Ignorance is Risk

Australia SME Cyber Preparedness Report 2019

CHUBB®

Contents

Welcome

Mr John DePeters
Cyber & Technology Industry
Practice Leader,
Chubb Australia & New Zealand

Following the positive feedback from Chubb's inaugural SME Cyber Preparedness Report for Australia in 2018, we are delighted to bring you the second edition of this report.

As one of the world's largest and longest-serving cyber insurers, we believe this report is important for raising awareness about the issues that small and medium-sized enterprises (SMEs) face in managing cyber risk. In the coming years, cyber risk is forecast to substantially cost businesses globally in lost revenue.

Last year we suggested that SME in the region were the "low hanging fruit" for threat actors. Though this year's statistics are no different, the story takes a different turn with many SMEs unaware of their regulatory obligations. Do SMEs think they are above the law?

In Australia, less than one third (31%) of Australian SMEs are aware of their obligations under the Notifiable Data Breaches (NDB) scheme and just under half (47%) say they are not aware. These trends are worrying and will only be amplified as the digital economy grows.

With SMEs making up 96% of all businesses in Australia, they will be hardest hit by cyber incidents without good risk mitigation, incident response planning and the consideration of cyber insurance.

We hope that you will find this report useful so that the insights can contribute towards reducing cyber risk for SMEs in Australia.

Ignorance is Risk

Cyber Risk Landscape

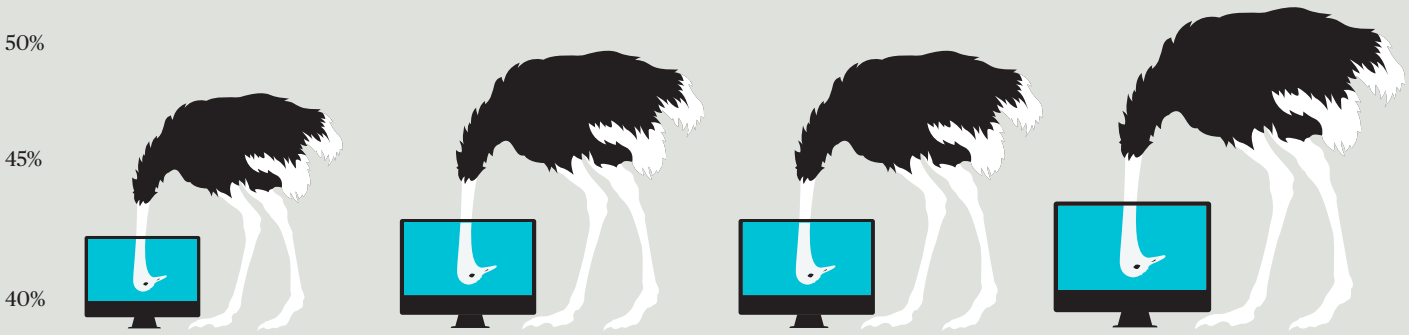
Amid rapid digitalisation, 516,380 cyber-attacks occurred in Australia in 2018 costing companies an average of US$1.9 million[1].

The Australian government has responded to the increasing cyber threats with the introduction of the Notifiable Data Breaches (NDB) scheme[2].

Digital Economy

The rapidly expanding digital economy in Australia will be worth US$315 billion in the next decade[3].

Key Survey Highlights



47%

of Australian SMEs are not aware of their obligations under the NDB scheme.

49%

of Australian SMEs were victims of cyber incidents in the past year.

49%

of Australian SMEs do not have a data breach response plan in place.

50%

of Australian SMEs have never been covered by cyber risk insurance.

[1] https://www.smartcompany.com.au/technology/from-millions-to-malware-cyber-attacks-in-australia-by-the-numbers/

[2] https://www.oaic.gov.au/privacy/notifiable-data-breaches/

[3] https://www.industry.gov.au/sites/default/files/2018-12/australias-tech-future.pdf

Blind to the Rules

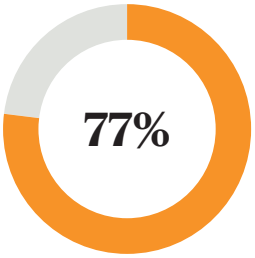
In February 2018, the Office of the Australian Information Commissioner (OAIC) introduced regulations making it mandatory for any organisation or agency covered by the Privacy Act of 1988 to report a data breach that is "likely to result in serious harm to an individual whose personal information is involved".

While larger companies seem to understand their obligations, SMEs may have missed the memo. Less than one third (31%) of Australian SMEs are aware of their obligations under the Notifiable Data Breaches (NDB) scheme and just under half (47%) say they are not aware. One in five (21%) of those surveyed say they did not fall under the scheme.

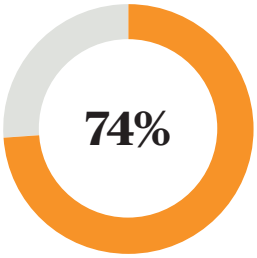
This is cause for concern. The NDB scheme received 967 breach notifications between 1 July 2018 through to 30 June 2019 and and it is highly likely there were many more breaches that have gone - and continue to go - unreported.

Understanding precisely what type of data breaches require notification remains patchy, even among those who said they were aware of their obligations.

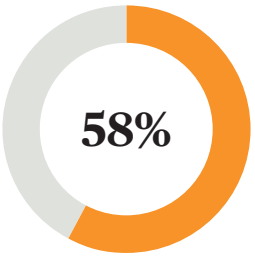
SMEs responses on their understanding of the type of data breaches requiring notification



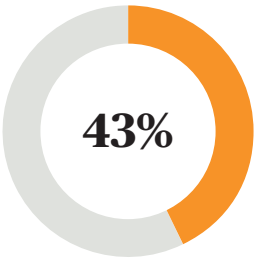
A database containing personal information is hacked



A device containing customers' personal information is lost or stolen



Personal information is mistakenly provided to the wrong person



An employee browsing sensitive customer records without any legitimate purpose

More broadly, only 50% of Australian SMEs are aware of their broader obligations to the OAIC regarding the reporting of cyber incidents and data breaches.

[4] https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Completed_inquiries/pre1996/q_balance/report/b01

[5] https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/

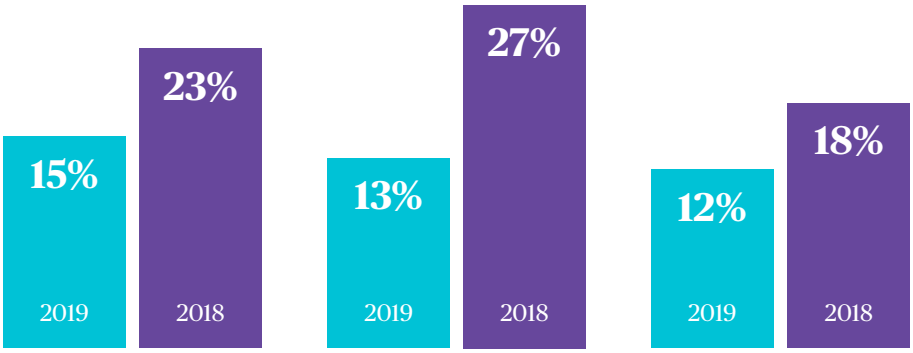
Is your business covered by the NDB scheme[5]?

- 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 A$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 particular types of information only (for example, small businesses that are required to secure tax file number information) do not need to notify data breaches that affect other types of information outside the scope of their obligations under the Privacy Act.

The Tide is Shifting

Despite Australia's increased regulatory obligations, the most common incidents Australian SMEs faced in the past 12 months were phishing compromises (21%), data loss (15%) and business interruption as a result of system malfunctions or technical faults (13%). There are some indications that the regulations are having - or starting to have - an impact on overall attitudes towards data protection:

Most common types of cyber incidents experienced in 2019 vs 2018



Data loss through system malfunction, technical fault

Business interruption from system malfunction, technical fault

Human error

Understanding of cyber risk has improved among SMEs

Cyber risk is becoming a shared problem. Fewer leaders (44%) see cyber risk as an "IT Problem" compared with 2018 (53%), and more leaders agree that there is good cross-department collaboration (45%).

Third-party liability is better understood. In 2018, 60% of leaders did not think they were fully aware of the potential exposure to third-party liability/consequences in relation to cyber risk. In 2019, this has fallen to 48%.

There is better understanding of cyber risk among employees. Fewer leaders (31%) feel that their employees do not recognise how serious the threat of cyber risk is to their business. Down from 45% in 2018.

However, there is still a long way to go. Close to half (49%) of SMEs do not have a data breach response plan yet, while 79% are confident they can overcome a breach by sophisticated hackers within 24-hours.

Case Study: Ransomware

Industry:
Construction

Annual revenue:
A$5 million

Costs over:
A$500,000

A construction related company suffered a ransomware attack that affected most of the Insured's key data. This included hard drives that contained the company's back-ups. The Insured was not able to successfully engage with the extortionist and had to manually re-enter lost data.

After the broker contacted the Chubb cyber claims staff directly, we engaged an incident response team to manage the event. First party insuring clauses were triggered initially with the Cyber Extortion insuring clause, the most clearly applicable policy response section, as well as Incident Response Expenses and Recovery Costs. Forensic IT experts were required to assist to understand the data affected and assess the ability to restore back-up files. The business income of the Insured was impacted as the lack of the IT system impeded the Insured's operations. This loss of net profit triggered Recovery Costs and Business Income Loss under Cyber Enterprise Risk Management (ERM).

The impact to the Insured was significant as they were unable to trade or obtain new business during the three month indemnity period. After the engagement of IT Forensics and legal experts, we were able to work with the Insured and our loss adjuster to calculate the financial impact suffered during the three month indemnity period.

Overconfidence Persists

In our 2018 survey, 64% of respondents said they had been the victim of a cyber incident. In 2019, this dropped to 49%.

Fewer incidents seem to have led to a significant increase in confidence amongst SMEs when it comes to their cyber risk preparedness. So much so, that one in three (32%) of senior leaders expect their business to be immune to cyber attacks. This confidence extends beyond the likelihood of a cyber breach. Of the locations covered by this research i.e. Malaysia, Hong Kong SAR and Singapore, Australian SMEs were consistently the least worried about the potential impact of a cyber incident on their business, customers and partners.

What impact, if any, would you expect a cyber incident to have on the following aspects of your business?

Moderate-Severe Impact	2019	2018
Reputation in the market	33%	47%
Relationship with customers	38%	51%
Revenue/sales	40%	50%
Company profits	40%	51%
Relationship with regulators	28%	42%
Ability to employ or retain staff	21%	32%
Direct expenses incurred	38%	51%

Case Study: Credential Stuffing

Industry:
Retail

Annual revenue:
A$250 - 350 million

Costs over:
A$ 700,000 and ongoing

The company, which operates physical stores and an on-line payment gateway to sell its merchandise experienced credential stuffing affecting tens of thousands of customers.

Credential stuffing is a type of cyber attack where stolen account credentials typically consisting of lists of usernames and/or email addresses and the corresponding passwords (often from a separate data breach or purchased on the dark web) are used to gain unauthorised access to user accounts through large-scale automated login requests directed against a web application. Credential stuffing attacks are made possible because many users will reuse the same password across many sites.

When the company informed Chubb, we immediately helped it to inform the appropriate external parties, supported a forensic investigation on three continents, guided them through their legal and regulatory response and set up call centre ID monitoring and crisis communications.

She'll Be Right

Perhaps unsurprisingly, few Australian SMEs are looking at ways to improve their overall cyber risk management strategies. Only 43% of SMEs in Australia are investing in the training of employees to improve their overall cyber risk management.

In addition, only a mere 20% adopt internationally recognised standards for cyber risk management and only 15% think that greater investment in insurance solutions is required to manage cyber risk.

Few SMEs are investing in measures to improve overall cyber risk management

Australia	2019	2018
Better training for all employees	43%	43%
Investment in better security software to protect systems	30%	38%
Regular monitoring of staff behaviour to check standards are upheld	29%	29%
Clearer communication from management to employees about the importance of cyber risk management	28%	31%
Better understanding of data assets, through categorisation/ classification etc.	24%	29%
Adoption of internationally recognised standards (e.g. ISO 27001)	20%	19%
Better cross-departmental working and sharing of best practice	17%	19%
Not applicable - my organisation does not need to improve its overall cyber risk strategy	17%	17%
Greater investment in insurance solutions	15%	17%
Don't know	9%	7%
Other	2%	-

Australian SMEs doubled down when asked what the weakest link in their cyber defences were, with 1 in 5 (21%) saying "there is no weak link". 14% said they didn't know, with employees (19%), security software (13%) and monitoring of the security software (11%) rounding out the top five weakest links.

Dwelling on the Downside

Persistent threats can last inside SME networks for years. Dwell time – the amount of time a threat spends inside a network before an organisation discovers and removes it – has become a significant problem for SMEs, according to a U.S. report released by Infocyte in July 2019. Dwell time for attacks with ransomware averaged 43 days - and rose to 798 days for all other persistent threats (non-ransomware). Alarmingly, dwell time for riskware - defined as unwanted applications, web trackers, and adware - averaged a whopping 869 days.

The report stated that 72% of SMEs had riskware and unwanted applications in their networks that took longer than 90 days to remove. While they were generally lower risk issues, the bigger takeaway is networks that fail to control riskware typically have a lower readiness to respond to high-priority threats when they are uncovered.

The report advises that if continuous monitoring is not an option, SMEs should at the very least bring in a third party to perform a compromise assessment.

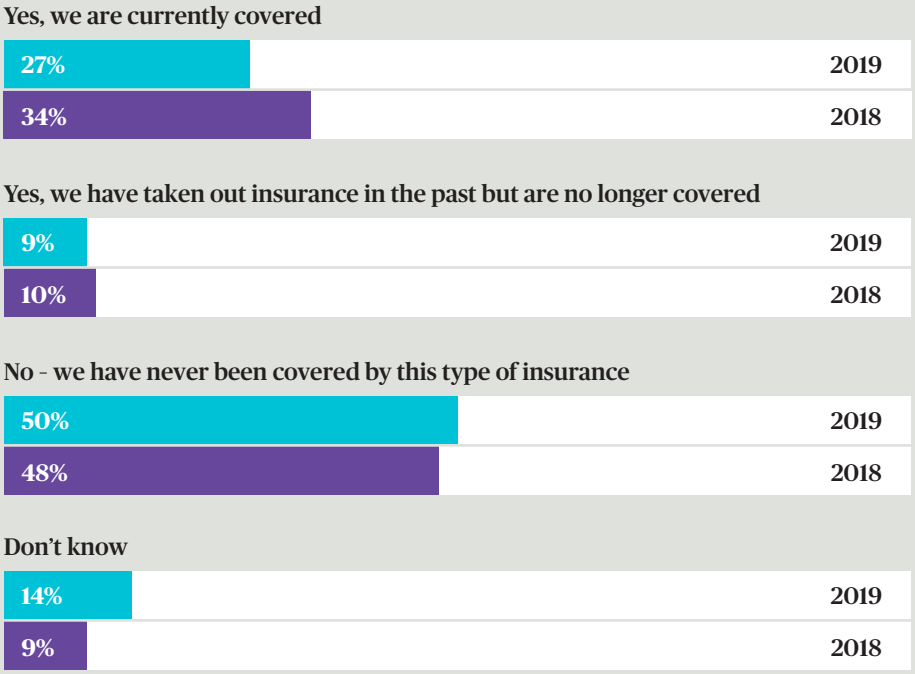
Reducing the Risk with Insurance

Currently, only one quarter (27%) of SMEs have cyber risk insurance (a similar figure to 2018), while half (50%) have never been covered. Nearly one in ten (9%) have let their cover lapse while a further 14% weren't sure if they have cover or not.

Half (49%) of SMEs did not purchase insurance either before or after an incident - still a high number, but an improvement on the 62% from 2018.

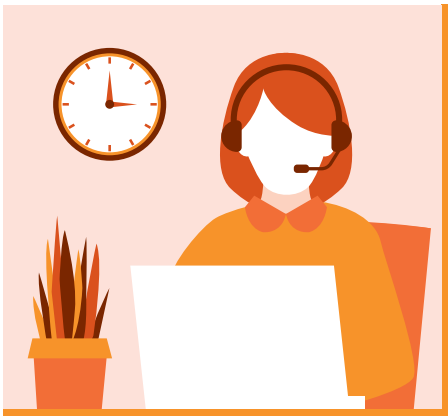
Despite this, 50% of those surveyed feel that insurance has an important role to play in helping SMEs manage cyber risk. Assistance from insurers was most appreciated by SMEs in the areas of speed of incident response (53%) and regulatory response (49%).

Australian SMEs With Cyber Risk Insurance



Loss Mitigation Services

Some important loss mitigation services which are available to all of Chubb's cyber insurance customers include:



Incident Response Platform

Chubb offers customers an Incident Response Platform to help contain cyber threats and limit potential damage. It includes an on-call crisis response hotline available 24/7/365 days; supported by contractual service level agreements. Response within one hour from an incident manager and coordinated management of a team of experts to assist, manage and mitigate a wide array of cyber incident scenarios, including denial of service attacks, ransomware, cyber crime and employee error; and post-incident reporting. In the past 12 months, Chubb's average initial incident response time for customers in Asia Pacific was 12 minutes.

Phishing Assessments

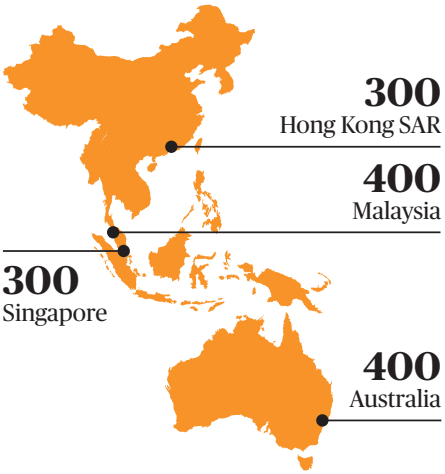
Chubb works with cyber phishing experts to offer phishing awareness assessments. The assessments include two simulated real-life phishing scenarios that are conducted over the course of four months for up to 500 individual email addresses.

Complimentary Password Management

Remembering passwords is difficult. Companies can choose to use an all-in-one solution that remembers and automatically fills in user passwords and logins. With a secure sharing feature, colleagues can even share logins without ever seeing each other's passwords. Dark web monitoring can also help to scan the web and alert users immediately if their personal information is ever found where it doesn't belong online.

About the Research

This report is based on a survey of 1,400 respondents from Small and Medium Enterprises (SMEs) in four locations;



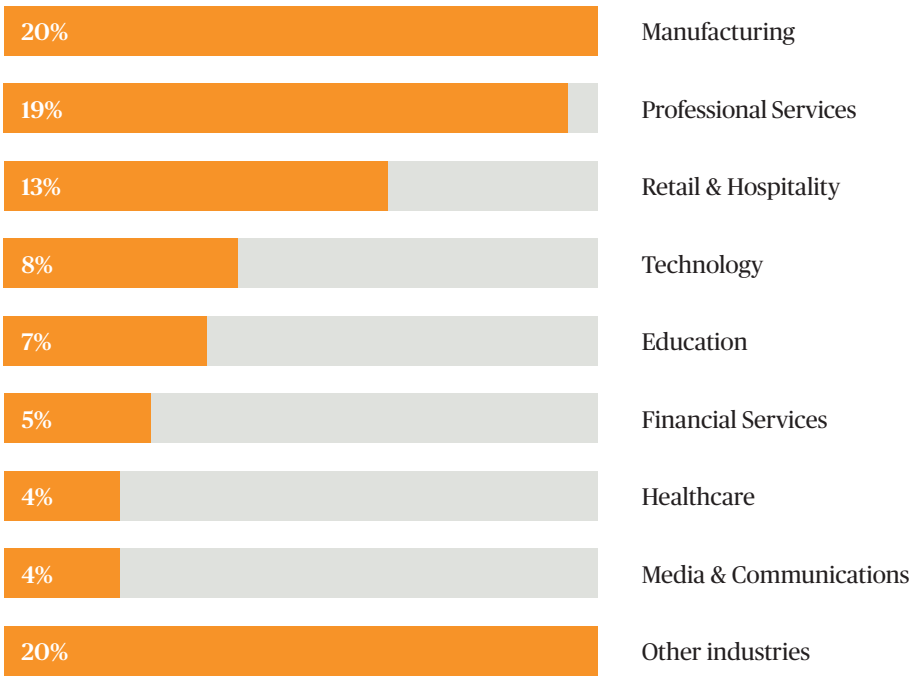
Respondents comprised of;

82%
Board-level executive

18%
Senior managers or directors below board level

from SMEs between 2 and 249 employees.

The industries respondents belonged to are:



Practical steps SMEs can take to protect their business:

Develop and enforce a written password policy - Your employees will not thank you for forcing them to make passwords difficult to remember, but that's the point. Make them complicated (letters, numbers and symbols) and change them regularly. Disable access once employees leave the business.

Create a Cyber Incident Response Plan - 40% of Australian SMEs admitted their current plan is ad hoc and not documented. Of those that do have a plan in place, only 35% test it regularly. We recommend preparing a cyber incident response plan with the help of a cyber expert and conduct simulated tests on your plan regularly.

Educate employees regularly on cyber security vigilance - It only takes one click on a malicious link to open a business up to a phishing or ransomware attack. Similarly, it only takes one call from "IT Support" to reveal passwords to cyber criminals.

Update IT equipment and deploy security software - Unpatched machines are much easier to access remotely, particularly if employees have elevated admin levels that they don't really need.

About Chubb

Chubb is the world's largest publicly traded property and casualty insurer. Chubb, via acquisitions by its predecessor companies, has been present in Australia for 100 years. Its operation in Australia (Chubb Insurance Australia Limited) provides specialised and customised coverages including Business Package, Marine, Property, Liability, Energy, Professional Indemnity, Directors & Officers, Financial Lines, Utilities as well as Accident & Health, to a broad client base, including many of the country's largest companies. Chubb also serves successful individuals with substantial assets to protect, and individuals purchasing travel and personal accident insurance.

Contact Us

Chubb Insurance Australia Limited
ABN: 23 001 642 020 AFSL: 239687

Grosvenor Place Level 38
225 George Street
Sydney NSW 2000

O +61 2 9335 3200
F +61 2 9335 3411

www.chubb.com/au

Chubb. Insured.[SM]

Important Notes:

All content in this material is for general information purposes only. It does not constitute personal advice or a recommendation to any individual or business of any product or service.

Please refer to the policy documentation issued for full terms and conditions of coverage.

Coverage are underwritten by one or more Chubb companies. Not all coverages are available in all countries and territories. Coverages are subject to licensing requirements and sanctions restrictions. This document is neither an offer nor a solicitation of insurance or reinsurance products.

Chubb10-625-1019