Security, Cyber Security and Privacy Challenges Post Covid-19

2020 has seen the COVID-19 pandemic drive overwhelming societal and organisational changes, such as challenges for security and privacy. It has seen the continued disruption for many government agencies and enterprises, and has fundamentally changed the way they do business. As the backbone of the Australian economy, it is imperative that government agencies and enterprises not only adapt and recover, but are also set up for success in the next normal future. This will require extraordinary flexibility, coordination, adaptability and resilience during what may be a prolonged period of recovery, uncertainty and change.

In response to these challenges IIM has created this resource on the topic of "Security, Cyber Security and Privacy Challenges Post Covid-19".

What is Privacy and Security?

Privacy is very often united with security; however, they are two separate concepts.

- Privacy is about the appropriate collection, use and sharing of personal information whereas
- Security is about protecting such information from loss, unintended or unauthorised access, use or sharing

What is Cyber Security?

- Cybersecurity is defined as the protection of systems, networks and data in cyberspace.
- Cyber security threats exploit the increased complexity and connectivity of critical infrastructure, networks and data systems. Cyber security threats might create a risk in protecting individuals, state secrets and countries from pilfering, fraud, and espionage attacks.
- You can take steps to protect your organisation from cyber security threats by incorporating a data breach plan into your security framework
- Cybersecurity is becoming a key component in the process for the identification, analysis and mitigation of risks to information and data assets.

Privacy and Security

- Privacy may have different meanings due to factors such as context, prevailing social standards, and geographic locations. The predominant concept persists that 'privacy' is the appropriate collection, use and sharing of personal information to accomplish business tasks.
- Although privacy and security are two separate concepts, the importance of these two ideas intersects for the customer if their personal data is not safeguarded.

What is Personal Data?

This might be a good time to distinguish between data generally and personal data. Personal data has a specific meaning under the General Data Protection Act and generally covers any set of information relating to individuals. In business terms it can be argued that the key to competing in the global digital world is the power and commercial opportunity determined by the quantity and quality of data sets that the organisation have and/or can access. Questions around privacy are more specifically associated with personal data and the control or custody of data is more of an established legal notion. Personal data stem from three data types these are self-reported, digital exhaust and profiling data (see Table 1).

Type	Description
Self-reported data	Information people volunteer about themselves, such as their email address, work, education, age and gender.
Digital exhaust data	For example, location data, browsing history which is created when using mobile devices, web services or other connected technologies.
Profiling data	Personal profiles used to make predictions about individuals' interests and behaviours which are derived by combining self-reported, digital exhaust and other data.

Table 1 – Personal data types

Personal data is described in privacy and information security circles as information that can be used on its own or with other information to identify, contact or locate a single person or to identify an individual in context. With the advent of rich geo-location data and associative analysis such as facial recognition the magnitude of personal data collected is greatly expanded and so are challenges for security in protecting such information from loss, or unintended or unauthorised access, use or sharing. Coupled with this, a further privacy challenge is the need to comply with a range of conflicting regulations on privacy especially as privacy regulations can vary by state, region and country.

Understanding the Three Data Collection Types

There are three main data collection types, these are Personally Identifiable Information, Customer Information and Personal Health Information (See Table 2).

Type	Description
Personally Identifiable Information (PII)	This information includes such things as first and last names, home or business addresses, email addresses, credit card and bank account numbers, taxpayer identification numbers, patient numbers and social security numbers. It can also include gender, age and date of birth, city of birth or residence, driver's license number, home and mobile (cell) phone numbers.
Customer Information (CI)	This information includes payment information such as credit or debit card numbers and verification codes, billing and shipping addresses, email addresses, phone numbers, purchasing history, buying preferences and shopping behaviour.
Personal Health Information (PHI)	This information includes sensitive patient information such as medical conditions, past history and/or even family medical history information.

Table 2 – Three Data Collection Types

Big Data and Dark Data

Government and business collect, process and store massive amounts of structured, semi-structured, unstructured and sensor data as an outcome of business activities (See Table 3. This data is referred to as Big Data.

Data Set Type	Description
Structured	• Fixed Layout • Defined Content • Consistent Formats
Semi-Structured	• Unknown Layout • Defined Content • Variable Formats • Tabular Data
Unstructured	• Unknown Layout • Variable Content • Multipage Documents
Sensor Data	• Data generated by various machines • For example, personal devices, smart grids, cyber physical systems, smart cities, autonomous vehicles, drones and objects.

Table 3 – Breakdown of the 4 data types structured, semi-structured, unstructured and sensor data

Big data poses extra challenges to the C.I.A. paradigm because of the sheer volume of data that needs to be safe guarded, the multiplicity of sources it comes from and the variety of formats in which it exists. The C.I.A. of security stands for 'Confidentiality, Integrity and Availability' (See Table 4) and is a triad model designed to provide guidance for enterprises in developing policies for information security.

C.I.A. Triad Security Model Terms	Brief Description
Confidentiality	Confidentiality is a set of rules that restricts access to data. Confidentiality is also closely linked with privacy.
Integrity	Integrity refers to the certainty that the data is not tampered with during or after submission. Integrity also involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.
Availability	Availability denotes that data is available when it is needed. Availability is also a guarantee of reliable access to the data by authorised people and/or groups. Availability also requires protection of data and technology against obsolescence.

Table 4 - C.I.A. Triad Security Model Terms and Brief Description

A further challenge for Big Data is the passage of time. Data (information) can become disjointed, the meaning for which it was collected is lost, records are forgotten, and files are lost within the organisation's digital repositories. This significant group of uncontrolled information is escalating and is referred to as 'Dark Data'.

Dark data is data (information) assets that are normally created and used once, such as log archives, zip files, project folders, duplication and even active data which becomes inactive and overtime is forgotten. The enormous volume of data being created, captured and stored is ever-increasing and as a consequence dark data is growing. Dark data can include confidential, personal or sensitive information and presents a challenge for security, privacy and compliance.

Digital Footprints and Digital Shadows

Governments and business also collect an inordinate amount of information from citizens and customers in the delivery of their products and services. When delivering these services governments and business create 'digital footprints'. Citizens and customers as consumers of these products and services leave 'digital shadows' this is personal data left behind by transactions and interactions on the internet, applications, and across other connected devices and sensors.

For clarification, a digital footprint is information that is projected, shared and managed by both public and/or private enterprises. While this footprint can be beneficial, information can be unintentionally exposed through the enterprise footprint; thereby it could be used maliciously and put at risk the security and privacy of information assets.

A digital shadow, on the other hand is a subset of a digital footprint. A digital shadow consists of exposed personal, technical or organisational information that is often highly confidential, sensitive or private. A digital shadow can leave the consumer of products and services vulnerable to cyber

stalkers and hostile groups exploiting the digital shadow to find an organisation's (the provider of the product or service) weak point to launch targeted cyber-attacks and plant a malicious insider.

Digital footprints and digital shadows are growing and as providers and consumers of products and services so is the information being collected about you the individual and/or the organisation. This vulnerability raises another set of challenges for security and privacy for both the individual and the enterprise.

What are Malicious Insiders?

Government and business are moving to cloud based business solutions and cloud offerings such as Software as a Service (SaaS) for example Office 365, Dropbox, SharePoint and products such as Salesforce CRM. However, due to the very nature of the internet, cloud, mobile, and social technologies are inherently oriented towards the sharing of resources. Consequently, it is essential that the products, information and services shared in the cloud are protected from security and privacy breaches.

Make certain that appropriate steps are taken to ensure that policy and procedures for security and privacy protection are in place to counteract pilfering, fraud, and espionage attacks from within the Cloud. Small business should be fully aware of third-party provider's responsibilities and accountabilities around how they are managing security and privacy risks. Without full knowledge and control, your business may be at risk of data loss and leakage, account hijacking and worst the malicious insider.

The malicious insider is the 'spy' or 'traitor' who represents an inside cyber threat. The malicious insider has access to the enterprise network from inside the perimeter barricades. Malicious insiders know about the business information systems, its structure, the people and its internal operations. They are like a rogue administrator who can access your sensitive data, steal information, steal private details and perform any number of other malicious activities.
There is a need to adopt a pro-active perspective for cyber security, privacy and risk management against external malicious breaches, inadvertent internal breaches and third-party partner breaches.

Application Programming Interfaces (API)

We hear about APIs but what exactly is an API? In brief, an API stands for Application Programming Interface. An API interface describes how to connect a dataset or business process with some sort of consumer application or another business process. APIs also allow for multiple consumer applications to be connected and are normally based on a contract between different applications and their partners. APIs are the connectors that are doing the heavy work of moving data and performing specialised tasks behind the scenes.

The contract between the different applications and partners include the administration, how the data will be structured, controls and the rules on how they exchange data. If the partners agree on a set of rules, information can run freely between their applications.

These API interfaces exchange data in the background and expose data to third-party applications. This data is also decoupled from how they are used and presented. This means that an API only has to exist once, but the data can be accessed and used in different ways. Therefore, there is potentially unlimited amount of completely different applications that can access the same API and use this data in entirely new situations. APIs have to date been mainly used in retail/marketing.
For example, Expedia which compares some 200 booking sites to find the ideal hotel, flights, cars and holiday packages at the best price. In this example Expedia is using a number of APIs. These

APIs are interrogating and searching across a number of different sites which have a hotel API, pricing API, flight API, car hire API and holiday package API to provide the consumer (customer) with a single holistic view. These APIs are only using real time data that is not normally highly secured because it is open access data and has little or no potential risk to the consumer or the supplier.

Storing Information and Data Assets in the Cloud

Storing information and data in the Cloud is sometimes referred to as 'Cloud Vaults'. The security, privacy and protection of the Cloud vault may rest with your third-party provider.

Executives, management and the business need to be fully aware of the third-party provider's responsibilities and accountabilities around how they are managing security and privacy risks around your information and data assets.

You need to make certain that information and data assets ownership and the geographical location of all storage sites are clearly articulated and that you can get your information and data assets back and/or migrate them to a new Cloud provider if needed.

Intellectual Property

Intellectual property is another key concern when it comes to cloud services, in some cases cloud providers own the infrastructure or the applications, while the user owns the data, this demarcation is not always clear.

For example, open source software often combines data and code, and it is not always clear who owns the rights to what. The following are some questions you might like to consider.

- Will you own your own information and data assets?
- Where will the information and data assets be located?
- How do you get your information and data assets back?
- How long will it take for you to get your information and data assets back?

FOR MORE INFORMATION CONTACT:

Institute for Information Management Ltd. (IIM)
Email: iim@iim.org.au
PO Box 4195, Balwyn East, Victoria, 3103 Australia
(03) 5424 8551