



Corporate and Government executives as well as company directors face unprecedented challenges living up to their responsibilities in an era of aggressive state actors, unrestrained cybercriminals and widespread information warfare. It is expensive to lose customers, trust is hard to build, easy to lose and too often based upon a complicated web of customer and vendor relationships and interdependencies. The effects of a cyber attack can be permanent and devastating.

Constantly Growing Threat

Over the period 1 July 2019 to 30 June 2020 the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) responded to 2,266 cyber security incidents and received 59,806 cybercrime reports at an average of 164 reports per day, or one every 10 minutes. Cybercrime in Australia is the most significant threat in terms of overall volume and impact to individuals and businesses. The ACCC's Targeting Scams 2019 report, identified that Australians lost over \$634 million to scams in 2019. While the true cost of cybercrime to the Australian economy is difficult to quantify, industry estimates have previously placed the cost of cyber security incidents as high as \$29 billion annually.

Throughout the pandemic, there was an increase in reported spear phishing campaigns and an increase of COVID-19

themed malicious cyber activity. Between 10 and 26 March 2020, the ACSC received over 45 pandemic themed cybercrime and cyber security incident reports, with the ACCC's Scamwatch receiving over 100 reports of COVID-19 themed scams. During March 2020, cybercriminals quickly adapted their phishing methods to take advantage of the COVID-19 pandemic.

According to the latest Australian Information Commissioner (OAIC Report, Jan 2021), the health sector remains the highest reporting industry sector, notifying 23% of all breaches, followed by finance, which notified 15% of all breaches.

OAIC received 538 breach notifications during this reporting period, an increase of 5% over the previous 6 months, and 1,051 notifications for the 2020 year. Data breaches resulting from human error accounted for 38% of notifications, an increase of 18%.

Top 5 industry sectors by notifications

Industry Sector	Total No. of Notifications
▪ Health Service Providers	123
▪ Finance (incl superannuation)	80
▪ Education	40
▪ Legal, accounting & management services	38
▪ Australian Government	33

Ref: OAIC Notifiable Breaches Report, July - Dec 2020

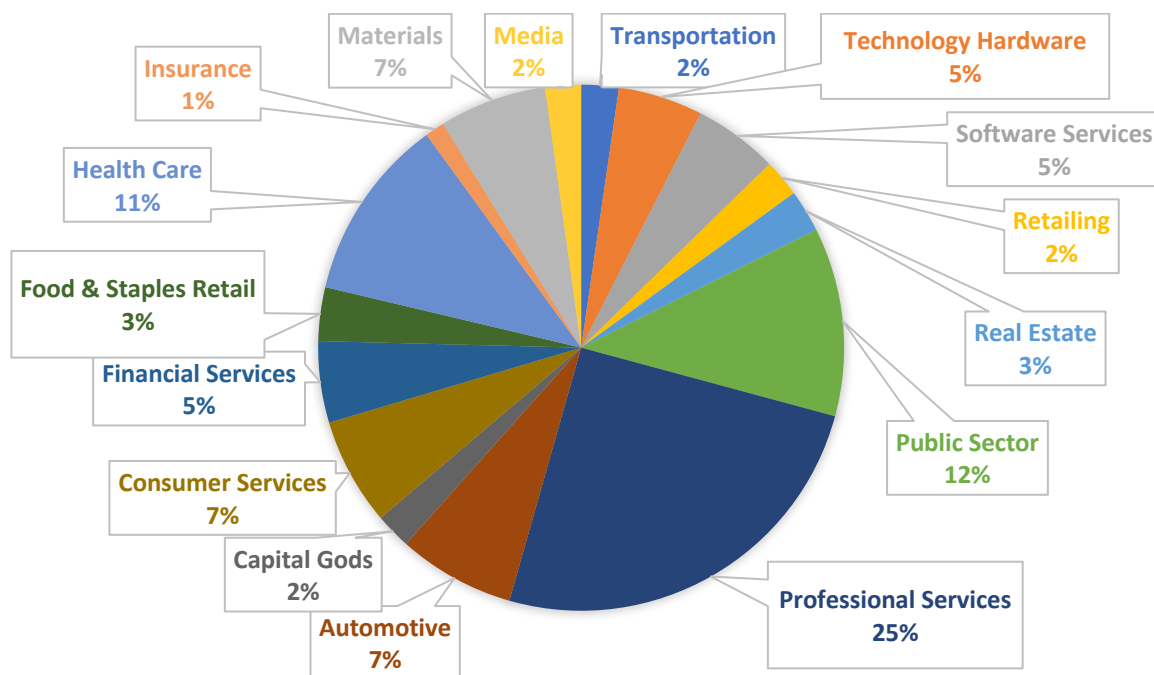
Health service providers have consistently reported the most data breaches compared to other industry sectors since

the Notifiable Data Breach (NDB) scheme began. Healthcare databases are heavily targeted by cybercriminals as they hold valuable and sensitive information such as medical histories, personal and financial data and more. Examples include the recent attack on Regis Aged Care in South Australia, targeted attacks on Victorian hospitals and health databases, as well as the WannaCry attack on the UK’s National Health System.

Ransomware

A recent survey conducted by CrowdStrike found that Australia is one of the world’s hottest targets for ransomware attacks, with 67% of respondents admitting that their organisation had suffered an attack in 2020.

Common Industries Targeted by Ransomware in Q3 2020



Ref: OAIC Dec 2020

Cybercrime-as-a-service is now offered in criminal marketplaces

Australian businesses are very attractive and profitable to cybercriminals because of our relative wealth, high levels of online connectivity and increasing delivery of services through online channels. Cybercrime-as-a-service (CaaS), or access to high-end hacking tools that were once only available to governments are now offered in criminal marketplaces. These marketplaces also offer less technical but equally valuable cybercrime enablers for personal information and other sensitive data such as compromised user credentials. Powerful cyber technology and tools, services and data can be purchased and used with minimal technical expertise to generate illegal income streams, launder the proceeds of cybercrimes and traditional crimes, or undertake network intrusions for other reasons.

Interconnectedness of Business - A Strength and Our Vulnerability

The occurrence and severity of cyber-attacks is also increasing due to our interconnected devices and systems and growing dependence on new information technology platforms. The increased use of consumer IoT devices such as internet-enabled home assistants, TVs, fridges, baby monitors and home security systems has created more vulnerabilities in networks. Insecure or misconfigured systems create opportunities for cybercriminals to compromise networks,

access company data, steal information and damage systems and businesses.

Cybersecurity is a major business risk. Online crime is growing exponentially in its frequency, scale and sophistication, and your ability as an executive or company director to manage and minimise those risks is not just critical to the success of your business but also a legal and regulatory requirement.

Legal Accountability of Boards and Senior Management

There is increased pressure on boards and senior management to demonstrate an accurate assessment of cyber risk and increased regulatory oversight. Compliance with any regulation does not equate to appropriate data protection. Nor does the amount you spend reflect your level of security. You cannot delegate this responsibility to others-you can't pass the buck. Even the most effective IT team can't manage the unfortunate reality that more than one in three cybersecurity events are the result of human error.

“There is increased pressure on boards and senior management to demonstrate an accurate assessment of cyber risk and increased regulatory oversight.”

We anticipate that voluntary guidelines issued by the ACSC – including recommendations for businesses to adopt data encryption, comprehensive firewalls, unique pass phrases, multi-factor

DATA PROTECTION IN THE NEW WORLD OF CORPORATE RESPONSIBILITY

authentication and secondary and tertiary control rooms will soon apply on a mandatory basis. It is likely that standalone cybersecurity legislation may be introduced giving the ASC, ASCS or a new regulatory body greater oversight and enforcement powers.

Gartner predicts 40% of boards will have a dedicated cybersecurity committee by 2025.

Behaviour, Processes, Technology and Governance

Businesses with sound data security and data resilience have the following elements well understood and well managed around areas of data vulnerabilities:

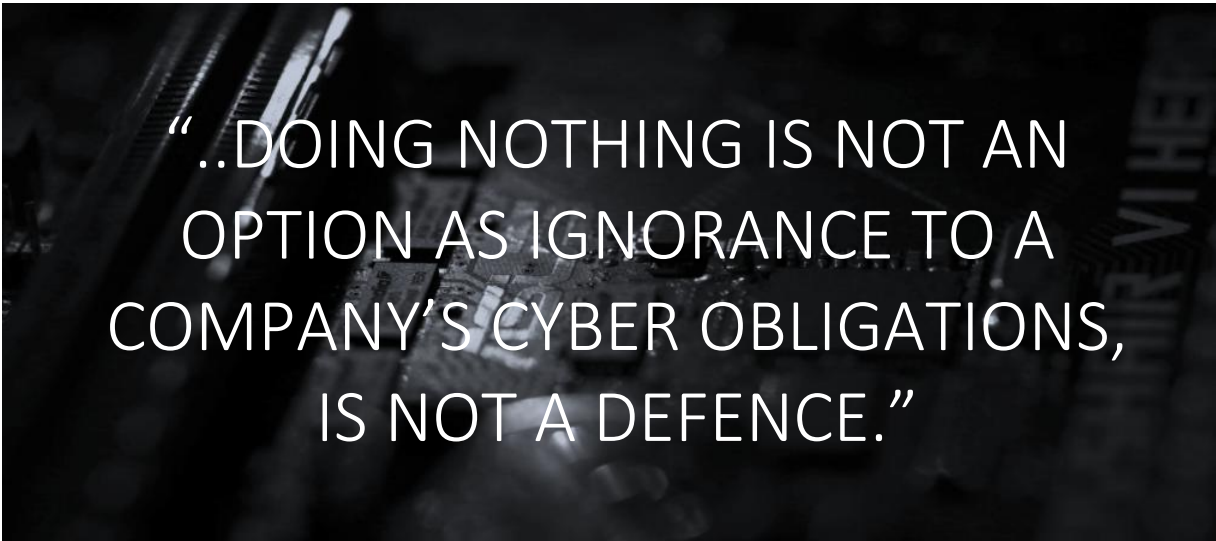
- Behaviour within the organisation;
- Processes touching data;
- Technology & tools; and
- Governance.

The application of processes, risk management principles, ongoing training and education are vital. This is why all

companies need to invest in both data security and data resilience. Security capabilities are a function of people, process and technology. However, leading with technology results in poor cybersecurity and business outcomes. A holistic and proactive approach is needed towards data security and data resilience.

The data security strategy is designed to minimise the risk of attacks getting through. But when they inevitably do, the data resilience strategy is there to minimise the impact.

Organisations have compliance, regulatory and legal responsibilities to adequately address cyber security issues. Clearly there needs to be an appropriate separation between board and executive responsibilities however doing nothing is not an option as ignorance to a company's cyber obligations, is not a defence. A failure by directors and officers to identify, protect against, respond to, and recover from cyber risks may constitute a breach of directors' duties.



“..DOING NOTHING IS NOT AN OPTION AS IGNORANCE TO A COMPANY'S CYBER OBLIGATIONS, IS NOT A DEFENCE.”

Radmis brings to clients more than 100 years of experience in data protection & data resilience with expertise in:

- Technology behavioural change
- Risk focussed process excellence
- Computer system security & innovation
- GRC and regulation

This is delivered in a seamless, no nonsense approach to increasing data protection to minimise the risk of attack, and data resilience to respond to, and recover from an attack when it inevitably happens.

Sectors include: **Health | Professional Services | Financial Services | Telecommunications | Government | Extractive Industries**

If required, Radmis also assists in AI strategy & implementation, data analysis & management, and IT cost reduction.

The threat landscape continues to evolve...

To find out more, contact us.



Penny: penny.wong@radmisadvisory.com

Mark: mark.taylor@radmisadvisory.com

Colin: colin.hickling@radmisadvisory.com

www.radmisadvisory.com