Australia's new mandatory data breach notification laws – Are you protected?

Effective 22 February 2018, all organisations with an annual turnover of $3 million are required to notify the Australian Information Commissioner and affected individuals after an eligible data breach.

Approximately 90% of ASX listed companies have experienced a breach of some kind. Each data breach puts businesses, their clients, and directors at risk. "Being aware of your data, and how to protect it, is the first step to ensure you are protected from potential data breaches" says Citadel's Cindy Schwartz.

What is a data breach? A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.

More than 700 private sector companies of national interest were affected last year and the Australian Government estimates that cybercrime costs the national economy up to $17 billion a year. For companies it is no longer a matter of if their information is compromised, but when.

Identifying at-risk-data: *Aiming to minimise data*

An audit of current data and the systems, software and assets where it is stored will help mitigate against attacks. Minimising the amount of data collected is important, and consideration is needed to determine if you need the data to carry out your business operations.

There are a number of common causes for data breaches:

- **System breaches** due to weak credentials
- **Poorly written or designed systems** enabling easy access to external parties
- **Malicious software** which allows easy access for hackers
- **Insider threats** including lack of internal controls
- **Complex access permissions** that are out of date or incorrect, allowing easy access for outsiders

Protecting your systems: *Requirements for security*

Protecting your systems and assets is key.

Laptop theft is amongst the highest causes of data breaches. A good encryption policy that is enforced on employee laptops will deter malicious activity in the event of a lost or stolen laptop.

Downloads can exploit your machine and malicious websites aren't as obvious as they used to be. Websites can look completely harmless and exploit your machine when you download software or information. Being able to block websites is key to solving this threat.

Data backup files are also the cause of many breaches and physical files can be easily compromised. A remote data backup service allows data to be securely protected online without using physical items that can be lost or stolen.

Patching is often not done comprehensively enough. IT teams often turn on the Microsoft updates and believe everything is protected. Other operating systems are also affected, including third-party applications that are not patched by Microsoft, such as Adobe.

The effects of a breach:
Penalties and public shaming

Cyber breaches become very public, very quickly. There are two classes of penalties – legal and public shaming. The legal penalties include a public investigation that may result in civil penalties of over $2 million.

Public shaming consequences are much more damaging to a business, including reputational damage, losing business to your competitors and most importantly, losing your clients' trust.

December 2017 – President Communications and Red Cross Blood Service

'President Communications, the contractor behind Australia's biggest-ever data breach, has been liquidated. It was revealed in October 2016 that the personal records of 550,000 donors to the Red Cross Blood Service were exposed online, including names, gender, physical and email addresses, phone numbers, dates of birth, and countries of birth.' Source: CRN

December 2017 – PayPal's TIO Networks

'PayPal Holdings acknowledged that a data breach at recently acquired payments processor TIO Networks compromised the personally identifiable information of roughly 1.6 million customers.' Source: SC Media

Detection and prevention:
Regular health checks

Many organisations do not perform regular health checks including vulnerability assessments, which need to be undertaken weekly. Today, organisations should perform vulnerability scans against every system in their network, both internal and external.

Intrusion detection and prevention should be used for all mission-critical systems and systems that are accessible through the Internet, such as web servers, email systems, servers that contain client or employee data, active directory servers and other systems that are deemed mission critical.

System monitoring should also be performed by the HR or compliance team to track employee or insider behaviour. This is invaluable to predict and prevent data attacks. Data loss prevention technology can set rules on specific data types and systems, where you can block content that you do not want to leave the network.

Protecting your business:
Minimum standards checklist

- ✓ Do you have appropriate security measures in place both internally and externally to ensure all access to data is appropriate?
- ✓ Do you have appropriate procedures in place to ensure that each data item is kept up-to-date?
- ✓ Do you have a defined policy on retention periods for all items of personal data?
- ✓ Do you have a data protection policy in place?
- ✓ Do you have procedures for handling access requests from individuals?
- ✓ Are your staff appropriately trained in data protection?
- ✓ Do you regularly review and audit the data which you hold and the way they are processed?

Data security insights:
A unique perspective

Citadel believes it should be standard practice to develop and implement a Cyber and Data prevention and recovery plan, in addition to their disaster recovery plans. "Dedicating time and resources into developing a plan that covers access control, data security, encryption, prevention of data loss and compromise, incident management and recovery, is crucial." says Schwartz.

Putting in time upfront to implement data protection safeguards is more beneficial to a business than dealing with the fall out of a data breach, which has a tremendous impact in terms of cost, resources and trust from the public. Reputational risk from data breaches cannot be understated.