Privacy and Security in the Digital Age

Presented by

Linda Shave, National Director IIM

Privacy and Security in the Digital Age

We now live in a digital age, in which things that used to be real and tangible are now machine generated or only exist in bits and bytes.

As government and the enterprise transition to digital services, there are now new evolving challenges. Government, enterprise and consumers are generating dark data and leaving behind digital footprints and shadows.

This dark data, digital footprints and shadows will continue to grow and so too will the issues around privacy and security.

Privacy and Security

Privacy is very often linked 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, or unintended or unauthorised access, use or sharing.

Privacy and Security Consequences

Although privacy and security are two separate concepts, the importance of these two concepts intersect:

- For the individual - if their personal data is illegally accessed, disclosed or mistakenly provided and the data breach might create a risk of damage to an individual.

- For the government or another enterprise - if their sensitive information is illegally accessed and pilfered and the data breach might be damaging to the government and/or the enterprise reputation, the safety of individuals or the country.

What is Personal Data?

Personal data stem from three data types:

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 are used to make predictions about individuals' interests and behaviours which are derived by combining self-reported, digital exhaust and other data.

What is Personal Data in the Digital Age?

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.

Further privacy challenges include the need to comply with a range of conflicting regulations on privacy especially as privacy regulations can vary by region and country.

Dark Data

Government and the enterprise continue to collect, process and store massive amounts of structured and unstructured data as an outcome of business activities.

As time passes the information becomes disjointed, the meaning for which it was collected is nonexistent, records are forgotten and files are lost.

This significant group of uncontrolled information is escalating and is referred to as ‘dark data’.

Dark data can include confidential, personal or sensitive information and presents a challenge for security, privacy and compliance.

Digital Footprints

Governments and the enterprise collect an inordinate amount of information from citizens and customers in the delivery of their products and services.

When delivering these services governments and the enterprise create ‘digital footprints’.

A digital footprint is the 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 enterprise information and unintentionally expose personal information.

Digital Shadows

Citizens and customers as consumers of 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.

A digital shadow, is a subset of a digital footprint. Digital shadows 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.

Enter the Malicious Insider - The Spy Within

The malicious insider is the ‘spy’ or ‘traitor’ who represents an inside cyber threat. This ‘spy’ or ‘traitor’ can be a person within the organisation, external to the organisation or an internet bot also known as web robot.

The malicious insider has access to the enterprise network from inside the perimeter barricades.

Malicious insiders are like a rogue administrator who can access your sensitive data, steal information, steal private details and perform any number of other malicious activities.

Cyber Security

Cyber security 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.

Risk Management, Governance and Compliance

Effective risk management, governance and compliance are enablers to ensuring that the security framework of people, policies and technology are consistent and measurable across the entire enterprise.

A component of your security framework should include a data breach plan. The data breach plan should identify the key responsible personnel and who should be notified in the event of a data breach.

The data breach plan should also include risk mitigation processes and set out the procedures for identifying how to respond to the data breach.

Data Breach Plan – Responding to Data Breach

The data breach plan should consider the following:

- How to contain the data breach
- Evaluate the associated risks
- Consider if you need to notify affected individual(s)
- Consider if you need to notify appropriate statutory bodies or other impacted organisations
- Put in place preventative actions for example preventing a repeat by documenting lessons learnt

Data Breach Plan - Evaluate Risk

To determine what other steps might be needed, you should identify the type of data involved in the breach and assess the risks associated with the breach. Factors to consider could include:

- What type of data is involved?
- Who is affected by the breach?
- What was the cause of the breach?
- What is the foreseeable harm to the organisation if the data breach was the theft of company sensitive information?
- What is the foreseeable harm to the affected individual(s) if the data breach was the theft of personal information?

Data Breach Plan – Preventative Actions

Produce a data breach report and include recommendations on how to prevent any further reoccurrence. Your data breach report might include the following preventative activities:

- Undertaking a security audit of both physical and technical security measures and controls
- Reviewing data protection, governance policies and any other policies and procedures that cover storing, protecting, security and privacy of data including the handling of personal data.
- Reviewing employee training procedures and practices
- Reviewing contractual obligations especially data protection clauses with contracted service providers and contractors.

THE END

ANY QUESTIONS?