxiety. It can also de-sensitise individuals so that they don't take a notification seriously, even when there is a real risk of serious harm. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

Consider:

- the obligations of the entity under the NDB scheme. Entities are required to notify individuals and the Commissioner about data breaches that are likely to result in serious harm. Part 4 of this guide provides further detail about the NDB scheme's requirements
- other circumstances in which individuals should be notified. For example, your entity may not have obligations under the NDB scheme, but have processes in place to notify affected individuals in certain circumstances
- how notification should occur, including:
    - what information is provided in the notification
    - how the notification will be provided to individuals
    - who is responsible for notifying individuals and creating the notification?
- who else other than affected individuals (and the Commissioner if the notification obligations of the NDB scheme apply) should be notified
- where a law enforcement agency is investigating the breach, it may be appropriate to consult the investigating agency before making details of the breach public
- whether the incident triggers reporting obligations to other entities.

Effective data breach response is about reducing or removing harm to affected individuals, while protecting the interests of your organisation or agency. Notification has the practical benefit of providing individuals with the opportunity

to take steps to protect their personal information following a data breach, such as by changing account passwords or being alert to possible scams resulting from the breach. It is important that staff can engage with individuals who have been affected by a data breach with sensitivity and compassion, in order not to exacerbate or cause further harm. Notification can also help build trust in an entity, by demonstrating that privacy protection is taken seriously.

STEP 4: REVIEW

Once steps 1 to 3 have been completed, an entity should review and learn from the data breach incident to improve its personal information handling practices.

This might involve:

- a security review including a root cause analysis of the data breach
- a prevention plan to prevent similar incidents in future
- audits to ensure the prevention plan is implemented
- a review of policies and procedures and changes to reflect the lessons learned from the review
- changes to employee selection and training practices
- a review of service delivery partners that were involved in the breach.

In reviewing information management and data breach response, an entity can refer to the OAIC's

GUIDE TO SECURING PERSONAL INFORMATION

When reviewing a data breach incident, it is important to use the lessons learned to strengthen the entity's personal information security and handling practices, and to reduce the chance of reoccurrence. A data breach should be considered alongside any similar breaches that have occurred in the past, which could indicate a systemic issue with policies or procedures.

If any updates are made following a review, staff should be trained in any changes to relevant policies and procedures to ensure a quick response to a data breach.

3.4 PART 4: (OAIC)

NOTIFIABLE DATA BREACH (NDB) SCHEME

The Privacy Act requires certain entities to notify individuals and the Commissioner about data breaches that are likely to cause serious harm.

The requirements of the NDB scheme are contained in Part IIIC of the Privacy Act and apply to breaches that occur on or after 22 February 2018.

This part of the guide covers the following topics:

- Entities covered by the NDB scheme.
- Data breaches involving more than one entity.
- Identifying eligible data breaches
- Exceptions to the notification obligation
- Assessing a suspected data breach
- Notifying individuals about an eligible data breach
- What to include in an eligible data breach statement
- The Australian Information Commissioner's role in the NDB scheme.

ENTITIES COVERED BY THE NDB SCHEME

Key points:

- Entities that have existing obligations under the Privacy Act to secure personal information must comply with the NDB scheme.
- This includes Australian Government agencies, businesses and not-for profit organisations that have an annual turnover of more than AU$3 million, private sector health service providers, credit reporting bodies, credit providers, entities that trade in personal information and tax file number (TFN) recipients.
- Entities that have Privacy Act security obligations in relation to types of information only (for example, small businesses that are required to secure tax file number information) do not need to notify about data breaches that affect other types of information outside the scope of their obligations under the Privacy Act.

AUSTRALIAN PRIVACY PRINCIPLES ENTITIES

The NDB scheme applies to entities that have an obligation under APP 11 of the Privacy Act to protect the personal information they hold (s 26WE(1)(a)).11 Collectively known as ‘APP entities’, these include Australian Government agencies and private sector and not-for-profit organisations with an annual turnover of more than $3 million. The definition of APP entity generally does not include small business operators, registered political parties, state or territory authorities, or a prescribed instrumentality of a state (s 6C). However, some businesses of any size are APP entities, including businesses that trade in personal

information12 and organisations that provide a health service to, and hold health information about, individuals (see Is my organisation a health service provider?).

For more information about APP entities, see Chapter B of the Australian Privacy Principal Guidelines (APP Guidelines).

Exempt acts and practices, including employee records.

The NDB scheme only applies to entities and personal information holdings that are already subject to security requirements under the Privacy Act. This means that acts and practices of APP entities that are exempt from the Privacy Act will also be exempt from the NDB scheme.

For example, in some circumstances, private sector employers do not have to comply with the APPs in relation to employee records associated with current and former employment relationships (s 7B(3)). If an exempt employee record is subject to unauthorised access, disclosure or loss, the private sector employer does not have to assess the breach or notify individuals and the Commissioner. This exemption does not apply to TFN information that is contained within an employee record. However, given community expectations around the handling of their personal information, it is recommended that employers notify affected individuals where a breach of an employee record is likely to result in serious harm. Doing so will enable affected individuals to take protective action against any potential harms, as well as illustrating to employees that the security of their records is taken seriously.

Further information about acts and practices that are exempt from the APPs and, by extension, the NDB scheme can be found in Privacy business resource 13: Application of the Australian Privacy Principles to the private sector.

SMALL BUSINESS OPERATORS

A small business operator (SBO) is an individual (including a sole trader), body corporate, partnership, unincorporated association, or trust that has not had an annual turnover of more than $3 million in any financial year since 2001 (s 6D).

Generally, SBOs (Small Business Operator) do not have obligations under the APPs unless an exception applies (s 6D(4)).

In certain circumstances an SBO must comply with the APPs, and therefore with the NDB scheme. That will be the case where the SBO:

- holds health information and provides a health service
- is related to an APP entity
- trades in personal information. That is, the SBO discloses personal information about individuals to anyone else for a benefit, service or advantage; or provides a benefit, service or advantage through the

collection of personal information about another individual from anyone else
- are a credit reporting bodies
- is an employee association registered under the Fair Work (Registered Organisations) Act 2009
- has 'opted-in' to APP coverage under s 6EA of the Privacy Act.

If an SBO carries on certain activities it must comply with the APPs, and therefore must comply with the NDB scheme, but only in relation to personal information held by the entity for the purpose of, or in connection with, those activities. Those activities include:

- providing services to the Commonwealth under a contract
- operating a residential tenancy data base
- reporting under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006
- conducting a protected action ballot
- information retained under the mandatory data retention scheme, as per Part 5-1A of the Telecommunications (Interception and Access) Act 1979.

More information about how to determine whether a business or organisation is an APP entity or subject to the APPs for some of its activities is available at Privacy business resource 10: Does my small business need to comply with the Privacy Act?.16

CREDIT REPORTING BODIES

A credit reporting body (CRB) is a business or undertaking that involves collecting, holding, using, or disclosing personal information about individuals for the purpose of providing an entity with information about the credit worthiness of an individual (s 6P). Credit reporting information is defined as credit information or CRB derived information about an individual (s 6(1)).

CRBs (Credit Reporting Body) have obligations under the NDB scheme in relation to their handling of credit reporting information (s 26WE(1)(b)), and in relation to their handling of any other personal information for which they have obligations under APP 11.

CREDIT PROVIDERS

The NDB scheme applies to all credit providers whether they are APP entities. The section of the Privacy Act under which a credit provider is required to comply with the scheme will depend on what kind of information is involved in the data breach.

If it is 'credit eligibility information' (defined in s 6(1)) the NDB scheme will apply because of the security requirement in s 21S (1) in relation to that information.

If the credit provider is also an APP entity the NDB scheme applies in relation to other personal information because of the security requirement in APP 11.

The organisations that are credit providers for the purposes of the Privacy Act (s 6G) are:

- a bank
- an organisation or small business operator if a substantial part of its business is the provision of credit, such as a building society, finance company or a credit union
- a retailer that issues credit cards in connection with the sale of goods or services
- an organisation or SBO that supplies goods and services where payment is deferred for seven days or more, such as telecommunications carriers, and energy and water utilities
- certain organisations or SBOs that provide credit in connection with the hiring, leasing, or renting of goods.

An organisation or SBO that acquires the right of a credit provider in relation to the repayment of an amount of credit is also considered a credit provider, but only in relation to that credit (s 6K).

For more information about categories of credit-related personal information, see Privacy business resource 3: Credit reporting – what has changed.

TFN RECIPIENTS

The NDB scheme applies to TFN recipients18 in relation to their handling of TFN information (s 26WE(1)(d)). A TFN recipient is any person who is in possession or control of a record that contains TFN information (s 11). TFN information is information that connects a TFN with the identity of a particular individual (s 6).

A TFN recipient may also be an APP entity or credit provider. In certain circumstances, entities that are not otherwise covered by the Privacy Act, such as state and local government bodies, may also be authorised to receive TFN information and will be considered TFN recipients.

The NDB scheme applies to TFN recipients to the extent that TFN information is involved in a data breach. If TFN information is not involved, a TFN recipient would only need to comply with the NDB scheme for breaches of other types of information if they are also a credit provider or APP entity.

More information about TFN recipients is available in Privacy business resource 12: The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information.19

Overseas activities

ENTITIES WITH AN 'AUSTRALIAN LINK'

The NDB scheme generally extends to the overseas activities of an Australian Government agency (s 5B (1)). It also applies to organisations (including small businesses covered by the Act, outlined above) that have an 'Australian link' (s 5B (2)).

An organisation has an Australian link either because it is, in summary, incorporated or formed in Australia (see s 5B(1A) for more detail), or where:

- it carries on business in Australia or an external Territory, and
- it collected or held personal information in Australia or an external Australian Territory, either before or at the time of the act or practice (s 5B (3)).

Further information about entities that are taken to have an Australian link is available in Chapter B of the APP Guidelines.

Disclosing personal information overseas

If an APP entity discloses personal information to an overseas recipient, in line with the requirements of APP 8.1, then the APP entity is deemed to 'hold' the information for the purposes of the NDB scheme (s 26WC (1)). APP 8.1 says that an APP entity that discloses personal information to an overseas recipient is required to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. This means that if the personal information held by the overseas recipient is subject to loss, unauthorised access, or disclosure, the APP entity is still responsible for assessing whether it is an eligible data breach under the Privacy Act, and if it is, for notifying individuals at risk of serious harm and providing a statement to the Commissioner.

There are exceptions to the requirement in APP 8.1 to take reasonable steps. APP entities that disclose information overseas under an exception in APP 8.2 are not taken to 'hold' information they have disclosed overseas under s 26WC. In these circumstances, if the personal information held by the overseas recipient is subject to a data breach, the APP entity does not have obligations to notify about the breach under the NDB scheme.

More information about APP 8 is available in Privacy business resource 8: Sending personal information overseas.21

Disclosing credit eligibility information

If a credit provider discloses credit eligibility information about one or more individuals to a person, a body or a related body corporate that does not have an 'Australian link' (s 26WC(2)(a)), the credit provider may also have obligations under the NDB scheme in respect of that information. If credit eligibility information held by the person or related body corporate is subject to loss, unauthorised access, or disclosure, the credit provider is responsible for assessing

whether there is an eligible data breach that needs to be notified to individuals at risk of serious harm and the Commissioner.

3.5 CASE STUDY: EQUIFAX DATA BREACH

In July 2017, credit reporting agency Equifax were the victims of a significant data breach which resulted in an estimated 143 million U.S. records containing customer information being stolen by hackers. This included social security numbers, dates of birth, and the credit card details of over 209,000 Americans. The breach also impacted other countries, with Equifax admitting that 15.2 million records of British citizens and 8000 Canadians were stolen in the breach. There was over a month's delay in disclosing the data breach. Senior executives were criticized for selling shares in the days before the breach was announced to the public.

The intruders managed to gain access to the records using a weakness in a popular back-end website application. The vulnerability was made public in March 2017, but Equifax were slow to fix the bug in their networks, highlighting the importance of maintaining the latest patches.

The Equifax hack had the markings of a sophisticated cyber-attack, leading to speculation about attribution, with some in the cyber security community blaming Chinese-backed groups due to similarities with other attacks such as the U.S. Office of Personnel hack in 2017.

The potential for the stolen Equifax data to be used in financial fraud has caused U.S. banks such as Citi Group and Wells Fargo to step up anti-fraud controls.

MODULE 4:
CYBERSEC INCIDENT MANAGEMENT MATURITY MODEL

The **SEI's Incident Management Maturity Model** is a practical framework that helps organizations assess and improve their capabilities for responding to security incidents. It is based on two existing models: the **Security Incident Management Maturity Model (SIM3)** and the **ENISA CSIRT (Computer Security Incident Response Team)** maturity approach. The SIM3 model was developed by the CSIRT community and has been applied by teams all over the world since 2009. It defines 44 indicators of maturity across four domains: organization, human, tools and processes. The ENISA CSIRT maturity approach was proposed by the European Union Agency for Cybersecurity (ENISA) and provides a three-tier classification of CSIRTs based on their services, cooperation, and quality management.

The SEI's Incident Management Maturity Model combines these two models and aligns them with the requirements of relevant EU policies, such as the NIS Directive. The model can be used by organizations to measure their current level of maturity, identify gaps and areas for improvement, and plan their development roadmap. The model also supports benchmarking and comparison among different organizations or sectors.

4.1 OVERVIEW

SEI'S INCIDENT MANAGEMENT MATURITY MODEL.

The **Software Engineering Institute** (SEI) has been at the forefront of American efforts to counter cyber threats for several decades. To this end, it has produced (in conjunction with others a maturity model that allows organisations to proactively evaluate and improve their ability to manage cyber security incidents.

It is intended for process improvement, it does not measure how well a given incident management activity is performed, only that it is performed. The rationale behind this approach is to allow individual organisations to devise their own implementation, having been given sufficient guidance to do so.

These incident management capabilities have evolved over many years. They are based on a set of metrics developed by the *US Defense Information Systems Agency* (DISA) and *National Security Agency* (NSA) in 2000-2002. The *Department of Homeland Security* (DHS) and *United States Computer Emergency Readiness Team* (US-CERT) funded the initial work to adapt the *U.S. Department of Defense* (DoD) version for Federal use in 2003–2005.

There are multiple aspects to successfully managing computer security incidents. Usually, the primary focus is on the response actions to remedy the incident. As a result, the organization fails to adequately consider that there is more to incident

management than reacting when a threatening event occurs. Being proactive is arguably more important than reactive alone; it is the combination of the two that works best.

The capabilities listed here provide a baseline of incident management practices. The incident management capabilities—each including a series of indicators—define the benchmark.

You can use these guidelines to assess how your current incident management functions are defined, managed, and measured. It provides the basis for improvements to the incident management function.

WHAT ARE THESE CAPABILITIES?

The capabilities are used to evaluate an incident management function. In any sizeable organization, one or more groups will be involved in incident management. Each group has a set of its own goals, tasks, and activities (their mission) that must be completed to support the overall strategic mission of the organization. The capabilities in this report explore different aspects of incident management activities for protecting, detecting, and responding to unauthorized activity in an organization's information systems and computer networks, as well as for establishing and sustaining the ability to provide those services.

Each capability includes a set of indicators, which are used by an assessment team to determine whether a capability has successfully been achieved or met. The results from an assessment can help an organization determine the comprehensiveness of its incident management function.

WHAT WE MEAN BY INCIDENT MANAGEMENT FUNCTION (IMF)

An incident management function is a set of capabilities (the people, processes, technology, etc. that provide an ability or capacity to perform some task) considered essential to protecting, detecting, and responding to incidents, as well as sustaining the incident management function (refer to Alberts and colleagues for more information [Alberts 2004]). These capabilities can be provided internally by security or network operators; be outsourced to managed security service providers (MSSPs); or be provided and managed by a computer security incident response team (CSIRT), security operations centre (SOC), or security team. We recognize that CSIRTs might not always be providing these capabilities.

For the sake of simplicity, the term incident management personnel are generally used in this report to refer to the groups (or individuals) performing incident management capabilities. The term incident management function includes everyone who is involved in the performance of incident management activities or the incident management process. The term constituency is used to refer to those who receive the services provided by whoever is performing incident management activities. The term organization is used to refer to the entire group

that is composed of the incident management personnel as well as their constituency. Occasionally we use the term CSIRT, which refers to a designated function or group of people to perform a portion of the incident management functions.

Incident management capabilities are grouped into the five categories described in **Table 1— Prepare, Protect, Detect, Respond, and Sustain**. Each category contains a range of subcategories with a set of one or more capabilities. Each capability includes a set of indicators that describe the essential activities leading to adequate performance of that capability.

Within the five major categories and many subcategories, each capability is assigned a priority. These priorities can be useful when making decisions about where to focus improvement efforts.

- **Priority I** capabilities are critical services that an incident management function must provide.
- **Priority II** capabilities are the important services that should ideally be provided.
- **Priority III** constitutes the remaining capabilities. They represent additional best practices that enhance operational effectiveness and quality.

PREPARE	PROTECT	DETECT	RESPOND	SUSTAIN
• Establish IM Function • Core Processes and Tools	• Risk Assessment • Prevention • Operational Exercises for Incident Management • Training and Guidance • Vulnerability Management	• Network and Systems Security Monitoring • Threat and Situational Awarenes s	• Incident Reporting • Analysis • Incident Response	• MOUs and Contracts • Project/Program Management • IM Technology Development, Evaluation, and Implementation • Personnel • Security Administration • IM Information Systems

Categories and Subcategories

OVERVIEW OF THE MAJOR CATEGORIES (CHS 1 & 2)

The next few paragraphs provide an overview of the major categories: Prepare, Protect, Detect, Respond, and Sustain.

PREPARE

Prepare focuses on establishing an effective, high-quality incident management function. This includes formally recognizing an incident management function, defining roles and responsibilities, and establishing interfaces between the various groups and individuals performing or affected by incident management functions. High-level processes must be defined, and essential tools, such as an incident tracking system, need to be acquired and embedded.

Trusted relationships, both internal and external, are established for the purpose of sharing relevant and necessary information.

PROTECT

Protect relates to the actions taken to prevent attacks and to mitigate the impact of those that do occur.

Preventative actions secure and fortify systems and networks, which helps to decrease the potential for successful attacks against the organization's infrastructure. In this model, Protect is focused on what changes can be made to the infrastructure as part of the response to contain or eradicate the malicious activity. It also includes taking proactive steps to look for weaknesses and vulnerabilities in the organization while understanding new threats and risks. Such steps can include:

- Performing security audits, vulnerability assessments, and other infrastructure evaluations to address weaknesses before they can be successfully exploited.
- Collecting information on new threats and evaluating their impact

Mitigation involves making changes in the constituent infrastructure to contain, eradicate, or fix actual or potential malicious activity. Such actions might include.

- Making changes in filters on firewalls, routers, or mail servers to prohibit malicious packets from entering the infrastructure.
- Updating intrusion-detection system (IDS) or anti-virus (AV) signatures to contain new threats.
- Installing patches for vulnerable software

Changes to the infrastructure may also be made, based on the process improvement changes and lessons learned that result from a post-mortem review done after an incident is handled. These types of changes are made to ensure that incidents do not happen again or that similar incidents do not occur.

DETECT

In Detect, information about current events, potential incidents, vulnerabilities, or other security or incident management information is gathered proactively and reactively. With reactive detection, information is received from internal or external sources in the form of reports or notifications. Proactive detection calls for action by the designated staff to identify suspicious activity through monitoring and analysis of a variety of logging results, situational awareness, and

evaluation of warnings about situations that can adversely affect the organization's successful operation.

RESPOND

Respond includes the steps taken to analyse, resolve, or mitigate an event or incident. Such actions are targeted at understanding what has happened and what needs to be done to enable the organization to resume operation as soon as possible or to continue to operate while dealing with threats, attacks, and vulnerabilities. Respond steps can include:

- Analysis of incident impact, scope, and trends.
- Collection of computer forensics evidence, following chain-of-custody practices.
- Additional technical analysis related to malicious code or computer forensics analysis.
- Notification to constituents, stakeholders, and other involved parties of incident status and corresponding response steps.
- Development and release of alerts, advisories, bulletins, or other technical documents.
- Coordination of response actions across the organization and with other involved internal and external parties.
- Verification and follow-up to ensure that response actions were correctly implemented, and that the incident has been appropriately handled or contained.

SUSTAIN

Sustain focuses on maintaining and improving the CSIRT or incident management function itself. It involves ensuring that:

- The incident management function is appropriately funded.
- Incident management personnel are appropriately trained.
- Infrastructure and equipment are adequate to support the incident management services and mission.
- Appropriate controls, guidelines, and regulatory requirements are followed to securely maintain, update, and monitor the infrastructure.
- Information and lessons learned from the Protect, Detect, and Respond processes are identified and analysed to help determine improvements for the incident management operational processes.

EXPLANATION OF THE CAPABILITY STRUCTURE

The capabilities are formatted in a workbook structure that can be used during an assessment to both conduct the assessment and capture information. The structure for each incident management capability provides two basic sets of information:

- the capability itself, presented as a primary capability statement, and a more detailed set of indicators that can be used by the assessor to assess the performance of the capability.
- explanatory information and scoring guidance—additional information explaining the significance of the capability and how to assess the performance of that capability.

Each capability also includes a set of cross-references to selected regulations or guidance: the *Federal Information Security Management Act* (FISMA), *National Institute of Standards and Technology* (NIST) publications, and relevant best practices.

Each capability includes indicators to assess the performance of that capability. Within these indicators, when the word personnel are used, it refers to whomever is performing the activities associated with the capability. If other roles or more specific types of roles are being referenced, the indicator will specify which type of personnel.

These indicators are grouped into three areas: Required, Recommended Best Practice, and Institutional and Quality Improvement. All the indicators in the Required area must be met for an organization to successfully meet this capability. The indicators in the Recommended Best Practice area represent additional aspects that are recommended for a more complete or robust capability. The indicators in the Institutional and Quality Improvement area are those needed to ensure this capability can be sustained, that is, those things that would ensure the continuity or resilience of the capability even in the face of personnel changes. In addition, there are four types of indicators, specified by the italicized word occurring before the indicator statement:

- Prerequisites must be met before this capability can be performed or be performed adequately.
- Controls are available or exist that direct the proper execution of the activities.
- Activities are performed as part of this capability (and could be observed by an assessor).
- Quality indicators measure effectiveness, completeness, usefulness, institutionalization, and other quality aspects of the activities.

To help the assessor use the tables, the following list explains how the information for each capability is organized. Reading the table from left to right, the fields are

- Capability subcategory and number (e.g., 2.1 Risk Assessment)
- Capability reference number and statement—represents major category number, subcategory number, and specific capability number and statement (e.g., 2.1.1 Security risk assessments (RAs) are performed on the organization.)

- Priority—I through III (where priority I is the most important)
- Clarification—additional information explaining the purpose and description of the capability team guidance—information to help an assessment team score this capability
- References—standards, guidelines, or regulations relating to this capability, including a placeholder for organization-specific references
- Organization response—optional field if early information was collected from an organization indicating how they would respond to the capability
- Examples of evidence—list of possible evidence the team should look for during interviews, documentation reviews, or observations
- Scoring criteria—the indicators (preceded by a unique indicator number), scoring choices (Yes/No), and room to list evidence (i.e., the specific criteria the assessors can see or examine during the assessment to help them determine whether the capability is being performed)
- Final score— "Met" if all required indicators are met; "Not Met" if any required indicator is not met, Not Applicable—used when capability is excluded from scoring, Not Observed—used when capability was not observed during the assessment
- Evidence collected place to identify what documents were reviewed, interviews conducted, or activities observed
- Notes—additional notes made by the assessment team either in preparation for the assessment or during the assessment
- Suggestions for improvement—additional ideas for an organization to consider if it works to improve this capability beyond implementing the concepts in each indicator

4.2 PERFORMING ASSESSMENTS

A C2M2 capability assessment is a process of evaluating the maturity of an organization's cybersecurity practices based on a standardized model. The C2M2 stands for *Cybersecurity Capability Maturity Model,* and it consists of the 10 domains (described earlier), such as Risk Management, Asset Management, Identity and Access Management, etc.

Each domain has a set of objectives and practices that describe different levels of capability, from 0 (Incomplete) to 3 (Optimized). To perform a C2M2 capability assessment, an organization follows these steps:

1. **Select a facilitator and a team** of participants who are familiar with the organization's cybersecurity activities and processes.
2. **Choose one or more domains to assess**, depending on the scope and purpose of the assessment.
3. **Review the C2M2 model and its components**, such as the objectives, practices, indicators, and target states.
4. **Conduct a self-assessment** using the C2M2 toolkit, which provides a questionnaire and a scoring tool for each domain.
5. **Analyse the results and identify the strengths and gaps** in the organization's cybersecurity capabilities.
6. **Develop an action plan** to address the gaps and improve the capabilities based on the priorities and resources of the organization.
7. **Implement the action plan and monitor the progress** and outcomes of the improvement efforts.
8. **Repeat the assessment periodically** to measure the changes and track the maturity level over time.

A C2M2 capability assessment can help an organization to benchmark its cybersecurity performance, identify areas for improvement, and align its practices with best practices and standards.

USING THESE CAPABILITIES TO ASSESS THE INCIDENT MANAGEMENT FUNCTION OF AN ORGANIZATION

This section provides an overview of how the capabilities can be used to assess and improve an organization’s incident management function. This section and the next provide an overview of the assessment methodology and considerations for scoring the capabilities. To generalize, this assessment method centres around using interviews, artefact reviews, and activity observations to determine how completely the incident management activities represented in the capabilities are performed.

It is possible to use these capabilities for a broad range of assessments. For example, the entire set of capabilities can be used to assess an organization’s entire incident management function. A subset can be used to focus on only the

specific responsibilities of an actual SOC, CSIRT, or security service provider. The extent or scope of an assessment is determined early in the process, based on the goals of the organization or the specific focus of the assessment sponsor. The assumption for this section is that the entire incident management function is being assessed. An assessment with a narrower scope would simply use fewer capabilities and assess fewer groups.

Incident management, as a complete function, includes activities that may be performed within a SOC, by a CSIRT, or by other groups across an organization. There may be several groups, each with some distinct or overlapping responsibilities that support management of cybersecurity events and incidents. In the latter case, applying these capabilities against only a designated centralized incident management function or CSIRT may result in an inaccurate or very limited view of the organization's total ability to effectively manage cybersecurity incidents. An assessment should consider all groups performing incident management activities to produce accurate results.

An assessment using these capabilities generally requires:

- **Assessment planning**: establishing points of contact, assessment scope, schedule, and resources and assembling the assessment team and supporting equipment and supplies
- **Pre-assessment**: preparing for on-site assessment activities; gathering information as needed before going onsite; analysing available documents and other artifacts; identifying groups and individuals (e.g., groups involved in Prepare, Protect, Detect, Respond, and Sustain activities) to interview onsite; allocating capabilities to those groups; and finalizing the onsite schedule
- **Onsite**: conducting interviews, observing activities, reviewing additional artefacts, documenting evidence collected, determining preliminary scores according to evidence rules, and gathering additional information, if possible, to fill any gaps
- **Post-assessment**: performing final analysis and scoring and, optionally, identifying recommendations for improvement, producing a report for stakeholders, and conducting required reviews
- **Close-out**: properly disposing or archiving of gathered information and conducting a "lessons learned" review

Some specific guidance for selecting assessment activities follows.

IDENTIFY THE GROUPS INVOLVED IN INCIDENT MANAGEMENT AND ALLOCATE THE CAPABILITIES

There are many techniques for identifying the groups involved in incident management. One technique uses a process model benchmark for incident management, such as that described by Alberts and colleagues. By comparing the organization to this process model of incident management activities, all groups performing such activities can be identified. An alternative is to use some form of work process modelling to map all groups and interfaces associated with incident

management activities. Once the groups and activities are identified, capabilities can then be allocated to each group (e.g., allocate Detect capabilities to the groups performing network monitoring).

Bear in mind that there may not be clearly defined roles that align with the categories, and you may need to ask more than one group about the same set of capabilities to achieve complete coverage. While you can adjust your schedule of interviews and observations when onsite, it is best to keep schedule adjustments to a minimum.

ASSESS EACH GROUP

The simplest means of assessing each group against its capabilities is to conduct interviews or group discussions, observe the activity being performed or a demonstration of the activity, and ask the assembled individuals about each capability that is applicable to their group. Artefacts related to the capabilities can be requested and reviewed and, when necessary, additional activities can be observed. The assessment team should use the general scoring guidance in Section 4 of the model and the specific guidance provided with each capability to guide its assessment. (See Section 2 of the model, "Explanation of the Capability Structure," for a description of the sections and indicators provided for each capability.)

When more than one group shares the responsibilities to perform a certain capability, the assessment team should conduct interviews (or group discussions, observations, or process demonstrations, as applicable) with at least two of the involved groups, and then compare and assess the collective results from the different sources. (See Section 3.3 for further guidance about groups that cannot be assessed.) When the results for capabilities or individual indicators differ between groups, the lowest score generally prevails (i.e., if one individual or group indicates "Yes" to an indicator but another individual or group says "No," the combined score for the organization for that indicator will generally be "No").

All indicators are scored as either Yes or No, and Capabilities are scored at the end as "Met," "Not Met," "Not Observed," or "Not Applicable."

- "**Met**"—At a minimum, all the required indicators have been met.
- "**Not Met**"—One or more of the required indicators has not been met.
- "**Not Observed**"—A capability cannot be assessed because the assessment team does not have access to the individuals who can provide the correct answer or cannot observe that the activity or capability was performed.
- "**Not Applicable**"—The activity is not included in the assessment, which may mean that it is deliberately not performed by the organization as part of the incident management processes. Capabilities that are not applicable should be identified during assessment scoping.

DETERMINE WHAT TO DO ABOUT GROUPS THAT CANNOT BE ASSESSED

Given the complexities and political realities of some organizations, it may not be possible to meet with some groups or obtain access to certain types of information. At the very least, the interface to that group or the way in which those groups interact should be assessed. The organization can then decide if those groups should be assessed later.

Alternatively, those groups could assess themselves using applicable information from these capabilities and then provide the results (or feedback) to appropriate individuals. Another option is to use an external or third-party organization to perform the assessment on relevant groups. If part of the incident management function is outsourced and the organization being assessed can provide sufficient evidence to prove that the outsourced contractor or group is performing the capability, the outsourced contractor or group may not need to be assessed. If specific information cannot be reviewed, the assessment team and assessment sponsor will need to decide if the remaining evidence is sufficient to indicate an actual score or if “Not Observed” needs to be used.

USE THE RESULTS TO DECIDE WHAT TO IMPROVE

The organization, using the assessment results, has a clear idea of how it is meeting these capabilities with respect to incident management. It knows what its strengths and weaknesses are. To improve the processes, the organization can look at the resulting scores and begin to create a strategy for improvement building on its strengths. For example, the candidates for improvement could be sorted by priority order, so that unmet Priority I capabilities come first, and so on.

Existing strengths can be used to improve weaker areas. For example, if some capabilities have exceptionally good procedures and policies, use those as a basis for developing policies and procedures for capabilities that are not as robust or are missing. If there is a strong training program for some types of personnel, expand that program to include additional types of training for capabilities that are lacking.

A further review of results may be needed when considering improvements in Priority II through Priority III capabilities. For example, improving a Priority III capability from “Not Met” to “Met” might be less critical than improving a Priority II capability from “Not Met” to “Met.” Each organization makes its own determination concerning the order in which to improve scores on any Priority II-III capabilities based on a review of the entire set and by considering the changes that are needed, the required resources, the mission, the goals, and the objectives.

Finally, a common type of improvement for all the capabilities can be found by looking at the non-required indicators: Recommended Best Practices and Institutional and Quality Improvement indicators. These types of improvements go beyond meeting the basic requirements and consider additional aspects that can build an exceptional incident management function. Even those capabilities

for which required indicators were successfully met can be improved by implementing the non-required indicators.

Each capability should be examined to consider the relative consequences of "doing" or "not doing" the capability or required indicators therein. This examination can provide elemental insight into whether improvement might yield an unexpected result. Look to the suggested improvements for ideas on enhancing performance or identifying ways to improve. When applying the capabilities to identify improvements, use judgment and common sense, respect the budgetary process, and stay abreast of changing regulations and standards in this ever-evolving environment.

Ultimately, the end goal for these capabilities (or other types of assessments) is to strive for continuous improvement of the processes, so it is also a recommended best practice to periodically re-assess to see what new "current" state has been achieved. This re-assessment could be done annually or as conditions change (e.g., as new technologies are deployed, the infrastructure changes, or new partnerships or supply chains are adopted).

These capabilities should be considered a starting place for identifying improvements. They are not a precisely defined path for every organization to build the perfect incident management function, but they can be used as a guideline for what to include in an incident management function, based on the organization's mission and the incident management function's services.

4.3 SCORING THE CAPABILITIES

GENERAL GUIDANCE FOR SCORING CAPABILITIES

This section discusses scoring issues that the assessment team needs to remember as it is conducting an assessment. Each capability can have a score of "Met" or "Not Met." To determine the score for a capability, the assessment team applies the rules of evidence against all the information gathered from interviews, demonstrations, observations, and document or artefact reviews. Interviews are question-and-answer sessions with one or more people with peer relationships where the assessment team uses the capabilities as the basis for asking questions. In observations, the assessment team watches one or more people conduct their actual IM activities; the team observes only and does not question or ask for additional actions. In demonstrations, the assessment team interacts with the people performing real or hypothetical IM activities, asking questions, getting demonstrations of what could occur, or how tools might be used in hypothetical situations. Observations and interviews are similar. Document or artefact reviews are conducted by assessment team members to understand relevant parts of IM-related documents.

For each capability, all Required indicators must have an answer of "Yes" to obtain a successful or passing score for that capability (i.e., the capability is met). If one or more of the Required indicators has an answer of "No," the score for the capability is "Not Met." The Recommended Best Practice indicators and the Institutional and Quality Improvement indicators include those that are not necessarily required to achieve success for the capability but are recommended. These indicators are not included in the final determination of a capability being met or not met. They are currently provided for improvement purposes. See Section 4.3 for alternative scoring ideas.

EVIDENCE COLLECTION REQUIREMENTS

Sufficient evidence for establishing a passing score requires more than one document, interview, observation, or demonstration. The indicators listed with each capability are used to assist in the collection of evidence. The Evidence column to the right of each indicator is used to record the type of evidence (e.g., interview, observation, demonstration, or document review) or a description of the evidence that was used to score that indicator.

If a capability is to be scored "Met," all Required indicators for that capability have been determined to be covered (checked "Yes"). The coverage rules for sufficiency of evidence to determine if an indicator can be checked "Yes" are provided in Table 2 below. In summary, it takes at least two different types of sources to confirm an indicator. Note that in the rules for sufficiency, an interview and a demonstration are considered equivalent. An observation, then, needs the confirmation of an interview or demonstration, or a document review. A document review needs the confirmation from either an observation or a

demonstration/interview. Also note that it takes at least one document, but in general, more than one document is preferred.

Evidence Rules

	Interview/ Demonstration	**Observation**	**Document/Artifact**
Interview/ Demonstration	Not Sufficient	√	√
Observation	√	Not Sufficient	√
Document/Artifact	√	√	Not Sufficient

CHECK COMPLETENESS AND QUALITY OF DOCUMENTED POLICIES AND PROCEDURES

When deciding if documented policies and procedures referenced in the indicators are adequate, assessment teams should consider the following:

- Does the policy or procedure adequately address the process, technology, requirements, expected behaviours, or another topic it is supposed to address?
- Do the procedures reflect what is done by personnel?
- Are the policies and procedures easily available to personnel?
- Are the policies or procedures being kept up to date? There should be a review and/or revision date or some indication that policies and procedures are reviewed and changed as needed. Also look for
  - a defined process and periodicity for reviewing and revising
  - established criteria for when to review (e.g., change in organization structure, major technology installation)
  - defined roles and responsibilities for review and update
  - a defined process for communicating changes and revisions throughout relevant parts of the organization
  - a change log history
  - indications the date was simply changed to make it look up to date5

It may also be useful to ask for any documents that are currently being revised to help evaluate their process for keeping documents up to date or to at least demonstrate that they are in the process of improving a current gap. Such findings will be useful when the organization decides what to improve. In most cases, policies (and processes) are included in the Required indicators, and documented, formal procedures are included in the Institutional and Quality Improvement indicators.

DETERMINE PERSONNEL KNOWLEDGE OF PROCEDURES AND SUCCESSFUL TRAINING

The assessment team should be able to determine from discussions with the personnel whether they understand the process (e.g., they are able to describe it intelligently and consistently). More importantly, the personnel should be able to easily show how they perform that work (e.g., show the forms that they fill in, describe the process they use to take information from an incident report that is displayed and extract information to feed into summary or other organizational or regulatory reports, or demonstrate how they perform analysis on a set of logs). A process can be consistently known and followed even without a formal, documented procedure. If a documented procedure does exist, the assessment team needs to determine if the procedure is followed.

Training can range from formal training that has complete packages with materials and dedicated instructors to informal, on-the-job mentoring by more senior, experienced personnel. The assessment team seeks to determine whether training is provided, that the training is sufficient to meet the needs of the organization, and, as shown in the Institutional and Quality Improvement indicators, that the personnel are knowledgeable and perform the procedures consistently.

During demonstrations, the assessment team can ask personnel to discuss the process they are following to show a level of understanding that supports knowledge of their capabilities about the activities being conducted. The observation of personnel performing tasks can also provide an indication of the maturity of their operations and training. For example, observation can show that personnel know the following:

- how to use the tools that support the capabilities
- where reports or data are archived
- what types of information are contained in reports or alerts or other documents and products
- where procedures, policy, or guidance documents are kept and how to access them if needed

SCORING VARIATIONS

It is possible for the assessment team and assessment sponsors to determine a different scoring algorithm (e.g., all the Required and Recommended Best Practice for a “Met” score). The only caution would be to use a consistent scoring algorithm over time to allow for accurate determination of improvement from one assessment to the next or for accurate comparison between assessed groups.

In addition to the “Met,” “Not Met,” “Not Observed,” or “Not Applicable” scores for a capability, some assessors have used a “Partial” score. “Partial” in this case would mean that some of the Required indicators have been met, but not all. “Partial” scores can be difficult to use as it becomes more subjective as to what

percentage or number of Required indicators is needed to reach a “Partial” as opposed to a “Not Met” score. Some assessment teams have also found it useful to use “Not Observed,” or “Not Applicable” for the indicators as well as the capability. In that case, on the worksheet, the indicator can be scored as either a “No,” and the evidence column used to state the rationale for it being not observed, or scored as a “Yes,” with the rationale for it not being applicable in the evidence column.

4.4 THE CAPABILITIES

THE INCIDENT MANAGEMENT CAPABILITIES

The remainder of this document contains Version 3.0 of the capabilities, split into five sections:

- **Prepare**: Section 1 of the capabilities
- **Protect**: Section 2 of the capabilities
- **Detect**: Section 3 of the capabilities
- **Respond**: Section 4 of the capabilities
- **Sustain**: Section 5 of the capabilities

These capabilities are a living document. Periodic changes may be made to these capabilities, and new versions may be released.

PREPARE: SECTION 1 OF INCIDENT MANAGEMENT CAPABILITIES

Prepare is getting the incident management function up and operational. This includes getting the incident management function established, creating and implementing the necessary plans, defining the key work processes that will be essential to the smooth functioning of an incident management function, and establishing the necessary working relationships with both internal and external experts and groups who will provide needed assistance and expertise.

Getting formal recognition and designation as an incident management function, regardless of whether it is a formal CSIRT, is essential to ensuring that the other parts of the organization understand and agree to accept the services provided and provide the required information to the incident management function. If that does not happen, the IM function may not be able to perform effectively. Defining roles, responsibilities, and interfaces among groups of people performing incident management capabilities is needed to ensure everyone knows what their job is and how to work efficiently with other groups to detect, analyse, and respond to incidents.

The plans that are developed will establish and sustain the incident management function in terms of how it will function, communicate, and deal with incidents when they occur. The core processes are needed to define how the various key activities will be carried out, and the essential tools needed by the incident management function must be acquired. Chief among these tools is the incident repository where all the information relevant to incidents will be retained. This repository allows not only the immediate analysis of current incidents but also later analysis for trends and patterns, forensic analysis, and so forth.

Finally, no incident management function can be effective if it operates in isolation. IM personnel must establish trusted relationships with other experts to be aware of events and other types of attacks going on outside the organization and to reach back for additional expertise and help when faced with a new or

unprecedented form of incident or the need for new tools. It takes time to get these relationships established and maintain them. This needs to be done as part of preparing.

Within the Prepare category, the subcategories and their capabilities include the following:

ESTABLISH IM FUNCTION

1.1 Establish IM Function—Establishing the IM function requires formal recognition and acceptance of its existence and its mission, who the people are who perform the activities and what they do and defining how it works with other groups.

1.1.1 An incident management function or CSIRT has been officially designated by the organization head or chief information officer (CIO).

1.1.2 An incident management plan has been developed and implemented for the organization.

1.1.3 Roles and responsibilities are documented for key incident management activities throughout the organization and followed.

1.1.4 Formal interfaces for conducting organizational incident management activities are defined and maintained.

1.1.5 Trusted relationships are maintained with experts who can give technical and nontechnical advice and information.

CORE PROCESSES AND TOOLS

1.2 Core Processes and Tools—An incident management function needs to establish the core practices and the basic tools that will be required for effective performance of incident management activities. That includes understanding how work will be managed, incident information will be retained, and how the potential for insider threat can be controlled.

1.2.1 A communication plan for incident management activities has been established and disseminated.

1.2.2 An IM information management plan is established and followed.

1.2.3 An inventory exists of mission-critical systems and data.

1.2.4 Workflow management processes and/or systems are implemented.

1.2.5 A central repository exists for recording and tracking security events and incidents.

1.2.6 Security events and incidents are categorized and prioritized according to organizational guidance.

1.2.7 An insider threat program exists within the organization

Refer to Incident Management Capability Assessment Workbook. December 2018 TECHNICAL REPORT CMU/SEI-2018-TR-007

4.5 INCIDENT MANAGEMENT CAPABILITIES

LIST OF INCIDENT MANAGEMENT CAPABILITIES

A simple list of all the capability statements contained in the ***SEI-CMU's Cybersecurity Maturity Model***.

Capabilities	Priority
Prepare	
Establish IM Function	
1.1.1 An incident management function or CSIRT has been officially designated by the organization head or chief information officer (CIO).	II
1.1.2 An incident management plan has been developed and implemented for the organization.	I
1.1.3 Roles and responsibilities are documented for key incident management activities throughout the organization and followed.	I
1.1.4 Formal interfaces for conducting organizational incident management activities are defined and maintained.	I
1.1.5 Trusted relationships are maintained with experts who can give technical and nontechnical advice and information.	III
Core Processes and Tools	
1.2.1 A communication plan for incident management activities has been established and disseminated.	II
1.2.2 An IM information management plan is established and followed.	II
1.2.3 An inventory exists of mission-critical systems and data.	I
1.2.4 Workflow management processes and/or systems are implemented.	III
1.2.5 A central repository exists for recording and tracking security events and incidents.	I
1.2.6 Security events and incidents are categorized and prioritized according to organizational guidance.	II
1.2.7 An insider threat program exists within the organization.	I
Protect	
Risk Assessment	

2.1.1 Security risk assessments (RAs) are performed on the constituents' organization.	I
2.1.2 The constituents get help correcting problems identified through security risk assessment (RA) activities.	II
Prevention	
2.2.1 The organization has an institutionalized malware prevention program.	I
Operational Exercises for Incident Management	
2.3.1 Operational exercises are conducted to assess the IM function of the organization.	II
Training and Guidance	
2.4.1 Guidance is provided to constituents on best practices for protecting their systems and networks.	II
2.4.2 Constituents are provided with security education, training, and awareness (ETA).	I
Vulnerability Management	
2.5.1 A patch management and alert program exists.	I
2.5.2 Proactive vulnerability assessment is performed on constituent networks and systems.	I
2.5.3 Constituents receive help to correct problems identified by vulnerability assessment activities.	II
Detect	
Network and Systems Security Monitoring	
3.1.1 Security monitoring is continuously performed on all constituent networks and systems.	I
External Sources of Incident Information	
3.2.1 Events and incidents are reported from outside the organization.	I
Threat and Situational Awareness	
3.3.1 Public monitoring of external security websites and other trusted sources of information is conducted.	I
3.3.2 Trend analysis is supported and conducted.	II

3.3.3 Network and system configurations or rule sets are reviewed and updated in response to changes in the threat environment, and constituents are notified of the updates.	I
3.3.4 Penetration testing is conducted on organizational networks and systems.	I
Respond	
Incident Reporting	
4.1.1 Events and incidents are reported from the constituency.	I
4.1.2 Incidents are reported to appropriate management in accordance with organizational guidelines.	I
4.1.3 Incidents are reported to and coordinated with the appropriate external organizations or groups in accordance with organizational guidelines.	I
4.1.4 Incident management is supported for restricted information, networks, and systems.	I
Analysis	
4.2.1 Incident management personnel conduct triage of events and incidents.	I
4.2.2 Incident analysis is performed on declared incidents.	I
4.2.3 Incident correlation is performed to identify similar activity.	II
4.2.4 Impact of an incident is determined.	II
4.2.5 Incident root cause analysis is conducted.	II
4.2.6 Fusion analysis is performed to identify concerted attacks and shared vulnerabilities.	III
4.2.7 Retrospective analysis is conducted.	III
4.2.8 Media analysis is performed on constituent networks and systems.	II
4.2.9 Artifact or malware analysis is conducted.	II
Incident Response	
4.3.1 General incident response guidance and procedures are distributed to constituents.	II
4.3.2 Incidents are resolved.	I

4.3.3 Incident management personnel coordinate incident response across stakeholders.	I
4.3.4 Incident management personnel create alerts and warnings and distribute them as needed.	I
4.3.5 Incident management personnel verify that a response is implemented, as appropriate, and that the incident is closed, in accordance with organizational guidance.	I
4.3.6 Postmortem reviews of significant incidents are conducted, and lessons learned are identified and acted upon, as appropriate.	I
Sustain	
MOUs and Contracts	
5.1.1 A list of incident management services provided by the designated incident management function is documented.	II
5.1.2 The constituency provides advance notification of all changes or planned outages to their networks.	III
5.1.3 Formal agreements exist for managing IM activities with third parties across the supply chain.	I
Project/Program Management	
5.2.1 A financial plan exists for incident management activities.	III
5.2.2 A workforce plan exists for incident management personnel.	II
5.2.3 A personnel security plan exists for incident management personnel.	I
5.2.4 A quality assurance (QA) program exists to ensure the quality of provided products and services.	II
5.2.5 An established plan exists to ensure continuity of operations for incident management.	I
5.2.6 The effectiveness of the incident management function in meeting its mission is routinely evaluated and improved.	III
IM Technology Development, Evaluation, and Implementation	
5.3.1 The incident management function has the tools it needs to meet its mission.	I
5.3.2 Software tools are tested for use within the incident management environment.	II
5.3.3 The IT infrastructure for incident management is adequate to support incident management operations.	I
Personnel	

5.4.1 A training program exists for incident management personnel.	I
5.4.2 Support for professional development exists for incident management personnel.	III
Security Administration	
5.5.1 Physical protective measures are in place to protect incident management IT systems, facilities, and personnel.	I
5.5.2 An operations security (OPSEC) program exists.	I
IM Information Systems	
5.6.1 An inventory exists of mission-critical incident management systems, data, and information.	I
5.6.2 Defense-in-depth strategies and methodologies exist for hardening the incident management computer networks and systems.	I
5.6.3 Processes and technologies exist to support the confidentiality, integrity, and availability of incident management data and information.	I
5.6.4 Network security monitoring is performed on all incident-management-related networks and systems.	I
5.6.5 Security risk assessments (RAs) are performed on the incident management function.	I
5.6.6 Vulnerability assessments are performed on incident management systems and networks.	I
5.6.7 A patch management program is in place for the incident management systems.	I
5.6.8 More than one communications system or mechanism (other than email) exists for receiving and distributing notifications, information about new viruses, incidents, vulnerabilities, threats, and other kinds of warnings.	II

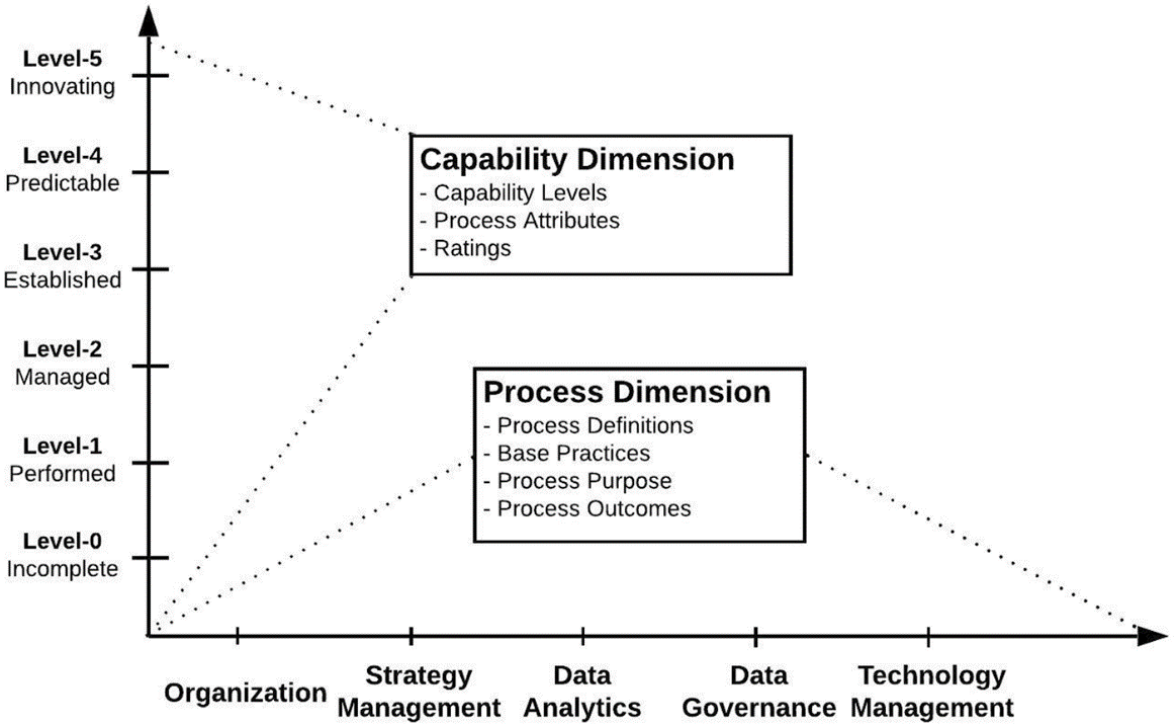
4.6 CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

The **Cybersecurity Capability Maturity Model (C2M2)** is a tool developed by the US Dept of Energy (DOE) to give organizations the means to consistently assess their cybersecurity capabilities. The assessment highlights way to *improve* an organisation's cybersecurity capability.

In this regard, the model helps organizations identify their current level of cybersecurity maturity and develop a roadmap for improving their cybersecurity posture over time.

The C2M2 is based on the SEI's *Capability Maturity Model Integration* (CMMI) framework, which is widely used in software engineering and other industries to assess and improve organizational processes.

The basic concept of the 'capability maturity models' has been applied across various industries and professions owing to its simple conceptual design and adaptability. They simply establish the comprehensive range of processes that must be performed for given discipline, then measures how well a particular process is being performed.



One of the advantages of the CMM (Capability Maturity Model) concept is that they are 'process model' that describes the process, but not how to execute the process, leaving that for the organisation to devise their own ways and means on the assumption that they know their business best. A 'one size fits all' model that prescribes the 'how' would not work in practice.

With this flexibility of application, but encompassing all required activities, a maturity model becomes an excellent process improvement tool. The concept was originally devised in the 1980's by Watts Humphrey at the Software Engineering Institute at Carnegie-Mellon University in Pittsburgh. There was a need to establish the means for the US Dept of Defense to evaluate the software development capabilities of suppliers of software intensive products to the DoD. And to provide those suppliers with the means to improve their capability.

The key rationale behind the design of CMMs (Capability Maturity Model) can be summarized as follows:

Assessing Current Capabilities - CMMs aim to provide a systematic and standardized way of evaluating an organization's current capabilities in a specific area. By assessing their capabilities against predefined maturity levels, organizations can gain insights into their strengths, weaknesses, and areas for improvement. This assessment helps organizations identify gaps and set realistic goals for enhancing their performance.

Establishing a Common Language - CMMs create a common language and shared understanding within an organization and across industries. They define key concepts, processes, and practices related to a specific domain, enabling organizations to communicate and collaborate effectively. This common language facilitates knowledge sharing, benchmarking, and comparison among different organizations.

Providing a Roadmap for Improvement - CMMs offer a structured roadmap for organizations to enhance their capabilities incrementally. By defining maturity levels and associated practices, CMMs provide organizations with a clear progression path. This roadmap allows organizations to prioritize and focus their efforts on areas that require improvement, ensuring a systematic and step-by-step approach to maturity enhancement.

Encouraging Continuous Improvement - CMMs emphasize the importance of continuous improvement and ongoing development. They recognize that maturity is not a static state but rather a journey of constant growth and evolution. CMMs encourage organizations to adopt a culture of learning, innovation, and adaptation, fostering a mindset of continuous improvement in their practices, processes, and performance.

Enabling Benchmarking and Best Practices - CMMs facilitate benchmarking against industry best practices and standards. They provide organizations with a reference point to compare their capabilities with peers and industry leaders. This benchmarking allows organizations to identify areas where they lag and learn from others' successes. It promotes knowledge sharing and collaboration, ultimately driving overall industry advancement.

Supporting Decision-Making and Resource Allocation - CMMs help organizations make informed decisions and allocate resources effectively. By providing a structured assessment of capabilities and areas for improvement, CMMs enable organizations to prioritize investments, allocate resources efficiently, and address critical gaps. This data-driven approach ensures that resources are allocated based on identified needs and strategic objectives.

In summary, the design of capability maturity models is grounded in the principles of assessment, improvement, common understanding, roadmap development, continuous learning, benchmarking, and resource allocation. CMMs serve as valuable tools for organizations to enhance their capabilities, establish industry best practices, and achieve higher levels of performance in a structured and systematic manner.

4.7 C2M2 MATURITY LEVELS

The C2M2 consists of five maturity levels, each with a set of capabilities that organizations must demonstrate to achieve that level. The five levels are:

INITIAL (LEVEL 1)

At this stage, cybersecurity practices are ad hoc and unorganized. The organization has limited awareness of cybersecurity risks and lacks a formal strategy. There may be a reactive approach to security incidents, and the focus is primarily on resolving immediate issues rather than implementing preventive measures.

The primary goal at this level is to establish a foundation for a structured cybersecurity program.

MANAGED (LEVEL 2)

At the managed level, the organization starts implementing *basic* cybersecurity controls and processes. There is a defined and documented cybersecurity policy and strategy. The organization has a better understanding of its critical assets and associated risks.

Incident response plans and procedures are established, and regular vulnerability assessments are conducted. The focus at this level is on establishing a management framework for cybersecurity.

DEFINED (LEVEL 3)

The defined level signifies a higher level of cybersecurity maturity. At this stage, the organization has a well-defined and documented set of cybersecurity processes and controls. Policies, procedures, and standards are in place and communicated throughout the organization.

Risk management processes are established, and cybersecurity responsibilities are clearly defined. Security awareness training programs are conducted for employees, and regular audits and assessments are performed to ensure compliance.

QUANTITATIVELY MANAGED (LEVEL 4)

At this level, the organization focuses on quantifying and measuring its cybersecurity capabilities. The organization collects and analyses security metrics to assess the effectiveness of its controls and processes.

Risk assessments are performed regularly, and security incidents are tracked and monitored using advanced tools and technologies.

Continuous improvement is a key aspect at this level, with the organization using data-driven insights to enhance its cybersecurity capabilities.

OPTIMIZED (LEVEL 5)

The optimized level represents the highest level of cybersecurity maturity. At this stage, the organization has a proactive and adaptive approach to cybersecurity. It continually monitors emerging threats and incorporates them into its security strategy.

The organization actively participates in information sharing and collaboration with industry peers and government entities. It leverages advanced technologies, such as artificial intelligence and machine learning, to detect and respond to cyber threats in real-time.

Regular testing, simulations, and exercises are conducted to ensure the effectiveness of cybersecurity controls and response plans.

4.8 PROGRESSING UP LEVELS

Once the organisation has implemented all the processes and controls associated with one level they can proceed to the next. And not before.

In this structured way, the *Cybersecurity Capability Maturity Model* lays out a definitive roadmap for organizations to identify their current maturity level, to set goals for improvement, and continuously improve their cybersecurity capabilities.

The assessment of an organization's maturity level is typically conducted through an assessment of its existing cybersecurity practices, policies, procedures, and technical controls. This assessment involves interviews, documentation reviews, and technical assessments. The results are then mapped against the maturity levels defined in the model to determine the organization's current level and identify areas for improvement. Evidence that processes are being performed is required when doing assessments.

This structured approach to building a robust cybersecurity program brings alignment with industry best practices and regulatory requirements. Customers may be interested to know a potential supplier’s maturity level and might prescribe a minimum level as a condition of doing business and integrating the organisation into a supply chain.

4.9 THE C2M2 DOMAINS

The C2M2 has comprehensive list of **10 domains** that must be addressed to achieve each maturity level:

1. Asset Management
2. Access Control
3. Awareness and Training
4. Data Security
5. Incident Response
6. Maintenance
7. Protective Technology
8. Risk Management
9. Situational Awareness
10. System and Communications Protection

Each domain is further divided into the maturity levels discussed above, which represent the degree to which the organization has implemented the associated cybersecurity practices.

Each of the domains listed above will have a maturity rating determined by the assessment. Typically, an organisation will have varied results across the domains, with some being performed more rigorously than others.

Again, the maturity levels in brief are:

1. **Initial**: The organization has not yet implemented any cybersecurity practices in this domain.
2. **Repeatable**: The organization has implemented some cybersecurity practices in this domain, but they are not consistently applied.
3. **Defined**: The organization has defined cybersecurity practices in this domain, and they are consistently applied.
4. **Managed**: The organization has established a process for managing cybersecurity in this domain.
5. **Optimized**: The organization has continuously improved its cybersecurity practices in this domain.

Organizations therefore use the C2M2 to consistently measure their cybersecurity capabilities over time, to identify target maturity levels based on risk, and to prioritize the actions and investments that allow them to meet their targets.

It is advisable to present the C2M2 as a useful tool for improvement, not as a kind of audit like the tax man might do to uncover wrongdoing. People become defensive if the wrong perception of this valuable tool for any organization that wants to improve its cybersecurity posture.

The C2M2 is aligned with internationally recognized cyber standards and best practices.

4.10 BENEFITS

In summary, the benefits of using the C2M2:

- Identify and prioritize cybersecurity risks.
- With a roadmap for improving cybersecurity capabilities.
- Measure their progress over time.
- Align cybersecurity with business objectives.
- Comply with cybersecurity regulations.

For more about the C2M2, you can visit the website: https://c2m2.doe.gov/ . The website provides a wealth of information about the model, including the model documentation, case studies, and resources for implementation.

MODULE 5:
META-COGNITION, ETHICAL DECISION MAKING, ETHICAL THEORIES

Meta-cognition in the context of ethical decision making as is the conscious awareness and control of one's thinking processes. It involves thinking about thinking, understanding how you learn, and making adjustments to improve learning outcomes. It's the foundation for effective study skills and problem-solving, allowing individuals to adapt their strategies and monitor their own comprehension and learning progress.

Ethical decision-making is the process of evaluating and choosing between moral dilemmas. It's a vital skill for IT professionals facing complex ethical choices. This process involves considering the ethical principles and values that guide one's actions, as well as the consequences of those actions on individuals and society. Ethical decision-making helps individuals navigate difficult moral issues with integrity and responsibility.

Ethical theories provide structured frameworks for understanding what is morally right or wrong. These theories offer different approaches to evaluating ethical questions. Understanding these ethical theories enables individuals to engage in informed ethical debates and make well-reasoned moral judgments. Each theory offers unique perspectives on how to address ethical dilemmas and make principled decisions.

5.1 HOW DO WE DEFINE ETHICS?

Ethics is the general name for the branch of moral philosophy that deals with behaviour that increases people’s well-being. Ethics in the context of this book is therefore about how technologists should behave to increase people’s well-being. Ethics is not about religion or being slavishly law-abiding, nor is it about going along with the majority view held by the people around you. Ethics is having your own moral compass.

Technology is ethical when it helps people reach their fullest potential; when it improves their quality of life, makes them happier and more fulfilled, and gives them the freedom to choose what they want to be. We consider the interests of people living here and now, but also the interests of future generations, other living creatures, and the preservation of the environment.

Technology is unethical when it dehumanises; when it makes a person less human than they were. It forces people to engage in behaviour that diminishes them or the environment in some way or creates a problem for future generations. Simply put, ethics is a guide to how to live well, how to be in the world in a way that creates benefit and minimises harm.

WHY DO WE NEED ETHICS?

Ethics allows us to live in harmony and cooperation with others. When people are ethical, we can trust one another. We can build communities and organisations that can achieve outcomes that a single, self-interested individual would be incapable of.

Without ethics, we would lack loyalty and be unable to trust others and form cooperative communities of interest. Long-term relationships would be difficult if not impossible. We could not have the economies that now exist in the developed world where wealth and a high standard of living are enjoyed by most. Life without ethics would likely be nasty, short, and brutish.

LEVELS OF ETHICS

Ethics or right behaviour has three broad levels of application:

Personal ethics guide how you live, what you do, and how you interact with others. It helps you to develop a sense of personal responsibility by making you think, both before and after you act. It considers how your behaviour impacts on others. As a rational being with free will, you choose how you behave on a day-to-day basis with full awareness of the consequences of your actions.

Organisational ethics is an aspect of organisational culture. It is how the organisation behaves and how it interacts with people. This level of ethics has explicit and implicit components. The explicit is clearly stated by management, written down and understood to be 'correct' behaviour. The implicit is not written down but is nonetheless understood to be the 'way things are done'.

As with personal ethics, this middle level should cultivate a sense of responsibility for how the organisation's actions impact on the world.

System ethics is concerned with how the overall economic and social systems behave, how it interacts with people. Ethics at the system level is codified into laws and codes of acceptable conduct; cultural practices that by consensus are widely understood and practices. As with the previous two levels, systems ethics cultivates a sense of responsibility for how the system impacts on the world in general. System ethics tries to create a system that best serves the interests of the greatest number of people.

As a citizen, you have a right to vote and to have your voice heard. You are free to argue for a more humane society.

VALUES & ETHICS

Values feed into ethics in four broad ways; (a) how to get along with each other, (b) what is a 'good life', (c) what are our obligations to each other, and (d) what are my rights?

If ethics is about behaviour, values are about what you believe to be important, and what you would like to see more of by means of more ethical behaviour.

For example, in western-style democracies, values are codified into 'rights'. Freedom of speech, freedom of religious worship, the pursuit of happiness and many other values are all considered to be our birth right as human beings.

Values come *before* ethics. The ethical standards of a society will reflect these pre-existing values. Values come from many sources; one's family, the media, religion, the community, one's education and life experiences.

Values change over time with the evolution of societies and culture. While it is true that much of our value system is created through our childhood experiences, they can nonetheless be changed through a process of conscious self-reflection and external influences.

ROLES & ETHICS

The *roles* we play have a strong determining effect on our ethics and on our behaviour generally. A role is simply a set of relationship responsibilities and expectations that we have adopted either voluntarily, or because they have been placed upon us through circumstance.

The first experience of roles for many is within the early environment where a child has a role in relation to their parent(s) or carers. Later we adopt a variety of roles by choice; we choose to get married, have children, and enter an occupation or profession. We might join a faith community and attend worship. We might become a volunteer for a worthy cause, or indeed any number of possible roles.

Each role has a set of responsibilities and expectations that belong to it and which we must fulfil if we are not be sanctioned in some way. Roles can come into conflict with each other, for example a member of a religious community might find a role conflict if s/he were to perform military service.

The obligations that go along with a role can form the basis of ethical conduct for that person.

5.2 ETHICS IS META-CONSCIOUSNESS

Ethics is the general name for the branch of moral philosophy that deals with behaviour that increases people's well-being. Ethics in the context of this book is therefore about how technologists should behave to increase people's well-being. Ethics is not about religion or being slavishly law-abiding, nor is it about going along with the majority view held by the people around you. Ethics is having your own moral compass.

Meta-cognition involves actively engaging the recently evolved parts of the brain, the places where higher, rational thought occurs, the place where you can recognise the causal links.

This state of mind contrasts with the semi-conscious autopilot that people commonly use as their default setting. Reacting to situations in a habit-driven, stimulus-response manner based on prior learning. Conditioned responses to specific situations have been acquired over time from social learning. Thus, a poorly programmed autopilot is why people continue to make the same mistakes time and again. Meta-cognition is the only remedy to lift oneself out of this semi-conscious mode into a fully conscious state where a person responds to situations in a rational way that is based on the needs of the situation at hand.

This rational, meta-cognitive ability is what sets humans apart from intelligent animals. The neural infrastructure of the evolved human brain is said by neuroscience to be the most complex biological structure ever to have existed on this planet. Our brains and the abstract thinking that it is capable of is what has made humanity the most adaptable creature living on this planet.

5.3 CODES OF ETHICAL CONDUCT

Computer societies are working towards *licensing* its members so that like doctors, lawyers, teachers, accountants and other professions, it is not lawful to work unless you are licensed. To be licensed, a practitioner must have completed an approved study program that includes instruction on professional ethics. They must agree to abide by the code of conduct.

This chapter presents typical code of conduct, based on the Australian Computer Society's (ACS) code. This code is used since The *Ethical Technologist* is the textbook used in an ethics course at an Australian university. We might just as well have a code from North America, the United Kingdom, Japan, Germany, France or any country in the developed world. The underlying code is the same.

The ACS Code is summarised into six core ethical values that it expects its members to always practice in their professional life (source ACS):

1. **The Primacy of the Public Interest**. You will place the interests of the public above those of personal, business or sectional interests.
2. **The Enhancement of Quality of Life**. You will strive to enhance the quality of life of those affected by your work.
3. **Honesty**. You will be honest in your representation of skills, knowledge, services and products.
4. **Competence**. You will work competently and diligently for your stakeholders.
5. **Professional Development**. You will enhance your own professional development, and that of your staff.

6. **Professionalism**. You will enhance the integrity of the ACS and the respect of its members for each other.

THE PRIMACY OF THE PUBLIC INTEREST

The term 'Primacy' indicates that this is the core ethical value that takes precedence over any personal, private, or sectional interests that you might have. Where a conflict exists, it must be resolved in favour of the public interest. There is no room for self-interest, looking after 'number one'.

As you go about your work, you act in the interests of your employer so long as this does not conflict with your duty to the public interest. This means that you should not be developing technology that will adversely affect public health, public safety and the natural or built environment.

You identify those who will be impacted by your work and actively consider their interests to avoid harming them.

If you become aware of conflicts between your professional work and any legal or social factors, you work with the stakeholders to resolve the conflict before the problem becomes more serious. These can include problems the stakeholder(s) might have with what you are doing, or any conscientious objections you yourself might have.

Your duty to the public interest includes preserving the integrity and public image of the profession, respect for other people's intellectual property and for the confidentiality of any information that might come into your possession.

THE ENHANCEMENT OF QUALITY OF LIFE

Information and Communication Technology (ICT) has the potential to create both harm and benefit. The ethical technologist considers the impact that technology has on society and individuals and actively works to minimise the negative effects while maximising the positive.

The ethical technologist cultivates an equity of access attitude that gives the under-privileged members of society the same access that the more privileged already have.

As an ethical technologist, you develop an awareness of the many ways that ICT can enhance people's quality of life, particularly those less advantaged people in society and the world generally (for example in the developing world).

The technology you develop should promote the health and safety of the people who use it or are affected by it. At the very least it should not harm anyone.

At a more abstract level, the use of technology should create a positive perception and a deeper sense of personal satisfaction in people. It should help people

become a fuller expression of their human potential by allowing them to do what they were previously unable to do, and which gives them great satisfaction to do.

This core ethical value is an extension of the Public Interest value discussed in the previous section.

HONESTY

It is imperative that you do nothing to undermine public trust in the profession, or the trust of the stakeholders in a situation (i.e., your employer, the users etc.). Trust is a valuable but fragile commodity. It requires much time and effort to build, and yet it can be destroyed the moment deception is detected.

Trust can only be maintained in the long-term by being consistently honest in your dealings with people. You must be perceived as a person who can be relied upon to act with integrity, someone who avoids deception even when there is little risk of discovery.

As an ethical technologist, you therefore avoid offering or receiving inducements (favours, bribes, gratuities) or place yourself in a position where you can be coerced. Any situation intended to bring favour to one stakeholder at the expense of another.

Neither shall you mislead anyone as to the suitability of a product or service. You keep your professional life separate from your personal or sectional interests. It is not uncommon for IT practitioners to act as agents for a commercial organisation without disclosing that conflict of interest to their employer or customer.

Any estimates you give will be accurate and unbiased, you qualify a professional opinion that is based on limited expertise, you give credit where credit is due for the work of others, nor do you attempt to build your own reputation at the expense of other(s).

COMPETENCE

Given the complex nature of technology as a global industry, no single technologist can possibly know everything about everything. Yet it is common for IT practitioners to pretend to know more than they do and knowingly accept work that they are unqualified to perform. This is done on the assumption that they can learn the required skill at short notice or as they go along. In this they are little more than a trainee masquerading as a competent professional. It is a practice commonly seen when people “pad their CV’s” with skills they do not possess.

The client has a right to know that the technologist they engage is competent to perform the work, so as an ethical technologist you only accept work that you know you are competent to perform and avoid over-stating your skills and capabilities.

You deliver products and services that meet your clients' operational needs and respect their proprietary interests. If you are aware of issues in relation to a project that are not in the clients' interests, you make the client aware of these issues even if it might be in your personal interests to say nothing (for example, allowing you to stay employed on a project for longer).

Competency also means taking responsibility for your work, avoiding putting the blame on others when things go wrong.

PROFESSIONAL DEVELOPMENT

In the age of exponentially advancing technology, finding the tie to stay up to date in your field can be a major challenge. It is tempting to let recent developments slip by when you realise that the work you did to learn the latest technology not so long ago is now redundant. The instinct we all must conserve energy suggests 'don't bother'. You must resist this 'economy of effort' mind-set, it is a major contributing factor to the burn-out and cynicism of mid and late-career members of the profession.

Professional development for the ethical technologist means taking the time and making the effort to not only stay abreast of the latest developments, but also to pass on your knowledge and experience to colleagues, particularly those in more junior roles. In the spirit of win-win, you understand that by helping others advance, you are ultimately benefiting everyone, including yourself. Win-win thinking benefits the profession.

So, the ethical technologist makes it their business to acquaint themselves with the technological issues having impact on the world, they encourage their colleagues and subordinates to do the same, and support educational initiatives aimed at the professional development of themselves and others.

PROFESSIONALISM

The computer industry, while global, is relatively new and does not yet have an established set of ethical standards. It takes time for the profession to mature. As an ethical technologist, you can help to establish these standards by always being professional and so improving the perception and image of the profession in the eyes of the public. The challenge is to build public confidence in the profession, particularly in the workplace.

The public has mixed feelings about computer technology; on the one hand they enjoy the convenience that it affords them, but on the other they do not understand it and sometimes fear that it might do them harm.

To dispel this fear, the ethical technologist takes a calm, objective and well-informed approach to their professional work.

As an ethical technologist, you encourage other practitioners to behave in accordance with the code and do nothing to tarnish the image of the profession. This includes ensuring that properly qualified people are not excluded from employment through unfair discrimination.

You also do what you can to extend public knowledge and appreciation of ICT, taking pride in being an IT professional.

A FINAL WORD

Professional societies around the world provide real assistance to practitioners in time of need. The excerpt below is from the Australian Computer Society, though every society will be offering the same service, should you need it:

'All people have a right to be treated with dignity and respect. Discrimination is unprofessional behaviour, as is any form of harassment. Members should be aware that the ACS can help them resolve ethical dilemmas. It can also provide support for taking appropriate action, including whistleblowing, if you discover an ACS member engaging in unethical behaviour'.

For more detail, visit: www.acs.org.au or the equivalent society in your country.

5.4 ETHICAL DECISION MODEL (EDM)

For the purpose of resolving ethical dilemmas, we define a *dilemma as a complex problem for which there is no obvious solution*. A solution exists but is obscured by the complexity. Common sense would suggest that the best way to deal with a complex problem is to *simplify* it. You can do this by breaking it down into more comprehensible pieces.

Here we outline the *Ethical Decision Model* (EDM), a general-purpose model for analysing complex situations in a range of domains including IT. It helps you to reveal optimal solution(s), ones that might be described as ethical, and be defended as such.

Appendix A is an example of how the EDM can be applied to an IT-related case study. The solutions in the example are indicative, not definitive.

The model has three main stages: *analysis, prioritisation, decision*.

1. **Analysis** is getting the facts and categorising them into *extrinsic* factors (legal, professional, employment, social, personal) and *intrinsic* (a person's individual attributes).
2. **Prioritisation** involves ranking the elements into order of importance by means of a priority table.
3. A **Decision** is made by rationally weighing up the relative importance of the elements.

No two people who approach a complex situation will perceive the various factors the same. Their perceptions are filtered through the lens of their personal experience and intrinsic leanings. The precise nature of what reaches their cognitive centre will be different for every person and might even differ for the same person on different occasions.

Applying the defined process of the EDM helps to remove the subjectivity from the situation and gives us an objective, process-based approach to the solving of ethical dilemmas.

STEP 1: ANALYSIS

In preparing for the ethical analysis, there are some questions that you should ask:

- *What are the relevant facts of this case?*
- *What do we know, what do we not know that we need to know before deciding?*
- *Who are the stakeholders?*
- *Is this a legal matter for which a prescribed course of action already exists?*

Every effort must be made to obtain satisfactory answers to these questions before proceeding.

It is the nature of ethical dilemmas that they are a complex mix of factors for which there is no obvious solution. Maybe there are two or more obligations that conflict with each other, or the outcomes of anything you do will be undesirable, or even that the cost of doing the right thing is too high.

The factors that comprise a given situation can be broadly categorised as *Extrinsic* and *Intrinsic*; those that exist in the outside world, and those that exist within the individual. The Extrinsic factors include Legal, Professional, Employment, Social and Personal. The Intrinsic factors have been grouped together under a single heading.

Extrinsic factors

1. ***Legal*** factors take precedence over the others since breaking the law will get you into serious trouble, even loss of liberty. There will be no conflict between Legal and Professional factors since professional bodies are in the business of creating a solid, respectable public image for its members and will never advocate acting illegally.
2. ***Professional*** factors are the obligations you have to the profession, as prescribed in their code of practice. These take precedence over the obligations you have to your employer since it is possible that your employer will ask or demand that you do something unprofessional (unethical) in the profitability interests of the employer. Many dilemmas stem from this source.
3. ***Employment*** factors. Most employers have their own code of ethical conduct, as prescribed in their mission statement and other documents that define the values of the organisation. This code sets standards of ethical conduct. These will be generally compatible with the legal, professional and social standards, since no organisation, particularly commercial ones, will want to be seen as deviating from the standards of society. There will be some exceptions to this in the case of organisations on the periphery of society, ones that do not share its mainstream ideals, one's with an extreme political agenda.
4. ***Social*** *Factors.* The society in which the employer operates will have its inherent standards that are reinforced by the family, at school, in the community generally and in the media and other institutions. All the ways a society communicates with itself. Society is complex, so standards will not always be unanimously agreed upon. Some members of society will agree, and others disagree on the rightness of various issues. We see this often in polarised political debate. Legal, professional and employment factors take precedence over social factors where there is disagreement.
5. ***Personal*** factors include those aspects of your make-up that psychologists categorise as coming from the 'Nurture' side of the 'Nature-Nurture' theory (of what makes us what we are). These are the factors that you acquire from the environment, your family, close friends and associates, your peer group, sporting association or faith community. While these are undoubtedly within you, they have their origin from outside of you. Personal factors account for much of a person's ethics, their morality. When there is variance between one's personal morality and that of the Social, Professional and Legal environments, a person will have the greatest difficulty resolving this ethical

conflict. How does one remain true to oneself and still behave ethically in a professional sense? The unpleasant truth for some is that one's professional obligations must take precedence over any personal qualms you might have about what is ethical. To be a member of a profession means to accept its standards and practice them. To act otherwise will exclude you from the profession.

Intrinsic Factors

Intrinsic factors include what psychologists categorise as the 'Nature' side of 'Nature-Nurture'. It is your set of innate qualities, the behavioural disposition with which you were born, the disposition that your genetic make-up has equipped you with. People are born with differing degrees of a wide variety of personality traits. These are summed up in *The Big Five Personality Traits* which are *extraversion, agreeableness, openness, conscientiousness,* and *neuroticism*. Each trait represents a continuum. Individuals fall anywhere on the continuum for each trait. For example, with the extraversion/introversion continuum you can be anywhere on the bell curve from very extraverted to very introverted or somewhere in between. The Big Five remain relatively stable throughout most of one's lifetime.

So, people's *Nature* can vary widely within the broad definition of being human. This is a complex area well beyond the scope of this chapter and this book. In addition to The Big Five, you might also google the Myers-Briggs personality profile to learn more on this fascinating subject.

Jonathan Haidt's Moral Foundation Theory. On a more general level, Haidt's Moral Foundation Theory suggests that there are six innate moral foundations that all humans are born with, the innate moral code that we all share:

- *Care/harm,*
- *Fairness/cheating,*
- *Liberty/ oppression,*
- *Loyalty/betrayal,*
- *Authority/subversion, and*
- *Sanctity/degradation* (discussed in later chapter).

Personal factors (previous section) and intrinsic attributes often exert the strongest yet most idiosyncratic influence on the process of ethical decision-making. While this is a potential problem, someone with the kind of personal and intrinsic attributes that makes them uncomfortable with what is generally accepted for an IT developer is unlikely to last long working in this capacity.

Applying the analysis to an example. Consider the case of the market research company that collects demographic information from the broader community and sells contact lists to interested parties who want to do targeted direct marketing.

The market research company obtains people's informed consent to collect and store this information. But now the company changes hands and the new owner

wants to increase profits. The owner instructs their web programmers to implement deceptive strategies aimed at gathering information for which they have no informed consent. This instruction contravenes privacy legislation, and the professional code of conduct. It is also contrary to community expectations on privacy. In this instance, when we prioritise the factors, it is clear what the developers should do – refuse to comply, even at the risk of losing their job.

For example, if the new owner agreed to supply a gay hate group with the names and addresses of people known to have an interest in gay culture. While it is clearly wrong from a legal, professional, and social perspective, if an IT developer working there is intrinsically homophobic, their disposition will influence their thinking on whether it is right to supply the names. The developer may well perceive this as an ethical dilemma, when the developer sitting in the next cubicle clearly sees it as a wrong act.

STEP 2: PRIORITISATION

Prioritisation is most easily performed by the making of a list that shows each factor in descending order of importance. It can be helpful to include a column that outlines related matters beside each factor. This has the same common-sense value as the Ben Franklin decision-making method of listing Pro's and Con's on a sheet of paper with a single vertical line drawn down the middle. The format with the EDM is somewhat different, but the principle is the same.

As a rule, the Legal and Professional factors take precedence since there is an obligation on everyone to abide by the law with no exceptions. This is a long-standing principle that was established for the benefit of the greatest number. The rule recognises personal freedom but says that there is a point where personal freedom ends and the public interest begins. A person can have their personal freedom curtailed by society if it is believed that such freedom is not in the public interest or the greater good.

Related to the obligation to abide by the law is the obligation to know the rules laid down by law. Ignorance of the law is not a defence in court for breaking the law.

Within the legal framework that governs society we have the various professions, medicine, law, accounting for example. All professions have a *Code of Professional Conduct.* It is always incumbent upon members to know it and practice it. Membership of that profession is conditional on a sincere undertaking that as a member you will do your utmost to follow the code.

Codes of Professional Conduct have relevance to professional standards legislation that exists in many jurisdictions. Breaches of the Code can be used as grounds for a claim of professional negligence. In legal proceedings, the Code can be quoted by an expert witness giving an assessment of professional conduct.

The Australian Computer Society's code of ethics can be summarised as follows; *always act in the public interest, your work should enhance people's quality of life, you should be honest, hard-working, competent and stay current with the latest developments, and finally do what you can to enhance the reputation of the profession*. If a conflict occurs between these values, the deciding factor is what is in the public interest, otherwise known as the 'greater good'.

Codes of conduct of professional computer societies in other countries will not be much different. The way in which they are expressed may be outwardly different but the essential, underlying meaning will be similar.

Codes of professional conduct and the larger laws of society are certain to be consistent with each other. For example, the first item in the ACS code clearly states that you should always act in accordance with the public interest, which by default is governed by law. Professional groups will never advocate behaviour that even hints at being unlawful or not consistent with the values of the society in which it operates. They want to establish a respectable place for themselves in society.

Social factors will also be broadly consistent with legal and professional factors. There is room for disagreement here because as society evolves, its values change, but the law, which is inherently conservative, does not change as quickly. There may be some gap between the two, with the legal taking precedence over the social. The process of law reform will take its course in time and the law will come to reflect community values.

Professional codes maintain a safe legal position. Extended debate within professional forums will perform the same role as the law reform bodies in larger society.

Prioritising the factors inherent in a situation should always have the legal, professional, and social factors at the top of the list. Most likely to conflict with these are *Work* factors. The goals, policies and culture of an organisation are at the discretion of the owners who may well perceive their first responsibility as being to their own financial interests and those of the shareholders. It is not being overly cynical to suggest that some business owners are more concerned with the question of whether they will get caught, not whether something is legal. Beyond the question of being caught, there is also the issue of how likely it is the state will prosecute, given that the law lags the pace of technological change. And given the expense of legal proceedings, Prosecutors will usually only pursue cases of significance that are likely to result in a conviction.

A commercial organisation's reason to exist is to make a profit or at least to survive and continue to trade. Despite outward appearances, many companies operate on the verge of collapse, delaying payment of their debts for as long as possible while trying to extract payment from debtors as quickly as possible. In desperate circumstances even a normally honest business owner has been known

to resort to unethical if not illegal strategies if they can get away with it. Most organisations are honest and ethical, but it is not difficult to see how a technologist working in *some* organisations are going to find themselves told to do 'questionable' things.

STEP 3: DECISION

Having drawn up a prioritised list that shows each factor in order of importance, you are now able to decide, based on rational choice, what will be the most ethical course of action.

In deciding, you might take into consideration which course of action*: does the most good or the least harm, respects stakeholder rights, treats people justly, best serves the public interest (not just some members), and which allows me to be the best kind of person I can be?*

If called upon, you should be able to make a strong argument, citing evidence as to why you chose as you did. Imagine that you have been called to explain yourself to the board of directors, or the ethics committee of a professional society or even the police/prosecutor. Your case should be strong enough that you could deliver it with confidence and a clear conscience.

5.5 THEORIES OF ETHICAL BEHAVIOUR

This section summarises the major philosophical theories that have bearing on ethics, the branch of philosophy that deals with morality. The list is a representative sample, not exhaustive. This level of detail is appropriate for a discussion on ethics in IT. For balance, the list covers both the philosophies of the West, starting with the classical Greeks, and then those of the East, including Buddhist, Confucist and Taoist philosophies. It should be noted that Buddhism, Confucism and Taoism are rightly called philosophies not religions since they concern themselves with how to think and behave correctly and recognize no deity. These Eastern philosophies are a kind of applied psychology which might explain their popularity in contemporary Western culture.

Each philosophy is useful, yet none are complete all the time in every situation. No one philosophy can be all things to all people. Therefore, the rational course of action is to consider them together and look for underlying common factors that may be present. We make allowances for superficial differences in the way they are expressed, since each is a product of the culture that created it.

Some discretion and judgment are required to know how best to apply them. As you will see, they can contradict each other, for example moral relativism and universalism. On the one hand Relativism says that right action is determined by circumstances, while Universalism says that right action is determined by principle, regardless of circumstance.

RELATIVISM

Relativism holds that moral or ethical propositions do not reflect objective and/or universal moral truths, but instead make claims relative to social, cultural, historical or personal circumstances. Right action is determined on a case-by-case basis, being dependent on who is involved and a host of situational factors.

Relativism is differentiated into *subjective* and *cultural* relativism.

SUBJECTIVE RELATIVISM

A personal and subjective moral core lies or ought to lie at the foundation of a person's moral acts. This is essentially an inward-looking approach to morality, with each person being their own ultimate authority on what is right action.

In the subjective view, public morality is merely a reflection of social convention. Only personal, subjective morality expresses true authenticity. The French philosopher Jean-Paul Sartre is a foremost exponent of this approach to morality.

CULTURAL RELATIVISM

In contrast to the subjective approach, in Cultural Relativism a person's beliefs and activities are understood in the context of his or her culture. Right action is

defined by cultural convention and exists as a commonly understood principle in that culture.

Since morality varies from culture to culture, with each culture having an equal claim as to what constitutes right action. This approach to morality grew out of the work of anthropologist Franz Boaz in the early 20th century. Anthropologists, if they are to properly understand a culture must not impose moral judgments on their practices even if they differ from the anthropologist's own cultural beliefs.

A criticism of both subjective and cultural relativism is that they differ fundamentally and take no account of the other. Arguably, both approaches have merit, and both deserve to be recognised, but not to the exclusion of the other. A blended approach that could simply be called Relativism is proposed, which takes both subjective and objective factors into account and tries to reconcile them. This would lead to a more balanced understanding of a given situation.

KANTIANISM

Immanuel Kant (1724–1804) was a notable German philosopher who argued with good reason that morality be based on a standard of rationality that he dubbed the *Categorical Imperative* (CI). Immorality is therefore a violation of the CI and is irrational.

The importance of being rational is a consistent theme in Western philosophy. The Stoic philosophers of classical Greece emphasises the use of logic and rationality to overcome the tendency to act emotionally and irrationally.

Kant's position can be summed in his categorical imperatives which form the foundation of his work.

Categorical Imperative (First Formulation): Act only according to that maxim whereby you can at the same time will that it should become a universal law. Ask yourself, *if I do this, would be all right if everyone did it?*

Categorical Imperative (Second Formulation): Act so that you always treat both yourself and other people as ends in themselves, and never only to an end. Ask yourself, *am I exploiting someone to get what I want?*

The first formulation is the foundation of the *Universalist* view of morality that if something is right, then it is always right, all the time. To make a special case exception is little more than a sense of selfish entitlement.

The second formulation lies at the heart of much of what the Ethical Technologist is about; the importance of helping people to come to a fuller expression of their potential. This position maintains that whatever you do must not harm other people or diminish them by treating them to an end.

Kant's theory belongs to the broader category of non-Consequentialist theories that determines whether an action is right or wrong by considering the underlying

rule or principle that motivates the action. Social Contract theory is another member of this category.

UTILITARIANISM

Utilitarianism asserts that moral behaviour is that which promotes happiness or pleasure; that which creates the greatest good and/or does the least harm.

A wrong act is one which produces unhappiness or suffering. The degree of 'wrongness' is determined by how much harm the act has caused. Therefore, the guiding principle in Utilitarianism is to do the thing that brings the greatest good to the greatest number.

Utilitarianism is sometimes known as a Consequentialist approach; if the outcome or consequence of an act is good, then the act itself is good. It is often used in the world of business and politics to achieve desired ends, sometimes incurring damage along the way. *The ends justify the means.* Though, the ends do *not* justify the means if significant harm is caused by doing so.

ACT UTILITARIANISM

With Act-utilitarianism the principle of utility is applied directly to each alternative act in a situation of choice. The right act is defined as the one which brings about the best results, or the least amount of harm.

Criticisms of this viewpoint to the difficulty of having full knowledge of the consequences of our actions.

Act-utilitarianism has been used to justify barbaric acts, for example suppose you could end a war by torturing children whose fathers are enemy soldiers to find out where the fathers are hiding.

Act utilitarianism is supremely pragmatic as it confines itself to a simple moral calculus; for example, if I can save 10,000 lives by killing one innocent person, the killing is a moral act.

RULE UTILITARIANISM

With Rule-utilitarianism the principle of utility is used to determine the validity of the *rules* of conduct, the moral principles that underlie.

For example, if we have a rule about keeping promises, it is because we have considered what the world would be like if people broke promises when they feel like it, compared with a world where people keep their promises. Moral behaviour is therefore defined by whether we follow the rules.

There are limits to how far Rule utilitarianism can be applied. When more and more exceptions to the rule are applied, it collapses into Act utilitarianism.

More general criticisms of this view argue that it is possible to generate *unjust rules* by resorting to the principle of utility. For example, slavery in ancient Greece might have been right if it led to an overall achievement of cultivated happiness at the expense of some mistreated individuals.

SOCIAL CONTRACT THEORY

Philosopher Thomas Hobbes argued that everybody living in a civilised society has implicitly agreed to (a) establish a set of moral rules to govern relations among citizens, and (b) establish a government capable of enforcing these rules. This is called the social contract.

In practical terms, Social Contract theory might also be construed to be a kind of reciprocal social obligation, society to the individual, and the individual to society. When individuals live in a society and enjoy the benefits of doing so (a place to live, meaningful work, the chance to raise a family in safety and so on), they have a reciprocal obligation to contribute to that society in whatever way they are best able to do. A person who takes and refuses to give according to their ability is little more than a parasite.

Social Contract theory belongs to the broader category of non-Consequentialist theories that determines whether an action is right or wrong by considering the underlying rule or principle motivating the action. Kant's theory is another member of this category.

MARCUS AURELIUS AND THE STOICS

Marcus Aurelius (full name Marcus Aurelius Antoninus Augustus, 121 – 180 AD) was an exceedingly rare individual; a genuine philosopher-king. His leadership is based on the often-misunderstood Stoic philosophy. The power and relevance of this philosophy is as potent today as it was when he was Roman Emperor (161 to 180AD).

Marcus Aurelius might have been a Roman, but his thinking had been shaped by the classical period of ancient Greece. Even today, classical Greek thinking is still at the foundations of Western civilisation.

Influenced by the earlier work of Socrates and Diogenes of Sinope, the Stoic school of philosophy was founded around 300 BC by Zeno of Citium. Speaking from beneath a painted portico (*Stoa Poikilē*) in Athens, signifying openness to anyone passing by Zeno taught that a wise person should not allow their emotions to rule them; instead, they should master their emotions and use logic to think rationally about how to behave in life. He urged his followers to carefully study the laws of Nature and to live in harmony with them. In this respect his ideas coincide with those of far distant Lao Tzu, the ancient Chinese philosopher who wrote the Tao Te Ching.

A central point in Stoic philosophy is the active relationship between the laws of Nature that rule the Cosmos, and human free will. A wise person derives maximum benefit and happiness in life by bringing his or her will into harmony with Nature. They come to know themselves, recognising that their inner nature (microcosm) is a representation of the outer macrocosm, or universe; it the same nature in both, only differing in scale.

Stoics conceived of the universe as being governed by Logos, what we today would think of as the Laws of Physics. Pure, abstract, these laws pervade the universe and make it behave in the way it does. The same informing principle resides in humans. Virtue is therefore gained by recognising this and working to harmonise one's inner self with the qualitatively similar outer world.

The Greek founders of Stoicism conceived of three interrelated elements that collectively make Philosophy. These are *logic, physics,* and *ethics*. Logic allows us to recognise truth when we see it, and to avoid making mistakes. Logic allows us to understand Physics, which is the way the world operates, the laws of Nature. Together, Logic and Physics allows us to practice Ethics, or moral behaviour that brings benefit.

Ethical behaviour is that which is in harmony with the unfolding laws of Nature. This unfolding is the cause of both pleasure and suffering in people. If we are to stay in accord with it, we must discipline our minds to become indifferent to suffering, accepting with grace that it is necessary and inevitable to suffer sometimes. This state of mind is called *apatheia*. Likewise, we must not become so attached to pleasure that we cannot relinquish it when it passes. The goal is to become self-sufficient, or *autarcheia*.

The Stoic therefore becomes equally indifferent to good fortune or bad, whether they are rich or poor, well-respected or despised. They understand that the approval or disapproval of others can exert undue influence to conform to values that may not be true. The Stoic does his or her duty in accordance with Nature as revealed by careful observation and logical enquiry. They do their duty regardless of whether it is easy or hard.

With its emphasis on duty and right action, Stoicism is therefore well-suited to the needs of those who would lead. It was used as a guide by the ruling class of Rome for centuries.

BUDDHISM & THE FOUR NOBLE TRUTHS

About the same time as the classical Greek philosophers were formulating their ideas a revolution in thought was taking place in northern India. Siddhartha Gautama, the man who would become the Buddha, or Awakened One, was formulating some ideas of his own. It is remarkable how similar in structure and meaning the philosophies of East and West at this time were. It is almost as if it was a good idea whose time had come to be brought into the world.

Buddhism is thought by many to be a religion, yet it recognizes no deity. In its basic form is an applied psychology expressed in the language of the time. It outlined a formula for how to become self-actualized. The foundation of Buddhist philosophy is the so-called Four Noble Truths and the Noble Eight-Fold Path. The eight-fold path aims to improve your (a) *Wisdom* by practicing right view and intention, (b) *Ethical conduct* by practicing right speech, action and livelihood, and (c) *Mental capabilities* by practicing right effort, mindfulness and concentration. We shall examine more closely the three aspects of ethical conduct.

RIGHT SPEECH

Words are powerful. Words can make or break a person's life, start wars or bring peace. Words can indeed be mightier than the sword, as great orators through the ages have proven. Right speech (including written words) is therefore the principle of expressing oneself in a way that enhances the quality of people's lives and does no harm. It means to refrain from (a) lies and deceit, (b) malicious language (including slander), (c) angry or offensive language, and (d) idle chit-chat (including gossip). Notice the correspondence between this principle and the prime ethical value in the ACS code of conduct to act in ways that improves people's quality of life.

Therefore, tell the truth, speak with warm gentleness when you do speak, and refrain from speaking when you have nothing important to say.

RIGHT ACTION

Right action can be defined open-endedly by prescribing what a person should *not* do. That then leaves the field wide open for choice. Broadly, right action means refraining from (a) harming any sentient creature, (b) stealing, and (c) sexual misconduct. Doing no harm to others covers a very broad range of behaviours. The worst a person can do is to take the life of sentient creatures, hence many Buddhists are vegetarians. Not stealing includes all forms of robbery, theft, deceit and fraud; essentially taking what you have not earned the right to have.

The ethical person is therefore kind and compassionate in their dealings with the world. They respect other people's property, and do not engage in sexual behaviour that harms another either at a physical or emotional level.

RIGHT LIVELIHOOD

Right livelihood is about earning one's living in ways that does no harm to others. Of all the possible ways a person might earn money, they should avoid those that exploit people's weaknesses.

Right livelihood means one should refrain from any employment that is contrary to the principles of right action and right speech, including but not limited to (a) trading in weapons, (b) trading in living beings, including slavery, prostitution and raising animals for slaughter, (c) butchery and meat processing, and (d) trading in drugs and poisons, including alcohol and recreational drugs.

LAO TZU & THE TAO TE CHING

The *Tao Te Ching* is said to have been written by Lao Tzu (604 – 531 BCE), the philosopher and Custodian of the Imperial Archives in the time of the Chou Dynasty in ancient China. It is uncertain when Lao Tzu was born or died, but he is said to be a contemporary of Confucius (551–479 BCE).

Central to Taoist philosophy is the avoidance of extremes, to always seek the middle way on our journey through life. Find the middle ground between the extremes and occupy that space and in doing so have the fewest consequences to deal with. The principle at work here is that extreme action always results in an equal and opposite reaction. As a pendulum swings to one extreme, it will always swing to the other extreme in equal measure. Following the middle path reduces the "swing" to a minimum. Only through this practice can harmony in society be achieved.

We are encouraged to sense the world around us directly and to contemplate our impressions deeply. It advises against relying on the structures and belief systems that have been created by others and put forward as orthodox truth. Such ideologies remove us from a *direct* experience of life and effectively cut us off from our intuition.

The middle path requires us to develop an awareness of the physical forces that shape our world. Such forces operate uniformly at all levels from the largest to the smallest. They operate in the universe as a whole and in the minds and lives of individual people. An understanding of these natural laws and the forces they direct give us the power to influence events in the world without force. Influence is achieved through guiding rather than coercion. The objective is always to avoid taking action that will elicit strong counter-reactions. In Nature, an excessive force in a particular direction always triggers the growth of an opposing force, and therefore the use of force cannot be the basis for establishing an enduring social condition.

We come to understand that everything in the universe is impermanent, in a state of change. The emotional and intellectual structures that we build for ourselves to feel secure are likewise subject to change by external forces that are largely beyond our control. The challenge is to accept the inevitability of change and not waste our energy trying to prop up these impermanent structures, defending them against criticisms, and trying to convince others to believe in them so that they might become recognised as permanent truth.

Lao Tzu wrote the Tao Te Ching from the point of view of the "superior man", the person who is transcending their base nature by consciously improving their lives through wise choices.

THE ETHICS OF CONFUCIUS

Confucius (551 BC – 479 BC) established a system of personal and governmental morality that has endured for 2,500 years. It concerns itself with correctness in

social relations during a time of great disturbance. The work of Confucius and Lao Tzu are both aimed at achieving social harmony and coherence to remedy the rampant chaos of the times.

Three key principles are emphasized in Confucius' teachings: the principles of *Li, Jen* and *Chun-Tzu*.

The term *Li* has several meanings; it is often translated as propriety, reverence, courtesy, ritual or ideal conduct. It is what Confucius believed to be the ideal standard of religious, moral, and social conduct.

The second principal *Jen* is the fundamental virtue of Confucian teaching, the virtue of goodness and benevolence. It is expressed through recognition of value and concern for others, no matter their rank or class. Jen is summarised as the Silver Rule: *Do not do to others what you would not like them to do to you*. (Analects 15:23) Li provides the structure for social interaction. Jen makes it a moral system.

The third principle, *Chun-Tzu* describes the idea of the true gentleman (should not be seen as gender-specific). This is the person who lives according to the highest ethical standards. The gentleman displays five virtues: *self-respect, generosity, sincerity, persistence*, and *benevolence*.

As a son, he is always loyal; as a father, he is just and kind; as an official, he is loyal and faithful; as a husband, he is righteous and just; and as a friend, he is faithful and tactful. In today's world, the words *she, mother* and *wife* could be substituted for he, father and husband.

THE UNIVERSAL MORAL CODE

To identify underlying moral principles across cultures, Kent W. Keith puts forward these two lists, one expressed in '*do this*' form and the other in the '*do not do this*' form. These principles are found embedded in the moral codes of diverse cultures. The first list*, do no harm*, essentially says, whatever you do, do not do these. The list can be seen as the foundation upon which a positive set of behaviours can be based, the *do-good* list.

Do no harm. *Do not do to others what you would not like them to do to you, do not lie, do not steal, do not cheat, do not falsely accuse others, do not commit adultery, do not commit incest, do not physically or verbally abuse others, do not murder, do not destroy the natural environment upon which all life depends.*

Do good. *Do to others what you would like them to do to you, be honest and fair, be generous, be faithful to your family and friends, take care of your children when they are young, take care of your parents when they are old, take care of those who cannot take care of themselves, be kind to strangers, respect all life.*

THE GOLDEN RULE

Perhaps the most often quoted moral absolute is the so-called *Golden Rule*. Beyond the religious or even the philosophical, this principle is recognisable in Physics as Newton's second law of motion; *the mutual forces of action and reaction between two bodies are equal, opposite and collinear*. What we do elicits an equal and opposite reaction. As humans, we are not separate from the laws of Physics. If we take the position that we are not masochists and we want good things to happen to us, then we have the Golden Rule:

Christianity. Therefore, all things whatsoever ye would that men should do to you, do ye even so to them: for this is the law and the prophets. *Matthew 7:12*

Confucianism. Do not do to others what you would not like yourself. Then there will be no resentment against you, either in the family or in the state. *Analects 12:2*

Buddhism. Hurt not others in ways that you yourself would find hurtful. *Udana-Varga 5,1*

Hinduism. This is the sum of duty; do naught onto others what you would not have them do unto you. *Mahabharata 5,1517*

Islam. No one of you is a believer until he desires for his brother that which he desires for himself. *Sunnah*

Judaism. What is hateful to you, do not do to your fellowman. This is the entire Law; all the rest is commentary. *Talmud, Shabbat 3id*

Taoism. Regard your neighbour's gain as your gain, and your neighbour's loss as your own loss. *Tai Shang Kan Yin P'ien*

Zoroastrianism. That nature alone is good which refrains from doing another whatsoever is not good for itself. *Dadisten-I-dinik, 94,5*

COMPARISON OF KNIGHTS' CODES

The Japanese Samurai and the chivalric knights of medieval Europe were separated by a great distance, and likely had no contact with each other. Yet independently they arrived at noticeably similar codes of ethical conduct as seen below. Interestingly, there is correspondence with the Australian Computer Society's code of professional conduct too.

Samurai Code	Knight's Code	ACS Code of Prof Conduct
Courage	Courage	Objectivity and Independence Integrity

Loyalty	Loyalty	Confidentiality
Honor	Nobility	Subordinates Responsibility to your Client
Honesty/ Trust	Defense Justice	The Public Interest The Image of the Profession Promoting Information Technology
	Prowess Franchise / replicate	Competence Keeping Up To Date
Rectitude	Faith	Right action
Respect	Humility	Respect for stakeholders
Benevolence	Generosity	Do what is in best interests of client and public

DIGITAL ETHICS & RESPONSIBLE AI

Artificial intelligence (AI) is transforming the world in many ways, from improving health care and education to enhancing productivity and innovation. However, AI also poses significant challenges and risks, such as potential bias, discrimination, privacy breaches, security threats, and ethical dilemmas.

How can we ensure that AI is used for good and not evil? How can we design and implement AI systems that are fair, transparent, accountable, reliable, and respectful of human values?

Follow the AI Ethics Principles

Many countries and organizations have developed ethical principles or guidelines for AI, such as **Australia's 8 AI Ethics Principles**, the **IEEE's Ethically Aligned Design**, or the **Berkman Klein Centre's report on ethical principles in eight categories**. These principles provide a common framework and a shared language for understanding and addressing the ethical issues of AI. They also help to build public trust and consumer loyalty in AI-enabled services.

The principles cover various aspects of AI, such as human wellbeing, human-centred values, fairness, privacy protection and security, reliability and safety, transparency and explainability, contestability, and accountability. By following these principles and committing to ethical AI practices, you can achieve safer, more reliable and fairer outcomes for all stakeholders.

5.6. ETHICAL AI & ALGORITHMIC BIAS

ETHICAL AI & ALGORITHMIC BIAS

Artificial intelligence (AI) is a powerful technology that can enhance decision-making, optimize processes, and create new value in various domains.

However, AI also poses ethical challenges that need to be addressed by IT professionals who design, develop, deploy, or use AI systems. One of the most pressing ethical issues in AI is algorithm bias, which is a kind of error or unfairness that can arise from the use of AI.

WHAT IS ALGORITHM BIAS AND WHY DOES IT MATTER?

Algorithm bias is a situation where an AI system produces outcomes that are systematically skewed or inaccurate, often resulting in unfair or discriminatory treatment of individuals or groups based on their characteristics, such as race, gender, age, or disability. Algorithm bias can have negative impacts on human rights, such as the right to equality, privacy, dignity, and justice.

Algorithm bias can occur for several reasons, such as:

- The data used to train or test the AI system is not representative of the target population or context, leading to overfitting or underfitting.
- The algorithm design or implementation is flawed or contains hidden assumptions or preferences that favour certain outcomes or groups over others.
- The interpretation or application of the AI results is influenced by human biases or prejudices, either intentionally or unintentionally.

Some examples of algorithm bias in real-world scenarios are:

- A facial recognition system that performs poorly on people of colour, resulting in false positives or negatives that can affect security, access, or identification.
- A hiring system that screens candidates based on their resumes but excludes qualified applicants who have non-traditional backgrounds or names that indicate their ethnicity or gender.
- A credit scoring system that assigns lower scores to people who live in certain neighbourhoods or have certain occupations, affecting their access to loans or insurance.

HOW CAN IT PROFESSIONALS ADDRESS ALGORITHM BIAS?

As IT professionals who are involved in the development or use of AI systems, we have a responsibility to ensure that our AI systems are ethical and aligned with human rights principles. We can do this by following some best practices, such as:

- Conducting a thorough analysis of the data sources, algorithms, and outcomes of the AI system, and identifying potential sources and impacts of bias.
- Applying appropriate methods and tools to mitigate or reduce bias in the data collection, processing, analysis, and validation stages of the AI system.
- Implementing transparency and accountability mechanisms to explain how the AI system works, what data it uses, what assumptions it makes, and what results it produces.
- Engaging with relevant stakeholders, such as users, customers, regulators, and experts, to solicit feedback, address concerns, and ensure compliance with ethical standards and legal requirements.
- Monitoring and evaluating the performance and impact of the AI system on an ongoing basis and updating or correcting it as needed.

Algorithm bias is a serious ethical challenge that can undermine the trustworthiness and value of AI systems. IT professionals have a key role to play in ensuring that our AI systems are ethical and respect human rights. By following some best practices, we can create AI systems that are fair, accurate, and beneficial for all.

THE IMPORTANCE OF ETHICAL AI POLICIES

AI poses significant challenges and risks, such as potential bias, discrimination, privacy breaches, and accountability gaps. Therefore, it is essential to develop and implement ethical AI policies that can ensure the safe, secure, and responsible use of AI for the benefit of individuals, society, and the environment.

WHAT ARE ETHICAL AI POLICIES?

Ethical AI policies are guidelines or principles that aim to align the design, development, and deployment of AI systems with human values and rights. Ethical AI policies can help to:

- Achieve safer, more reliable, and fairer outcomes for all stakeholders affected by AI applications.
- Reduce the risk of negative impacts or harms caused by AI systems.
- Build public trust and confidence in AI systems and their providers.
- Encourage innovation and competitiveness in the AI sector.
- Comply with existing laws and regulations related to AI.

Ethical AI policies can be developed and implemented by various actors, such as governments, businesses, researchers, civil society, and international organizations. Ethical AI policies can also vary in their scope, level of detail, and enforceability.

EXAMPLES OF ETHICAL AI POLICIES

Several countries and regions have developed or are developing ethical AI policies to guide their AI strategies and initiatives. For example:

Australia has published its AI Ethics Framework, which includes eight voluntary AI Ethics Principles that cover human, social, and environmental wellbeing; human-centred values; fairness; privacy protection and security; reliability and safety; transparency and explainability; contestability; and accountability.

The **European Union** has proposed its Artificial Intelligence Act, which is a comprehensive legal framework that aims to regulate high-risk AI systems and promote trustworthy AI based on four ethical principles: respect for human dignity and autonomy; prevention of harm; fairness; and democratic values.

The **United States** has issued its Executive Order on Maintaining American Leadership in Artificial Intelligence, which directs federal agencies to foster public trust and confidence in AI technologies by promoting reliable, robust, trustworthy, secure, portable, and interoperable AI systems.

In addition to governments, many private sector companies have also adopted their own ethical AI policies or principles to demonstrate their commitment to responsible AI practices. For example:

Microsoft has established its *Responsible AI Standard*, which is a set of requirements and processes that help its teams design, develop, deploy, and operate AI systems in a manner consistent with its six ethical principles: fairness; reliability and safety; privacy and security; inclusiveness; transparency; and accountability.

Google has published its *Responsible AI Practices*, which is a collection of best practices and tools that help its engineers build AI systems that are aligned with its seven principles: socially beneficial; avoid creating or reinforcing unfair bias; be built and tested for safety; be accountable to people; incorporate privacy design principles; uphold high standards of scientific excellence; and be made available for uses that accord with these principles.

MITIGATING BIAS

IDENTIFY AND ASSESS POTENTIAL SOURCES OF BIAS

The first step to mitigate bias is to identify and assess the potential sources of bias in the IT system or decision. This can be done by conducting a thorough analysis of the data, algorithms, processes and outcomes involved in the system or decision. Some questions to ask are:

- What are the objectives and criteria of the system or decision?
- What are the data sources, methods and quality of the data collection and processing?

- What are the assumptions, limitations and trade-offs of the algorithms and models used?
- How are the results interpreted, communicated and acted upon?
- Who are the stakeholders, beneficiaries and potential victims of the system or decision?
- What are the ethical, legal and social implications of the system or decision?

Some tools that can help with this step are:

- IBM's AI Fairness 360 toolkit, which provides a set of metrics, algorithms and visualizations to detect and mitigate bias in datasets and machine learning models.
- IBM's AI Factsheets, which provide a standardized way to document the characteristics, capabilities and limitations of AI systems.
- IBM Watson OpenScale, which provides a platform to monitor, explain and improve AI performance, fairness and compliance.

IMPLEMENT BIAS MITIGATION STRATEGIES

The second step is to implement bias mitigation strategies that address the identified sources of bias. This can be done by applying various techniques, such as:

- Data augmentation, transformation or sampling to improve the representativeness, diversity and balance of the data.
- Algorithm selection, modification or regularization to reduce the complexity, opacity or sensitivity of the models.
- Human review, feedback or intervention to provide oversight, validation or correction of the results.
- Stakeholder engagement, consultation or participation to ensure transparency, accountability and inclusiveness of the system or decision.

Some examples of bias mitigation strategies are:

Conflicts and Biases in the Boardroom, which provides guidance on how to address conflicts of interest and common biases that impact board decisions.

Algorithmic bias detection and mitigation: Best practices ... - Brookings, which provides policy recommendations on how to detect and mitigate algorithmic bias in consumer harms.

AI Ethics Part 2: Mitigating bias in our algorithms - CMO, which provides best practices on how to build fairness and bias metrics and run a model governance process.

EVALUATE AND MONITOR BIAS MITIGATION OUTCOMES

The third step is to evaluate and monitor the outcomes of the bias mitigation strategies. This can be done by measuring, testing and reporting on the performance, fairness and trustworthiness of the system or decision. Some questions to ask are:

- How effective are the bias mitigation strategies in achieving the objectives and criteria of the system or decision?
- How fair are the system or decision outcomes for different groups of stakeholders?
- How trustworthy are the system or decision processes and results for different audiences?
- How robust are the system or decision against changes in data, algorithms or contexts?
- How adaptable are the system or decision to new requirements, feedback or challenges?

Some tools that can help with this step are:

- IBM Watson OpenScale, which provides a platform to monitor, explain and improve AI performance, fairness and compliance.
- IBM Watson Discovery, which provides a service to analyse text data for sentiment, emotion, tone and personality insights.
- IBM Watson Assistant, which provides a service to build conversational agents that can interact with users and provide feedback.

Mitigating bias in IT governance is a complex and ongoing challenge that requires a holistic and proactive approach. By following these three steps - identify and assess potential sources of bias, implement bias mitigation strategies, and evaluate and monitor bias mitigation outcomes - IT leaders can ensure that their systems and decisions are more ethical, fair and trustworthy.

ETHICAL AI IN CRITICAL DOMAINS

Certain domains, such as criminal justice and healthcare, hold significant ethical ramifications for AI usage. Biased algorithms in predictive policing can lead to unjust targeting, while healthcare AI biased against certain demographics might exacerbate health disparities. Ethical AI policies should emphasize thorough evaluation and validation of algorithms in these critical contexts.

IDENTIFY THE ETHICAL PRINCIPLES FOR AI

The first step to build ethical AI is to identify the ethical principles that should guide its development and use. There are many sources of ethical principles for AI, such as the OECD Principles on AI, the World Economic Forum's 9 Ethical AI Principles for Organizations, or the Ethics of Artificial Intelligence course by Coursera. These principles usually include values such as fairness, transparency, accountability, privacy, security, human oversight, and social good.

However, these principles are not enough by themselves. They need to be translated into concrete norms and practices that can be implemented and governed in specific contexts and domains. For example, what does fairness mean for an AI system that diagnoses diseases or recommends treatments? How can transparency be achieved for an AI system that predicts criminal behaviour or assesses legal risks? How can accountability be ensured for an AI system that controls autonomous vehicles or drones?

To answer these questions, we need to conduct a thorough ethical analysis of the AI system and its impacts and implications for the stakeholders involved.

CONDUCT AN ETHICAL ANALYSIS OF THE AI SYSTEM

The second step to build ethical AI is to conduct an ethical analysis of the AI system and its impacts and implications for the stakeholders involved. This analysis should consider the following aspects:

- **The purpose and goals of the AI system**. What problem does it aim to solve? What benefits does it provide? What risks does it entail?
- **The data and algorithms of the AI system**. What data is used to train and test the AI system? How is it collected, processed, stored, and shared? What algorithms are used to analyse the data and generate outputs? How are they designed, validated, and updated?
- **The outputs and outcomes of the AI system**. What outputs does the AI system produce? How are they interpreted and used? What outcomes do they lead to? How are they measured and evaluated?
- **The stakeholders of the AI system**. Who are the stakeholders of the AI system? How are they affected by its outputs and outcomes? What are their needs, preferences, values, and expectations?
- **The ethical issues of the AI system**. What ethical issues arise from the AI system's purpose, data, algorithms, outputs, outcomes, and stakeholders? How can they be identified, prioritized, and addressed?

To conduct this analysis, we need to use critical skills and methods that can help us clarify and ethically evaluate the AI system in different domains of life. We also need to consult with relevant experts and stakeholders to ensure that we capture their perspectives and concerns.

IMPLEMENT ETHICAL SOLUTIONS FOR THE AI SYSTEM

The third step is to implement ethical solutions for the AI system that can address the ethical issues identified in the previous step. These solutions may include:

- **Ethical design**. Applying ethical principles and values in the design process of the AI system, such as user-cantered design or value-sensitive design.

- **Ethical development**. Applying ethical standards and guidelines in the development process of the AI system, such as code of ethics or best practices.
- **Ethical testing**. Applying ethical criteria and methods in the testing process of the AI system, such as audits or impact assessments.
- **Ethical deployment**. Applying ethical rules and regulations in the deployment process of the AI system, such as policies or laws.
- **Ethical governance**. Applying ethical mechanisms and structures in the governance process of the AI system, such as oversight boards or ethics committees.

To implement these solutions, we need to use appropriate tools and techniques that can help us operationalize ethics in practice. We also need to monitor and evaluate the impacts and outcomes of the AI system on a regular basis.

Ethical AI is not only a moral duty but also a strategic advantage for organizations that want to create value and trust with their customers, employees, partners, regulators, and

MODULE 6: INTELLECTUAL PROPERTY & COPYRIGHT

Intellectual property and copyright are legal concepts that protect the rights of creators and owners of original works, such as books, music, software, and inventions. They grant them exclusive control over how their works are used, distributed, and modified by others.

Digital rights management (DRM) is a technology that restricts the access and use of digital content, such as e-books, movies, and games. DRM aims to prevent unauthorized copying, sharing, or modifying of protected content. However, DRM also raises ethical and technical issues, such as limiting the fair use rights of consumers, interfering with the interoperability of devices and platforms, and creating security vulnerabilities.

Open-source software licensing is a type of software licensing that allows anyone to access, use, modify, and distribute the source code of a software program. Open-source software is often developed collaboratively by a community of developers who share a common vision and values. Open-source software licensing promotes innovation, transparency, and freedom of choice for users and developers.

6.1. INTELLECTUAL PROPERTY & COPYRIGHT

WHAT IS INTELLECTUAL PROPERTY?

Intellectual property (IP) is any creation of the mind that has commercial value. It includes inventions, designs, artistic works, symbols, names and images. IP can be protected by law through patents, trademarks, copyrights and trade secrets.

WHY IS IP IMPORTANT FOR CYBERSECURITY?

IP is one of the most valuable assets of any business. It gives a competitive edge, attracts customers and investors, and generates revenue. However, IP is also vulnerable to cyberattacks, theft, misuse, and infringement. Cybersecurity is the process of protecting IP from unauthorized access, use, disclosure, modification, or destruction.

HOW TO PROTECT IP FROM CYBER THREATS?

Here are some tips to keep IP safe from cyber threats:

- Identify your IP assets and their value. Conduct an IP audit to find out what IP you have, who owns it, where it is stored and how it is used.
- Implement appropriate security measures for your IP assets. Use encryption, authentication, access control, backup and recovery systems to safeguard your IP data.

- Educate your employees and partners about IP protection. Provide training and awareness programs on IP policies, procedures and best practices. Monitor and enforce compliance with IP rules and agreements.
- Register your IP rights where possible. Apply for patents, trademarks or copyrights to secure legal protection for your IP assets. Use notices and labels to indicate your ownership and rights.
- Monitor your IP environment and respond to incidents. Use tools and services to detect and prevent IP breaches, such as firewalls, antivirus software, intrusion detection systems and threat intelligence. Report and resolve any IP issues as soon as possible.

THE ESSENCE OF INTELLECTUAL PROPERTY & COPYRIGHT

IP is the intangible creation of the human mind, such as inventions, artistic works, designs, symbols, names and images. IP is protected by laws that grant exclusive rights to the creators or owners of IP, such as patents, trademarks, designs and copyright.

WHY IP MATTERS IN CYBERSPACE

Cyberspace is the virtual environment where people communicate and interact through computer networks. Cyberspace is becoming a hub for IP infringement, as it is easy to copy, distribute and modify digital content without the owner's consent. IP infringement can harm the owner's reputation, revenue, and competitive advantage. It can also expose the infringer to legal risks and liabilities.

Some common examples of IP infringement in cyberspace are:

- Using another person's logo, brand name or domain name without permission
- Copying or downloading another person's software, music, video, e-book or game without a licence
- Making a profit by using another person's creation without paying royalties or fees
- Modifying or adapting another person's work without authorisation
- Selling counterfeit or pirated goods online

HOW TO PROTECT YOUR IP IN CYBERSPACE

Take the following steps to protect your IP in cyberspace:

- **Identify and audit your IP assets**. Know what IP you have, who owns it, how it is used and how it is protected.
- **Register your IP rights**. Apply for patents, trademarks and designs to secure your exclusive rights in Australia and overseas
- **Monitor your IP online**. Use tools and services to detect and prevent unauthorised use of your IP on the internet.

- **Enforce your IP rights**. Act against infringers by sending cease and desist letters, filing complaints or initiating legal proceedings.
- **Commercialise your IP**. Negotiate and draft licensing, technology transfer, distribution and content agreements to generate income from your IP

WHERE TO FIND MORE INFORMATION

Visit the following websites:

- [Intellectual Property Lawyers | Gilbert + Tobin](https://www.gtlaw.com.au/expertise/intellectual-property): A leading Australian law firm that provides advice on all aspects of IP law
- [Intellectual Property, Technology & Cyber Security | HopgoodGanim] (https://www.hopgoodganim.com.au/page/expertise/services/intellectual-property-technology-cybersecurity): A market-leading team of lawyers with scientific or technical qualifications in IP, technology and cyber security
- [Intellectual Property in Cyberspace | GeeksforGeeks] (https://www.geeksforgeeks.org/intellectual-property-in-cyberspace/): A website that explains the basics of IP in cyberspace with examples
- [Intellectual Property Crime | Australian Federal Police] (https://www.afp.gov.au/what-we-do/crime-types/intellectual-property-crime): A website that provides information on how to report IP crime and what actions the AFP can take

CYBERSECURITY RISKS

One of the main challenges of digital transformation is ensuring the security of your data and software systems. Data breaches are becoming more frequent and costly, exposing sensitive information, damaging reputations and causing legal liabilities.

According to a report by Norton Rose Fulbright, there were 4,100 publicly disclosed data breaches in 2022 alone, comprising some 22 billion records that were exposed. Moreover, software systems are becoming more complex and vulnerable, especially with the rise of artificial intelligence and generative AI, which can create realistic but fake content that can deceive or manipulate users.

Therefore, it is important to adopt a proactive and comprehensive approach to cybersecurity, that includes:

- Developing a framework that aligns your technology strategy with your business goals and risk appetite.
- Implementing zero trust architectures that assume all systems can or will be compromised and require continuous verification of users, devices and data.

- Applying encryption, authentication and access control measures to protect your data at rest and in transit.
- Monitoring and auditing your systems for any anomalies or suspicious activities.
- Updating and patching your software regularly to fix any vulnerabilities or bugs.
- Educating and training your employees and customers on cybersecurity best practices and awareness

PRIVACY RISKS

Another challenge of digital transformation is respecting the privacy rights of your customers, employees and partners. Privacy laws are becoming more stringent and diverse across jurisdictions, requiring you to comply with various rules and regulations on how you collect, use, store and share personal information. For example, the General Data Protection Regulation (GDPR) in the European Union imposes strict obligations on data controllers and processors, such as obtaining consent, providing transparency, ensuring data minimization and enabling data portability. Failing to comply with privacy laws can result in hefty fines, lawsuits and reputational damage. Therefore, you need to adopt a privacy-by-design approach that incorporates privacy principles into every stage of your digital transformation process, such as:

- Conducting privacy impact assessments to identify and mitigate any potential privacy risks or harms.
- Implementing privacy-enhancing technologies that anonymize, pseudonymize or encrypt personal data.
- Establishing privacy policies and notices that inform your data subjects about their rights and choices.
- Obtaining valid and informed consent from your data subjects before processing their personal data
- Responding to data subject requests to access, correct or delete their personal data.
- Reporting any data breaches or incidents to the relevant authorities and data subjects within the prescribed time frames.

INTELLECTUAL PROPERTY RIGHTS

Finally, one of the most important aspects of digital transformation is protecting your intellectual property rights. Intellectual property rights are the legal rights that grant you exclusive ownership and control over your creations, such as inventions, designs, trademarks, logos, slogans, software code, content etc. Intellectual property rights are essential for fostering innovation, competitiveness, and differentiation in the digital economy. However, digital transformation also poses new threats to your intellectual property rights, such as:

- Copying or stealing your software code or content by hackers or competitors.
- Infringing or violating your patents, trademarks or copyrights by using them without authorization or paying royalties.
- Diluting or tarnishing your brand image or reputation by creating confusingly similar or disparaging products or services.
- Challenging or invalidating your intellectual property rights by claiming prior art or public domain status.

Therefore, you need to adopt a strategic and proactive approach to intellectual property protection that includes:

- Registering your intellectual property rights with the relevant authorities and agencies.
- Enforcing your intellectual property rights against any infringers or violators through legal action or alternative dispute resolution.
- Licensing your intellectual property rights to others for mutual benefit or collaboration.
- Monitoring the market for any potential infringements or violations of your intellectual property rights.
- Updating your intellectual property portfolio to reflect any changes or improvements in your products or services.

Digital transformation comes with significant risks that can jeopardize your cybersecurity, privacy and intellectual property rights.

NAVIGATING THE AUSTRALIAN COPYRIGHT ACT

WHAT IS COPYRIGHT?

Copyright is a legal right that gives the creator of an original work the exclusive right to control how it is used, reproduced, communicated, or performed. It covers a wide range of works, such as books, music, films, software, databases, artworks, photographs and more. It also covers some types of online content, such as websites, blogs, podcasts, and social media posts.

WHY IS IT IMPORTANT?

Protecting your intellectual property is important for many reasons. It can help you:

- Reward your creativity and innovation.
- Prevent others from copying or exploiting your work without your permission.
- Generate income from licensing or selling your work.
- Enhance your reputation and brand recognition.
- Contribute to the cultural and economic development of society.

HOW DOES IT WORK IN AUSTRALIA?

Australia has a complex and evolving legal framework for copyright protection. Some of the key features are:

- You do not need to register or apply for copyright protection. It is automatic once you create an original work in a material form.
- You do not need to use the © symbol or any other notice to indicate your ownership. However, it may be helpful to do so as a reminder to others.
- You have the right to take legal action against anyone who infringes your copyright, such as by copying, distributing, displaying, or modifying your work without your consent.
- You may also have some moral rights, such as the right to be attributed as the author and the right to object to any derogatory treatment of your work.
- You may grant or transfer some or all your rights to others through a licence or an assignment agreement. You should always read and understand the terms and conditions before signing any contract.
- You may also allow others to use your work for free under certain circumstances, such as for fair dealing purposes (e.g. research, study, criticism, review, parody or satire) or under a Creative Commons licence.
- You must respect the rights of other creators when you use their works. You should always seek permission or rely on a valid exception before using any copyrighted material.
- You must comply with any applicable laws and regulations that affect your online activities, such as the Online Safety Act 2021 (Cth), the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth) and the Security Legislation Amendment (Critical Infrastructure) Bill 2021 (Cth). These laws aim to enhance the security and safety of online platforms and services and may impose new obligations and responsibilities on you as a user or provider.

DIGITAL RIGHTS MANAGEMENT (DRM) BALANCING RIGHTS & ACCESS

Digital Rights Management (DRM) is a set of technologies and protocols that protect digital content from unauthorized access, reproduction, and distribution. It is used to enforce copyright protection, licensing agreements, and access control for various forms of digital media, such as music, videos, eBooks, software, and more.

BENEFITS OF DRM

DRM provides a crucial layer of protection for content creators and owners. It helps them safeguard their intellectual property rights and prevent piracy or data breaches. By using DRM, content creators can:

- Control how their content is used, shared, or modified by authorized users.
- Generate revenue from their content by charging fees or subscriptions.
- Monitor the usage and performance of their content.
- Enhance the user experience by providing high-quality and secure content.

DRM also benefits content consumers by ensuring that they receive legitimate and quality content. It also helps them respect the rights and wishes of the content creators.

CHALLENGES OF DRM

DRM is not without its limitations. Some of the common issues that DRM faces are:

- Compatibility. Different platforms and devices may use different DRM systems, which can cause problems for users who want to access the same content across multiple devices
- Usability. DRM may impose restrictions or requirements that can affect the user experience, such as requiring internet connection, limiting the number of devices or downloads, or preventing offline access
- Privacy. DRM may collect personal or behavioural data from users, which can raise concerns about data protection and consent
- Fair use. DRM may interfere with the rights of users to use the content for legitimate purposes, such as education, research, criticism, or parody.

BEST PRACTICES FOR DRM

To balance the rights and access of both content creators and consumers, it is important to follow some best practices when implementing or using DRM solutions. Some of these are:

- Choose a suitable DRM system that meets your needs and goals. There are different types of DRM systems available, such as encryption-based, watermark-based, or fingerprint-based. You should consider factors such as cost, complexity, security level, compatibility, and scalability when selecting a DRM system.
- Use a multi-DRM strategy to protect your streams on all platforms with strict licensing rules. A good DRM vendor will allow you to do all the following to protect your streams:
- Prevent screen capture.
- Prevent downloading of the streams by using the strictest variants of the DRM available.
- Ensure a strict expiration date in the license beyond which the stream will be inaccessible.

- Provide the option to rotate the DRM keys during the live streams to frustrate hackers.
- Communicate clearly with your users about the terms and conditions of your DRM policy. You should inform them about what they can and cannot do with your content, how long they can access it, what data you collect from them, and how you protect their privacy.
- Respect the fair use rights of your users and allow them some flexibility in using your content for legitimate purposes. You should also provide them with options to contact you or request permission if they have any questions or issues with your DRM policy.
- Keep up to date with the latest developments and trends in DRM technology and legislation. You should monitor the changes in the market and the legal environment and adjust your DRM strategy accordingly.

OPEN SOURCE & LICENSING CONSIDERATIONS

OSS is software that uses publicly available source code that anyone can see, modify, and distribute. OSS can offer many benefits, such as affordability, flexibility, and quality, but it also comes with some risks and challenges that you need to be aware of.

TYPES OF OPEN-SOURCE LICENSES

One of the main challenges of using OSS is complying with the terms and conditions of the open-source licenses. These are legal agreements that specify what you can and cannot do with the OSS and its derivatives. There are two main types of open-source licenses: permissive and copyleft.

Permissive licenses are the more business-friendly ones, as they allow you to use, modify, and distribute the OSS for any purpose if you give proper attribution to the original authors. Some examples of permissive licenses are the MIT license, the Apache license, and the BSD license.

Copyleft licenses are the more restrictive ones, as they require you to share your modifications and derivatives under the same or compatible license as the original OSS. This means that if you use copyleft OSS in your proprietary software, you might have to disclose your source code and allow others to use it for free. Some examples of copyleft licenses are the GNU General Public License (GPL), the GNU Lesser General Public License (LGPL), and the Mozilla Public License (MPL).

RISKS AND BEST PRACTICES

Using OSS can introduce some risks to your cybersecurity projects, such as:

- **Excessive access**. Open access means that anyone can see and manipulate the source code, which creates opportunities for malicious actors to introduce vulnerabilities or backdoors.

- **Lack of verification**. There are no guarantees that the OSS is tested and reviewed by qualified experts, which can make it prone to errors and security flaws.
- **Lack of support**. Most OSS does not have dedicated support teams, which means that updates and patches may not be available or timely. This can leave your software exposed to known or unknown vulnerabilities.

To mitigate these risks, you should follow some best practices when using OSS, such as:

- **Conduct a thorough due diligence.** Before using any OSS, you should check its license type, terms, and conditions, and make sure they are compatible with your intended use and distribution. You should also check its reputation, quality, security, and maintenance status.
- **Use a software composition analysis tool**. This is a tool that can help you identify and manage the OSS components in your software. It can help you track their licenses, versions, dependencies, vulnerabilities, and compliance status.
- **Implement a security policy**. You should have a clear and consistent policy for using OSS in your projects. This policy should define the roles and responsibilities of your team members, the criteria for selecting OSS components, the processes for reviewing and updating them, and the procedures for reporting and resolving any issues.

Using OSS can be a great way to enhance your cybersecurity projects with high-quality software components. However, you need to be careful about the legal and security implications of using OSS. By following the types of open-source licenses, understanding their risks, and applying best practices, you can use OSS safely and effectively.

FAIR USE & FLEXIBILITY

WHAT IS FAIR USE AND FLEXIBILITY?

Fair use and flexibility are legal doctrines that allow the use of copyrighted material without permission or payment under certain circumstances. They are essential for promoting creativity, innovation, education, research, and public interest.

In the context of cybersecurity, fair use and flexibility can enable security professionals to access, analyse, test, and improve the security of digital systems and data. For example, fair use and flexibility can allow security researchers to reverse engineer software, conduct vulnerability assessments, disclose security flaws, and develop patches or workarounds.

WHY IS FAIR USE AND FLEXIBILITY IMPORTANT FOR CYBERSECURITY?

Fair use and flexibility are important for cybersecurity because they can help:

- Enhance the security posture of organizations and individuals by allowing them to identify and mitigate risks, protect their assets, and respond to incidents.
- Foster a culture of security awareness and collaboration by allowing security professionals to share their findings, insights, and best practices with others.
- Support the development of new security technologies and solutions by allowing security professionals to experiment with different methods, tools, and techniques.
- Advance the state of the art in cybersecurity by allowing security professionals to contribute to the scientific knowledge and innovation in the field.

WHAT ARE THE CHALLENGES AND RISKS OF FAIR USE AND FLEXIBILITY IN CYBERSECURITY?

Fair use and flexibility are not absolute rights. They are subject to limitations and exceptions depending on the jurisdiction, context, purpose, nature, amount, and effect of the use. They are also balanced against the rights and interests of the copyright holders.

Therefore, fair use and flexibility in cybersecurity can pose some challenges and risks, such as:

- **Legal uncertainty and liability**. Security professionals may face legal challenges or lawsuits from copyright holders who claim that their use of the material was unauthorized or infringing. Security professionals may also face criminal charges or penalties if their use of the material violates other laws or regulations.
- **Ethical dilemmas and conflicts**. Security professionals may encounter ethical dilemmas or conflicts when deciding whether, how, when, and with whom to use or share the material. Security professionals may also face criticism or backlash from their peers, employers, clients, or the public for their use or disclosure of the material.
- **Operational difficulties and costs**. Security professionals may face operational difficulties or costs when obtaining, storing, processing, or transmitting the material. Security professionals may also face technical challenges or limitations when using or modifying the material.

DIGITAL COMMONS & COLLABORATIVE CREATION

WHAT ARE DIGITAL COMMONS AND COLLABORATIVE CREATION?

Digital commons are resources that are shared by a community of users online, such as open-source software, open data, open educational resources, and

creative commons licenses. Collaborative creation is the process of producing digital content or knowledge by working together with others, such as through wikis, blogs, podcasts, or social media platforms.

WHY ARE THEY IMPORTANT?

Digital commons and collaborative creation can foster innovation, creativity, education, and social inclusion. They can also reduce costs, increase efficiency, and improve quality of digital products and services. For example, Wikipedia is a collaborative encyclopedia that anyone can edit, which provides free and reliable information to millions of users around the world. Linux is an open-source operating system that powers many servers, devices, and applications, which benefits from the contributions of thousands of developers and users.

WHAT ARE THE CYBERSECURITY RISKS?

However, digital commons and collaborative creation also pose cybersecurity risks that need to be addressed. These risks include:

- Unauthorized access or modification of digital resources by hackers, competitors, or malicious insiders
- Theft or leakage of sensitive or personal data by cybercriminals, spies, or whistleblowers
- Infringement or violation of intellectual property rights by copycats, pirates, or trolls
- Disruption or sabotage of digital services or infrastructure by activists, terrorists, or state actors
- Misinformation or manipulation of digital content or users by propagandists, fraudsters, or bots

HOW TO PROTECT THEM?

These include:

- Implementing strong authentication and authorization mechanisms to verify the identity and access rights of users and contributors.
- Encrypting data in transit and at rest to prevent unauthorized interception or extraction.
- Applying digital signatures or watermarks to prove the origin and integrity of digital resources.
- Monitoring and auditing the activity and performance of digital systems and networks to detect and respond to anomalies or incidents.
- Educating and engaging the community of users and contributors to raise awareness and foster trust and cooperation.

WHERE TO LEARN MORE?

If you want to learn more about digital commons and collaborative creation, you can visit the following websites:

[Rebuilding digital trust for a cyber-inclusive future | World Economic Forum] (https://www.weforum.org/agenda/2021/11/rebuilding-digital-trust-for-a-cyber-inclusive-future/)

[Cybersecurity, cybercrime and cybersafety: a quick guide to key internet links – Parliament of Australia] (https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1819/Quick_Guides/CybersecurityCybercrimeCybersafety)

[The Digital World Is Changing Rapidly. Your Cybersecurity Needs to Keep Up.] (https://hbr.org/2023/05/the-digital-world-is-changing-rapidly-your-cybersecurity-needs-to-keep-up)

6.2. DIGITAL RIGHTS MANAGEMENT

Digital rights management (DRM) is a term that encompasses the methods and technologies used to protect and control the access and use of digital content, such as books, music, videos, software, and data. DRM aims to prevent unauthorized copying, sharing, modification, or distribution of digital content by applying various restrictions and encryption techniques to the content or the devices that can access it.

WHY IS DRM IMPORTANT?

DRM is important for several reasons. First, it helps content creators and owners to safeguard their intellectual property rights and their financial and creative investments in their work. By limiting what users can do with their content, DRM ensures that content creators and owners can benefit from their work and prevent others from exploiting it without permission or compensation.

Second, DRM helps users to respect the legal and ethical boundaries of using digital content. By complying with the terms and conditions of DRM, users can avoid infringing on the rights of content creators and owners and avoid potential legal consequences or penalties.

Third, DRM helps to maintain the quality and integrity of digital content. By preventing unauthorized modification or alteration of digital content, DRM ensures that users can access and enjoy the original and authentic version of the content as intended by the content creators and owners.

HOW DOES DRM WORK?

DRM works by using various technologies and tools to implement different types of restrictions and encryption on digital content. Some of the common DRM methods are:

Copy protection. This method prevents or limits users from making copies of digital content or transferring it to other devices or platforms.

Access control. This method requires users to have a valid license, password, or authentication to access digital content or certain features or functions of it.

Expiration. This method sets a time limit, or several uses for accessing digital content, after which the content becomes inaccessible or unusable.

Geolocation. This method restricts access to digital content based on the user's location or IP address.

Watermarking. This method embeds a visible or invisible mark on digital content that identifies the source or owner of the content.

Encryption. This method scrambles the data of digital content using a secret key that only authorized users can decrypt.

WHAT ARE SOME EXAMPLES OF DRM?

DRM is widely used across various types of digital content and industries. Some examples are:

E-books. Many e-books use DRM to prevent users from copying, printing, sharing, or modifying them. Some e-books also use DRM to limit the number of devices or platforms that users can read them on.

Music. Many music files use DRM to prevent users from copying, sharing, or converting them to other formats. Some music files also use DRM to limit the number of devices or platforms that users can play them on.

Videos. Many videos use DRM to prevent users from copying, sharing, or editing them. Some videos also use DRM to limit the resolution, quality, or playback speed of them.

Software. Many software programs use DRM to prevent users from installing, copying, sharing, or modifying them. Some software programs also use DRM to require online activation, registration, or subscription to use them.

Data. Many data sets use DRM to prevent users from accessing, copying, sharing, or analysing them. Some data sets also use DRM to require payment, permission, or attribution to use them.

BENEFITS AND DRAWBACKS OF DRM

DRM can have positive effects for both content providers and users. For content providers, DRM can help them:

- Protect their intellectual property rights and prevent revenue loss from piracy and unauthorized copying.
- Enhance their reputation and brand image by ensuring the quality and authenticity of their content.
- Increase their market share and customer loyalty by offering different options and incentives for accessing their content.
- Innovate and create new business models and revenue streams by leveraging the potential of digital technologies.

For users, DRM can help them:

- Access a wide range of digital content at affordable prices and convenient formats.
- Enjoy a better user experience and quality of service by avoiding malware, viruses, glitches and errors.
- Support their favourite content creators and contribute to the development of the digital economy.
- Exercise their rights to privacy, security, anonymity and fair use by choosing the content providers and platforms that respect these rights.

However, DRM can also have negative effects for both parties. For content providers, DRM can:

- Increase their costs and complexity of developing, maintaining and updating their DRM systems.
- Reduce their flexibility and adaptability to changing market conditions and customer preferences.
- Expose them to legal risks and liabilities if their DRM systems violate users' rights or infringe on other parties' intellectual property rights.
- Damage their reputation and customer satisfaction if their DRM systems are perceived as intrusive, restrictive or unfair.

For users, DRM can:

- Limit their access, use and enjoyment of digital content by imposing technical or contractual restrictions.
- Interfere with their legitimate activities and expectations, such as sharing, lending, reselling or modifying the content.
- Violate their rights to privacy, security, anonymity and fair use by collecting, storing or disclosing their personal data or monitoring their online behaviour.
- Harm their devices or data by introducing malware, viruses, glitches or errors.

CHALLENGES & CONTROVERSIES OF DRM

DRM is not without its challenges and controversies. Some of the common issues are:

User rights. Some users argue that DRM violates their fair use rights or their right to own and control their purchased digital content. They claim that DRM restricts their ability to make personal copies, backups, modifications, or adaptations of digital content for their own purposes.

User experience. Some users complain that DRM negatively affects their user experience by making digital content less accessible, convenient, compatible, or functional. They claim that DRM causes technical problems, errors, glitches, or incompatibilities with their devices or platforms.

User privacy. Some users worry that DRM invades their privacy by collecting their personal information, tracking their online activities, or exposing them to security risks. They claim that DRM requires them to share their personal data with third parties, such as content providers, service providers, or advertisers.

User activism. Some users resist or challenge DRM by circumventing it using various tools or techniques, such as cracking codes, hacking systems, or creating alternative platforms. They claim that they are exercising their civil disobedience rights or their freedom of expression rights.

DESIGN PRINCIPLES FOR DRM SYSTEMS

Given these benefits and drawbacks, how can we design and implement DRM systems that balance the interests of both content providers and users? Here are some principles and guidelines that I suggest:

Respect the law. DRM systems should comply with the relevant laws and regulations in the jurisdictions where they operate. They should not infringe on other parties' intellectual property rights or violate users' rights to privacy, security, anonymity or fair use.

Respect the ethics. DRM systems should follow the ethical standards and values of the society where they operate. They should not harm or exploit users or other stakeholders. They should promote social justice, human dignity and public interest.

Respect the users. DRM systems should consider the needs, preferences and expectations of the users. They should provide clear information about the terms and conditions of accessing the content. They should offer choices and options for different user groups. They should ensure a high quality of service and user experience.

Respect the content. DRM systems should protect the integrity and authenticity of the content. They should not degrade or distort the content. They should not interfere with the artistic or creative expression of the content creators.

Respect the innovation. DRM systems should foster innovation and creativity in the digital economy. They should not stifle or hinder the development of new technologies, products or services. They should not create artificial barriers or monopolies in the market.

ETHICAL IMPLICATIONS OF DRM

Digital rights management (DRM) applies to the copying, sharing, or modifying of digital content such as music, movies, software, or e-books. DRM can be seen to protect the rights and revenues of the creators and distributors of digital content, but it can also raise ethical issues for the users and consumers of such content.

WHAT IS RESTRICTIVE DRM?

Restrictive DRM is a type of DRM that imposes strict limitations on how users can access, use, or transfer digital content. For example, restrictive DRM may:

- Stop a cell phone from working with a different wireless provider.
- Make a DVD from a certain region unplayable in other regions of the world.
- Encrypt software to prevent copying or installing on multiple devices.
- Prevent children from accessing adult content.

- Require online verification or authentication to use certain products or services.

Restrictive DRM can be implemented through hardware, software, or legal means. Some examples of restrictive DRM technologies are:

- Region codes on DVDs or Blu-ray discs.
- Activation codes or serial numbers for software products.
- Digital locks or encryption keys on e-books or music files.
- Online platforms or services that require subscription or registration.

Restrictive DRM can also be enforced through legal measures such as the Digital Millennium Copyright Act (DMCA) in the United States, which prohibits the circumvention of DRM technologies or the distribution of tools or devices that can bypass them.

WHY IS RESTRICTIVE DRM ETHICAL?

Some of the arguments in favour of restrictive DRM are:

- It protects the intellectual property rights and interests of the creators and distributors of digital content, who invest time, money, and effort to produce and deliver quality products and services.
- It prevents piracy and illegal use of digital content, which can harm the revenues and reputation of the content industry and reduce the incentives for innovation and creativity.
- It enables new business models and revenue streams for the content industry, such as subscription-based services, pay-per-view models, or dynamic pricing strategies.
- It provides users with features and benefits that they want or need, such as parental controls, trial versions, or personalized recommendations.

Some of the sources that support restrictive DRM are:

- The Entertainment Software Association of Canada (ESAC), which represents the video game industry in Canada. ESAC argues that DRM is necessary to protect the investments and innovations of game developers and publishers, and to provide consumers with diverse and high-quality gaming experiences.
- The Alliance of Canadian Cinema, Television and Radio Artists (ACTRA), which represents performers in the audiovisual media sector in Canada. ACTRA advocates for DRM to ensure fair compensation and recognition for artists whose works are distributed digitally.
- Microsoft Corporation, which is one of the leading developers and providers of software products and services in the world. Microsoft uses DRM technologies to secure its products and platforms, such as

Windows operating system, Office suite, Xbox console, or Azure cloud service.

WHY IS RESTRICTIVE DRM UNETHICAL?

Some of the arguments against restrictive DRM are:

- It infringes on the rights and freedoms of users and consumers of digital content, who may face restrictions or barriers to access, use, or share content that they have legally acquired or paid for.
- It creates technical and legal challenges for users and consumers of digital content, who may encounter compatibility issues, performance problems, privacy risks, or legal liabilities when using or transferring content across different devices, platforms, or regions.
- It stifles innovation and competition in the content industry, as it creates entry barriers for new entrants or alternative providers who may offer better quality or lower prices for digital content.
- It reduces the social and cultural value of digital content, as it limits the possibilities for remixing, reusing, or transforming content into new forms of expression or knowledge.

Some of the sources that oppose restrictive DRM are:

- The Electronic Frontier Foundation (EFF), which is a non-profit organization that defends civil liberties in the digital world. EFF campaigns against DRM as a threat to user rights, fair use, privacy, security, accessibility, and innovation.
- The Canadian Library Association (CLA), which is a national association that represents libraries and librarians in Canada. CLA opposes DRM as an obstacle to access to information, education, culture, and democracy.
- The Free Software Foundation (FSF), which is a non-profit organization that promotes free software and free culture. FSF rejects DRM as a form of digital restriction management that violates user freedom and autonomy.

Restrictive DRM is a controversial topic that involves ethical dilemmas for both producers and consumers of digital content. On one hand, restrictive DRM can be seen as a legitimate and necessary way to protect the rights and interests of the content industry, and to provide users with features and benefits that they want or need.

On the other hand, restrictive DRM can be seen as an illegitimate and unnecessary way to infringe on the rights and freedoms of users and consumers, and to create technical and legal challenges, stifle innovation and competition, and reduce the social and cultural value of digital content. The ethical implications of restrictive DRM depend on the perspective, values, and interests of the

stakeholders involved, as well as the context, purpose, and effects of the DRM technologies or measures used.

6.3. OPEN-SOURCE SOFTWARE LICENSING

THE ESSENCE OF OPEN SOURCE

Open-source software is software that allows anyone to use, modify, and share its source code. The source code is the set of instructions that tells the computer what to do. By making the source code available, open-source software enables collaboration, innovation, and transparency.

WHY OPEN-SOURCE MATTERS

Open-source software has many benefits for users, developers, and society. Some of these benefits are:

Users can choose from a variety of software options that suit their needs and preferences. They can also inspect the source code to verify its quality, security, and functionality.

Developers can learn from other developers' work, improve existing software, or create new software based on existing code. They can also contribute to the development of software that they use or care about.

Society can benefit from the collective knowledge and creativity of the open-source community. Open-source software can also promote social good by addressing common problems or serving public interests.

HOW OPEN-SOURCE WORKS

Open-source software is governed by licenses that define the terms and conditions for its use, modification, and distribution. There are many different open-source licenses, but they generally fall into two categories: permissive and copyleft.

Permissive licenses allow users to do whatever they want with the software, provided they give credit to the original author. Examples of permissive licenses are the MIT License and the Apache License.

Copyleft licenses require users to share their modifications of the software under the same or compatible license as the original. This ensures that the software remains open-source and accessible to everyone. Examples of copyleft licenses are the GNU General Public License and the Mozilla Public License.

HOW TO CHOOSE AN OPEN-SOURCE LICENSE

Choosing an open-source license depends on your goals and preferences as a software developer. Some factors to consider are:

- How much control do you want to have over your software and its derivatives?
- How much credit do you want to receive for your work?

- How compatible do you want your license to be with other open-source licenses?
- How important is it for you to protect your software from potential legal risks?

Choose a License website to compare different open-source licenses and find one that matches your needs. You can also consult a lawyer or an expert in IT governance, policy, ethics, and law if you have specific questions or concerns.

By choosing an open-source license, you can define how others can use, modify, and distribute your software. You can also join a community of developers who collaborate on creating and improving open-source software.

THE ETHICS OF COLLABORATION & INNOVATION

OPEN-SOURCE SOFTWARE LICENSING

Open-source software (OSS) is software that is distributed with a license that allows anyone to use, study, change, or share its source code, without restrictions on how the software is used or by whom.

OSS has become ubiquitous across all areas of software development, as it enables developers to reuse existing code and create more functionality at greater speed. OSS also promotes the adoption of transparent standards and makes applications more interoperable.

However, OSS also raises some ethical questions about how the software is used and who benefits from it. Some developers do not want their work to be used for harm, such as military or surveillance purposes, while others think that restricting OSS is contradictory or impractical. Moreover, some OSS licenses may impose obligations on the users or distributors of the software, such as disclosing the source code, providing attribution, or sharing modifications.

THE HIPPOCRATIC LICENSE

One example of an ethical OSS license is the Hippocratic License, created by Coraline Ada Ehmke in 2019. This license is based on the MIT license but adds a condition that the software may not be used for systems or activities that violate the United Nations Universal Declaration of Human Rights. The Hippocratic License aims to give developers more control over how their software is used and to prevent it from being used for evil.

However, the Hippocratic License is not approved by the Open-Source Initiative (OSI), which governs the most widely used OSS licenses. The OSI argues that the Hippocratic License is not conformant with the Open-Source Definition (OSD), which requires that OSS licenses do not discriminate against persons, groups, or fields of endeavour. The OSI also claims that the Hippocratic License is vague and

subjective, as it relies on the interpretation of human rights by different users and jurisdictions.

THE OPENCHAIN PROJECT

Another approach to address the ethical issues of OSS licensing is the OpenChain Project, which is an initiative by the Linux Foundation to establish best practices for OSS compliance. The OpenChain Project provides a specification and a certification program for organizations that use OSS in their products or services. The OpenChain Project aims to ensure that OSS users respect the rights and obligations of OSS developers and licensors, and that they provide clear and consistent information about the OSS components they use.

The OpenChain Project does not impose any ethical restrictions on how OSS is used, but rather focuses on improving the transparency and accountability of OSS usage. The OpenChain Project also helps organizations to avoid legal risks and reduce costs associated with OSS compliance.

Developers who create or use OSS should be aware of the different types of OSS licenses and their implications for collaboration and innovation. Developers should also respect the intentions and expectations of other developers who contribute to or depend on OSS. By following best practices and standards for OSS compliance, developers can ensure that they use OSS in a responsible and ethical manner.

WHAT IS AN OPEN-SOURCE LICENSE?

An open-source license is a type of software license that complies with the Open-Source Definition. In brief, it allows software to be freely used, modified, and shared by anyone for any purpose, if the license terms are respected. There are many different open-source licenses, and they vary based on the restrictions or conditions they impose on the software users.

CHOOSING AN OPEN-SOURCE LICENSE

Some general factors to consider are:

Compatibility. Some open-source licenses are compatible with each other, meaning that you can combine or distribute software under different licenses without violating any terms. Some licenses are incompatible with each other, meaning that you cannot do so without obtaining additional permissions or agreements. You should check the compatibility of your chosen license with other licenses that you may want to use or interact with in the future.

Copyleft. Some open-source licenses are copyleft, meaning that they require any modified or derived versions of the software to be distributed under the same or equivalent license. This ensures that the software remains open-source and preserves the original author's rights and intentions. Some licenses are permissive, meaning that they do not impose such a requirement and allow more

flexibility for the software users. You should decide whether you want your software to be copyleft or permissive, depending on your preferences or objectives.

Popularity. Some open-source licenses are more popular or widely used than others, meaning that they have more recognition or acceptance in the open-source community. This can affect how easy it is to find or collaborate with other projects that use the same or similar licenses. You should consider whether you want your software to use a popular or less popular license, depending on your needs or expectations.

ETHICAL CONSIDERATIONS

OSS comes with several ethical challenges and responsibilities for both contributors and users.

WHY ETHICS MATTER FOR OSS

OSS is not just a technical matter; it is also a social and political one. OSS can have positive or negative impacts on society, depending on how it is used and by whom. For example, OSS can be used for military purposes, surveillance, misinformation, or discrimination.

OSS can also be vulnerable to security breaches, bugs, or malicious code. Therefore, OSS contributors and users should consider the ethical implications of their actions and decisions.

AVOIDING ETHICAL DILEMMAS

OSS also poses some ethical challenges for developers and users, such as:

- How to respect the human rights and dignity of those who may be affected by the software?
- How to ensure the quality and security of the software and prevent harm or misuse?
- How to balance the freedom of OSS with the responsibility of its creators and contributors?
- How to deal with ethical conflicts or dilemmas that may arise from the use of OSS in different contexts or for different purposes?

RESPECT THE HIPPOCRATIC PRINCIPLE: DO NO HARM

The Hippocratic principle is a moral principle that states that one should do no harm or avoid doing harm. It is derived from the Hippocratic oath, a code of ethics for physicians that dates to ancient Greece. The Hippocratic principle can be applied to OSS development and use, as a way of ensuring that the software does not cause harm to individuals, groups, or society at large.

One way of respecting the Hippocratic principle is to adopt an ethical license for OSS, such as the Hippocratic License, which was created by Coraline Ada Ehmke, a software developer from Chicago. The Hippocratic License is a license that puts ethical restrictions on the use of OSS code, such as prohibiting its use for violating human rights or dignity. The Hippocratic License aims to give developers more control over how their software is used and to prevent its use for harmful purposes.

MODULE 7:
LEGAL GOVERNANCE, CYBER FORENSICS, CYBER INTELLIGENCE

Agencies in Australia that Investigate Cybercrime. Australia has established several key agencies dedicated to investigating cybercrime. These include the Australian Cyber Security Centre (ACSC), the Australian Federal Police (AFP), and the Australian Criminal Intelligence Commission (ACIC). These agencies work collaboratively to combat cyber threats, protect national interests, and maintain cybersecurity. Understanding their roles and cooperation is vital in the fight against cybercrime within the country.

Cyber forensics is a crucial discipline in the realm of cybersecurity. It involves the collection, preservation, analysis, and presentation of digital evidence to uncover cybercrimes. Cyber forensic experts use their skills to track down hackers, investigate data breaches, and support legal proceedings. This field plays a pivotal role in maintaining the security and integrity of digital information and is essential for both cybersecurity professionals and law enforcement agencies.

Cyber intelligence is the collection and analysis of data related to cyber threats and vulnerabilities. It provides insights into potential cyberattacks, helping organizations and governments take proactive measures to protect their information systems. In Australia, agencies like the Australian Signals Directorate (ASD) engage in cyber intelligence activities to safeguard national security. Cyber intelligence is a critical component of modern cybersecurity, enabling timely responses to emerging threats and ensuring the resilience of digital infrastructure. Understanding its principles is vital for cybersecurity professionals and policymakers alike.

7.1 AGENCIES THAT INVESTIGATE CYBER CRIME

The Commonwealth of Australia has a *National Plan to Combat Cybercrime* that includes a wide variety of agencies and stakeholders. The list that follows shows the spectrum of government agencies whose combined efforts amount to Australia's response to cybersecurity and cybercrime prevention.

- **Attorney-General's Department (AGD)**: formulates Commonwealth criminal law policy for parliament to enact. It includes such matters as personal identity security, privacy and wire-tapping policy.
- **Australian Criminal Intelligence Commission (ACIC)**: Australia's national criminal intelligence agency provides independent advice to government on current and developing risks of organised crime. ACIC has wide-ranging investigative capabilities from which it produces strategic intelligence assessments. It coordinates the effort to disrupt the impact of organised crime in Australia.

- **Australian Federal Police (AFP)**: Enforcement of federal criminal law and the proactive protection of Australia's interests from crime at home and overseas. The AFP has high capability to investigate, disrupt and apprehend cyber-criminals.
- **Australian Transaction Reports and Analysis Centre (AUSTRAC)** is the Australian government's financial intelligence agency that monitors financial transactions to detect money laundering, organised crime, tax evasion, welfare fraud and terrorism.
- **Commonwealth Director of Public Prosecutions (CDPP)**: Works with AFP and ACIC to prosecute offenders. Also provides advice to other prosecuting and investigating agencies at the State level in relation to cybercrime offences.
- **State and Territory law and justice agencies**: Concerned with criminal law policy at the state and Territory level.
- **State and Territory police**: Enforcement of State and Territory law. Police cybercrime units investigate all cyber offences against the person, business, and state, territory and local government.

Other related agencies:

- **CERT Australia**: The initial point of contact for cyber security incidents occurring in or impacting on Australian networks.
- **Australian Communications and Media Authority (ACMA)**: Notifies Internet Service Providers of transient threats such as malware identified among their customers. Also provides a channel of communication for reporting illegal online content.
- **Australian Competition and Consumer Commission (ACCC)**: Disrupts scams and prosecutes under the *Competition and Consumer Act 2010 (Cth)*.
- **Australian Security Intelligence Organisation (ASIO)**: Concerned with cyber activity for the purpose of espionage, sabotage, terrorism or other forms of politically motivated violence. Works with other investigatory agencies to prevent efforts directed against Australia.
- **Australia New Zealand Policing Advisory Agency (ANZPAA)**: A trans-Tasman advisory and coordinating body that provides policy advice on cross-jurisdictional issues.
- **CrimTrac**: A national database aimed at disseminating timely advice to state and federal agencies and stakeholders.
- **Department of Broadband, Communications and the Digital Economy (DBCDE)**: Responsible for the provision of internet services to government, industry and the community.
- **Department of Defence's Cyber Security Operations Centre (CSOC)**: Concerned with identifying sophisticated cyber threats against Australia.
- **Department of Foreign Affairs and Trade (DFAT)**: Protects Australia's interests by combating cybercrime internationally.
- **Department of the Prime Minister and Cabinet (PM&C)**: Central coordinator of cyber policy.

7.2 CYBER FORENSICS

Cyber forensics is an extensive discipline in its own right -- a fit topic for a course all its own. This section gives an overview of the discipline, highlighting methods and important considerations. While it will not make the average cyber-security professional a forensics expert, it will nonetheless acquaint them with the principles, and equip them to communicate with forensics consultants in a meaningful way.

LEGAL ISSUES

While a data breach cause might be determined through the application of forensic techniques, certain legal issues might complicate matters. For example, the *'Trojan Defence'* which allows an apparent perpetrator to argue that it was not they, but a piece of malicious computer code, or Trojan, that performed the actions unbeknown to them. A competent forensic investigator could anticipate this defence and obtain evidence to dismiss the argument.

SCENE OF THE CRIME

Information systems, as any cybersecurity professional will agree can be the 'scene of a crime' when a data breach has occurred. There will be evidence left behind of the perpetrators in the form network logs and other traces.

Organisations in recent years have employed forensics to investigate cases of:

- Hacking of commercially sensitive material
- Intellectual Property (IP) theft
- Fraud
- Forgery
- Bankruptcy
- Improper or illegal system use in the workplace
- Regulatory compliance

EVIDENCE MUST BE ADMISSIBLE IN COURT

Admissibility is a key consideration, and this means the evidence is accurate, not prejudicial and was legally obtained.

To ensure admissibility:

1. **Data** that may be subsequently relied upon in court **must not have been changed** during collection.
2. Persons with access to said data **must be competent** and have a legitimate reason for access.
3. **Access logs are kept** providing an audit trail of access, complete with details of who, what, where when and how access occurred, and any actions performed.

4. The **chief investigator has oversight** and is responsible for ensuring the law is always respected.

The forensic investigator will use a *"write-blocker"* to make an exact copy of an original hard disk, thus preserving the original in unchanged form.

INVESTIGATORY STAGES

Broadly speaking, the process can be divided into six stages:

1. **Readiness** – a proactive stance that ensures a system is in a state of functional readiness for forensic investigation. There are two aspects; the IT staff have been briefed and knows what needs to happen in the case of a breach, and secondly the investigator must be trained and competent.
2. **Evaluation** – in the event of an incident, it must be clear to all concerned what their role is and what the impact of the incident is likely to be.
3. **Collection** – the process of collecting evidence in a way that ensures admissibility in a court of law. This includes placing items in tamper-resistant bags and labelling them properly, conveying them to a secure environment as designated by law enforcement. Is also likely to involve interviewing various people.
4. **Analysis** -- must be accurate, thorough, impartial, recorded, repeatable and completed within the time-scales available and resources allocated.
5. **Presentation** – preparation of a report on findings written in plain language that non-forensic experts would understand. This would be in accordance with the initial instructions, plus any other relevant information.
6. **Review** – performed afterwards as a kind of lessons learned, process improvement exercise that identifies how the process might be done more efficiently in the future.

COUNTERMEASURES

Criminals engage in an on-going game of cat and mouse in which they constant seek loopholes in existing defences to exploit. Encryption is one such way; to prevent forensic analysis data may be over-written to render it unrecoverable. A files metadata can be changed, or the file subjected to "obfuscation" to disguise it.

7.3 DATA BREACH INTELLIGENCE

Data breach intelligence forms a subset of a larger threat intelligence landscape. There are categories of threat intelligence that agencies of all kinds (government and private) use to gather information that might be useful in proactively managing threat.

If you are a commercial organisation, or government department not directly concerned with legally sanctioned intelligence gathering, some of these methods will not be legally available.

INTELLIGENCE SOURCES

Cyber Security Intelligence analyses and disseminates tactical information about cyber threats, actors, and incidents. Cyber Security Intelligence can help organizations improve their cyber defence, response, and resilience.

Here are nine sources of Cyber Security Intelligence that can provide valuable insights and data:

PRIMARY SOURCES OF CYBER INTELLIGENCE

Cyber intelligence (CYBINT) is the collective name for data derived from a variety of intelligence-collection disciplines, as discussed below. CYBINT often gathers data from SIGINT (Signals intelligence), OSINT (Open-source intelligence) and ELINT (Electronic Intelligence). Less often it is derived from SOCMINT (Social Media Intelligence), HUMINT, GEOINT (discussed after this section).

1. **Signals intelligence** (SIGINT) derived from having listened into or intercepted the signals of persons of interest. In civil society, this is likely to be illegal, though in the defence of national interest, such methods are legally employed.
2. **Tech intelligence** (TECHINT) relates to information on the hardware and software capabilities of adversaries, allowing proper countermeasures.
3. **AlienVault Open Threat Exchange.** Categorised as Open-Source Intelligence (OSINT). This is one of the largest and most popular free open-source intelligence platforms, with over 100,000 participants sharing threat data and indicators of compromise (IOCs).
4. **ACSC Annual Cyber Threat Report**. Open-Source Intelligence (OSINT). This is an official report by the Australian Cyber Security Centre (ACSC), which provides an overview of key cyber threats impacting Australia, how the ACSC is responding to them, and crucial advice for Australian individuals and organisations to protect themselves online.
5. **CrowdStrike Global Threat Report**. Open-Source Intelligence (OSINT). This is an annual report by CrowdStrike, a leading cybersecurity company, that provides in-depth analysis of threat trends, adversary tactics, techniques, and procedures (TTPs), and recommendations for enhancing security posture.

6. **Threat Intelligence Communities.** Open-Source Intelligence (OSINT). Groups of individuals or organizations that share threat intelligence information and collaborate on cyber security issues. Threat intelligence communities can be formal or informal, public, or private, and have different levels of trust and access.
7. **Endpoint Devices**. These are the devices that connect to a network, such as computers, smartphones, tablets, and IoT devices. Endpoint devices can store useful data about user activity, system configuration, installed applications, and potential malware infections.
8. **Network Traffic**. This is the data that flows through a network, such as packets, protocols, ports, and IP addresses. Network traffic can reveal information about network topology, device communication, data exfiltration, and malicious activity.
9. **Threat Intelligence Platforms**. These are software tools that aggregate, correlate, and analyse threat data from multiple sources, such as feeds, reports, endpoints, and networks. Threat intelligence platforms can help automate threat detection, prioritization, and response.
10. **Threat Intelligence Providers**. Organizations that offer threat intelligence services or products to customers, such as reports, feeds, alerts, or analysis. Threat intelligence providers can have different areas of expertise, such as industry-specific threats, regional threats, or threat actor profiles.

SECONDARY SOURCES OF CYBER INTELLIGENCE

1. **Market intelligence** (MARKINT) helps in understanding the commercial environment of an adversary.
2. **Human intelligence** (HUMINT) through direct or indirect contact with people likely to have useful information. Might also be gathered through observation.
3. **Geospatial intelligence** (GEOINT) derived from sources such as GPS data and maps.
4. **Financial intelligence** (FININT) is information relating to the finances, or financial capabilities of adversaries. FININT is a principle tool in the fight against money laundering.

CREATE A CYBERTHREAT INTELLIGENCE PROGRAM (CIP)

As a complement to your Incident Response (IR) a Cyberthreat Intelligence Program (CIP) is an aspect of organisational risk management working in conjunction with the security operations centre (SOC) and producing information on request from management and board.

The CIP allows for the prioritization of attacks and the necessary updating of protective measures. It facilitates the early detection of incidents. It includes *operational* and *strategic* components. The operational component identifies and investigates incidents and fine-tunes the protection and detection processes. The

strategic component allows for networking with external parties who might be helpful, for example information sharing and analysis centres (ISACs) and other threat-sharing communities as well as specialist information providers. This networking allows for the identification of evolving threats, and of new and possibly disruptive technologies.

When setting up your CIP, the following points will be useful to consider.

- Identify from where you will be getting your data – this is a pre-requisite of properly defining the threat landscape.
- Concentrate your efforts on your specific business or sector because collecting intelligence that is not relevant will deplete your resources and divert attention.
- Create your table of priorities early and be disciplined in giving proper focus to the higher priorities, not allowing peripheral matters to deflect your efforts into less productive areas.
- Think of your CIP as a work-in-progress and deliberately build in the kind process improvement feedback loops that will allow the plan to evolve strategically over time.
- As far as possible automate the processing and dissemination of intelligence, as relying on manual processing is time consuming and limited in capability.

7.4 LEGAL ASPECTS OF CYBER RISK: STATE, NATIONAL & INTERNATIONAL

The ***International Legal Guide*** group based in London publish an excellent up-to-date country-by-country resource of the legal statutes applicable to cybersecurity at a state and national level.

The information available at their website is written in layperson's language but expressed with the precision that is the hallmark of legal writing. I would not attempt to summarise at the risk of misunderstanding and misrepresenting an issue in a small but significant way.

Follow the link below and peruse the entries to gain a view of the laws currently in force in relation to cybersecurity in Australia.

URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia

It is segmented as follows:

1. **Cybercrime**
2. **Cybersecurity Laws**
3. **Preventing Attacks**
4. **Specific Sectors**
5. **Corporate Governance**
6. **Litigation**
7. **Insurance**
8. **Investigatory and Police Powers**

7.5 CASE STUDIES

Case Study 1: X, the sales manager of Company A gives 4 weeks' notice. Soon after he leaves, Company A receives advice from several clients that they received emails from an unknown Hotmail account containing defamatory information about Company A. Computer Forensics NZ Ltd (CFNZ) is instructed to search for evidence on X's PC that the emails originated from it.

During the briefing CFNZ suggests that the PC be examined for any evidence of any confidential data being copied to removable external media during the preceding 4 weeks.

Every bit and byte on the PC's hard disk is acquired and preserved using rigorous procedures as employed by NZ Police, the Serious Fraud Office, NZ Customs etc. The data is then meticulously analysed and various data (deleted) and system files are recovered showing that email data was created at the date and time that X was known to be operating the PC.

Detailed analysis also shows that during the last 3 days of X's employment 1 MYOB data file and 1 Microsoft Access file were copied to a USB drive. The files and detailed report are provided to Company A and appropriate discussions are held with the company's legal advisors for recommended action.

Case Study 2: Computer Forensics - Cyber CrimeIt was noticed by her manager that C's work output had been dropping over the previous 3 weeks, which coincided with the provision of broadband Internet to her department. It is visually established that she is spending many hours Internet 'surfing', which is specifically banned under her terms of employment.

She is cautioned appropriately but she continues with the unauthorised activity. Workmates also note that pornographic images are seen on her PC after the second caution.

The company subsequently dismisses her and within 14 days the company receives formal advice that it would be served with a charge of unjustified dismissal.

The manager convinces Management that all correct procedures were followed and that the Internet use was clearly beyond any amount or type that could be considered reasonable. Management decides to contest the action, especially as a significant amount of money is at risk and instructs CFNZ to analyse her PC for evidence of excessive Internet activity and deliberate entry to pornographic sites.

Analysis of her PC by CFNZ shows that incontestable evidence exists proving conclusively that the company's assertions were correct.

Finally, costs are awarded to the employer.

MODULE 8:
IMPACT OF IT ON SOCIETY

Social media and online behaviour. Social media platforms such as Facebook, Twitter and Instagram allow us to connect with people around the world, share our opinions and interests, and access information and entertainment. However, they also pose some challenges and risks, such as cyberbullying, fake news, privacy breaches and addiction. We need to be aware of these issues and use social media responsibly and ethically.

Technology for social good. IT can also be used to address social problems and improve the lives of people in need. For example, IT can help with disaster relief, health care, education, environmental protection and human rights. There are many initiatives and organizations that use IT for social good, such as the United Nations, the Red Cross, Khan Academy and Wikipedia. We should support and participate in these efforts to make a positive difference in the world.

Accessibility and inclusion. IT can also help to reduce barriers and inequalities for people with disabilities, minorities, women and other marginalized groups. For example, IT can provide assistive devices, adaptive software, online learning and remote work opportunities for people with disabilities. IT can also promote diversity, inclusion and empowerment for people from different backgrounds, cultures and perspectives. We should respect and celebrate the diversity of people in the IT field and society at large.

8.1. SOCIAL MEDIA & ONLINE BEHAVIOUR

Social media platforms have become an integral part of our lives, connecting us with people, information and entertainment.

There are significant risks for individuals and organisations, such as cyberattacks, privacy breaches, misinformation and ethical dilemmas. How can we use social media responsibly and safely, while enjoying its benefits?

PROTECT YOUR DATA & DEVICES

One of the main threats of social media is that hackers can exploit the data you share online to launch cyberattacks, steal your identity or access your accounts. To prevent this, you should:

- Use strong passwords and change them regularly.
- Enable two-factor authentication for your accounts.
- Avoid clicking on suspicious links or attachments.
- Update your software and antivirus regularly.
- Review your privacy settings and limit what you share publicly.
- Be careful when using public Wi-Fi or devices.

BE RESPECTFUL & ETHICAL

Another challenge of social media is that it can amplify negative emotions, opinions and behaviours, such as anger, hatred, discrimination and harassment. To avoid this, you should:

- Think before you post or comment.
- Respect the views and feelings of others.
- Avoid spreading rumours or false information.
- Report or block abusive or offensive content.
- Follow the rules and guidelines of each platform.
- Seek help if you experience cyberbullying or distress.

LEARN AND GROW

Social media can also be a valuable source of learning and growth, if used wisely and critically. You can:

- Follow reputable sources of information and news.
- Verify the accuracy and credibility of what you read or watch.
- Seek diverse perspectives and opinions.
- Engage in constructive and respectful dialogue.
- Explore new topics and interests.
- Share your knowledge and skills with others.

Social media is a powerful tool that can have positive or negative impacts on society, depending on how we use it. By following these tips, you can make the most of social media, while protecting yourself and others from its risks.

THE NEED FOR ETHICAL POLICIES

Ethical policies are not only beneficial for individuals and society, but also for IT professionals and organizations. They can help to foster trust, reputation, innovation, and competitiveness in the IT sector. They can also prevent or mitigate legal, financial, and reputational damages that may result from unethical IT practices.

Some examples of ethical policies that can be adopted or implemented in the IT field are:

Data protection and privacy policies. These policies aim to protect the personal data of users and customers from unauthorized access, use, disclosure, or deletion. They also specify the rights and obligations of data subjects and data controllers regarding data collection, processing, storage, and transfer.

Cybersecurity policies. These policies aim to ensure the security and integrity of IT systems and networks from malicious attacks or threats. They also define the roles and responsibilities of IT staff and users regarding cybersecurity measures, such as encryption, authentication, backup, and incident response.

Social responsibility policies. These policies aim to promote the positive social impact of IT and to minimize its negative effects on society and the environment. They also encourage the involvement of IT stakeholders in social issues, such as digital inclusion, education, health care, and sustainability.

Professional ethics policies. These policies aim to uphold the ethical standards and principles of the IT profession. They also provide guidance and codes of conduct for IT professionals regarding their duties, rights, and responsibilities towards their clients, employers, colleagues, and society.

Ethical policies are not static or universal. They need to be updated and adapted to the changing IT landscape and to the diverse cultural and legal contexts. They also need to be communicated and enforced effectively to ensure compliance and accountability. Moreover, they need to be supported by ethical education and awareness programs that foster a culture of ethics among IT stakeholders.

Ethical policies are not a burden or a constraint for IT. They are an opportunity and a necessity for IT to contribute positively to society and to achieve its full potential.

PRIVACY PROTECTION & DATA SHARING

As an IT professional, you have a responsibility to protect the privacy of your clients, customers, and users. Privacy is a fundamental human right, and it is also essential for trust, innovation, and competitiveness in the digital economy. However, privacy protection is not always easy or straightforward, especially when it comes to data sharing. Data sharing can have many benefits, such as improving efficiency, quality, and collaboration, but it can also pose significant risks, such as data breaches, identity theft, and discrimination.

How can you balance the need for data sharing with the respect for privacy?

Know the law. Different countries and regions have different laws and regulations regarding privacy and data protection. You should be aware of the legal requirements and obligations that apply to your data processing activities and comply with them accordingly. For example, if you are dealing with personal data from the European Union, you should follow the General Data Protection Regulation (GDPR), which sets high standards for data protection and gives individuals more rights and control over their data.

Know your data. Before you share any data, you should know what kind of data you have, where it came from, how it was collected, what it is used for, and who has access to it. You should also classify your data according to its sensitivity and value and apply appropriate security measures to protect it. For example, you should encrypt sensitive data such as health records or financial information, and limit access to authorized personnel only.

Know your purpose. You should only share data for a specific and legitimate purpose that is compatible with the original purpose of collection. You should not share data for purposes that are unrelated, incompatible, or harmful to the individuals or groups involved. For example, you should not share customer data with third parties for marketing or advertising purposes without their consent.

Know your partners. You should only share data with trustworthy and reliable partners who have a similar or higher level of privacy protection than you. You should also establish clear and transparent agreements with your partners that specify the terms and conditions of data sharing, such as the purpose, scope, duration, security, and accountability of data processing. You should also monitor and audit your partners' compliance with the agreements and the applicable laws.

Know your limits. You should only share the minimum amount of data that is necessary to achieve the purpose of data sharing. You should also respect the rights and preferences of the individuals or groups whose data you are sharing and give them choices and control over their data. For example, you should inform them about the data sharing activities, obtain their consent when required, allow them to access, correct, or delete their data when possible, and respond to their complaints or requests promptly.

ONLINE HARASSMENT & CYBERBULLYING

Online harassment and cyberbullying are serious issues that affect many people, especially children and adolescents. They can cause emotional, psychological and even physical harm to the victims, as well as damage their reputation and relationships.

ONLINE HARASSMENT & CYBERBULLYING

Online harassment and cyberbullying are forms of bullying that use digital technologies, such as social media, messaging platforms, gaming platforms and mobile phones, to intimidate, humiliate, threaten or harm someone else. They can include:

- Spreading lies, rumours or embarrassing photos or videos about someone online
- Sending or requesting nude or nearly nude images or videos (also known as sexting)
- Excluding someone from online groups or conversations
- Making fun of someone's appearance, identity, beliefs or abilities
- Stalking someone online or offline
- Impersonating someone online or hacking their accounts
- Sending hateful or violent messages or threats

Online harassment and cyberbullying can happen to anyone, but some groups are more vulnerable than others, such as girls, LGBTQ+ youth, ethnic minorities and

people with disabilities. Online harassment and cyberbullying can have negative effects on the victims' mental health, self-esteem, academic performance and social skills. They can also increase the risk of depression, anxiety, loneliness, self-harm and suicide.

PREVENTING HARASSMENT & CYBERBULLYING

The best way to prevent online harassment and cyberbullying is to promote a culture of respect, kindness and empathy online. Here are some tips to help you do that:

- Be aware of what you post online and how it might affect others. Think before you share something that could be hurtful, offensive or inappropriate.
- Respect other people's privacy and boundaries. Do not share personal or private information about someone else without their consent. Do not send or ask for nude or nearly nude images or videos.
- Be a positive role model for others. Use positive language and compliments online. Support those who are being harassed or bullied online. Report any abusive or harmful content or behaviour you see online.
- Educate yourself and others about online safety and digital citizenship. Learn how to protect your personal information, passwords and devices online. Learn how to recognize and avoid scams, phishing and malware. Learn how to use privacy settings and blocking features on different platforms. Learn about your rights and responsibilities online.

COPING WITH HARASSMENT & CYBERBULLYING

If you are experiencing online harassment or cyberbullying, you are not alone and you do not deserve it. Here are some steps you can take to cope with it:

- Do not respond or retaliate to the harasser or bully. This might only make things worse or escalate the situation. Instead, ignore them or block them if possible.
- Save the evidence of the harassment or bullying. Take screenshots or record the messages, posts or comments that are abusive or harmful. This can help you report them later or seek legal action if needed.
- Report the harassment or bullying to the platform where it happened. Most platforms have policies and tools to deal with online abuse and hate speech. You can also report the harasser or bully to their school, employer or authorities if they are breaking the law.
- Seek support from someone you trust. Talk to a friend, family member, teacher, counsellor or helpline about what you are going

through. They can offer you emotional support, advice and resources to help you cope.

- Take care of yourself. Online harassment and cyberbullying can affect your physical and mental health. Try to do things that make you happy and relaxed, such as hobbies, exercise, meditation or music. Avoid drugs and alcohol as they can worsen your mood and health.

8.2. TECHNOLOGY FOR SOCIAL GOOD

ETHICAL INNOVATION & POSITIVE IMPACT

Ethical Innovation & Positive Impact: How to Use Technology for Social Good

How can we ensure that our innovations are aligned with our values and contribute to positive social impact?

DEFINE YOUR PURPOSE AND VISION

Before you start developing or implementing any technology solution, you need to have a clear idea of what problem you are trying to solve, who you are serving, and what impact you want to achieve. This will help you set your goals, measure your progress, and communicate your value proposition to your stakeholders.

ENGAGE WITH YOUR USERS AND BENEFICIARIES

Technology for social good should be designed with and for the people who will use it and benefit from it. You need to understand their needs, preferences, expectations, and feedback. You also need to respect their rights, dignity, privacy, and autonomy. Engaging with your users and beneficiaries will help you create solutions that are relevant, accessible, inclusive, and empowering.

CONSIDER THE BROADER CONTEXT AND IMPLICATIONS

Technology for social good should not operate in isolation, but in relation to the social, cultural, economic, environmental, and political context in which it is deployed. You need to consider how your solution will interact with other systems, actors, and norms. You also need to anticipate the potential positive and negative consequences of your solution, both intended and unintended, and mitigate any risks or harms.

ADOPT ETHICAL PRINCIPLES AND STANDARDS

Technology for social good should be guided by ethical principles and standards that reflect your values and commitments. You need to define what ethical innovation means for you and your organization, and how you will operationalize it in your processes, practices, and policies. You also need to align your solution with the relevant laws, regulations, codes of conduct, and best practices in your field.

EVALUATE YOUR IMPACT AND LEARN FROM YOUR EXPERIENCE

Technology for social good should be continuously monitored and evaluated to assess its impact and effectiveness. You need to collect data and evidence that show how your solution is performing, what outcomes it is producing, and what impact it is having on your users, beneficiaries, and society at large. You also need to learn from your experience, reflect on your successes and failures, and improve your solution accordingly.

THE ESSENCE OF TECHNOLOGY FOR SOCIAL GOOD

Technology needs to be guided by ethical principles, aligned with social values, and informed by evidence-based practices.

TECHNOLOGY FOR SOCIAL GOOD

Technology for social good is the use of technology to address social problems, such as poverty, inequality, health, education, environment, and human rights. Technology for social good can take many forms, such as:

- Digital platforms that connect people, resources, and information across borders and sectors.
- Mobile applications that provide access to essential services, such as health care, education, and banking.
- Data analytics that help measure and improve the impact of social interventions.
- Artificial intelligence that enhances human capabilities and supports decision making.
- Blockchain that enables transparency and accountability in transactions and governance.
- Internet of things that enables smart and sustainable solutions for energy, water, and waste management.

POLICIES GUIDING ETHICAL INNOVATION

It is important to have policies that guide ethical innovation and ensure that it aligns with the values and needs of the people it serves.

ETHICAL FRAMEWORK FOR INNOVATION

One possible ethical framework for innovation is based on the Principles for Digital Development, which are nine guidelines that help integrate best practices into technology-enabled programs. They include:

- **Design with the user**. Involve the user throughout the design process and test the solution in real contexts.
- **Understand the existing ecosystem**. Assess the strengths and weaknesses of the current system and identify potential partners and stakeholders.
- **Design for scale**. Plan for growth and sustainability from the start and consider how to reach more users over time.
- **Build for sustainability**. Secure long-term funding and support and ensure that the solution can operate independently of external resources.
- **Be data driven**. Collect, analyse and use data to inform decision making and improve performance.

- **Use open standards, open data, open source, and open innovation**. Adopt interoperable and transparent approaches that facilitate collaboration and sharing of knowledge and resources.
- **Reuse and improve**. Learn from existing solutions and adapt them to the local context and needs.
- **Do no harm**. Assess and mitigate the risks and harms that the innovation may cause to the users, communities and environment.
- **Address privacy and security**. Protect the data and information of the users and respect their rights and preferences.

Ethical innovation is about ensuring that technology is human-centered, inclusive, responsible and impactful. By following these principles, innovators can design solutions that are more likely to achieve social good and avoid unintended consequences.

DATA PRIVACY & SECURITY

Data privacy is the right of individuals to control how their personal data is collected, used, shared and stored by others. Data security is the protection of data from unauthorized access, use, modification or destruction. Data privacy and security are closely related, but not the same. Data privacy focuses on the rights and choices of individuals, while data security focuses on the technical and organizational measures to safeguard data.

IMPLEMENTING BEST PRACTICES FOR DATA PRIVACY AND SECURITY

Here are some of the best practices for data privacy and security for technology for social good:

Assess and classify data. First, assess your business data comprehensively to understand what types of data you have. Then, classify your data according to its sensitivity and the value it adds to your business.

Practice minimal data collection. A rule of thumb when collecting data is to only collect what you need. Avoid collecting unnecessary or excessive data that may increase the risk of exposure or misuse.

Get consent and be transparent. Before collecting or using someone's data, get a clear go-ahead from the user. And this shouldn't be buried in jargon; it should be as clear as day. Let them know why and how you are collecting their data, how you will use it, who you will share it with and how long you will keep it.

Practice robust data security. Use encryption, authentication, access control and other technical measures to protect your data from unauthorized access or loss. Also implement policies, procedures and training to ensure that your staff and partners follow the best practices for data security.

Encourage education and awareness. Privacy can become a way to engage with your customers and show them you respect their data. Educate them about their rights and choices regarding their data, and provide them with easy ways to access, update or delete their data if they wish.

Create achievable policies and SLAs with third parties. If you work with third parties who handle your data, such as cloud providers, vendors or contractors, make sure they adhere to the same standards of data privacy and security as you do. Establish clear policies and service level agreements (SLAs) that define the roles, responsibilities and expectations of each party.

By following the best practices outlined in this article, you can ensure that your technology respects the rights and interests of your users and beneficiaries, while also creating value and impact for your organization and

ADDRESSING ETHICAL DILEMMAS

Identify the stakeholders and their values. Who are the people or groups that are affected by the technology, directly or indirectly? What are their needs, preferences, rights, and responsibilities? How do they value the benefits and risks of the technology?

Analyse the ethical issues and principles. What are the moral values or principles that are relevant to the technology and its use? For example, privacy, autonomy, justice, transparency, accountability, etc. How do they conflict or align with each other and with the stakeholders' values?

Evaluate the alternatives and consequences. What are the possible actions or decisions that can be taken regarding the technology and its use? What are the potential outcomes and impacts of each alternative on the stakeholders and their values? How likely and how severe are they?

Choose the best option and justify it. Based on the analysis and evaluation, what is the most ethical option that balances the interests and values of all stakeholders? How can you explain and defend your choice using ethical reasoning and evidence?

Monitor and revise as needed. How can you monitor the implementation and effects of your choice? How can you identify and address any new or unforeseen ethical issues that may arise? How can you learn from your experience and improve your ethical decision-making in the future?

8.3. ACCESSIBILITY & INCLUSION

THE DIGITAL DIVIDE

The digital divide is the gap that exists between those who have access to digital technology and the internet, and those who do not. It affects millions of people in Australia, especially in remote and regional areas, low-income households, older people, and people who speak a language other than English at home.

The digital divide can limit people's ability to participate in society, access essential services, communicate with others, learn new skills, and find opportunities. It can also increase social isolation, disadvantage, and inequality.

There are ways to bridge the digital divide and promote digital inclusion. Digital inclusion means ensuring that everyone can access, afford, and use digital technology and the internet effectively. It also means helping people develop their digital ability, which is the knowledge, skills, and confidence to use digital technology safely and creatively.

HOW TO MEASURE DIGITAL INCLUSION

One way to measure digital inclusion is to use the Australian Digital Inclusion Index (ADII). The ADII is a tool that uses survey data to measure digital inclusion across three dimensions: access, affordability, and digital ability. The ADII also explores how these dimensions vary across the country and across different social groups.

The latest ADII report shows that digital inclusion at the national level is improving, but there are still significant gaps and challenges. For example, 11 per cent of Australians are "highly excluded" from digital services, meaning they do not have access to affordable internet or don't know how to use it. That equates to about 2.8 million people.

The report also shows that the divide between metropolitan and regional areas has narrowed but remains marked. People in capital cities are more likely to be online than those in regional areas, and unsurprisingly, low-income earners struggle to connect. There are different reasons for the digital divide – many older Australians lack online literacy, while in some areas a lack of infrastructure limits options.

BRIDGING THE DIGITAL DIVIDE

Bridging the digital divide requires a collaborative effort from various stakeholders, including governments, businesses, community organisations, educators, researchers, and users themselves. Some of the strategies that can help bridge the digital divide are:

- Improving the availability and quality of internet infrastructure and services in remote and regional areas
- Providing affordable and flexible internet plans and devices for low-income households
- Offering free or subsidised access to public internet facilities such as libraries, community centres, or Wi-Fi hotspots
- Developing and delivering digital literacy programs that cater to the needs and preferences of different groups of users
- Supporting online safety and security awareness and education
- Encouraging and facilitating online participation and engagement in social, cultural, economic, and civic activities
- Promoting innovation and creativity in using digital technology for personal and professional development

LEGAL & ETHICAL IMPERATIVES

Accessibility and inclusion are not only good practices, but also legal and ethical obligations for organisations that provide products, services or information to the public.

WHAT IS ACCESSIBILITY AND INCLUSION

Accessibility involves designing systems to optimise access for people with disability or other diverse needs. Inclusion is about giving equal access and opportunities to everyone wherever possible, and respecting and valuing diversity.

Accessibility and inclusion benefit not only people with disability, but also other groups such as older people, people from different cultural backgrounds, people with low literacy or digital skills, and people in remote areas.

WHAT ARE THE LEGAL AND ETHICAL FRAMEWORKS FOR ACCESSIBILITY AND INCLUSION?

There are several laws and standards that require organisations to provide accessible and inclusive products, services or information. These include:

The Disability Discrimination Act 1992 (DDA), which makes it unlawful to discriminate against people with disability in various areas of public life, such as employment, education, accommodation, access to premises, goods, services and facilities.

The Web Content Accessibility Guidelines (WCAG), which are internationally recognised standards for making web content accessible to people with disability. The Australian Government has adopted WCAG as the minimum level of accessibility for all government websites.

The United Nations Convention on the Rights of Persons with Disabilities (CRPD), which is an international treaty that promotes and protects the human rights of people with disability. Australia ratified the CRPD in 2008 and has obligations to ensure that people with disability can access information, communication, technology, education, health, employment, justice and other services on an equal basis with others.

Apart from legal compliance, accessibility and inclusion are also ethical imperatives for organisations that want to demonstrate social responsibility, respect for human dignity, and commitment to diversity and innovation .

IMPLEMENTING ACCESSIBILITY AND INCLUSION

To implement accessibility and inclusion effectively, organisations need to adopt a holistic approach that covers all aspects of their operations, such as:

Developing an Accessibility Action Plan that outlines the organisation's vision, goals, strategies, actions, responsibilities, timelines and measures for improving accessibility and inclusion for people with disability as employees, customers and stakeholders.

Making workplace adjustments that anticipate the needs of people with disability and provide reasonable accommodations for individuals, such as ergonomic equipment, assistive technology, flexible working hours and locations.

Communicating and marketing in accessible ways that ensure that all communication channels, such as websites, social media, emails, brochures, videos and podcasts are accessible to people with disability and can be adjusted for individual preferences.

Designing products and services that value people with disability as customers, clients or service users and address their needs when developing and delivering products or services.

Recruiting and retaining people with disability as employees at all levels of the organisation and providing them with career development opportunities.

Engaging suppliers and partners that reflect and enable the organisation's commitment to accessibility and inclusion and expect them to follow best practices.

Innovating practices and processes that continually strive to do better in accessibility and inclusion and seek feedback from people with disability to improve outcomes.

PROMOTING INCLUSIVITY

WHY IS INCLUSIVITY IMPORTANT?

Inclusivity is not only a moral duty, but also a strategic advantage for organizations. By promoting inclusivity, organizations can:

- Enhance their reputation and trust among customers, employees, partners and regulators.
- Increase their innovation and creativity by tapping into diverse perspectives and experiences.
- Reduce their legal and ethical risks by complying with relevant laws and standards.
- Improve their efficiency and effectiveness by avoiding bias, errors and waste.

PROMOTING INCLUSIVITY

Promoting inclusivity requires a holistic approach that involves all stakeholders in the IT governance, policy, ethics and law domains. Here are some best practices that I recommend based on my research and experience:

- Establish a clear vision and strategy for inclusivity that aligns with the organization's mission, values and goals.
- Define and communicate the roles and responsibilities of each stakeholder in ensuring inclusivity throughout the IT lifecycle.
- Conduct regular assessments and audits to measure the level of inclusivity and identify gaps and opportunities for improvement.
- Provide training and education to raise awareness and skills on inclusivity issues and solutions.
- Implement policies and standards that support inclusivity principles and practices.
- Adopt tools and methods that enable inclusive design, development, testing and evaluation of IT solutions.
- Engage with diverse groups of users, customers, experts and communities to solicit feedback and input on IT solutions.
- Monitor and review the impacts and outcomes of IT solutions on different groups of people and society at large.

MODULE 9:
CYBER LOSS PROCESS & CYBER INSURANCE

Trends in Cyber Loss Processes. The environment of cyber threats has led to a shift in how organizations manage cyber losses. This dynamic field is experiencing trends in incident response, mitigation, and recovery. Cyber loss processes now focus on swift detection, effective containment, and resilient recovery strategies. Understanding these trends is crucial for organizations to adapt and safeguard their digital assets.

Cyber Insurance. With the increasing frequency and sophistication of cyberattacks, cyber insurance has emerged as a critical tool in risk management. This insurance provides coverage for losses resulting from data breaches, ransomware attacks, and other cyber incidents. It plays a vital role in helping organizations recover financially from the fallout of cyberattacks. As a key component of a comprehensive cybersecurity strategy, cyber insurance is essential for mitigating the financial risks associated with cyber threats. Understanding its principles and benefits is crucial for businesses in today's digital landscape.

9.1 TRENDS IN CYBER LOSS PROCESSES

Several trends have emerged in cyber loss processes as organizations seek to improve their cyber risk management and response capabilities. These trends include:

- **Incident Response Automation** - organizations are adopting automation tools and technologies to improve their incident response capabilities. Automated incident response systems can detect and respond to cyber threats in real-time, reducing response times, minimizing the impact of attacks, and improving overall cyber resilience.
- **Threat Intelligence Sharing** - collaboration and sharing of threat intelligence between organizations, industries, and even across national borders has become crucial. By sharing information on emerging threats, attack techniques, and vulnerabilities, organizations can proactively defend against cyber threats and better protect their systems and networks.
- **Cyber Insurance** - demand for cyber insurance has been on the rise as organizations recognize the financial risks associated with cyber incidents. Cyber insurance policies help mitigate potential financial losses by covering costs such as incident response, legal expenses, customer notifications, and business interruption.
- **Focus on Cyber Resilience** - rather than solely relying on prevention measures, organizations are shifting their focus towards building cyber resilience. This involves implementing strategies and technologies to enable quick recovery and continuity of operations in the face of a cyber

incident. Cyber resilience includes measures such as regular data backups, incident response planning, and robust business continuity management.

- **Regulatory Compliance and Data Privacy** - with the increasing number of data protection regulations worldwide (e.g., GDPR, CCPA), organizations are prioritizing compliance efforts. This includes implementing strong data privacy practices, conducting privacy impact assessments, and ensuring secure data handling and processing.
- **Cloud Security and Third-Party Risk Management** - as organizations embrace cloud computing and rely on third-party vendors for various services, managing cloud security risks and assessing third-party cyber risk have become critical. Organizations are implementing robust security measures, conducting thorough due diligence on vendors, and establishing clear contractual agreements to mitigate potential risks.
- **Cybersecurity Training and Awareness** - recognizing that human error is a significant factor in cyber incidents, organizations are investing in cybersecurity training and awareness programs for their employees. These programs aim to educate staff about common cyber threats, best practices for data protection, and the importance of maintaining good cyber hygiene.
- **Cyber Exercise and Simulation** - organizations are conducting regular cyber exercises and simulations to test their incident response plans and identify potential gaps. These exercises involve simulating realistic cyber-attack scenarios to assess the effectiveness of response processes, train incident response teams, and improve overall preparedness.

By staying informed and adapting to these trends, organizations can enhance their cyber loss processes, better mitigate cyber risks, and respond effectively to cyber incidents.

DATA EXFILTRATION

Data exfiltration is the unauthorized extraction or theft of data from a computer network, system, or device. It involves the unauthorized transfer of sensitive, confidential, or valuable data from an organization's internal network to an external location or unauthorized recipient.

Data exfiltration can occur through various methods, such as exploiting vulnerabilities in the network, using malware or malicious software, leveraging social engineering techniques, or unauthorized physical access to devices. The stolen data can include intellectual property, financial information, personally identifiable information (PII), trade secrets, or any other valuable data assets. Data exfiltration is a significant risk to organizations, including financial loss, reputational damage, regulatory compliance issues, and potential legal repercussions.

Data exfiltration continues to be the predominant cause of insured losses, with individual companies suffering significant data breaches. While the frequency of

smaller data breaches has reduced in United States, incidences are increasing in most other countries. The sizes of successful breaches are increasing, and breaches are becoming costlier in many jurisdictions. There has been a significant shift towards large scale data breaches occurring outside of the U.S., particularly in Asia.

RECORD-BREAKING SIZE OF DATA EXFILTRATION EVENTS

In May 2017, one of the largest data breaches ever recorded occurred in China, where 2 billion phone records were stolen from the popular Chinese call-blocking tool DU Caller. The U.S. has still suffered from large scale and high-profile data breaches. Equifax, the U.S. based credit reporting agency, was subjected to a high-profile data breach, which resulted in an estimated 143 million U.S. customers personal and financial information stolen. Yahoo's parent company Verizon, which officially acquired Yahoo in June 2017, announced in a statement that the 2013 data breach has resulted in all 3 billion email accounts being compromised. Evidence that the data is being sold on the black market by an Eastern European hacking collective may result in an increase in email fraud and account takeovers. The disclosure of further data loss and evidence of fraudulent use of this data could increase financial liabilities in the future.

DECREASING INCIDENCE RATES OF DATA BREACHES

Data exfiltration events in U.S. increased rapidly during the period 2009 to 2014. Events since 2014 have continued to occur at a similar incidence rate, with variation year-on-year, but have not continued the rapid rate of increase of the previous five years and show signs of declining.

This correlates with major increases in investment in cyber security across many of the companies at risk, and a focus on prevention and awareness in staff that is reducing

the number of accidental data loss incidents and smaller breaches. It may also reflect the decreasing 'return on effort' for hackers as black-market prices fall for stolen data.

Cyber-criminals are finding easier ways to make money, including ransomware and extortion. Hackers are making less money out of data exfiltration, as the black-market sale price of stolen records from data breaches has fallen with the abundant supply of stolen personal data now being offered for sale.

Cyber attackers may instead be turning to less secure targets in other countries, and to other forms of cybercrime, such as extortion. Data exfiltration remains a very lucrative form of crime for the more professional cyber criminals, who focus on larger scales of thefts from their targets. The median size of successful data exfiltration attacks has continued to increase over time.

INCREASING MAGNITUDE OF GLOBAL LARGE-SCALE DATA BREACHES

While the overall numbers of data breaches has fallen due to improved methods of prevention, the severity of data incidents has nonetheless grown. The number of records stolen per breach of P3 and higher (greater than 1000 records) has tripled over the past three years. Severity of large-scale data breaches have generally increased over time, with the data being skewed by a few extremely large data loss events. Professional hackers are becoming more sophisticated in their approaches to data exfiltration.

Company	Country	Number of Records	Date	Severity
Du Group DBA Du Caller	China	2 Billion	2017	P8
River City Media	United States	1.37 Billion	2017	P8
Netease, Inc.	China	1,22 Billion	2017	P8
Emailcar	China	268 Million	01/01/2017	P8
Deep Root Analytics	United States	200 Million	2017	P8
Equifax Inc.	United States	143 Million	2017	P8
National Social Assistance Programme (NSAP),	India	135 Million	01/11/2016	P8
Tencent Holdings Limited	China	130 Million	2017	P8
Reliance Jio Infocomm Ltd	India	120 Million	2017	P8
Youku	China	91 Million	2017	P7
Edmodo	United States	77 Million	2017	P7
Jigsaw Holdings (Pty) Ltd	South Africa	60 Million	2017	P7
Uber Technologies, Inc.	United States	57 Million	13/10/2016	P7
Republic of The Philippines Commission On Elections	Philippines	55 Million	11/01/2017	P7
Altel Communications	Unknown	50 Million	01/01/2014	P7
Dun & Bradstreet	United States	33 Million	2017	P7
Yahoo Inc.	UK	32 Million	2017	P7
Sina Corporation Dba	China	31 Million	2017	P7
Unitebook Smart	China	30 Million	01/01/2017	P7

Selected Recent Large Data Breaches

COMPANIES ARE HOLDING MORE DATA

"Data is the new gold": Companies are harvesting data from their customers and mining it for insights in ever increasing volumes. The total amount of business data being stored is estimated to be doubling every 12 to 18 months. This means that the potential for data exfiltration of sensitive information is increasing rapidly. The size of datasets, and the aspects of people's lives and behaviours that could potentially be exfiltrated, is a constantly upward trend. The magnitude of data exfiltration losses can be expected to increase in the future.

DATA BREACHES BY BUSINESS SECTOR

Other the past eight years, data exfiltration incidences have been most frequent in organizations involved in public sector, education and healthcare. Certain types of data are worth more than others and personal health records (PHI (Private Health Insurance)) and personal identifiable information (PII) are worth more on

the black market, relative to credit cards and other personal finance records. The fact that these organizations hold more of these types of data, combined with potentially lower security standards, make these sectors more attractive targets.

Recent incidence rates of data loss for different business sectors remain broadly consistent with previous patterns. Data breach rates have increased in IT services, manufacturing sectors, and have doubled in retail. An emerging recent target for data breaches has been offshore legal firms in tax havens, with a string of incidences of whistle-blower tax filings, including another exfiltration, following on from the Panama Papers in 2016, of the so- called 'Paradise Papers' where 1.4TB of sensitive financial and legal information about clients of offshore legal firm Appelby was leaked to the public.

COST TRENDS IN DATA BREACHES

There has been an increasing trend in the average cost per record of data loss for incidents over 100,000 records. This is attributed to the regulatory costs, escalating legal complexity and growing cost of compensation. Costs of data exfiltration attacks vary significantly between countries and increases in countries with lower compensation costs have resulted in average costs worldwide apparently decreasing, but costs are generally increasing over time in many countries, as regulations tighten. The highest cost per record remains in the U.S. due to the increasing notification costs. Average costs per record are reported to have decreased recently in Western Europe, particularly in the U.K., Austria and Denmark. Costs of data breaches are expected to increase in Europe with the implementation of GDPR. Costs in other countries are likely to rise, such as Asia-Pacific countries as they move towards tougher data breach laws including the new Cyber Security Laws introduced in China.

Cyber insurers are increasingly moving their larger insured accounts to 'managed response' relationships, where they control the claim costs when they occur, and this is managing to reduce the cost of data breaches in those client accounts.

The business impact of a data breach has reduced, with some of the consequences having diminished, such as churn (number of customers lost due to a data breach) which has reduced in Western Europe.

DATA LOSS MAINLY CAUSED BY EXTERNAL OUTSIDERS

The main cause of data breaches is attacks from malicious outsiders rather than accidental losses or 'whistle-blower' leaks from employees. While external actors remain the most pertinent threat, internal threats are still a concern to most corporations. The escalating use of third-parties such as sub-contractors is responsible for a growing proportion of loss events. Contractor-breaches result from businesses being granted, access to vital systems within a company's network. One of the higher profile 'contractor- breaches' was from National Security Agency (NSA), which demands the highest level of vetting for employees.

ACCIDENTAL DATA LOSS REMAINS SIGNIFICANT

Unintended disclosure of data remains a significant loss process. While the forensic costs are often less when data is unintentionally disclosed, cost to insurers can still be substantial due to the high notification and credit monitoring costs.

CONTAGIOUS MALWARE

Malware that can replicate and spread through networks of communication has been one of the longest-standing cyber threats. Recent events have shown that malware remains a potent trigger for loss, even in companies with high standards of security. Most significantly WannaCry and NotPetya demonstrated that contagious malware can scale and to cause systemic loss to thousands of companies.

WANNACRY AND NOTPETYA

WannaCry and NotPetya demonstrated the disruptive capabilities of viruses, worms, and trojan horses to spread through populations of organizations, see case studies.

Many of these infections affected organizations of different geographical location, industry and size.

CYBER CONTAGION AND CYBER PHYSICAL

These contagious cyber attacks have had significant effects on physical operating environments. They have affected critical infrastructure and public services, imperilling public safety. Previous extortion attacks, for example on hospitals remained compartmentalized to an individual hospital or specific department. The WannaCry event threatened public safety across large numbers of hospitals. WannaCry affected 81 out of 236 National Healthcare System Trusts throughout United Kingdom, and 603 primary care providers. The disruption locked up important medical equipment such as MRI scanners, and caused the diversion of patients, the cancelling of appointments and surgeries, and forced a reversion to manual record keeping.

WannaCry affected over 300,000 machines, many critical to national infrastructure such as power stations and transportation hubs, localized and international banking systems, global manufacturing networks and logistics and delivery centres.

RANSOMWARE ATTACKS ON THE RISE

The use of ransomware, where malware is infiltrated into the networks of a company and disables servers or locks up data until a ransom is paid, has become one of the most pressing concerns for cyber security specialists. Attempts to extort major companies using cyber-attacks have grown in frequency, scope and

ambition. Many companies have developed contingencies for ransomware attacks in the future. Some commentators have suggested that companies stockpiling BitCoin in case of extortion attacks may have fuelled the recent surges in BitCoin demand.

Estimates of ransomware extorted in 2017 exceed five billion dollars, a 15-fold increase over the previous two years. Ransomware has historically afflicted personal computers and small and medium sized enterprises, but recent developments have seen large multinational corporations affected, with security companies seeing some 42 percent of all ransomware infections in the first half of 2017 targeting organizations in an interconnected and networked environment.

CYBER EXTORTION FROM LARGE COMPANIES

Ransomware is not the only method of cyber-attacks that has been used for extortion. There have been several high-profile instances where data exfiltration attacks have resulted in ransom demands. In the July 2017 HBO breach, hackers threatened to release upcoming episodes of hit shows if a price was not met. Another targeted attack, utilizing the ransomware Erebus against a South Korean web hosting company, Nayana, in which all its servers were encrypted, resulted in a $1 M ransom being paid and the bankruptcy of the company. Increasingly, the interconnectedness of things has been exploited by cyber criminals. The past year has seen a rise in targeted attempts to extort major multinational corporations, often compromising thousands of machines across these organizations

FINANCIAL THEFT

Financial theft has continued to be a major source of cyber-attacks and cyber-enabled fraud.

Compromising networks of trust to misappropriate financial transfers remains a significant threat, despite major efforts to improve security. Cyber-attacks on customer systems continue to be a major cause of loss.

CUSTOMER SIDE FINANCIAL THEFT

Cyber attacks on the customer side of financial institutions continue to dominate, with online fraud plaguing the e-commerce, airline and retail industries. Physical fraud on ATM’s and point-of-sale (POS) terminals also remain a key threat.

An emerging threat is complex attacks on the financial institutions and their company’s internal systems (back-end systems) and key counterparty networks of trust, involving sophisticated threat actors. This is evident from the Bangladeshi and Taiwanese SWIFT attacks (see case study) and the Polish financial regulator attack in early 2017. which are both linked to the North Korean hacking group Lazarus.85 Cyber-attacks for financial theft and fraud are still a more significant element of cyber loss than ransomware, with 2.5 times the annual detection of cyber-attacks involving financial malware.

MUTED EMV IMPLEMENTATION IN THE U.S.

The U.S. remains a key location for credit card fraud, accounting for 24 percent of total credit card use, but 47 percent of global credit card fraud. In 2016, Visa, Mastercard, and Europay credit card companies introduced new rules in the U.S. requiring retailers to upgrade their point-of-sale terminals to accept EMV-chip enabled cards. These rules are accompanied by an EMV fraud liability shift requiring retailers to bear the costs for card-present and other point-of-sale (POS) fraudulent card transactions if merchants did not upgrade their systems.

Implementation of the EMV post-liability shift has been slow, with only 52% of U.S. card-accepting merchants upgraded to EMV technology88 compared with 84.9% of European vendors. Sluggish rollout of EMV in the U.S. has been attributed to the cost of implementing EMV technology, regulatory confusion, and lack of awareness of the risk of cyber-fraud, particularly for small-medium sized enterprises. U.S. continues to see many types of card-present and point-of-sale fraud, including cashing counterfeit EU payment cards.

DIGITAL CURRENCY AND FINANCIAL THEFT

Cyber-attacks have increased against third-party cryptocurrency wallets to steal digital currency, exploiting weaknesses in factor security verification in wallets. Reports of financial theft from wallets is wide-spread, with at

least 36 major heists on cryptocurrency exchanges since 2011. In July 2017, three separate cyber-attacks occurred across cryptocurrency platforms, including 153,000 Ethereum worth $30 million stolen from the widely used Parity Wallet. Cyber-attacks in cryptocurrency markets undermines attempts to validate digital currency and impedes the introduction of insurance against digital financial theft.

FINANCIAL TRANSACTION THEFT REMAINS KEY THREAT

A major source of large loss from cyber-attacks is the emergence of cyber criminals targeting financial institutions by penetrating banks internal systems, including inter-bank transaction networks. The Lazarus SWIFT financial theft in early 2016 was one of the most audacious cyber bank heists of its kind, which could have resulted in a theft of more than a billion dollars. The 2016 campaign successfully stole $81 million, with dozens of banks and central banks compromised including the U.S. Federal Reserve. The hackers hit the SWIFT network by repeatedly using specially-crafted software which allowed them to gather information on standard practices and send fraudulent requests for funds across the network.

In response to the cyber-attack, SWIFT in 2017 announced an updated security protocol. The vulnerability was not in the SWIFT technology itself, but a weakness in the security of some of the member banks, so SWIFT introduced the Customer Security Control policy which gives advice on how to segregate SWIFT and critical systems from a member bank's general framework. Further security measures

include a new real-time payment controls service to reinforce existing fraud controls and cyber-crime prevention.

The security update in 2017 has become more pertinent because of a further attack on the SWIFT network involving Taiwanese banks (see case study). Although the amount stolen was smaller, the risk of large losses from compromises of financial transaction systems remains significant

HIGH STANDARDS OF CYBERSECURITY IN FINANCIAL COMPANIES

Banks and financial service companies are fully aware of their susceptibility to attempted hacks and are leaders in the implementation of security systems and measures for preventing cyber theft. Expenditure on cybersecurity by banks has been high profile and extensive; the banking industry is the single largest sector of cybersecurity expenditure. Bank of America disclosed that it spent $400 million on cybersecurity in 2015 and, in January 2016, its CEO said that its cybersecurity budget was unconstrained.

JP Morgan Chase and Co. announced the doubling of its cybersecurity budget from $250 million in 2015 to $500 million. Financial services continue to be the largest investors in cyber security.

CLOUD OUTAGE

Cloud computing is being adopted increasingly rapidly. The failure of a cloud service provider, while very unlikely, represents a potential cyber insurance systemic exposure as many cyber policies include coverage for outages. Failures of individual services or availability regions have the potential to cause losses to thousands of users.

Cloud computing has successfully inundated the global markets, creating a utility-like service for over 90% of companies.103 Adoption rates for use of the public cloud reached an estimated 18% with up to $246 Billion in revenue worldwide. Large numbers of companies depend on the cloud, particularly in the ecommerce sector which accounts of 8.9% of total sales in the U.S. This represents a significant exposure to a potential failure of cloud service providers in cyber-affirmative IT insurance portfolios.

CONCENTRATION RISKS IN BIG FOUR CLOUD SERVICE PROVIDERS (CSPS)

The global market of CSPs continues to be dominated by Amazon Web Services (AWS) at 47%, followed by Microsoft Azure at 10%, Google Cloud Platform with 4%, & IBM Softlayer with 3%.

While Amazon’s position of market leader has yet to be seriously threatened by its competitors, the highest cloud adoption rates went to Microsoft Azure, particularly in application workloads. Azure adoption grew from 20 to 34 percent in a single year, while AWS maintained a steady 57 percent. While this could be due to the size of AWS relative to Microsoft Azure, Azure’s marketability to

companies aiming to work in hybrid cloud may have begun to tip the scales. Azure's infrastructure is marketed to support data within a company's data centre and within the Azure cloud, which may catch the attention of prospective clients. 67% of cloud users currently report using a hybrid cloud strategy which allows processes in-house and on the cloud.

HIGH RESILIENCE STANDARDS OF CLOUD SERVICE PROVIDERS

To be competitive in the public CSP (Cloud Service Providers) market, providers need to minimize downtime and deliver on promised reliability ratings. While companies can state that their products are designed to deliver '99.999999999% durability', the Service Level Agreements (SLAs) for AWS' compute service 'EC2', and Microsoft Azure's cloud services, dictate an official commitment to their customers of 99.95% reliability for each region.

To maintain such high levels of reliability, the architecture of CSPs focuses on strategic isolation to protect the spread of malicious software and geographic redundancies for datacentres to reduce downtime. With plans for continued growth across the industry, the AWS Cloud operates 44 Availability Zones within 16 geographic Regions around the world, Microsoft with 36 regions, Google with as 13 regions, 39 zones, and IBM with 60 IBM Cloud data centres.

POTENTIAL DISRUPTION FROM CSP FAILURE

While agreements of 99.95% reliability are impressive, anything less than 100% translates to damaging downtime. The critical minutes or hours of downtime have proven to be costly to both the CSPs and their clients. The committed 99.95% reliability of the top 4 CSPs would legally allow for roughly four and a half hours of downtime for customers.

The cost of downtime for 98% of organizations for a single hour totals $100,000, with 33% of those enterprises reporting that one hour of downtime costs their firms $1-5 million.

Downtime for a CSP rarely translates to a shutdown of the entire cloud. Rather, CSP downtime often manifests in service interruption to a single service, or, in the case of interdependent services, all those associated with the single service. Interruption to 'compute' and 'storage' services have the potential to cause greatest impact on customers as interdependencies within the cloud are often traced back to these essential services. Isolation between CSP availability zones limits the impact of the down service(s) - aiming to prevent global interruption.

DENIAL OF SERVICE ATTACKS

Distributed Denial of Service (DDos) attacks continue to be a major component in the cyber risk landscape. A third of all organizations reportedly experience DDoS attacks, twice as many as a year ago. This trend of growing likelihood of attack is

likely to continue across sectors, geographies, and activity areas, as the firepower capacity of attackers increases, and they seek out new targets.

INCREASING COMPLEXITY OF DDOS ATTACKS

A Distributed Denial of Service attack uses internet traffic to overwhelm servers forcing a shut-down of the system or a slowing of services. This increased traffic denies access and limits usability to legitimate users or systems. Not only is the number of DDoS attacks increasing, but so too is the complexity.

Instead of tactics focused on single aspect of a company's infrastructure, DDoS attacks are taking a more diversified approach, alternating targets within a single attack including web application servers, firewalls, and other infrastructure components. Additionally, by varying the modes within of attack, an additional layer of complexity can be added. Attack types are broadly categorized into Volume Based Attacks, Protocol Attacks, and Application Layer Attacks each with a different method of overwhelming site bandwidth. The increased complexity of a multi-modal attack makes these attacks difficult for a company to defend its networks both proactively and reactively.

PULSE DDOS ATTACKS

The typical attack pattern of DDoS attacks has also grown in complexity. While previously a DDoS attack pattern was pictured as a prolonged wave leading to a peak in activity followed by a rapid descent, a new tactic known as the 'pulse wave attack' has changed the timing of attacks.

A pulse wave attack is a rapid succession of attacks with the interval between each attack being used to mount the next attack on a different target. It may take attackers only minutes to bring down a server which will take hours to reinstate. Pulse DDoS attacks can extend for days at a time and thus pose a significant risk to the accessibility of a company's network.

The significance of complex successive attacks is that large commercial servers designed to deal with high traffic volumes are resilient against attacks of low intensity, but very-high intensity attacks with frequently changing targets within a network's infrastructure can bring down even the strongest websites. It is possible that no web server will be resilient to disruption from DDoS attacks if the intensity of attacks continues to scale up.

REPEATED ATTACKS ON TARGETS

Repeat attacks on targets are a common characteristic of DDoS attacks. The average number of DDoS attacks per target is increasing. Over 75% of targets are reportedly hit multiple times, an increase from 43.2% in 2016.118 There is a wide variation in number of attacks per target, with some companies reporting several hundreds of attacks.

INTERNET OF THINGS: A TECHNOLOGY FOR DDOS ATTACKS

Much of the firepower from recent DDoS attacks has been drawn from Internet of Things (IoT) devices connected to the web. In addition, IoT devices can also become vulnerable targets for DDoS attacks: computers, mobile devices, tea-kettles, fish tanks, all being used in recent DDoS attacks. IoT devices serve as an ideal platform for DDoS attacks. Networks for IoT devices are notoriously vulnerable and offer high speed connections on a consistently switched on network. Until manufacturers of IoT devices address network security, these devices will continue to pose an increasingly large threat as a platform for DDoS attacks as IoT devices are projected to account for more than two-thirds of the 34 billion internet connected devices by 2020.

POLITICAL USE OF DDOS ATTACKS

The motivations for recent DDoS attacks have been evolving, with politically-motivated DDoS attacks gaining the focus of the media globally. DDoS attacks accompanied the Qatar Crisis, with an attack on Al Jazeera, the largest news network in the area, the presidential elections in France where Le Monde and Le Figaro websites were targeted, and voter registration for Brexit in U.K. among others.

SECTORAL PREFERENCES IN DDOS TARGETING

Profiling the business sectors that experience the highest number of DDoS attacks has consistently indicated that the Gaming Industry, with its need for reliable, high-speed connections, is a preferred target for DDoS cybercriminals. Other popular targets for DDoS attacks for 2017 included the Software & Technology Sector as well as Internet & Telecom and Financial Services. Other sectors including Media & Entertainment, Retail & Consumer Goods, and Education sectors have all reported frequent DDoS attacks.

BUSINESS DISRUPTION FROM DDOS ATTACK

For most competitive companies, internet access is as essential as basic utilities. A DDoS attack, regardless of platform threatens the accessibility of network traffic from legitimate customers and thereby the bottom line of web-based sales. Business interruption loss poses one of the most severe financial outcomes of a DDoS attack as without reliable access to internet functionality, significant financial losses can result. A DDoS attack which is designed to cause such disturbances to essential network infrastructure has recently been estimated to cost companies up to $2.5 million per attack. Insurance agencies have paid out Business Interruption claims specifically for DDoS and DDoS extortion attacks with pay- outs nearing half a million dollars.

DDOS PROTECTION

Many cyber security companies offer DDoS protection and tracking software which create intelligent resilience solutions for customers. These solutions include protective firewalls, large networks which can absorb DDoS attacks, and monitoring software to keep track of network traffic.

By monitoring the internal and external network traffic, and defining 'normal' traffic patterns, companies can be alerted when they deviate from the norm. DDoS traffic can usually be traced to bots or hijacked web-browser rather than personnel, so it is important to monitor signatures and identifiable attributes of network traffic. The best protection for a company is to diversify protection techniques. An internal understanding of the norm for a company's network, paired with the software to monitor and protect this norm allows for expedited mitigation techniques from emergency response services in the event of a DDoS attack.

CASE STUDY: THE RETURN OF LAZARUS: MORE SWIFT FINANCIAL THEFTS IN 2017

Sophisticated cyber-attacks continued to enable financial thefts from the SWIFT inter-banking financial transaction system, following on from the major attacks in 2016. The victim of the 2017 attack was Far Eastern International Bank (FEIB) based in Taiwan. The gang used a vulnerability in the bank's security, which allowed the group to secretly implant their malicious malware onto the bank's computers and servers.97 This lead to a SWIFT terminal operated by the bank becoming compromised.

Once the group gained access to the SWIFT network and acquired the credentials necessary for payment transfers, the group attempted to fraudulently transfer $60 million to accounts in United States, Cambodia and Sri Lanka.98 Due to a mistake by the criminals causing an error in the specific fields of the SWIFT transfer, banking officials were alerted and all but $500,000 was recovered.

As with previous attacks on the SWIFT network, the attackers used a specifically-crafted malware with many layers of subterfuge to avoid discovery. The sophistication of the attack is highlighted due to the incorporation of ransomware in the attack, which is likely to have been used to mislead the cyber security community. However, the money laundering process was less sophisticated than in previous attacks on the SWIFT network, and two 'money mules' were arrested attempting to physically withdraw stolen funds from a bank account in Sri Lanka.

Some have attributed this attack to the North Korean state-sponsored hacking group Lazarus due to the similarities in the method of attack.100 This group is a sophisticated advanced persistent threat (APT) group which has been associated with many high-profile financial thefts including Bangladeshi SWIFT attack in 2016 and the 2017 attack on Polish banks.

The continuation of attacks on financial network highlights that these are attractive targets offering big rewards to cyber criminals. Systems in place continue to manage to stop the criminals extracting the full potential from the initial penetration, although other attacks are known to succeed

9.2 CYBER INSURANCE

The growing cyber insurance market is continuing to be profitable but has had some near misses that could have substantially impacted the industry loss ratio. Growth is coming from new sectors and markets. Implementing growth and loss control strategies is a major priority.

RAPID GROWTH

The cyber insurance market continues to demonstrate consistent growth at around 30% year on year. Estimates for 2020 range from between $5 to 10 billion, with several analysts expecting by 2025 the market could be as large as $20 billion.

While this represents substantial growth, it remains modest in comparison with the overall commercial insurance market of $247 billion. It is also relatively small in comparison with the overall corporate cyber risk management spend, with Gartner reporting worldwide cybersecurity spending at over $75.4 billion.

DRIVERS OF GROWTH

A review of many cyber insurance policies seen by RMS suggests the growth in the U.S. has been driven by increased take up from non-traditional purchases of cyber insurance (outside healthcare, technology and retail), as well as additional premiums generated from the availability of larger limits. International growth has also played a key part, with several markets demonstrating strong growth including Australia, Japan, and the United Kingdom.

Looking more long term, RMS expects substantial growth for the industry driven by not just cyber but a broader category of digital risks. Businesses are becoming increasingly reliant on technology to run their operations and while this brings obvious benefits, it also means they are increasingly vulnerable to system failures, data losses and cyber-attacks. As the rate of technology change continues apace, the digital environment is likely to become even more complex and the amount of digital information will grow exponentially.

Corporate risk managers need to develop comprehensive digital risk management strategies that involve a range of mitigations with risk transfer solutions through insurance being critical. Given the pervasive nature of technology as the foundation of the modern economy, digital risk provides a once in a generation opportunity for the insurance industry.

MARKET PARTICIPANTS AND INCREASED COMPETITION

The market continues to see a substantial concentration of premium within a handful of insurers. In the U.S. just 4 domestic writers and one Lloyd's insurer generate almost 60% of all premium, according to an analysis of the NAIC statutory filings. This market leading position has allowed these organizations to

develop a wealth of experience and data, affording them a substantial competitive advantage.

However, a key trend observed over the last two years has been the entrance of many new carriers. There are now more than insurers reporting cyber premiums, although their participation remains limited. In 2016, 68 insurers reported premiums greater than a million dollars, and of these only 28 had more than $5 million.

The increased competition is having an impact, with rates reportedly down over the last 12 months as well as a general loosening of coverage terms. Despite high profile systemic cyber events over the last 12 months, the limited impact on the cyber insurance industry has likely only exacerbated this issue.

INTERNATIONAL GROWTH

While most premiums emanate from the U.S., there are substantial signs of growth internationally, with Europe, Japan and Australia all seeing significant rises in GWP, albeit from a relatively small base.

New data protection regulations coming in to place in Australia appear to be stimulating the market, and it is expected that GDPR will have a similar impact for the EU.

PROFITABILITY OF CYBER LINES

RMS estimates the industry loss ratio for 2016 at 54.6%. This is based on an extensive review into the occurred events and insurance penetration for 2016. This is slightly higher than the 47.6% reported from the admitted business in the U.S.132 However, it is still healthy return compared with more mature insurance markets.

LOSS PROCESSES

RMS analysis shows that breach of privacy events (such as data exfiltration) continues to contribute the largest financial impact to losses. As has been widely reported, the proliferation of ransomware (see previous section) has resulted a large spike in the frequency of extortion and BI claims.

To date the costliest losses have been driven by individual large loss events rather than more systemic events. This has had the impact of spreading the losses unevenly across insurers, with loss ratios varying substantially between carriers, with writers of larger corporates seeing volatile losses. Some have been fortunate enough to return single digit loss ratios while others have ratios greater than 150%.

NEAR MISSES

But it is fair to say it could have been a very different picture had the WannaCry and NotPetya events played out differently. An analysis of the WannaCry incident

carried out by RMS calculated that with just a few small variations in the way it played out, insured losses for the industry would have exceeded $3 billion.

CYBER REINSURANCE

The cyber reinsurance market has continued to develop over the last 12 months. Insurers are now more aware of the potential for systemic incidents to trigger substantial losses and are looking to the reinsurance market to transfer some of this risk off their balance sheets.

Most reinsurance contracts remain as per risk quota share with some aggregate stop loss terms adding additional protection for the reinsurer. However, over the last 12 months RMS is seeing several brokers structuring more complex treaties including excess of loss.

MANAGING CYBER EXPOSURE

Driven by increased regulatory pressures and improved awareness at the board level, insurers have looked to implement practices to manage cyber risk. However, substantial challenges exist in providing the clear visibility required.

As many commentators have stated, cyber coverage can be found in numerous other lines of business, including property, general liability, crime, kidnap and ransom, and potentially many others. This is either through endorsements or silent 'non-affirmative' coverage.

CONSISTENT APPROACHES

Implementing a consistent approach to managing risk across these diverse classes of business is a challenge for many insurers. Some of the main challenges are with the inconsistency in policy wordings, ambiguity in the strength of exclusions, and varying data quality approaches to data capture across multiple often legacy systems.

The clear need for visibility into cyber risk has led insurers to tackle these challenges head on. RMS has worked with many insurers over the last 12 months to implement robust but practical exposure management approaches leading to significantly improved visibility.

PRICING CYBER RISK

Approaches to pricing cyber risk have yet to come to a consensus across the industry. A review of the rate fillings provided to insurance commissioners in the U.S. highlight the challenges of pricing cyber risk given the limited historical data and the relatively dynamic peril. Among the approaches documented includes borrowing from other classes; "we chose to use fiduciary liability data because it has a similar limit profile and expected development pattern [as cyber losses]",

and “factors are taken from our Miscellaneous Professional Liability product”– a less than ideal approach.

RISK CAPITAL ALLOCATION

At the portfolio level, the potential impact of cyber catastrophe risk is predominantly monitored through deterministic models. This has led to increased awareness of the potential for systemic risk to have a material impact on a cyber portfolio and provides insurers with an approach to identify and mitigate risk accumulations. However, approaches to assigning return periods to losses, and thereby supporting the inclusion of modelled results within capital modelling applications have to date been limited.

These challenges highlight the need for improved data and risk models to support the industry’s growth in a resilient manner.

9.3 CASE STUDY: WANNACRY MALWARE ATTACK

WannaCryptor ransomware spread via file-sharing network protocols on computers using outdated Windows XP and v8 OS. It resulted in 300,000 infections of computers across 150 countries. WannaCry used a NSA exploit codenamed EternalBlue (released the previous August by ShadowBrokers). It mainly affected personal users, public sector organizations, and SME-sized companies, affecting unpatched boxes and equipment on dedicated older operating systems. Several dozens of large companies also reported disruption and losses from infections of their systems. Of the roughly 400 million actively-used Windows computers running version 8 or earlier operating system, approximately 0.1 percent were infected. The great majority of the Windows computers running version 8 or earlier were protected by a Microsoft patch MS17-010 issued two months earlier, in March 2017.

The event highlighted the issue of equipment software latency, i.e. that machines and sub-networks within organizations may rely on specific versions of operating system that render them vulnerable. In these cases, although most systems within organizations ran more up-to-date operating systems, certain departments and activities were maintaining the older versions that contained the vulnerability. Machines such as medical MRI scanners and X-Ray machines that were certified on XP and v8 and maintained on those operating systems, were among those that were crippled by the attack.73 Businesses reported substantial losses from lock-outs of systems around the world, such as manufacturing processes, dispatch and ordering systems, gas pump payment applications, and telephone exchange equipment. We estimate the direct costs and indirect business disruption losses from WannaCry to be around half a billion dollars.

If the WannaCry malware was created to generate ransom payments then it was remarkably unsuccessful. The BitCoin accounts that it requested payments into received less than $150,000 in payments and may not have been claimed by the criminals. No company that paid a ransom got its data back. The motivation was more likely to sabotage some of the affected companies, rather than generate funds for the hackers. It is possible that the widespread economic disruption was collateral damage to mask a targeted destructive attack.

The propagation of WannaCry was stopped after four days by a researcher finding a kill-switch within the software. Otherwise the infection could have spread to many more machines and had a more severe impact. RMS counterfactual analysis suggests that if the kill-switch had not been triggered, and if the attack had occurred prior to the issuing of the MS17-010 patch for Windows 8, the infection rates and losses could have been an order of magnitude higher, perhaps reaching $3 to $6 billion.

MODULE 10:
E-GOV & DIGITAL TRANSFORMATION

E-government and digital transformation are two related concepts that aim to improve the quality of life and the efficiency of public services. E-government refers to the use of information and communication technologies (ICTs) to deliver government services, information and participation to citizens, businesses and other stakeholders. Digital transformation is the process of rethinking and redesigning how government operates, interacts and innovates using digital tools and data.

One of the main goals of e-government and digital transformation is to **enhance citizen engagement**, which means involving citizens in the decision-making and policy-making processes of government. Citizen engagement can take various forms, such as online consultations, feedback mechanisms, crowdsourcing, co-creation and participatory budgeting. Citizen engagement can increase the transparency, accountability and legitimacy of government actions, as well as the satisfaction and trust of citizens.

Another goal of e-government and digital transformation is to **create smart cities and ethical urbanization**. Smart cities are urban areas that use ICTs to collect, analyse and use data to improve the management and planning of various aspects of urban life, such as transportation, energy, waste, health, education and security. Ethical urbanization is the principle that smart cities should respect the human rights, dignity and diversity of their inhabitants, as well as promote social inclusion, environmental sustainability and economic development.

A third goal of e-government and digital transformation is to **enable remote work and privacy**. Remote work is the practice of working from a location other than the traditional office, such as home, co-working spaces or public places. Remote work can offer benefits such as flexibility, productivity, cost savings and work-life balance. However, remote work also poses challenges such as communication, collaboration, security and privacy. Privacy is the right of individuals to control their personal information and how it is used by others. Privacy is essential for protecting the identity, reputation and autonomy of remote workers, as well as their personal and professional data.

10.1. E-GOVERNMENT & CITIZEN ENGAGEMENT

E-government initiatives are the use of information and communication technologies (ICTs) to deliver public services, improve government efficiency and transparency, and enhance citizen participation and trust.

Governments worldwide are adopting technological advancements to create more efficient and accessible public services through e-government initiatives. This is an on-going process.

As these initiatives take shape, it becomes necessary to have policies cover a range of considerations, including:

- Data privacy,
- Security,
- Accessibility and,
- Citizen engagement.

Alongside these policies, a range of ethical considerations play a central role in ensuring that e-government efforts are not only efficient and convenient but also uphold.

- Democratic principles,
- Respect individual rights, and
- Promote transparency.

Identify and map your stakeholders based on their interest in and influence on your objectives. Determine the issues on which you need stakeholder input and develop strategies for engagement.

Be clear about what you are trying to achieve, be open about your limitations and constraints, tell people where their input is going, and manage expectations around the outcome and decision-making process.

Use information and communication technologies to facilitate the daily administration of government, improve citizen access to government information, services and expertise, ensure citizen participation in and satisfaction with the government process, and enhance cost-effectiveness and efficiency.

Foster civic engagement through interactive, easy-to-understand data publishing and visualizations. Provide context for your data and help citizens understand what it signifies.

Consult the public on which capital improvement projects to prioritize, update citizens on the progress of projects, and report and communicate the impact of a capital project.

Value information as a national resource and a national asset. Ensure information security, privacy, integrity, accountability, innovation and improvement across all the processes of government.

THE RISE OF E-GOVERNMENT INITIATIVES

The rise of e-government initiatives is driven by various factors, such as the increasing demand for online services, the availability of digital infrastructure and data, the pressure to reduce costs and improve performance, and the opportunities to foster innovation and collaboration.

The benefits of e-government initiatives include improved service quality and accessibility, increased citizen satisfaction and empowerment, reduced administrative burden and corruption, enhanced policy making and accountability, and greater social inclusion and cohesion.

The challenges of e-government initiatives include technical issues, such as interoperability, security, privacy, and digital divide; organizational issues, such as leadership, culture, change management, and human resources; and legal and ethical issues, such as data protection, transparency, accountability, and participation rights.

The best advice on the topic of the rise of e-government initiatives is to adopt a holistic and strategic approach that considers the needs and expectations of all stakeholders, the goals and objectives of the government, the opportunities and risks of ICTs, and the legal and ethical implications of e-government. Some of the key steps are:

- Conduct a situational analysis to assess the current state of e-government in terms of strengths, weaknesses, opportunities, and threats.
- Develop a vision and a roadmap for e-government that defines the desired outcomes, priorities, indicators, and milestones.
- Establish a governance framework for e-government that clarifies the roles and responsibilities of different actors, the decision-making processes, the coordination mechanisms, and the monitoring and evaluation systems.
- Implement e-government projects that are aligned with the vision and roadmap, follow user-centric design principles, ensure interoperability and security standards, involve stakeholder participation and feedback, and evaluate the impacts and outcomes.
- Foster a culture of innovation and learning for e-government that encourages experimentation, collaboration, knowledge sharing, and continuous improvement.

POLICIES FOR DATA PRIVACY & SECURITY

Since e-government involves the collection, storage, and processing of citizen data, there must be robust policies for data privacy and security.

Data privacy and security are essential for e-government and citizen engagement, as they ensure trust, transparency and accountability in the use of personal and public information.

E-government policies should comply with relevant laws and regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the US, that protect consumer rights and choices about how their data are used.

E-government policies should also follow best practices and standards, such as the Information and Data Governance Framework of the National Archives of Australia, that promote data interoperability, quality and value across government agencies and services.

E-government policies should involve citizen participation and feedback, as well as collaboration with other stakeholders, such as private sector, civil society and academia, to ensure data are used for public good and innovation.

ACCESSIBILITY BRIDGING THE DIGITAL DIVIDE

Ethical e-government policies extend to accessibility, ensuring that digital services are available to all citizens, including those with disabilities or limited technological access.

Governments must prioritize designing platforms that adhere to accessibility standards, making sure that no citizen is excluded from utilizing vital services due to physical or digital barriers.

This commitment to accessibility reflects an ethical imperative to create inclusive and equitable digital landscapes.

ENGAGEMENT & INCLUSIVITY

A primary consideration of e-government is to enhance citizen engagement and participation in governance.

Ethical considerations demand that these initiatives be inclusive, providing avenues for *all* citizens to voice their opinions, provide feedback, and influence decision-making processes.

Policies should therefore outline mechanisms for soliciting public input, fostering meaningful dialogue, and ensuring that diverse perspectives are considered when shaping policies and services.

E-government initiatives must also respect and uphold individual rights, both online and offline. Ethical policies should ensure that citizens' rights to privacy, freedom of expression, and access to information are not compromised.

Measures should be in place to prevent the misuse of citizen data, surveillance abuses, or any actions that could infringe upon fundamental rights.

TRANSPARENCY & ACCOUNTABILITY

Transparency is a cornerstone of ethical governance. E-government initiatives should promote transparency by giving citizens access to relevant information about government activities, decisions, and processes.

Policies should mandate the publication of data, budgets, reports, and other pertinent information in formats that are easily accessible and understandable to the public.

This transparency works towards proper accountability and empowers citizens to hold governments to ethical standards.

THE DIGITAL DIVIDE

While e-government initiatives aim to enhance efficiency and accessibility, they also raise concerns about exacerbating existing digital divides.

Ethical policies should address these concerns by prioritizing initiatives that bridge these divides, such as providing digital literacy training and ensuring that marginalized communities have access to necessary technology.

This approach ensures that the benefits of e-government are distributed equitably.

CONVENIENCE VS CONSENT

E-government services often require citizens to share personal information for authentication and verification.

Ethical policies must need to balance the convenience of streamlined services with the necessity of obtaining informed consent from citizens.

Clear communication about how data will be used and the ability to opt-out should be integral to these policies, respecting citizens' autonomy over their personal information.

DIGITAL LITERACY & INFORMED PARTICIPATION

Citizen engagement in e-government initiatives is most effective when citizens are digitally literate and well-informed and have a willingness to engage with e-government.

Ethical considerations extend to providing educational resources that train citizens to navigate digital platforms, understand their rights and responsibilities, and actively participate in governance processes. Policies should encompass strategies for promoting digital literacy and awareness.

E-government has great potential to revolutionize the relationship between citizens and governments, fostering transparency, accessibility, and engagement.

However, realizing this potential requires a foundation of ethical policies that prioritize data privacy, security, inclusivity, transparency, and respect for individual rights.

E-government, guided by ethical considerations, becomes a force for positive change, bridging gaps, enhancing accountability, and ultimately strengthening the democratic fabric of society.

10.2. SMART CITIES & ETHICAL URBANIZATION

Smart cities are urban areas that use digital technologies to improve the quality of life of their inhabitants. They can also help address some of the challenges that cities face, such as congestion, pollution, crime, and inequality. However, smart cities also raise some ethical issues and concerns that need to be considered and addressed by policymakers, developers, and citizens.

NETWORK INFRASTRUCTURE

One of the key features of smart cities is the network infrastructure that connects various devices, sensors, and systems to collect, store, and analyse data. This data can be used to optimize urban services, such as transportation, energy, waste management, and public safety.

However, this also poses some risks of control, surveillance, data privacy, and ownership. Who owns the data generated by smart city technologies? How is it protected from unauthorized access or misuse? How is it shared among different stakeholders and for what purposes? How can citizens have a say in how their data is used and by whom?

POST-POLITICAL GOVERNANCE

Another aspect of smart cities is the post-political governance model that relies on data-driven decision-making and public-private partnerships. This model can enhance efficiency, transparency, and accountability in urban management.

But it can also undermine democratic participation, deliberation, and representation. How are the interests and values of different groups and communities considered in smart city projects? How are the trade-offs and conflicts among them resolved?

How are the roles and responsibilities of public authorities and private actors defined and regulated? How can citizens have a voice and a choice in shaping their smart city?

SOCIAL INCLUSION

A third dimension of smart cities is the social inclusion of citizens in the benefits and opportunities offered by smart city technologies. This includes ensuring access, affordability, usability, and literacy of digital services for everyone.

It also involves promoting citizen participation, engagement, and empowerment in co-creating and co-governing their smart city. However, this also requires addressing the challenges of inequality, discrimination, and exclusion that may arise or persist in smart cities.

How are the needs and preferences of diverse and marginalized groups considered and met in smart city design and implementation? How are the potential harms and disadvantages of smart city technologies for some groups

prevented or mitigated? How can citizens have a sense of belonging and identity in their smart city?

SUSTAINABILITY

A fourth dimension of smart cities is the sustainability of their environmental impact and long-term development.

This entails using smart city technologies to reduce greenhouse gas emissions, conserve natural resources, enhance resilience to climate change, and improve environmental quality. It also implies aligning smart city goals with the broader agenda of sustainable development that encompasses social, economic, and cultural aspects.

This also demands balancing the costs and benefits of smart city technologies for different generations and regions. How are the environmental impacts of smart city technologies measured and monitored? How are they aligned with the global commitments and targets on climate action? How are they integrated with the local contexts and cultures of different cities?

THE RISE OF SMART CITIES REDEFINING URBAN LIVING

Smart cities are urban areas that use digital technologies to enhance the quality of life, efficiency of services, and sustainability of the environment. They aim to solve the challenges of urbanization, such as congestion, pollution, waste, and social inequality.

INVOLVE THE STAKEHOLDERS

Smart cities are not just about technology, but also about people. It is important to engage the citizens, businesses, civil society, and public sector in the planning and decision-making process of smart city initiatives. This can foster trust, collaboration, and innovation among the stakeholders, as well as ensure that the solutions are tailored to the local needs and preferences.

THE HOLISTIC APPROACH

Smart cities are complex systems that require coordination and integration across different domains, such as transportation, energy, health, education, and security. It is essential to adopt a holistic approach that considers the interdependencies and trade-offs among these domains, as well as the potential impacts on the economy, society, and environment. A holistic approach can also help to avoid silos, duplication, and fragmentation of resources and efforts.

ETHICAL & LEGAL COMPLIANCE

Smart cities rely on data collection, analysis, and sharing to provide intelligent services and solutions. However, this also raises ethical and legal issues, such as privacy, security, accountability, and transparency. It is crucial to ensure that the data collection and use are compliant with the relevant laws and regulations, as

well as respect the rights and interests of the data subjects. Moreover, it is advisable to adopt ethical principles and guidelines that can guide the design and implementation of smart city technologies and policies.

PROMOTE INNOVATION & LEARNING

Smart cities are dynamic and evolving entities that need to adapt to the changing needs and expectations of the citizens and the environment. It is important to promote a culture of innovation and learning that encourages experimentation, creativity, and risk-taking. This can help to foster new ideas, solutions, and practices that can improve the performance and outcomes of smart city initiatives. Furthermore, it is beneficial to establish mechanisms for monitoring, evaluation, and feedback that can provide evidence-based insights and lessons for continuous improvement.

ETHICAL DIMENSIONS OF SMART CITIES

Smart cities are urban areas that use digital technologies to improve the quality of life, efficiency of services, and sustainability of resources. They can offer many benefits, such as reducing traffic congestion, enhancing public safety, and promoting social inclusion. However, smart cities also pose ethical challenges that need to be addressed, such as privacy, security, accountability, and participation.

PRIVACY

Smart cities collect and process large amounts of data from various sources, such as sensors, cameras, mobile devices, and social media. This data can reveal sensitive information about the behaviour, preferences, and activities of citizens. How can we ensure that this data is used in a transparent, fair, and respectful way, without violating the rights and dignity of individuals?

SECURITY

Smart cities rely on complex and interconnected systems that are vulnerable to cyberattacks, natural disasters, or human errors. These systems can affect critical infrastructure, such as transportation, energy, or health care. How can we protect these systems from malicious or accidental threats, while ensuring their resilience and reliability?

ACCOUNTABILITY

Smart cities involve multiple actors, such as governments, businesses, civil society, and citizens. These actors have different roles, responsibilities, and interests in the design, implementation, and evaluation of smart city initiatives. How can we ensure that these actors are accountable for their actions and decisions, and that they comply with ethical standards and legal regulations?

PARTICIPATION

Smart cities aim to improve the well-being and empowerment of citizens by providing them with more choices, opportunities, and services. However, not all citizens have equal access to or influence on these benefits. How can we ensure that smart city initiatives are inclusive, participatory, and responsive to the needs and expectations of diverse and marginalized groups?

By applying ethical principles and values to smart city projects, we can ensure that they are not only smart but also fair, responsible, and human-centered.

DATA PRIVACY & SECURITY

Data privacy and security laws aim to protect citizens from the misuse, loss, unauthorized access or disclosure of their personal information by government agencies or private organisations.

WHY IS DATA PRIVACY & SECURITY IMPORTANT?

Data privacy and security are important because they respect the fundamental human right to privacy and dignity of individuals.

They foster trust and confidence in the digital economy and society and enable citizens to exercise control and choice over their personal information.

They also prevent identity theft, fraud, cybercrime and other harms that can result from data breaches or misuse, and support innovation and competitiveness by creating a level playing field for data-driven businesses.

BEST PRACTICE FOR DATA PRIVACY AND SECURITY

Data privacy and security best practices are based on the following principles:

Lawfulness, fairness and transparency. Personal information should be collected and processed only for legitimate, specified and explicit purposes, with the consent or authorization of the individuals concerned, and in a clear and open manner.

Data minimization. Personal information should be adequate, relevant and limited to what is necessary for the purposes for which it is processed.

Accuracy. Personal information should be accurate, complete and up-to-date, and corrected or deleted if inaccurate or outdated.

Storage limitation. Personal information should be kept only for as long as necessary for the purposes for which it is processed, and securely disposed of when no longer needed.

Integrity and confidentiality. Personal information should be protected from unauthorized or unlawful processing, accidental loss, destruction or damage, using appropriate technical and organisational measures.

Accountability. Data controllers and processors should be responsible for complying with data privacy and security laws and regulations, and demonstrate their compliance through documentation, audits, reporting and other means.

DATA PRIVACY & SECURITY LAWS: THE WORLD

Data privacy and security laws vary from country to country, depending on their legal systems, cultures and values. However, there is a growing trend towards harmonization and convergence of data protection standards across regions and jurisdictions. Some of the major data privacy and security laws around the world are:

The General Data Protection Regulation (GDPR). This is the most comprehensive and influential data protection law in the world, which applies to the European Union (EU) and the European Economic Area (EEA), as well as to any organisation that offers goods or services to, or monitors the behaviour of, individuals in the EU or EEA. The GDPR grants individuals a set of rights over their personal information, such as the right to access, rectify, erase, restrict, port or object to its processing. It also imposes strict obligations on data controllers and processors, such as obtaining valid consent, conducting data protection impact assessments, appointing data protection officers, notifying data breaches, implementing data protection by design and by default, and transferring data only to countries with adequate levels of protection. The GDPR also empowers national data protection authorities to enforce the law and impose fines of up to 20 million euros or 4% of global annual turnover, whichever is higher.

The California Consumer Privacy Act (CCPA). This is the first comprehensive data protection law in the United States (US), which applies to California residents as well as to any business that collects or sells their personal information. The CCPA grants individuals a set of rights over their personal information, such as the right to know what is collected, shared or sold; the right to access, delete or opt out of its sale; and the right to non-discrimination for exercising their rights. It also imposes obligations on businesses to provide notice, transparency and choice to consumers; to implement reasonable security measures; to honour consumer requests; and to avoid selling personal information of minors without consent. The CCPA also authorizes the California Attorney General to enforce the law and impose civil penalties of up to $7,500 per violation.

The Privacy Act 1988. This is the main data protection law in Australia (AU), which applies to Australian Government agencies (and the Norfolk Island administration) and organisations with an annual turnover more than $3 million. The Privacy Act gives individuals a set of rights over their personal information, such as the right to access or correct it; the right to complain about its mishandling; the right to stop receiving unwanted direct marketing; and the right to be notified of data breaches. It also imposes obligations on agencies.

RESPONSIBLE USE OF AI AND AUTOMATION

ETHICAL AI IN GOVERNMENT

The Australian Government has developed four principles for the ethical use of AI in government, based on interim guidance from the Digital Transformation Agency (DTA) and the Department of Industry, Science and Resources (DISR) . These principles are:

- Support the responsible and safe use of technology.
- Minimise harm, and achieve safer, more reliable and fairer outcomes for all Australians.
- Reduce the risk of negative impact on those affected by AI applications.
- Enable the highest ethical standards when using AI.
- Increase transparency and build community trust in the use of emerging technology by government.

These principles should guide the design, development, deployment, and evaluation of any AI or automation project in the public sector. They should also be aligned with the agency's ICT obligations and policies, as well as relevant laws and regulations.

USING GENERATIVE AI

Generative AI platforms are third-party AI platforms, tools or software that can create new content or data based on existing data or inputs.

Examples of such platforms are ChatGPT, Bard AI or Bing AI. These platforms can offer new and innovative opportunities for government, such as generating summaries, reports, or responses to queries. However, they also involve potential risks, such as data quality, security, privacy, accountability, and bias.

The DTA and DISR have provided some tactical guidance for Australian Public Service (APS) staff who want to use publicly available generative AI platforms. Some of the key points are:

- Assess the potential risks and benefits for each use case.
- Use generative AI platforms only for low-risk purposes that do not involve personal or sensitive information, decision making, or official communication.
- Do not rely solely on generative AI outputs without human verification or quality assurance.
- Clearly disclose the use of generative AI platforms to stakeholders and users

- Monitor and evaluate the performance and impact of generative AI platforms regularly.

BEST PRACTICES FOR DIGITAL TRANSFORMATION

Digital transformation is not just about using digital technologies to automate or augment existing processes. It is also about reimagining how government can deliver value to citizens and businesses in new ways. According to BCG , some of the best practices for digital transformation in government are:

- Define a clear vision and strategy for digital transformation that aligns with the agency's mission and goals.
- Establish a dedicated digital team or unit that can drive innovation and collaboration across the agency.
- Adopt agile methods and tools that enable rapid experimentation and iteration.
- Leverage data and analytics to generate insights and improve decision making.
- Engage with stakeholders and users throughout the design and delivery process to ensure user-centricity and feedback.
- Foster a culture of learning and change that supports continuous improvement and adaptation.

By following these principles, government agencies can use AI and automation responsibly and effectively in E-Gov & Digital Transformation. This can lead to better outcomes for citizens, businesses, and society.

10.3. REMOTE WORK & PRIVACY

FLEXIBILITY, PRODUCTIVITY, & INDIVIDUAL RIGHTS

The rise of remote work has revolutionized the way we work, offering unprecedented flexibility and accessibility. However, as organizations embrace this new paradigm, concerns about privacy in remote work environments have come to the forefront.

Remote work offers many benefits for both employers and employees, such as increased flexibility, productivity, and satisfaction.

However, remote work also poses some challenges for individual rights and privacy, such as blurred boundaries between work and personal life, potential surveillance and monitoring by employers, and increased cyber risks.

To address these challenges, it is important to establish clear policies and guidelines for remote work that respect the rights and preferences of workers, while ensuring accountability and security.

Some best practices for remote work policies include:

- Setting realistic and measurable goals and outcomes for remote workers, rather than focusing on hours or attendance.
- Providing adequate training and support for remote workers to use the necessary tools and technologies effectively and safely.
- Communicating regularly and transparently with remote workers to maintain trust, collaboration, and feedback.
- Respecting the autonomy and flexibility of remote workers to choose their preferred work location, schedule, and style, if they meet their obligations and expectations.
- Protecting the privacy and data of remote workers by implementing appropriate security measures, such as encryption, VPNs, firewalls, etc..
- Avoiding excessive or intrusive monitoring or surveillance of remote workers that may violate their rights or harm their well-being.

THE REMOTE WORK REVOLUTION

Advances in technology have paved the way for remote work to become a mainstream practice.

Develop standard security rules and procedures for your remote teams that cover regulatory compliance, remote access control, backup and media storage, data protection, remote system management, system ownership and return, and information disposal.

Define PII standards that meet the obligations for *personally identifiable information* compliance in all territories in which your organization operates.

Train and educate team members on how to protect themselves and others from the latest cybersecurity threats, especially those related to remote work, such as physical theft of devices, packet sniffers on public Wi-Fi networks, email scams, and spoof sites.

Don't leave your electronic devices unattended in public or in an unsecured office. Set laptops and mobile devices to automatically lock after a period of inactivity. Do not leave passwords written down or visible to others.

Use a password manager to generate and store strong, unique passwords for each account and service you use. Change your passwords regularly and avoid using the same password for multiple accounts.

Use a VPN and 2-factor authentication whenever possible to encrypt your online traffic and add an extra layer of security to your login credentials. Avoid using public Wi-Fi networks or shared computers to access sensitive data or perform online transactions.

Perform all transactions on a secure, password-protected network. Even if you are using a VPN, it's better safe than sorry. Look for the padlock icon and the https prefix in the address bar of your browser before entering any personal or financial information.

THE PRIVACY PUZZLE

Remote work introduces a unique set of privacy challenges. As employees work from home, the boundaries between professional and personal life blur, potentially leading to privacy infringements.

The Privacy Puzzle is a term that refers to the challenges and risks of protecting personal and confidential information in a remote or hybrid work environment.

Remote work has increased the exposure of sensitive data to potential threats such as unsecured networks, phishing attacks, device theft, and visual hacking.

To address these challenges, IT governance, policy, ethics and law experts recommend the following best practices:

- Implementing robust security technologies such as incident response platforms, anti-virus software, identity management and authentication systems, and encryption tools.
- Developing and enforcing clear privacy policies that specify the responsibilities and expectations of remote or hybrid workers, as well as the consequences of non-compliance.
- Providing regular training and awareness programs that educate employees on the importance of data privacy, the common threats they may face, and the mitigation methods they should use.

- Adopting privacy-enhancing solutions such as privacy screens, webcam covers, secure file sharing platforms, and VPNs.
- Monitoring and auditing the compliance and performance of remote or hybrid workers, as well as the security and privacy of the data they handle.

REMOTE WORK & PRIVACY POLICIES

Remote work poses unique challenges and opportunities for privacy protection. As a professional in IT governance, policy, ethics and law, you should be aware of the legal requirements, best practices and ethical principles that apply to remote work and privacy policies.

According to the Privacy Act 1988, you may need to have a clear and up-to-date privacy policy that details how you collect, store, use and disclose personal information of your employees, customers and other stakeholders. You should also comply with the Australian Privacy Principles, especially if you handle sensitive personal information or operate across borders.

You should also ensure that your remote work policy covers the following aspects:

- **Communication**. You should establish clear and consistent communication channels and protocols for remote workers, such as email, phone, video conferencing, instant messaging and collaboration tools. You should also inform remote workers of their rights and responsibilities regarding privacy and confidentiality and provide them with regular feedback and support.
- **Position and employee eligibility**. You should determine which positions and employees are suitable for remote work, based on their roles, skills, performance, availability and preferences. You should also consider the impact of remote work on their wellbeing, productivity, collaboration and career development.
- **Documentation**. You should document your remote work policy and procedures and make them accessible and transparent to all relevant parties. You should also keep accurate records of remote work arrangements, such as hours worked, tasks completed, expenses incurred, and outcomes achieved.
- **Remote work expectations**. You should set clear and realistic expectations for remote workers, such as work hours, deliverables, quality standards, deadlines, reporting requirements and performance indicators. You should also monitor and evaluate their work outcomes and provide them with constructive feedback and recognition.
- **Remote equipment and tools**. You should provide remote workers with the necessary equipment and tools to perform their work effectively and securely, such as laptops, smartphones, software

applications, VPNs and cloud services. You should also ensure that they have adequate internet connection and technical support.

- **Cybersecurity and internet connection**. You should implement appropriate cybersecurity measures to protect your data, systems and networks from unauthorized access, use or disclosure. You should also educate remote workers on how to prevent and respond to cyber threats, such as phishing, malware, ransomware and data breaches. You should also ensure that they use secure internet connections and devices when working remotely.
- **Adapting existing policies**. You should review and update your existing policies to reflect the changes brought by remote work, such as health and safety, leave entitlements, expense reimbursements, travel allowances and insurance coverage. You should also consult with your employees, managers, unions and legal advisors on any policy changes or issues.
- **Training**. You should provide remote workers with adequate training on how to use the equipment and tools provided by you, how to comply with your privacy policy and procedures, how to manage their time, workload and stress levels, how to communicate effectively with their colleagues and customers, how to maintain their professional image and reputation online.

By following these best practices for remote work and privacy policies, you can ensure that your business operates efficiently, ethically and legally in the digital age. You can also enhance your employee satisfaction, engagement and retention rates by offering them flexibility, autonomy and trust.

PRIVACY IN DIGITAL COMMUNICATION

Privacy in digital communication is a crucial issue for remote workers, as they may share sensitive information with their employers, clients, colleagues, or other parties over various platforms and devices.

Remote workers should be aware of the data privacy regulations that apply to their location, industry, and type of data, such as GDPR or CCPA, and follow the best practices to comply with them.

Remote workers should also take steps to protect their own privacy and security, such as using strong passwords, encryption, VPNs, anti-virus software, and identity management tools.

Remote workers should communicate clearly and respectfully with their managers and co-workers about their expectations, boundaries, and preferences regarding privacy and data sharing.

Remote workers should seek advice from IT governance, policy, ethics, and law experts if they encounter any challenges or dilemmas related to privacy in digital communication.

DATA SECURITY IN REMOTE WORK

Data security in remote work is the practice of protecting sensitive information and systems when employees work from home or in remote locations.

Data security in remote work involves encrypting data at rest and during transit, safeguarding it from interception, compromise, or theft. It also involves preventing data loss or leakage, which can happen when employees use personal devices, unsecured networks, or unauthorized applications.

Data security in remote work requires a strong security policy that covers the roles and responsibilities of remote workers, the acceptable use of devices and applications, the encryption and backup of data, and the reporting of incidents.

It also requires ongoing education and training for remote workers, so they are aware of the proper security protocols, the importance of data security, and how to look for potential cyber threats.

Security can be enhanced by embracing cloud technology, which can provide more flexibility, scalability, and resilience for data storage and access. However, cloud technology also introduces new challenges, such as ensuring compliance with data privacy regulations, managing access rights and permissions, and monitoring cloud activity.

This is a critical issue for businesses that want to maintain their competitive edge, reputation, and customer trust. It is also a shared responsibility that requires collaboration and communication between IT teams, managers, and remote workers.

BALANCING MONITORING & TRUST

Balancing monitoring in remote work and privacy is a challenging but important task for employers and employees alike.

Monitoring can have benefits such as improving productivity, ensuring compliance, and mitigating risks, but it can also have drawbacks such as eroding trust, harming job satisfaction, and increasing stress.

To monitor employees effectively and ethically, employers should follow some best practices, such as:

- Choosing metrics that are relevant, fair, and transparent, and involving all stakeholders in the process.
- Communicating clearly with employees about what is being monitored, why, and how.

- Offering incentives and feedback as well as consequences for performance.
- Recognizing that employees may face challenges and distractions in their remote work environment and being flexible and supportive.
- Monitoring their own systems to ensure that they are not biased or discriminatory against certain groups of employees.
- Decreasing monitoring when possible and respecting employees' privacy rights.

Trust is essential for remote work and privacy, as it fosters collaboration, innovation, and well-being. Employers should build trust with their employees by:

- Providing them with the tools, resources, and training they need to work remotely.
- Empowering them to make decisions and manage their own work schedules.
- Encouraging them to communicate openly and frequently with their managers and peers.
- Appreciating their contributions and celebrating their achievements.
- Respecting their personal lives and boundaries.

REMOTE WORK EQUIPMENT & PRIVACY

Remote work equipment and privacy are closely related issues that affect both employers and employees in a distributed work environment.

Employers have a duty to ensure the health and safety of their workers, as well as the security and compliance of their data and systems, when they work from home or elsewhere.

Employees have a right to expect reasonable privacy and autonomy when they use their own or employer-provided equipment for work purposes.

To balance these interests, employers and employees should follow some best practices, such as:

- Providing adequate and ergonomic equipment for remote workers that meets their individual needs and preferences.
- Establishing clear policies and procedures on providing equipment for remote workers, including who owns, pays for, maintains, repairs, replaces, and returns the equipment.
- Implementing effective technologies and tools for protecting privacy and security in a remote or hybrid work environment, such as incident response platforms, anti-virus/anti-malware software, big data analytics for cybersecurity, identity management and authentication.

- Educating and training remote workers on how to use the equipment safely and securely, as well as their rights and responsibilities regarding data privacy.
- Monitoring and auditing the use of equipment for work purposes only when necessary and proportionate, and respecting the personal use of equipment when allowed.

CONSENT & TRANSPARENT PRACTICES

Consent and transparent practices are essential for ensuring the privacy and trust of employees who work remotely.

Employers should follow the Australian Privacy Principles (APPs) when collecting, storing, using and disclosing personal information of their remote workers.

Employers should have a clear privacy policy that explains what information they collect, why they collect it, how they use it, who they share it with, and how employees can access or correct it.

Employers should seek consent from their remote workers before monitoring their activities, such as their emails, social media accounts, or workspaces.

Employers should be transparent with their remote workers about the purpose and scope of monitoring, and the benefits and risks involved.

Employers should offer incentives and feedback to their remote workers based on their performance, not on their compliance with monitoring.

Employers should respect the diversity and individual circumstances of their remote workers, and avoid any discrimination or bias based on personal information.

Employers should review and update their privacy practices regularly and consult with their remote workers and other stakeholders on any changes.

INDIVIDUAL PRIVACY VS. ORGANIZATIONAL NEEDS

Individual privacy vs. organizational needs is a key challenge for remote work, especially in the post-pandemic era.

Remote workers may face different expectations and norms than on-site workers, which can affect their sense of belonging, trust, and performance.

Organizations should consider the following best practices to balance privacy and needs in remote work:

- Establish clear and consistent policies for remote work that address issues such as working hours, communication tools, data security, and performance evaluation.

- Communicate frequently and transparently with remote workers to foster a shared culture and identity, and to avoid misunderstandings or isolation.
- Provide adequate support and resources for remote workers to ensure their well-being, productivity, and engagement.
- Respect the boundaries and preferences of remote workers and avoid micromanaging or intruding on their personal space.
- Involve remote workers in decision making and feedback processes and recognize their contributions and achievements.

FLEXIBLE WORKING HOURS & PRIVACY

Flexible hours are arrangements that allow employees to adjust their work schedules and locations to suit their personal and professional needs.

This can benefit both employers and employees by increasing productivity, engagement, retention, diversity, and well-being.

Flexible hours can also pose some challenges, such as communication difficulties, performance management, security risks, and legal compliance.

To implement flexible working hours successfully, employers need to establish clear policies and guidelines, consult with employees and stakeholders, provide adequate technology and support, and monitor and evaluate the outcomes.

And to make the most of flexible working hours, employees need to communicate effectively, manage their time and tasks, balance their work and personal responsibilities, and maintain their health and safety.

MANAGING SENSITIVE INFORMATION

Managing sensitive information in a remote work environment is crucial for protecting your data and intellectual property, as well as complying with legal and ethical obligations.

Management (you) should set up and communicate clear policies and guidelines for your employees on how to handle sensitive information, such as personal, financial, health, or confidential data, when working remotely.

You should use secure tools and platforms that encrypt your data at rest and in transit, such as Microsoft Teams, which also allows you to apply data loss prevention and sensitivity labelling to prevent unauthorized access or sharing of sensitive information.

You should monitor and mitigate insider risks, such as accidental or malicious disclosure of sensitive information by your employees, by using incident response platforms, big data analytics, identity management, and authentication systems.

You should provide regular training and awareness programs for your employees on the importance of visual privacy, VPN security, personal device regulation, and communication channel security when working remotely.

CULTURAL AND LEGAL DIVERSITY

Remote work can enhance workplace diversity by allowing access to a wider pool of talent, reducing geographic and social barriers, and accommodating different needs and preferences of employees.

However, remote work also poses some challenges for diversity and inclusion, such as potential isolation, exclusion, or misunderstanding of employees from different backgrounds, identities, or locations.

To address these challenges, remote workers and managers need to be aware of the cultural differences that can impact global teams, such as communication styles, decision-making processes, conflict resolution strategies, and feedback preferences.

Remote workers and managers also need to be mindful of the legal diversity that can affect remote work and privacy, such as data protection laws, employment laws, tax laws, and anti-discrimination laws that may vary across countries or regions.

Therefore, it is advisable for remote workers and managers to follow some best practices for cultural and legal diversity in remote work and privacy, such as:

- Developing workplace policies and training that promote cross-cultural awareness and respect.
- Holding regular virtual meetings and events that celebrate workplace diversity and encourage employees to share their cultures and experiences.
- Using clear and inclusive language and communication tools that suit the needs and preferences of different employees.
- Seeking feedback and input from diverse employees on important decisions and projects.
- Ensuring compliance with relevant laws and regulations in different jurisdictions where remote workers are located.
- Providing support and resources for remote workers to deal with any legal or cultural issues that may arise.

ADDRESSING BURNOUT & OVERWORK

Addressing burnout and overwork in remote work is a crucial challenge for many hard-working IT professionals, who often face high demands, tight deadlines, and complex tasks.

Burnout can have a range of negative consequences for individual well-being, team performance, and organizational outcomes, such as increased turnover, reduced productivity, and lower customer satisfaction.

To prevent and reduce burnout in remote work, IT professionals should follow some evidence-based strategies, such as:

- **Creating an environment for communication**. Remote workers may feel isolated, disconnected, or misunderstood by their colleagues and managers. To foster a sense of belonging and trust, IT professionals should communicate frequently, clearly, and empathetically with their team members and leaders. They should also seek feedback, share achievements, and celebrate successes.
- **Lifting morale — genuinely**. Remote workers may lack the motivation, engagement, or recognition that they would receive in a physical office. To boost morale and enthusiasm, IT professionals should find meaningful and enjoyable aspects of their work, express gratitude and appreciation to others, and participate in social activities that foster camaraderie and fun.
- **Simplifying remote work systems**. Remote workers may struggle with the complexity, ambiguity, or inefficiency of their work processes and tools. To streamline remote work systems, IT professionals should use reliable and user-friendly technology platforms, establish clear and consistent expectations and guidelines, and prioritize and delegate tasks effectively.
- **Reducing or eliminating meetings**. Remote workers may experience meeting fatigue, which can drain their energy, attention, and creativity. To minimize meeting overload, IT professionals should only attend meetings that are relevant, necessary, and productive. They should also limit the duration and frequency of meetings, prepare agendas and objectives beforehand, and follow up with action items afterward.
- **Addressing the elephant**. Remote workers may face personal or professional challenges that are specific to their situation, such as juggling caregiving responsibilities, coping with mental health issues, or dealing with technical difficulties. To address these challenges, IT professionals should be honest and proactive about their needs and concerns, seek support from their managers or peers, and access available resources or services.
- **Investing time and attention in themselves**. Remote workers may neglect their own well-being by working long hours, skipping breaks, or ignoring physical or emotional signs of stress. To take care of themselves, IT professionals should set healthy boundaries between work and life, practice self-care activities that enhance their mood and energy, and take regular recovery time to relax and recharge.

EDUCATION & TRAINING

Ensure that you comply with IP, ethics and privacy policies and procedures in ICT environments, as outlined in the relevant training packages.

Locate and access the organisation's IP, ethics and privacy policy and procedures, and determine how they apply to your remote work situation.

Analyse legislation and standards that relate to IP, ethics and privacy in ICT, such as the Privacy Act 1988 (Cth), the Australian Privacy Principles, the Copyright Act 1968 (Cth), the Code of Ethics for Professional Conduct by the Australian Computer Society, etc.

Contribute to policy and procedures improvements in code of ethics and privacy policy documents in the ICT industry, by providing feedback, suggestions and recommendations based on your experience and expertise.

Use technology competently and securely to deliver education and training remotely, such as using encryption, passwords, firewalls, antivirus software, VPNs, etc.

Uphold your professional and ethical obligations while working remotely, such as maintaining supervision, client confidentiality, communication, quality of service, etc.

APPENDICES

The Appendices are a collection of useful information on a variety of topics.

Appendix A is a list of acronyms used in this text.

Appendix B is a sample case study that illustrates how the Ethical Decision Model (EDM) can be applied.

Appendix C is a collection of common scenarios faced by technologists in their daily work.

Appendix D outlines the basics of software licensing. It informs software developers and consumers alike about the various kinds of software licenses, what they cover, how they work etc.

Appendix E is a summary of the mass persuasion techniques (commonly called propaganda) that governments, organisations, institutions and groups all use to mould the opinions and values of their members.

Appendix F discusses military technology.

Appendix G is a select bibliography of sources.

APPENDIX A: LIST OF ACRONYMS

A&O	analysis and operations
ACL	access control list
ADS	anomaly detection system
A/V	audio/video
AV	anti-virus
AVS	anti-virus software
C&A	certification and accreditation
CAESARS	Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report
CBK	Common Body of Knowledge
CBT	computer-based training
CCV	Cybersecurity Capabilities Validation
CD	compact disc
CERT/CC	CERT Coordination Center
CIA	confidentiality, integrity, and availability
CIO	chief information officer
CISO	chief information security officer
CISSP	Certified Information Systems Security Professional
CM	continuous monitoring
CMMI	Capability Maturity Model Integration
CMU	Carnegie Mellon University
CND	computer network defense
CNDSP	computer network defense service provider
COBIT	Control Objectives for Information and related Technology
CONOPS	concept of operations
COOP	continuity of operations
COP	common operational picture
CP	contingency planning
CSIRT	computer security incident response team
CVE	Common Vulnerabilities and Exposures
D/A	department/agency
DDOS	distributed denial of service
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMZ	demilitarized zone
DNS	domain name system
DoD	Department of Defense
DoS	denial of service
ETA	education, training, and awareness
F-CND	Federal-Computer Network Defense
FAX	facsimile
FCD	Federal Continuity Directive
FCMR	Federal Cybersecurity Maturity Roadmap
FE	framework extension
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standards
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act of 2002

FNR	Federal Network Resilience
FNS	Federal Network Security
FOUO	for official use only
FYI	for your information
GFIRST	Government Forum of Incident Response and Security Teams
GnuPG	GNU Privacy Guard
GRS	General Records Schedule
HR	human resources
IA	information assurance
IC	intelligence community
IDPS	Intrusion Detection and Prevention System
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IG	inspector general
IM	incident management
IMF	Incident Management Function
IP	internet protocol
IPS	intrusion prevention system
IR	incident response
ISAC	Information Sharing and Analysis Center
(ISC)2	International Information Systems Security Certification Consortium
ISCM	information system continuous monitoring
ISCP	Information System Contingency Plan
ISF	Information Security Forum
ISO	information security officer OR International Organization for Standardization
ISP	internet service provider
IT	information technology
ITGI	Information Technology Governance Institute
ITIL	IT Infrastructure Library
JWICS	Joint Worldwide Intelligence Communications System
LE	law enforcement
LOA	letter of agreement
MEF	mission essential function
MIME	Multipurpose Internet Mail Extensions
MO	modus operandi (mode of operation)
MOA	memorandum of agreement
MOU	memorandum of understanding
MSSP	managed security service provider
NARA	National Archives and Records Administration
NDA	non-disclosure agreement
NEF	national essential function
NFAT	network forensics analysis tools
NIC	network information centre
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
NITTF	National Insider Threat Task Force
NOC	network operations centre
NSA	National Security Agency
NVD	National Vulnerability Database

OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OGC	Office of Government Commerce
OLRC	Office of the Law Revision Counsel
OMB	Office of Management and Budget
OPSEC	operations security
OS	operating system
PC	personal computer
PE	physical and environmental
PGP	Pretty Good Privacy
PII	personally identifiable information
PKI	public key infrastructure
PMEF	primary mission essential function
POC	point of contact
QA	quality assurance
RA	risk assessment
RDF	resource description framework
RFC	request for comments
RSS	RDF Site Summary
SA	situational awareness
SCIF	Sensitive Compartment Information Facility
SDLC	system development lifecycle
SEI	Software Engineering Institute
SEIM	security event and incident management
SIPRNET	Secret Internet Protocol Router Network
SKiP	Security Knowledge in Practice
SLA	service level agreement
S/MIME	Secure/Multipurpose Internet Mail Extensions
SME	subject matter expert
SMS	short message service
SOC	security operations centre
SOP	standard operating procedure
SP	special publication
SSP	system security plan
STE	secure terminal equipment
SWO	senior watch officer
TERENA	Trans-European Research and Education Networking Association
TICAP	Trusted Internet Connection Access Provider
TS	top secret
TT&E	testing, training, and exercise
US-CERT	United States Computer Emergency Readiness Team
VPN	virtual private network
VS	vulnerability scanning
XML	Extensible Markup Language

APPENDIX B: APPLYING THE EDM

This sample case study illustrates how the Ethical Decision Model can be applied in practice.

Case Scenario. Luke Vandenberg always wanted to be an interactive web designer since he was about halfway his High School years. He started working as an intern for a design studio while he was in his final year and got a lot of good experience from this. After he finished High School, Luke enrolled in a multimedia degree at Altiora University.

The degree required him to do a year work experience after completing the second year. After this year, he would return to full time study and complete the final year. This extended a three year degree to four years, but Luke was OK about this because he was able to land an intern job with a leading interactive design studio (TT INTERACTIVE) that worked closely with advertising agencies to develop the web component of major ad campaigns.

During his time at TT INTERACTIVE, Luke worked on a big project that involved the design and implementation of a web portal for Altiora University who wanted to re-badge their image, and market itself more effectively while improving the scope and functionality of their existing web portal. It was a big job for a high profile client and TT INTERACTIVE wanted someone who not only had the design skills but also had some familiarity with the culture at Altiora, so Luke got the job.

Luke was part of a three person project team. It was a demanding but highly satisfying project that was almost finished by the time he finished his intern year, and was due to return to university for the final year. TT were a hard task-master. Though he was being paid the bare minimum, he was expected to work long hours. He was told the experience he was getting was worth a lot. Nonetheless, he had mixed feelings; on the one hand he was indeed getting some great experience, but he could not help feeling somewhat exploited by TT management who seemed to care more about project outcomes than the people making the project happen.

Luke was a careful person by nature, and routinely made backups of the project files that he stored off-site for safe-keeping. He had lost hours of work before and was in the habit of making off-site backups. He did not think or realize that this constituted a breach of the agreement he had signed with TT to not remove any intellectual copy off-site without the permission of a TT Director. And so it was that when he left TT INTERACTIVE he happened to have a more-or-less complete set of project files for the new Altiora University web portal. He did not at this stage intend to do anything with this material.

During his final year at Altiora, Luke was gratified, in fact delighted to see the new web portal come on-line. He felt like he was making a difference in the world. Despite some teething problems, and some disparaging comments from his fellow

students, the new portal was a success. He felt justifiably proud of himself. When he finished his degree he had been told there would probably be a job for him at TT but they were by this time fully staffed. Luke was a free agent in the world, looking for a way to apply his talents. With the experience he now had as a co-developer of a major new portal he was able to secure a similar position at a rival studio, Tangential. A year goes by, and Luke has settled in to his new job at Tangential. He becomes a team leader in due course. One day his boss calls him in for a conversation. How would Luke like to take the lead on a project to develop a web portal for Charleston Technical University? Tangential have successfully tendered for the project. This is important. Tangential management is quite excited about it.

The boss hints that anything Luke might have "learned" while at TT INTERACTIVE would be helpful. Something in the Boss's manner strikes Luke as a bit odd. Then he remembers having mentioned in passing over drinks some months earlier that he still had the backup project files from his earlier job working on the Altiora portal for TT. Luke feels a little uneasy at what his boss seems to be suggesting, but is nonetheless excited by the project, and is keen to do a good job and perhaps get ahead in the industry, maybe one day open his own studio. Why not? Luke has recently married, and his wife and he had been discussing only the other day how good it would be to find a bigger place to live, maybe even start a family.

The upshot of the meeting is that Luke enthusiastically accepts the challenging new team lead role on the Charleston Technical University web portal project. Without any discussion with anyone, he digs out his old backups of the Altiora project (done while at TT) and dusts them off. Yes, he decides, this could be useful; this could be the framework that will save a lot of time and effort. He wonders briefly whether he is doing the right thing, but finishes by telling himself that "This is my own work. Don't I have a right to use it? Why reinvent the wheel?"

So Luke takes his earlier work (and that of his fellow developers at TT who worked on the Altiora project) and modifies it so that it is superficially different from the original (a user would not notice much similarity), but under the skin, at a programming level, it was largely based on his earlier work.

The Charleston Technical University web portal is ultimately delivered. The client is happy, Tangential is happy, and Altiora and TT INTERACTIVE do not allege the theft of their intellectual property.

Years pass. Luke becomes a senior project manager and continues to build a successful career, culminating in the opening of his own studio. One day, as Director of his own studio, he receives a phone call from Altiora University. They flatter him as a successful alumnus, and ask if he would consider taking on an intern or two for the following year. He thinks for a moment, and somewhere in the back of his mind, a troubling thought takes shape ... End of Case Study

FACTORS & RELATED ISSUE

1. Intellectual Property Theft (Legal). Creating Backups off site without Directors permission.
2. Breach of Agreement with TT (Legal). Creating Backups off site.
3. Privacy Legislation(Legal). Discussed his past job (work files) of the web portal from TT with the Tangential Manager.
4. Confidentiality (Legal). Discussed his prior jobs completed at a different organisation with his new employer.
5. Piracy (Legal). When Luke used the backup files for assistance from TT, the programming & framework
6. Code of Ethical conduct (Legal). Luke has minimised his integrity since the moment he made that first backup offsite.
7. Acknowledged Backups (Professional). When Luke mentioned to his manager at Tangential about the work he stole from TT.
8. Manager Signifying theft (Professional). When Luke was in his manager's office getting offered the lead role & felt uneasy about using the work from TT by the Tangential Manager.
9. Project outcomes (Employment & Social). No gratitude was acknowledged to the workers only keeping the project outcomes in sight at TT.
10. Work Experience (Employment & Social). Luke's work Experience was highly valuable for his forthcoming.
11. Existing Student (Employment & Social). The fact TT hired Luke as an intern for their upcoming project would be valuable.
12. Long Hours (Employment & Social). Luke felt under appreciated.
13. Insufficient money (Employment & Social). Luke felt he was not getting paid enough.
14. Comments (Employment & Social). When Luke's fellow students were not happy about the portal at Altiora by voicing disparaging comments.
15. Get ahead (Personal). Luke was ignorant of the law to get ahead in his career.
16. Married (Personal). Luke got married.
17. Bigger Place (Personal). Luke & his wife need a bigger place to live in.
18. Family (Personal). Luke and his wife want a family one day.
19. Own Studio (Personal). Luke wants to have his own studio.
20. Lead Role (Personal). Did Lead role for a web portal for a high end client while at Tangential.
21. Senior Director (Personal). Had the job description as Senior Director.
22. 1 year work experience (Intrinsic). Luke did one year work experience at TT to achieve his degree.

23. Co-developer (Intrinsic). During that year of experience Luke gained co-developer skills
24. Multimedia degree (Intrinsic). Luke received his multimedia degree.
25. Team leader (Intrinsic). Luke became a team leader at Tangential.
26. Senior project manager (Intrinsic). Luke achieved the job description senior project manager at tangential for his efforts.
27. Own studio (Intrinsic). Luke owns his own studio.
28. Director (Intrinsic). Luke is the director at his own studio.

SAMPLE SOLUTION 1

LEGAL FACTORS

Factor 1, Contract Breach In the case study, Luke Vandenberg did some work experience for TT INTERACTIVE working on the Altiora web portal project. Luke Vandenberg had signed a contract with TT INTERACTIVE which stated that he was not to remove any intellectual property off-site without the expressed permission of the TT director. However, Luke did make off-line backups. This is a legal factor because there are Australian laws which govern contracts.

Factor 2, Copyright infringement In the case study, Luke had been working at a second company, Tangential Software. Luke was working on a web portal project like the one he had worked on with TT INTERACTIVE but for Charleston technical university. Luke used the work from the Altiora project and altered it superficially, effectively copying the work he and others had worked on at TT INTERACTIVE. This is a legal factor because the work Luke used was not his own. This is a breach of Australian copyright law

PROFESSIONAL FACTORS

Factor 3, Professional Contract Obligations As described earlier Luke Vandenberg made a breach of his contract with TT INTERACTIVE. This is not only a legal factor but also a professional factor as is stated in the Australian computer society's code of professional conduct and professional practice under H3.

Factor 4, Professional Confidentiality Luke copied the intellectual property of his previous employer, TT INTERACTIVE without permission. Copying the Altiora project is a professional factor as well as a legal one as is stated in the Australian Computer Society's code of conduct under A3.

EMPLOYMENT & SOCIAL FACTORS

Factor 5, Luke cheated TT INTERACTIVE As mentioned Luke copied the Altiora web portal he worked on at TT INTERACTIVE and used it in a similar project for rival company Tangential software. Society does not like cheaters and thieves. By copying the Altiora project without crediting TT INTERACTIVE, Luke effectively

stole the project and cheated TT INTERACTIVE and its employees. Luke Vandenberg is a member of society; he should have contributed to society. Instead, Luke behaved like a parasite, taking without giving credit or giving back to the organization he was once a part of.

Factor 6, Luke was treated poorly at TT INTERACTIVE Luke was made to work long, hard hours whilst working at TT INTERACTIVE. Luke had mixed feelings about his time at TT INTERACTIVE. Luke was getting good experience but he felt that he was worked too hard for his minimum wage. TT INTERACTIVE worked Luke very hard which could have made Luke feel oppressed. This is a social factor because people in society usually resent those whom oppress them or take away their freedom. Society has a general dislike for bullies like TT INTERACTIVE.

Factor 7, Luke Broke a Promise Luke signed a contract with TT INTERACTIVE, promising not to make off-site backups without permission from the TT director. Luke breached this contract by making off-site backups. This is a social factor because society generally does not like it when people break promises. For example when a government party promises to lower taxes and does not deliver on the promise, people in society become resentful towards party.

Factor 8, Luke's boss pressured him Luke's boss at Tangential asked him to use whatever he had learned from the previous project. Luke felt that his boss' manner was odd. This was because the boss knew about Luke's copy of the Altiora web portal project and was suggesting that Luke copy this work for the new Tangential web portal project. This is an employment factor because Luke's boss suggested he take part in an un- professional act.

Factor I, Luke was misled Luke was told that there would probably be a place for him at TT INTERACTIVE after he finished his university degree however TT INTERACTIVE did not have a place for him. This is an employment factor because the organisation, TT INTERACTIVE may have disappointed Luke.

PERSONAL FACTORS

Factor 10, Luke committed plagiarism Luke committed plagiarism by copying the Altiora web portal project without giving credit to TT INTERACTIVE, the rightful owner and therefore committed plagiarism. This is a personal factor because Luke's personal environment was once at Altiora University and universities are very strict on plagiarism.

Factor 11, Luke was from an I.T (Information Technology) background Luke made off-site copies of the Altiora web portal project whilst at TT INTERACTIVE. Luke made these copies because he wanted to make sure he did not lose his work. Also when Luke copied TT INTERACTIVE's web portal he said to himself, "Why reinvent the wheel?" These are personal factors because they come from Luke's information technology background.

Factor 12, Peer pressure Luke's boss at Tangential subtly told Luke to copy what he could from TT INTERACTIVE's web portal project. This is a personal factor because Luke's boss applied peer pressure on Luke. It is part of what caused Luke to copy TT INTERACTIVE's web portal project.

INTRINSIC FACTORS

Factor 13, Luke's personal gain Luke wanted the new project with Tangential to go successfully as this may lead to Luke getting ahead in the industry. Luke had ambitions to open his own studio in the hopes of earning enough money so he and his wife could move into a larger home. This is a personal factor because it is what motivated Luke to copy TT INTERACTIVE's Altiora web portal project.

Factor 14, Luke was a safe person Luke was a safe person by nature. This is what led him to making off-line backups of the Altiora web portal project. This is an intrinsic factor because it is to do with Luke's own experiences and it is part of who he is as a person. Factor O, Luke's mixed feelings toward TT INTERACTIVE Luke had mixed feelings about working at TT INTERACTIVE and felt he was taken advantage of. This is an intrinsic factor as it is part of Luke's own experiences and Luke may have felt negatively towards TT INTERACTIVE because of it.

SAMPLE SOLUTION 2

LEGAL FACTORS

The first subject I have in this list of legal factors is the intellectual property theft. The reason I have chosen this as the first legal priority is because while Luke was working at TT he was taking backups of his work off site which is legally the property of TT. Although he may have been under the assumption that he was doing the right thing for TT by making off site backups, it does not eliminate the fact that being ignorant of the law does not make it ok to break the law. The second legal factor which is still within relation of the first is the breach of agreement that Luke has committed. Being employed by TT and gaining the work experience he was achieving I'm sure Luke could have been intelligent enough to talk to the director about implementing other systems in regards to making backups off site and not take it into his own hands which has initiated this breach. The third legal factor is when Luke breached the privacy legislation. The time he was having a few drinks then he had mentioned to the Tangential manager that he still had backups of the work he done when he was working at TT interactive. This act is highly unethical. This action has created a negative reaction further down the lines when the Tangential manager calls him in for chat about the new project of the portal. The fourth is confidentiality as at the point when without hesitation Luke used his original backups from TT as the framework for his new project with Tangential & spoke to his boss about the work he had done with TT. The fifth legal factor is that Mr Vandenberg has breached his own Code of ethical conduct as he had committed the above breaches mentioned and never owned

up to his mistake hence decreasing the integrity of himself. The sixth legal breach that has been committed is piracy at the time in the case study when Luke used the framework from TT as the framework for Tangential web portal.

PROFESSIONAL FACTORS

The night that Luke was having few drinks with his manager from Tangential & he mentioned that he still had backups of the work he had done while he was employed by a rival competitor at TT interactive. As Months went by then one day Luke got called into the office by his manager at Tangential.

The news of the new project they are beginning for the web portal gets informed to Luke. The next instant Luke catches hints from his employer about the backups he had from the last portal that he had designed at TT would be a great asset to the project. Could this be the reason Luke was given the opportunity to be the Lead worker of this project?

EMPLOYMENT AND SOCIAL FACTORS

Despite Luke received disparaging comments from fellow students he was still justifiably happy with the web portal produced by TT. The time Luke was working at TT INTERACTIVE he was doing long hours and earning the base wage minimum. The justification of this circumstance was that the fact that the experience he is receiving is much more treasured. However Luke still felt underappreciated and what some could say being de humanised slightly. No gratitude was being acknowledged towards the workers just to the future outcomes of the project being completed. The fact that Luke was an existing student at Altiora University assisted in TT interactive giving him the internship as they wanted someone who was familiar with the culture at the university.

PERSONAL FACTORS

Luke had great justification in the fact that getting the lead role for the project at Tangential would really assist in taking the path of being senior director then concluding to his dream of opening his own studio. His priority was that just after recently getting married Luke & his wife discussed that they would like to have a bigger place and possibly have children (family) one day.

INTRINSIC FACTORS

Luke has attended university for 4 years in total. Luke was required to do 1 year work experience as part of his multimedia degree. This was the time when TT interactive was doing the web portal for Altiora University. The entire project had taken the whole entire year that Luke was doing as work experience. This also gave him co-developer experience. Once Luke went back to university for his final year he was under the impression that he would have a job at TT however this was not the case as TT was fully staffed on the completion of Luke’s degree. None

the less Luke gained employment at a competitor of TT called Tangential. As time goes by with his employment Luke becomes Team leader at Tangential. The opportunity arises that would help him get ahead in the industry. Further along down the line Luke becomes a senior project manager which then he decides to open and run his own studio as the director.

Please note this sample is for illustrative purposes only.

APPENDIX C: COMMON SCENARIOS

TELL US OUR COMPETITOR'S SECRETS

Often people are hired for a job on the strength of what they have learned working for a competitor. The assumption, often unstated, is that the new-hire will bring specific knowledge of their former employer's competitive advantage.

In this situation, it is permissible to bring *general* knowledge of a competitor's business to a new employer. You will have signed a legally binding employment contract with the first employer, and this prohibits the disclosure of any *proprietary* information to a third party without written permission. So you must not make copies of commercial-in-confidence material, and especially not sell that information to competitors, whether directly or by going to work for them. Severe penalties apply for proven breaches.

A recent press report describes how a man was sued by his former employer because he took with him 17,000 followers of a promotional Twitter account when he left. The former employer alleges that each follower is worth $2.50 and was seeking damages. The man was working for a competitor by this time.

Intellectual property protection or copyright applies to specific implementations of an idea. It is the implementation that is copyright. Organisations can try to patent or copyright an idea, but it is often problematic. An abstract idea can be implemented in any number of ways. If the implementation is sufficiently different from the original then copyright breach cannot be proven.

The history of innovation is full of instances where good ideas have been thought of independently yet simultaneously. The underlying idea might be similar, but the way it is implemented will differ significantly.

WORK FOR US, BUT WE WON'T PAY YOU

It is common practice for unscrupulous employers to hire interns; enthusiastic, usually young developers on low or non-existent salary, on the understanding that the *experience* they are getting is adequate compensation.

The employer exploits the intern by obliging them to work long hours, often at some considerable personal cost. Most people will burn out after a few months of this, and when that happens, they are discarded and replaced by a new wave of intern.

While it may be true that you are getting experience that will look good on your resume, as a rule you should not allow yourself to be exploited in this way, at least not for long. You deserve fair payment for the work you do. This may not be much money, given your lack of experience, but if you are creating something useful and profitable for your employer, you deserve to be paid.

Any attempts to exploit you like this should be treated with the contempt it deserves (short-term internships may be acceptable). If an employer's business model relies on using free, skilled labour, it is questionable.

THE COSTLY PATCH

It is common practice by some software development companies to release defective software to their clients and then charge them to fix the defects that should not be there in the first place.

In some cases, the developer becomes aware that all their customers have a potential problem, yet instead of proactively sending out a patch to their customers, they wait for a customer to complain, and then charge them to fix the problem.

It is understandable why a developer might want to use a strategy like this, but it is clearly unethical if the software has been sold on the understanding that it is defect free. It is most unlikely that the customer agreed to accept faulty goods that they would be required to pay twice for, or three times if there is a maintenance/support agreement in place.

NO, THAT DOESN'T FIT WITH OUR STRATEGY

Software development companies with an idea for a software product will often look for a client who is willing to finance the production of the software which will then be sold to as many of the client's competitors as possible.

If the client can be persuaded to pay full price, then so much the better. To secure the deal, the developer may offer a discount.

The client probably realises that they are funding a project that will not only benefit them, but also their competitors. Perhaps they trust a non-disclosure agreement with the developer to safeguard their interests. This trust may prove to be misplaced.

As development proceeds, there are sure to be times when the client says to the developer, *thinking about it, we now want the software to do this or that (specific requirements).* Unless this fits with the developer's own product strategy, the client is likely to be told, *no that cannot be done*. It would be a rash or arrogant developer who then says, *it cannot be done because it does not fit with our development strategy*, though I have personally heard these words spoken in a client-developer meeting.

If the client is paying for it, they are entitled to get what they are paying for. If the developer wants to go in a different direction, they should do it at their own expense, on their time.

TWO SETS OF ACCOUNTS

Some businesses that accept cash money have been known to keep two sets of accounts; one for the purposes of paying tax, the other to tell the full financial story strictly for in-house use.

As a software professional working on an organisation's accounts, you are likely to see information that your employer expects you to keep confidential. It may only be relatively minor matters, not necessarily a whole second set of book.

Confidentiality of the employer-employee relationship is extremely important in professional practice. Like a doctor or lawyer, what you learn must not be disclosed to a third party except under certain prescribed circumstances.

Becoming a whistle-blower is an extreme act, though sometimes it is justified. Before doing it, it is highly recommended that you seek the advice of your professional association. With good advice, your ethical concerns can be resolved without breaching your obligation to treat your employer's information confidentially.

You should be aware that whistle-blowers, regardless of how well-intentioned they be, almost invariably become despised and unemployable.

APPENDIX D: SOFTWARE LICENSING

This section contains useful reference information for software developers wanting to understand the intricacies of software licensing.

- An independent software author owns the copyright on the program
- Enables author to regulate the copying, using and adapting of the program
- Must specify conditions of use (license).
- Several standard licenses are possible

CATEGORIES OF LICENSE

- Exclusive rights
- Standard licenses
  - The GNU General Public License
  - The BSD license
  - The Artistic License
  - Public domain
- Writing your own software license

EXCLUSIVE RIGHTS

- Author has the right to restrict copying, modification & distribution
- Author may authorise others to distribute software, with or without charge.
- The conditions of this authorisation is specified in the License.
- License can be specific for one particular recipient (this is often the case with custom-made applications), but it can also be written in a generic way, like with most of the standard software sold in stores or available for download on the Internet.
- If Author desires to sell their software, a carefully drafted license is essential.
- If author desires to give their software freely, a License is still required to specify the conditions under which users may execute and distribute the software.
- Two options; use a standard license, or write their own.

STANDARD LICENSE

- GNU General Public License, BSD license, Artistic License, Public domain.

- Many programs are distributed under standard licenses.
- Advantage is everybody knows what is and is not permitted
- After wide usage, the wording is likely to be accurate and legally binding.
- Saves time and effort in producing own License.
- May not be exactly what Author wants though.
- It also saves the author from having to spend time and effort in
- Most standard licenses allow 3rd parties to sell.

GNU GENERAL PUBLIC LICENSE

- The original and best known
- Software may be used by anyone for commercial and non-commercial purposes
- May be redistributed without restrictions
- Conditional on including the source code
- GPL restricts the creation of derived works (permitted but only if the derived work is also licensed under GPL)
- This prevents GPL-licensed software from being transformed into a proprietary (Exclusive Rights) product (with secret source code).
- Examples include Linux, MySQL, GCC compiler, EMACS editor and hundreds of other programs.

BSD LICENSE

- The BSD license is very simple, therefore short.
- Only condition is that people must mention the name of the Author if they incorporate the software in their own programs.
- All other use and redistribution is permitted (including for commercial purposes)
- Popular among Author's who desire to have their work used by the largest number of people, and who do not object to others making money from their software
- The operating systems FreeBSD and OpenBSD and the web server Apache are notable examples
- A comparable license is the MIT license in which the user indemnifies the Author from any liability arising from the use

ARTISTIC LICENSE

- Software may be used and redistributed without further restrictions.

- Modifying the software is also permitted, but modified versions may only be redistributed if the modifications are freely available to all.
- It is not permitted to sell software covered by the Artistic License (which is permitted by most other standard licenses)
- Notable example is the Perl interpreter (with which Perl scripts are executed)

PUBLIC DOMAIN

- Strictly speaking not a license
- Means that there is no copyright on the software whatsoever
- Without restriction, the software can be used, distributed, modified and distributed by anyone, anywhere, anytime.
- No restrictions on commercial expectation of public domain software
- Not required to identify the original author
- Author yields all rights and does not restrict anything third parties do with the software.
- Author is not liable for damages.

WRITING YOUR OWN SOFTWARE LICENSE

- Author may write own License (or have lawyer draft)
- It is notoriously difficult to anticipate all possible circumstances under which people will want to use and/or distribute the program. For example;
    - May someone put the program on a CD-ROM and sell that?
    - Does it matter whether the CD-ROM contains a collection of software or only that program?
    - May modified versions bear the same name?
- Even if an Author has determined the conditions under which they are making the software available, it is very difficult to properly express these conditions in legally binding terms.
    - A license such as "Permission is hereby granted to use this program in any way and for any purpose, to modify it and to distribute it" does not authorize third parties to distribute modified versions, although this was probably the intent of the author.
- Unless Author has a compelling reason to do so and is prepared to engage a lawyer to actually the License, it is recommended to use a standard license.

Sources: IUS Mentis: Law & Technology Explained, and Karl Fogel (see References for details)

APPENDIX E: PROPAGANDA TECHNIQUES

People are inherently social creatures, and which makes us suggestible. Being open to the influence of others lies at the very heart of what it is to be human. Even for those among us who identify as introverts and claim not to need people, it is still a question of degree as to how suggestible we are.

An essential skill of the ethical technologist, and indeed the self-aware citizen of the world, is to recognise when attempts are being made to manipulate us by playing on our emotions.

This appendix outlines the seven principal ways that you can recognise an attempt to manipulate or brainwash you. The advertising industry and politicians have been using them for a long time. If you know what they are, you can avoid being unduly influenced. Forewarned is forearmed. If you know what propaganda looks and sounds like and how to deal rationally with it, you can then make an informed decision about whether to go along with it.

The techniques outlined here were developed by the *Institute of Propaganda Analysis (IPS)*, a U.S.-based organization set up in 1937 by Mather, Filene and Miller. These techniques are as true today as they were then and will still be true in the future. Why? Because they are rooted in human social psychology, and we do not evolve very quickly. We are innately susceptible to these techniques. It is not culturally defined.

The techniques include the following:

- Name Calling
- Glittering Generalities
- Transfer
- Testimonial
- Plain Folks
- Card Stacking
- Band Wagon

The techniques have one thing in common; they are designed to appeal to our emotions rather than to reason. Neuroscience tells us that our emotions are an aspect of our primitive brain, the part we have in common with animals. Reason is a function of our evolved brain, the part that developed in more recent times. A normally reasonable person becomes unreasonable when their emotions are inflamed.

The best defence against any of these techniques is to stay rational and gather enough information from independent sources to make an informed decision. The IPS suggests specific defences for each technique, as seen in italics below.

NAME CALLING

Name calling is declaring something is bad without any real evidence. No further discussion or investigation is required. The matter is closed. The bad name is the conclusion that we should all accept and start repeating. It works to create fear and loathing towards the target, and it can be applied against individuals, groups, belief systems, religions, institutions and nations. Name calling is a substitute for a reasoned weighing up of the merits of something. It is characterised by a tone of scorn, sarcasm and ridicule.

The best way to deal with this technique is to calmly ask yourself what does the name really mean? Is there a real connection between the idea and the name being used? Does the idea have merit if the name is left out?

GLITTERING GENERALITIES

Propagandists as well as charismatic leaders are adept at using catchphrases that connect with deeply held values and beliefs in the audience. Little or no supporting evidence is given. Glittering generalities appeal to abstract ideas like honour, glory, love of country, desire for peace, security, freedom and family values. The words used are vague enough to mean what people want them to mean, but the implication is always favourable. No-one can prove it wrong because it says very little in concrete terms.

The best defence is to calmly ask yourself what does the slogan or catch-phrase mean? Is there a real connection between the idea and the slogan being used? Does the idea have merit if the slogan is left out?

TRANSFER

The Transfer technique tries to extend the authority and approval of something or someone we respect to something the propagandist would have us believe. Symbols play an important role with this technique, for example flag waving or idealised images of womanhood or manhood, anything that can stir the emotions and win our approval.

The best defence is to calmly ask yourself what exactly is the speaker trying to pitch? What does it mean? Is there a legitimate connection between the suggestion and the person or product? Does the proposal have any merit by itself? Try to do this independently of the convictions you already have about other persons or ideas.

TESTIMONIAL

Testimonials are an implementation of the Transfer technique, but where the respected or authoritative person themselves seeks to make the transfer rather than a third person. The respected person gives something their stamp of approval, essentially making an ethical appeal based on their authority as an expert to encourage the audience to follow their example.

The best defence is to calmly ask yourself who exactly is this authority figure? Is there a good reason we should believe they are qualified to make this recommendation? Is there any merit to what is being proposed? The technique falls apart if you can see that the person is not actually an authority but somebody with a secret agenda, or show that other experts disagree with them.

PLAIN FOLKS

The Plain Folks technique presents a spokesperson from humble origins, a simple, decent, good-natured person who has our best interests at heart. The spokesperson uses common, everyday speech and mannerisms to get people to identify with them and so accept their point of view.

The best defence is to calmly ask yourself is this person believable and trustworthy when removed from the situation being discussed? Are they trying to cover up anything? What are the facts of the situation? Try to consider the ideas contained in the proposal separately from the personality of the presenter.

BANDWAGON

The Bandwagon technique aims to get you to follow the crowd. It creates the impression that something has widespread support, and plays on the instinct to be on the winning side. It also plays on feelings of loneliness or social isolation if these are present. The message simultaneously encourages those not on the bandwagon to join, and for those already on the bandwagon to stay on board.

A variation is to say if you do not join now, you will be left behind, abandoned. Either way, a person is encouraged to get with the strength on-board the bandwagon.

The best defence is to calmly ask yourself what exactly is the propagandist's program? What are the pro's and con's of the program? Others might be supporting it, but is there a good reason for me to do so?

CARD STACKING

In the Card Stacking technique, the propagandist cherry-picks only those facts that strongly support their case, while presenting their opponent's case in the worst possible light. It is dishonest because we are being urged to accept a carefully selected sub-set of the truth as the whole truth.

The technique is difficult to detect because it does not present all the information necessary to make an informed decision, while implying that this is the whole truth.

The best defence is to calmly ask yourself are the facts being distorted, or are they missing altogether? Does anyone else independently support this point of view?

THE ETHICAL TECHNOLOGIST

Propaganda techniques like these have been successfully used in organisations to shape culture and instil values. Most of the time, there is nothing unethical about this. Sometimes though, the corporate culture is about profit above scruples. If you find yourself in such an environment, at the very least you should be aware of what kind of people you are associating with and becoming like. You would be well-advised to leave gracefully and as soon as possible.

APPENDIX F: MILITARY TECHNOLOGY

No discussion is complete without mention of the dilemma of military technology. How can we reconcile the existence, if not the need for military technology in the world when its primary purpose appears to be to dehumanise, often in the most extreme ways?

KILL-BOTS

This truly is a dilemma that remains unresolved. This appendix tries to unravel the issues so that we may see them more clearly. The military ethicist Peter W. Singer of the Brookings Institute (not to be confused with Peter A. Singer who is a professor of Bioethics at Princeton University) concluded in a 2010 article in the *Journal of Military Ethics* that in a world of 'killer apps', robotic weapons that can function autonomously, it is necessary to open up a constructive dialogue on how to deal with the moral dilemmas created by this new category of weaponry.

Singer notes that throughout history, certain technological advances have been 'game-changers'. For example the printing press, gunpowder, the steam engine, or the atomic bomb. Not only are the current military technologies game-changers, they are part of a cresting wave of advances that are coming at us thick and fast. These include *directed energy weapons (Lasers), precision guided weapons ('smart' IEDs), nanotech and microbotics (The Diamond Age), bioagents and genetic weaponry (DNA bombs), chemical and hardware enhancements to the human body (IronMan meets Captain America), autonomous armed robots (Terminators), electromagnetic pulse weaponry (The Day After, Ocean's 11), and space weaponry (Star Wars).* These may seem to be the stuff of science-fiction, but all of them are currently in development and are likely to be deployed in active service around 2030 or sooner.

History clearly shows us that many of the technologies that we use and depend on in everyday life have their origins as military technology that has become de-classified and then commercialised. Indeed, the modern phenomenon of computer technology owes much to trying to win World War II. For example, in the U.S. the ENIAC machines were developed to help the US Army with artillery aiming by quickly calculating ballistic trajectories. In Germany, Konrad Zuse and his Z series computers were helping the German war-effort in no small way. In Britain, the Colossus computer was developed to decode the German Enigma cipher that allowed the allies to know where to find and destroy the U-boats that were taking such a toll on the supply convoy ships carrying materials across the Atlantic from the US to Britain. These were truly breakthrough, game-changing technologies.

Highly secret at the time, in the 1950's and beyond, much of this computer technology was later commercialised, leading to the world as we know it now in the 21st Century. Indeed, wars and conflict throughout human history have been responsible for rapid advances in technology. It is a little-known fact that

Leonardo da Vinci, known for his love of humanity, not to mention his art and science, was also a well-paid military engineer whose inventions helped the wealthy city states of Renaissance Italy defend themselves against plunderers.

US AND THEM

The tendency for one group of people to go to war with another group is deeply ingrained in human nature, as evolutionary psychology recognises. As a species, humans evolved in cooperative groups (extended families). Loyalty to the group was essential for survival because the scarcity of resources meant that one group would often get what it needed at the expense of another group, inevitably leading to conflict. We have all heard of the term *'us and them'* and instinctively understand the concept of in-groups and out-groups.

Notwithstanding these evolutionary factors, it can be strongly argued that people today need to be able to transcend these ancient patterns of behaviour, these instincts, by using our more recently evolved rational minds. Much of this book focuses on just this point. Realistically, instincts can never be gotten rid of or repressed; they can only be transcended or over-ridden by logic.

One strategy is to transcend the 'us and them' mind-set that makes us see 'them' as sub-human and so be able to kill them in good conscience, with the more enlightened attitude that 'us and them' in the modern world is an illusion. We are all one species, all essentially the same under the skin, all of us members of the one big human family. If we widen our *'circle of care'* as the other Peter Singer (from Princeton) suggests, from our immediate family to include an ever-widening circle of people in the world, then we will naturally come to act more compassionately towards everyone, not just our immediate family.

Another strategy is put forward by Robert Wright in his 2001 book *Nonzero: the logic of human destiny*. He makes the compelling point that we are less likely to want to go to war against someone if we have an economic connection with them, such that by harming them, we harm ourselves. It does not make sense to hurt our own interests. The global economy in the 21st century is a single interconnected entity. We can no longer act in isolation. The consequences of our actions are transmitted everywhere.

Wright quotes Charles Darwin to good effect: *'As man advances in civilization, and small tribes are united into larger communities, the simplest reason would tell everyone that he ought to extend his social instincts and sympathies to all members of the same nation, though personally unknown to him. This point being once reached, there is only an artificial barrier to prevent his sympathies extending to the men of all nations and races.'* — Charles Darwin, *The Descent of Man.*

Wright's and Darwin's perspectives can help us to transcend the 'us and them' mentality that has kept humanity perpetually at war throughout our blood-stained history. It will take a long time for the world to change because there is

immense inertia built-up in the system, but the observable trend suggests that the change will come in time. Perhaps not soon enough for some but come it will.

In practical terms, where does this leave us now? We currently live in a world where war is still a reality. There are bad actors who would go on the offensive unless their intended victims are well-defended. If nations are going to safeguard their interests, there will be a continuing, though hopefully lessening need for military technology to support this imperative.

SEVEN QUESTIONS

Singer (2010) suggests these seven questions to help a technologist decide what an ethical course of action is:

1. From whom is it ethical to take research and development money? From whom should one refuse to accept funding?
2. What attributes should one design into a new technology, such as its weaponization, autonomy or intelligence? What attributes should be limited or avoided?
3. What organizations and individuals should be allowed to buy and use the technology? Who should not?
4. What type of training or licensing should the users have?
5. When someone is harmed because of the technology's actions, who is responsible? How is this determined?
6. Who should own the wealth of information the technology gathers about the world around them? Who should not?

(Singer, 2010)

As a general principle, *the abuse of something should not in itself prohibit the use of it*. The potential for people to abuse something should not prevent it from being used in non-harmful ways. Motor cars and drugs would be two examples out of many. Military technology would be another. If the net good outweighs the net harm, a compelling argument exists to use it. Where to draw the line is often unclear. Each case must be considered individually and on its merits.

APPENDIX G: SELECT BIBLIOGRAPHIES

SELECT BIBLIOGRAPHY FROM CARNEGIE MELLON UNIVERSITY

URLs are valid as of the publication date of this document.

Alberts, Chris; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. Defining Incident Management Processes for CSIRTs: A Work in Progress. CMU/SEI-2004-TR-015 ADA453378. Software Engineering Institute, Carnegie Mellon University. 2004. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153

Alberts, Chris; Dorofee, Audrey; Ruefle, Robin; & Zajicek, Mark. An Introduction to the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC). CMU/SEI-2013-TN-015.

Software Engineering Institute, Carnegie Mellon University. 2013. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91452

Barker, William C. Guideline for Identifying an Information System as a National Security System (NIST Special Publication 800-59). 2003. http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf

Cichonski, Paul; Millar, Tom; Grance, Tim; & Scarfone, Karen. Computer Security Incident Handling Guide (NIST Special Publication 800-61, Rev 2). 2012. http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Dempsey, Kelley; Sha Chawlaa, Nirali; Johnson, Arnold; Johnston, Ronald; Clay Jones, Alicia; Orebaugh, Angela; Scholl, Matthew; & Stine, Kevin. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST Special Publication 800-137). 2010. http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

Department of Homeland Security. DHS Federal Continuity Directive 1: Federal Executive Branch National Continuity Program and Requirements: Annex C. 2008. http://www.fema.gov/pdf/about/org/ncp/fcd1.pdf

Department of Homeland Security. DHS Federal Continuity Directive 2: Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process. 2008. http://www.fema.gov/pdf/about/org/ncp/fcd2.pdf

Department of Homeland Security. A Roadmap for Cybersecurity Research. 2009. https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf

Department of Homeland Security. Department of Homeland Security Federal Network Security Branch. Continuous Asset Evaluation, Situational

Awareness, and Risk Scoring Reference Architecture Report (CAESARS). 2010. https://csrc.nist.gov/csrc/media/publications/nistir/7756/draft/documents/draft-nistir-7756_second-public-draft.pdf

Department of Homeland Security. Cybersecurity Capability Validation (CCV) Assessment Method and Process Guidance Version 1.1. U.S Department of Homeland Security. 2012.

Department of Homeland Security. IT Program Assessment: Department of Homeland Security (DHS) Analysis and Operations (A&O) Common Operating Picture (COP). U.S. Department of Homeland Security. 2012. http://www.dhs.gov/xlibrary/assets/mgmt/itpa-ao-cop2012.pdf

Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. Incident Management Capability Metrics, Version 0.1. CMU/SEI-2007-TR-008 ADA468688. Software Engineering Institute, Carnegie Mellon University. 2007.

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8379

ENISA. CSIRT A Step-by-Step Approach on How to Set Up a CSIRT. 2006. https://www.enisa.europa.eu/publications/csirt-setting-up-guide

ENISA. CSIRT Good Practice Guide for Incident Management. 2010. https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

Federal Financial Institutions Examination Council (FFIEC). IT Examination Handbook InfoBase. 2006. http://ithandbook.ffiec.gov/

Grance, Tim; Nolan, Tamara; Burke, Kristin; & Good, Travis. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (NIST Special Publication 800-84). 2006. http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf

Hash, Joan; Bartol, Nadya; Rollins, Holly; Robinson, Will; Abeles, John; & Batdorff, Steve. Integrating IT Security into the Capital Planning and Investment Control Process (NIST Special Publication 800-65). 2005. http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf

International Information Systems Security Certification Consortium (ISC)^2. Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK). 2007. http://www.isc2.org/official-isc2-textbooks.aspx

Information Security Forum. The Standard of Good Practice for Information Security. 2012. https://www.securityforum.org/tool/the-isf-standardrmation-security/

International Organization for Standardization. Information technology — Security techniques — Information security management systems—Requirements (ISO/IEC 27001:2005). 2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

International Organization for Standardization. Information technology — Security techniques — Code of practice for information security management (ISO/IEC 27002:2005) 2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

IT Governance Institute. Control Objectives for Information and related Technology (COBIT) 5. 2012. http://www.isaca.org/cobit

Johnson, Arnold; Dempsey, Kelley; Ross, Ron; Gupta, Sarbari; & Bailey, Dennis. Guide for Security-Focused Configuration Management of Information Systems (NIST Special Publication 800-128). 2011. http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf

Joint Task Force Transformation Initiative. Guide for Conducting Risk Assessments (NIST Special Publication 800-30 Rev 1). 2012. http://csrc.nist.gov/publications/nistpubs/800-30- rev1/sp800_30_r1.pdf

Kent, Karen & Souppaya, Murugiah. Guide to Computer Security Log Management (NIST Special Publication 800-92). 2006. http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

Kent, Karen; Chevalier, Suzanne; Grance, Tim; & Dang, Hung. Guide to Integrating Forensic Techniques into Incident Response (NIST Special Publication 800-86). 2006. http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. State of the Practice of Computer Security Incident Response Teams (CSIRTs). CMU/SEI-2003-TR-001, ADA421664. Software Engineering Institute, Carnegie Mellon University. 2003. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6571

Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. Organizational Models for Computer Security Incident Response Teams (CSIRTs). CMU/SEI-2003-HB-001, ADA421684. Software Engineering Institute, Carnegie Mellon University. 2003. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6295

Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. CSIRT Services. Software Engineering Institute, Carnegie Mellon University. 2002. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=53046

Mell, Peter; Waltermire, David; Feldman, Larry; Booth, Harold; Ragland, Zach; Ouyang, Alfred; & McBride, Timothy. CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture (Second Draft). 2012. http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-NISTIR-7756_second-public-draft.pdf

Mell, Peter; Bergeron, Tiffany; & Henning, David. Creating a Patch and Vulnerability Management Program (NIST Special Publication 800-40, Version 2.0). 2005. http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

Mell, Peter; Kent, Karen; & Nusbaum, Joseph. Guide to Malware Incident Prevention and Handling (NIST Special Publication 800-83). 2005. http://csrc.nist.gov/publications/nistpubs/800- 83/SP800-83.pdf

The National Archives and Records Administration. General Records Schedule 24—Information Technology Operations and Management Records. 2010. https://www.archives.gov/files/records- mgmt/grs/grs24.pdf

National Institute of Standards and Technology. Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199). 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

National Institute of Standards and Technology. Minimum Security Requirements for Federal Information and Information Systems (FIPS PUB 200). 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

National Institute of Standards and Technology, Joint Task Force Transformation Initiative. Recommended Security Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53, Rev 3). 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

National Institute of Standards and Technology. NIST Special Publications, 800 Series. 2009. http://csrc.nist.gov/publications/PubsSPs.html

National Institute of Standards and Technology, Joint Task Force Transformation Initiative. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach (NIST Special Publication 800-37 Rev 1). 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

National Institute of Standards and Technology, Joint Task Force Transformation Initiative. Guide for Assessing the Security Controls in Federal Information Systems (NIST Special Publication 800-53A Rev 1). 2010.

http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

National Institute of Standards and Technology, Joint Task Force Transformation Initiative. Managing Information Security Risk: Organization, Mission, and Information System View (NIST Special Publication 800-39). 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39- final.pdf

National Institute of Standards and Technology. Computer Security Incident Handling Guide (Draft) (NIST Special Publication 800-61 Rev 2 DRAFT). 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Institute of Standards and Technology. Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53 Rev 4). 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Network Working Group. Expectations for Computer Security Incident Response. 1998. http://www.ietf.org/rfc/rfc2350.txt

Office of Government Commerce. IT Infrastructure Library (ITIL). 2006. http://www.itil-officialsite.com/

Office of the Law Revision Counsel, U.S. House of Representatives. United States Code, Title 44, Sections 3541-3549 “Federal Information Security Management Act of 2002.” 2003. http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title44-chapter35- front&num=0&edition=prelim

Office of Management and Budget. Circular No. A-130, Revised, Appendix III, Security of Federal Automated Information Resources. 1996. https://a130.cio.gov/appendix3/

Office of Management and Budget. Safeguarding Against and Responding to the Breach of Personally Identifiable Information (memorandum). 2007. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

Reid, Gavin & Schieber, Dustin. CSIRT Case Classification (Example for Enterprise CSIRT). 2004. https://www.first.org/resources/guides/#CSIRT-Case-Classification-Example-for- enterprise-CSIRT

Ross, Ron; Swanson, Marianne; Stoneburner, Gary; Katzke, Stu; & Johnson, Arnold. Guide for the Security Certification and Accreditation of Federal Information Systems (NIST Special Publication 800-37) 2004. https://security.health.ufl.edu/VA_Research/NIST%20800-37-Security%20Cert%20and%20Accred%20for%20FIS.pdf

Scarfone, Karen & Mell, Peter. Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST Special Publication 800-94). 2007. http://csrc.nist.gov/publications/nistpubs/800- 94/SP800-94.pdf

Scarfone, Karen; Souppaya, Murugiah; Cody, Amanda; & Orebaugh, Angela. Technical Guide to Information Security Testing and Assessment (NIST Special Publication 800-115). 2008. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Scarfone, Karen & Hoffman, Paul. Guidelines on Firewalls and Firewall Policy (NIST Special Publication 800-41, Rev 1). 2009. https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

Sharp, Alec & McDermott, Patrick. Workflow Modelling: Tools for Improvement and Application Development. Boston, MA: Artech House. 2001. http://www.artechhouse.com/Main/Books/Workflow-Modeling-Tools-for-Process-Improvement- an-1298.aspx

Software Engineering Institute. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). Software Engineering Institute, Carnegie Mellon University. 2003. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=309051

CMMI Product Team. CMMI for Development, Version 1.3. CMU/SEI-2010-TR-033. Software Engineering Institute, Carnegie Mellon University. 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm

CMMI Product Team. CMMI for Services, Version 1.3. Software Engineering Institute, Carnegie Mellon University. 2010. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9661

Stine, Kevin; Kissel, Rich; Barker, William C.; Fahlsing, Jim; & Gulick, Jessica. Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories (NIST Special Publication 800-60 Rev 1). 2008. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

Swanson, Marianne & Guttman, Barbara. Generally Accepted Principles and Practices for Securing Information Technology Systems (NIST Special Publication 800-14). 1996. http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Swanson, Marianne; Hash, Joan; & Bowen, Pauline. Guide for Developing Security Plans for Federal Information Systems (NIST Special Publication 800-18, Rev 1). 2006. http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

Swanson, Marianne; Bowen, Pauline; Wohl Phillips, Amy; Gallup, Dean; & Lynes, David. Contingency Planning Guide for Federal Information Systems (NIST Special Publication 800-34, Rev 1). 2010. http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Tracy, Miles; Jansen, Wayne; Scarfone, Karen; & Butterfield, Jason. Guidelines on Electronic Mail Security (NIST Special Publication 800-45 Version 2). 2007. http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf

West-Brown, Moira J.; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. Handbook for Computer Security Incident Response Teams (CSIRTs) (CMU/SEI-2003-HB-002, ADA413778). Software Engineering Institute, Carnegie Mellon University. 2003. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

Wilson, Mark & Hash, Joan. Building an Information Technology Security Awareness and Training Program (NIST Special Publication 800-50). 2003. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

SELECT BIBLIOGRAPHY FROM CAMBRIDGE UNIVERSITY

Accenture Security. 2017 Cyber Threatscape Report: Midyear Cybersecurity Risk Review-Forecast and Remediation's. Accenture Security, 2017.

Advisen. Information Security and Cyber Risk Management. Seventh Annual Survey, 2017. Akamai. State of the internet/security: Q2 2017 Report.

Allianz. A Guide to Cyber Risk. Allianz Global Corporate & Specialty White Paper, 2017.

Amazon (1). "Amazon Simple Storage Service (S3) — Cloud Storage — AWS". Amazon Web Services, Inc. 2018. Amazon (2). "Amazon EC2".

Aon. Global Cyber Market Overview, June 2017. BAE. "When cyber attacks meet financial crime".

Barth, Bradley. "DDoS attacks delay trains, halt transportation services in Sweden". SC Magazine. October 16, 2017. BBC (1). "Qatar Crisis: What you need to know." July 19, 2017.

BBC (2). "Theresa May accuses Vladimir Putin of election meddling." November 14, 2017. BBC (3). "NHS cyber-defender Marcus Hutchins to appear in U.S. court." August 4, 2017. BBC (4). "Dark web markets boom after AlphaBay and Hansa Busts". August 1, 2017.

BBC (5). "South Korean firm's 'record' ransom payment", June 20, 2017.

Berr, Jonathan. "'WannaCry' ransomware attack losses could reach $4 billion". CBS Moneywatch. May 16, 2017.

Beazley (1). "Ransomware attacks steal headlines, but accidental data breaches remain a major cause of loss". August 1, 2017. Beazley (2). "Technology, Media & Business Services First Party Computer Claims".

Blodget, Henry. "Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data". Business Insider. April 28, 2011. Boey, Darren. "North Korean Hacker Group Linked to Taiwan Bank Cyber Heist." Bloomberg Technology. October 17, 2017.

Brook, Chris. "DDOS Attacks Can Cost Businesses up to $2.5 Million per Attack, Report Says". Threat Post. May 2, 2017. Burgess, M. "What is GDPR? WIRED explains what you need to know". Wired, January 2, 2018.

Chappell, Bill. "'Petya' Ransomware Hits at Least 65 Countries; Microsoft Trace it to Tax Software." NPR. June 28, 2018. Cimpanu, Catalin. "95% of All Ransomware Payments were Cashed out via BTC-e Platform". Bleeping Computer. July 27, 2017. Coles, Cameron. "Overview of Cloud Market in 2017 And Beyond". Skyhigh.

Comptroller and Auditor General. Investigation: WannaCry cyber attack and the NHS. National Audit Office. Department of Health. October 27, 2017.

Council of Europe. International Co-operation under the Convention on Cybercrime. Project on Cybercrime. 18 August, 2017. Cybereason. Paying the Price of Destructive Cyber Attacks. Whitepaper, 2017.

EMVco. "EMVCo Reports 6.1 Billion EMV Chip Payment Cards in Global Circulation". June 5, 2017. European Commission. "Protection of personal data". Europa, 2017.

Europol. Internet Organised Crime Threat Assessment. 2017.

Field, Tom. "The Blurred Lines Between Criminals and Nation-States". Bank Info Security. June 19, 2017. Forester, Conner. "NotPetya ransomware outbreak cost Merck more than $300M per quarter". Tech Republic.

Finkle, Jim (1). "Your medical record is worth more to hackers than your credit card". Reuters. September 24, 2014.

Finkle, Jim.(2) "Cybersecurity Firm: North Korea Was Likely Behind Cyber Heist In Taiwan". Business Insider. October 16, 2017.

Gabel, Detlev and Hickman, Tim. K. Key definitions-Unlocking the EU General Data Protection Regulation. Whitecase publications, September 2017.

Gammons, Brianna. “6 Must-Know Cybersecurity Statistics for 2017”. Barkly (Blog), January, 2017. Gartner (1). “Gartner Says Worldwide Public Cloud Services Market to Grow 18% in 2017”. 2017.

Gartner (2). “Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017”.

August 16, 2017.

Gerstein, Josh. “Alleged leaker Reality Winner said she stuffed NSA report in her pantyhose”. Politico. September 27, 2017. Gibbs, Samuel (1). “Shadow Brokers threaten to unleash more hacking tools”. The Guardian. May 17, 2017.

Gibbs, Samuel (2). “Game of Thrones: HBO hackers threaten leak of season finale”. The Guardian. August 21, 2017. Gogan, Marcell. “Insider Threat as the Main Security Threat in 2017”. TRIPWIRE. April 11, 2017.

Google (1). “Google Cloud Computing, Hosting Services & Apis”. Google Cloud Platform. Google (2). “Cloud Locations”.

Graham, Chris. “NHS cyber attack: Everything you need to know about ‘biggest ransomware’ offensive in history”. The Telegraph.

May 20, 2017.

Gray, Alistair. “U.S. banks to introduce new anti-fraud measures after Equifax Hack”. Financial Times. October 15, 2017. Greenberg, Andy (1). “How An Entire Nation Became Russia’s Test Lab for Cyberwar.” Wired. June 19, 2017.

Greenberg, Andy (2). “The Biggest Dark Web Takedown Yet Sends Black Markets Reeling”. Wired. July 14, 2017. Greenberg, Andy (3). “No One Wants to Buy Those Stolen NSA-Linked ‘Cyberweapons’”. Wired. August 16, 2016.

Greenough, J. “The ‘Internet of Things’ Will Be The World’s Most Massive Device Market And Save Companies Billions Of Dollars”. Business Insider. November 18, 2014.

IBM. “IBM Blue Mix”. IBM.

IBM X-Force Research. The weaponization of IoT devices: Rise of the thingbots. New York: IBM, 2017.

IDC. “Worldwide Spending On Security Technology Forecast To Reach $81.7 Billion In 2017, According To New IDC Spending”.

Research Press Release. March 29, 2017.

Imperva. Global DDoS Threat Landscape Q1 2017. 2017

Information Commissioner's Office. Guide to the General Data Protection Regulation. ICO, 2017.

Jolly, Jasper. "Massive hack at Equifax exposes personal records of Brits and 142m Americans". CITY A.M. September 8, 2017. JLT. "Asia Moves Towards Tougher Data Breach Rules". December 8, 2017.

Johnson, Tim. "Here's one tally of the losses from WannaCry ransomware attack". McClatchy.

Jun, Kwanwoo and Yousef, Nancy. "North Korea Suspected of Hacking U.S.- South Korean War Plans." The Wall Street Journal. October 10, 2017.

Kan, Michael. "Yahoo uncovered breach after probing a black market sale". CIO. September 22, 2016. Kar, Ian. "The chip card transition in the U.S. has been a disaster". Quartz. July 29, 2016.

Kaspersky Lab (1). APT Trends Report Q2 2017. SECURELIST, 2017. Kaspersky Lab (2). KSN Report: Ransomware in 2016-2017. Security List,2017.

Khalimonenko, Alexander, Oleg Kupreev, and Timur Ibragimov. DDoS attacks in Q2 2017. SecureList DDOS Reports. Khandelwal, Swati. "Hackers Stole $32 Million in Ethereum; 3rd Heist in 20 days". The Hacker News. July 19. 2017.

Kshetri, Nir and The Conversation. "Cryptocurrencies May Be a Dream Come True for Cyber-Extortionists". Fortune. September 19, 2017.

Lin, Adela, and Ondaatjie, Anusha. "Sri Lanka Makes Arrests In $60 Million Taiwanese Bank Cyberheist". Bloomberg. October 12, 2017. Lloyds. Bitcoin: Risk Factors for Insurance. London: Lloyd's Innovation Series, 2015.

Ludwin, Adam. "How Anonymous is Bitcoin? A Backgrounder for Policymakers". Coindesk. January 25, 2015.

Morgan, Steve. "Global ransomware damage costs predicted to exceed $5 billion in 2017, up from $325 million in 2015". CSO. May 23, 2017.

McCrank (1), John. "Equifax says 15.2 million U.K. records exposed in cyber breach". Reuters. October 10, 2017.

McCrank (2), John and Saxena, Aparajita. "Equifax clears executives who sold shares after hack". Reuters. November 3, 2017. Michael, Casey. "The Kremlin's California Dream." Slate. May 4, 2017.

Microsoft Azure. "Cloud Locations". Google Cloud Platform.

National Association of Insurance Commissioners. "The National System of State Regulation and Cybersecurity". December 12, 2017. Nakashima, Ellen. "Prosecutors to seek indictment against former NSA contractor as early as this week". The Washington Post. February 6, 2017.

National Audit Office. Investigation: WannaCry Cyber Attack and the NHS. Report by the Comptroller and Auditor General, Department of Health. HC 414 Session 2017–2019 October 27, 2017.

Newton, Casey. “How A Typo Took Down S3, The Backbone Of The Internet”. The Verge. March 2, 2017.

Nichols, Shaun. “AWS’s S3 Outage Was So Bad Amazon Couldn’t Get into Its Own Dashboard to Warn The World”. The Register.

March 1, 2017

O’Conner, Fred. “NotPetya Still Roils Company’s Finances, Costing Organizations $1.2 Billion In Revenue”. Cybereason. November 9, 2017.

Office of the Director of National Intelligence. “Assessing Russian Activities and Intentions in Recent U.S. Elections”. ICA, 2017- 01D. January 6, 2017.

Oliphant, Roland and McGoogan, Cara. “NATO warns cyber-attacks ‘could trigger article 5’ as world reels from Ukraine hack.”

The Telegraph. June 28, 2017.

Paganini, Pierluigi. “Imperva Report Q2 2017- Over 75% Of DDoS Targets Were Hit Multiple Times”. Security Affairs. October 3, 2017. Palmer, Danny. “A massive cyberattack is hitting organizations around the world”. ZD Net. June 27, 2017.

Perlroth, Nicole. “All 3 Billion Yahoo Accounts Were Affected by 2013 Attack”. New York Times. October 3, 2017.

Popper, Nathaniel and Ruiz, Rebecca. “2 Leading Online Black Markets Are Shut Down by Authorities”. New York Times. July 20, 2017.

PYMNTS. “Dark Web Down but Not Out”. August 21, 2017

Rayome, Alison. “33% of businesses hit by DDoS attack in 2017, double that of 2016”. Tech Republic. October 11, 2017. Right Scale. 2017. State Of the Cloud Report.

Riley, Michael (1), Anita Sharpe and Jordan Robertson. “Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed”. Bloomberg. September 18, 2017.

Riley, Michael (2), Jordan Robertson and Anita Sharpe. “The Equifax Hack Has the Hallmarks of State-Sponsored Pros”. Bloomberg. September 29, 2017.

Romanosky, Sasha, Lillian Ablonm Andreas Kuehn and Therese Jones. Content Analysis on Cyber Insurance. RAND Working Paper, September 2017.

Shepardson, David. “Equifax failed to patch security vulnerability in March: former CEO”. Reuters. October 2, 2017.

Shevchenko, Sergei, Hirman Muhammad bin Abu Bakar, and James Wong. “Taiwan Heist: Lazarus Tools and Ransomware”. BAE Threat Research (Blog). October 16, 2017.

Solon, Olivia and Siddiqui, Sabrina. “Russia-backed Facebook posts ‘reached 126m Americans’ during U.S. election.” The Guardian. October 31, 2017.

Sputnik News. “Chinese Phone App Leaks 2 Billion Private Numbers, High Officials’ Among Them”. May 14, 2017.

Stecklow, Steve, Alexandra Harney, Anna Irrera and Jemima Kelly. “Chaos and hackers stalk investors on cryptocurrency exchanges”. Reuters. September 29, 2017.

Symantec. Internet Security Threat Report. ISTR, 2017. Symantec. ISTR Ransomware 2017. July 2017.

Symantec. “Attackers target dozens of global banks with new malware”. Symantec Official Blog. February 12, 2017. Symantec. Internet Security Threat Report: Financial Threats Review 2017. 2017.

Symantec. “Attackers Target Dozens of Global Banks With New Malware”. Symantec Official Blog (Blog). The Conversation. “By concealing identities, cryptocurrencies fuel cybercrime”. Editorial. September 26, 2017. Thomson, Iain. “Virus (cough, cough Petya) goes postal at FedEx, shares halted”. The Register. June 28, 2017.

Turner, Karen. “The Equifax hacks are a case study in why we need better data breach laws”. Vox. September 14, 2017.

United State Department of the Treasury Financial Crimes Enforcement Network. “FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drugs Sales”. FinCen. July 26, 2017.

Viner, K. “How technology disrupted the truth.” The Guardian. July 12, 2016. Wolff, Josephine. “The New Economics of Cybercrime”. The Atlantic. June 7, 2017.

Wolfram, Hedrick, Gerald Wong and Jaclyn Yeo. Cyber Risk in Asia-Pacific: The Case For Greater Transparency. OLIVER WYMAN, 2017.

Woo, G.; 2017; Counterfactual Analysis of WannaCry Malware Attack. RMS Webinar, Nov 2017; and blog ‘Reimagining the WannaCry Cyberattack’

Woodward, Matt. “How Much Does 1 Hour of Downtime Cost the Average Business?”. RAND Group.