Too Small to Fail?

Australia SME Cyber Preparedness Report

CHUBB®

Contents

Introduction

Cyber risk - an international threat

There has never been a time when companies and organisations have been more at risk of having their data made public or stolen, be it through a deliberate cyber attack from an external or internal party, or as a result of system or human error.

The Australian Bureau of Statistics defines a small business (in the non-agricultural sector) as one which employs less than 20 people in the non-manufacturing industries, and less than 100 employees in the manufacturing industries. According to the Australian Bureau of Statistics, small businesses account for about 860,000 (96%) of all businesses in Australia and employ around 3 million out of 5.5 million people employed in the private sector[1].

Clearly, Small and Medium Enterprises (SMEs) are a hugely important part of the economy. They are deeply interconnected with consumers and with organisations of all sizes, making their ability to protect themselves from cyber risks essential.

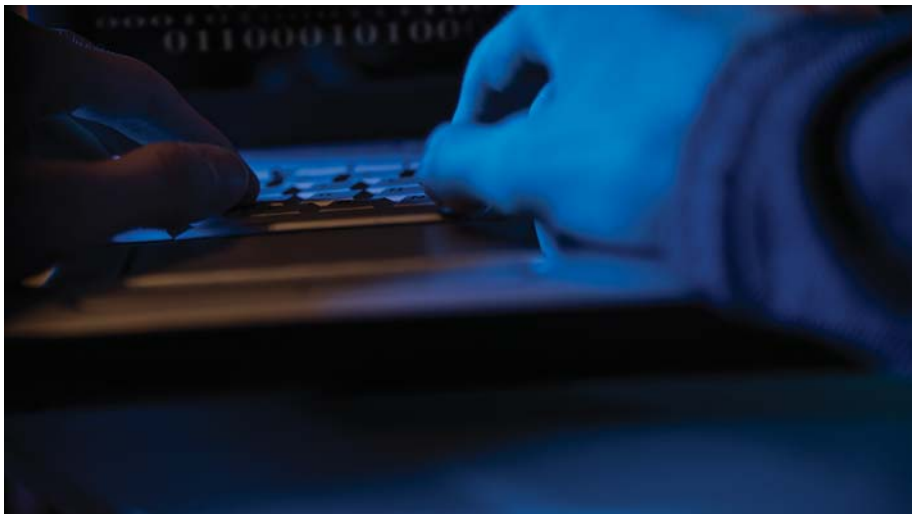
In August and September 2018, the world's largest publicly traded property and casualty insurer Chubb, partnered with YouGov to conduct a survey among 400 SMEs in Australia to gauge their attitude to cyber risks. We specifically wanted to know how vulnerable they believe they are; how they protect themselves and prepare for potential risks; and, if exposed, how they react.

The results of our survey reveal a significant gap between the hard reality of cyber risk and how well small companies are prepared to deal with it.

Chart 1: SMEs in Australia:

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

Digital disasters



2017 saw two major global cyber events that affected many industries across multiple countries. These events pushed cyber resilience up the agenda of governments and corporations alike.

In May, the WannaCry virus struck first in Europe before spreading across the globe. The virus was indiscriminate. It crippled SMEs as well as major companies, infecting more than 300,000 systems across 150 countries in a matter of days. This was followed by the more sinister malware, NotPetya, that brought several U.S. government departments and major companies to a halt, costing billions of dollars in damage and lost revenue. These attacks highlighted our unpreparedness to deal with cyber incidents, and our dependency on technology to conduct commerce.

However, it is not just data breaches, but data exposure which organisations need to heed - when data is stored and defended improperly, it can be accessed by anyone with even basic skills.

Australian universities and other critical infrastructure, including hospitals, were in the headlines in 2018 after an attack by overseas agencies and nation states. The 33 universities were targeted by a 'spear phishing' campaign as part of a sophisticated attempt to steal intellectual property and academic research[2].

The Office of the Australian Information Commissioner reports on its website a record of how many Australian businesses are allowing customers' private information to be made public. This serves as a warning and deterrence for both businesses and their customers.

[2] *https://www.smh.com.au/education/australian-universities-targets-of-iran-hack-campaign-says-fbi-20180329-p4z6ts.html*

Are larger companies more vulnerable to cyber risk? Hint: No

With the news headlines focusing on incidents taking place in large corporations and within governments, it could be easy to conclude that smaller companies are relatively incident-free. According to our research, nearly two thirds of respondents in Australia (60%) believe they are in a better position than their larger competitors.

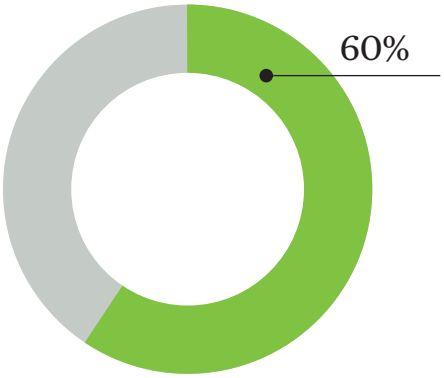
However, nothing could be further from the truth.

Our research shows that the majority of small businesses in Australia (60%) have experienced a cyber incident in the past 12 months.

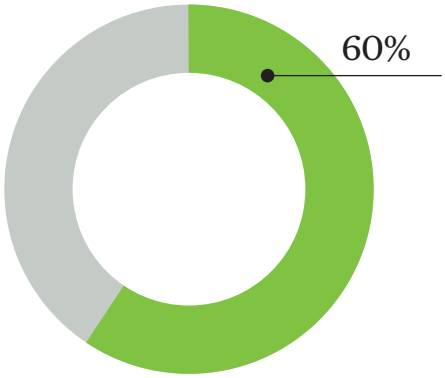
In fact, smaller companies face a far bigger risk exposure. Large businesses spend enormous sums of money on corporate cyber security to institute sophisticated defences. SMEs face many of the same threats. However, most do not have the means to make anywhere near the investment required to implement comprehensive protection, leaving significant risk uncovered.

As a result, it is becoming increasingly likely that if an SME has a security weakness, it will be targeted sooner rather than later. This is why, for cyber criminals, these businesses are the proverbial "low-hanging fruit". Not only are they easy targets, they also offer a substantial cumulative payoff. In fact, SMEs, with their low or no investment in cyber security measures, are actually the ideal, and consequently the most common, target for online crimes.

Chart 2: Sentiments of SMEs towards cyber risks



Percentage of respondents who believe they are better off than large companies



Percentage of respondents who have experienced a cyber incident in the last 12 months

"Some SMEs believe they are too small to be targeted by cyber criminals or any internal issues will not greatly impact them. In effect, they think they are "too small to fail". However, every report, survey or set of statistics on cyber events tell us that all businesses are exposed, whether big or small. "

Andrew Taylor
Cyber Underwriting Manager, Chubb Asia Pacific

Case Study:
Hackers steal online retailer's data

Retail
Industry

US$200,000
Claim Amount

US$35 million
Annual Revenue

A retail store with a large proportion of products sold via online trading platforms had its website compromised due to weak password management and security surrounding Virtual Private Network (VPN) access to the company's website. This enabled the external hackers to steal personal information from over 1,000 customers and to then conduct further phishing scams against the company's customers.

Police and regulators were required to investigate the company and two customers brought civil litigation against the retail store. First-party costs and forensics costs were incurred to investigate the source of the breach as well as incident response costs to identify and contact the affected customers. Solicitors would have been required to defend the civil litigation.

SMEs score ‘own goals’

While small businesses are hugely at risk from external cyber attacks, our research shows that the majority of data loss incidents actually occur because of system breakdowns or human error.

These findings do not in any way reduce the impact of external attacks but demonstrate that companies need to ensure their houses are in order at the same time as guarding against outside predators.

Three of the top four causes of cyber incidents among the companies we surveyed in the past 12 months were internal factors:

- Business interruption from system malfunction or technical fault 27%
- Data loss through a system malfunction or technical fault 23%
- Business interruption or data loss through human error, such as a lost or stolen memory device or employees unintentionally exposing their company data to risk 18%

Chart 3: Cyber incidents experienced by SMEs in the past 12 months

Incidents	%
Business interruption from system malfunction, technical fault	27%
Business interruption due to reliance on a third party service provider that has suffered downtime	23%
Data loss through system malfunction, technical fault	23%
Business interruption or data loss through human error, such as a lost or stolen memory device or employees unintentionally exposing their company data to risk	18%
Malicious parties disrupting operations	12%
Hackers/cyber criminals stealing or compromising your customer records	12%
A supplier or business partner losing your data or causing it to be compromised	11%
Cyber criminals defrauding your business	11%
Cyber criminals compounding critical operational data and holding it to ransom	11%
Disgruntled employees or other malicious parties leaking compromising company emails or other files	10%
Competitors stealing your Intellectual Property (IP), R&D or other proprietary information	9%
State-sponsored agencies stealing your IP, R&D or other proprietary information	8%
Other notable cyber incident or data breach	3%
Don’t know	3%

“Chubb’s claims data shows clearly that the majority of cyber or data issues have internal causes. Over the past 20 years of underwriting cyber insurance, it’s become clear to me that cyber risk is an enterprise-wide issue, it’s not just about technology. Good cyber mitigation strategies include strong governance processes, vendor management and employee education.”

Andrew Taylor
Cyber Underwriting Manager, Chubb Asia Pacific

Case Study:
Stolen laptop results in invasion of privacy

Energy
Industry

US$325,000
Claim Amount

US$20 million
Annual Revenue

An energy company executive's laptop was stolen from a corporate vehicle. The laptop contained significant private customer and employee information. Although the file was encrypted, the overall password protection on the laptop was weak and the PIN for accessing the encrypted information was compromised.

After assessing the information on the laptop with a forensic expert and outside compliance counsel at a cost of US$50,000, the energy company voluntarily notified relevant customers and employees and afforded call centre, monitoring, and restoration services, as appropriate. While the additional first-party cost was US$100,000, the energy company also incurred US$75,000 in expenses responding to a multi-state regulatory investigation.

Ultimately, the company was fined US$100,000 for deviating from its publicly stated privacy policy.

Confidence – or over-confidence – in managing a cyber issue

Our research reveals that the vast majority of SMEs are confident in their ability to overcome a cyber incident. In Australia, 87% of the respondents believe they can overcome a cyber event and more than half (56%) believe they can contain an incident within 12 hours. At the same time, 67% said that an incident made them realise they are more vulnerable than they had previously thought and 72% believe a similar incident is less likely to occur in the future.

This presents us with a dilemma. While we see a high level of confidence among SMEs, the survey also revealed results which seem to contradict this.

Perhaps the reason for these seemingly conflicting results lies in the fact there is disagreement on where the responsibility for cyber risk should rest. Respondents to our survey were divided – 38% believe the Head of IT or the Chief Information Officer should be responsible, while 32% believe this role belongs to the Chief Executive.

Chubb's view is that cyber security is everyone's responsibility, but it should be led by someone who has the authority to effect change.

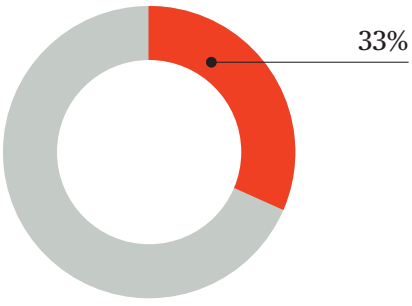
Chart 4: SMEs are generally unaware of the risks they face

***67%** believe they are not aware of all the cyber threats they face.*

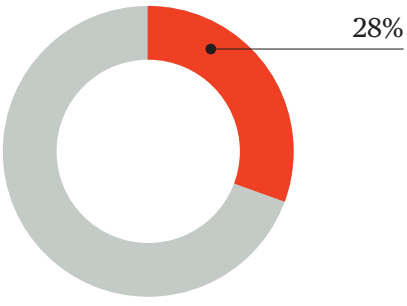
***45%** are not confident that all their employees who have access to sensitive data are fully aware of their data privacy responsibilities.*

***30%** of SMEs who experienced cyber incidents did not know which data files were affected.*

Chart 5: Actions taken by SMEs following a cyber incident



Increased their security

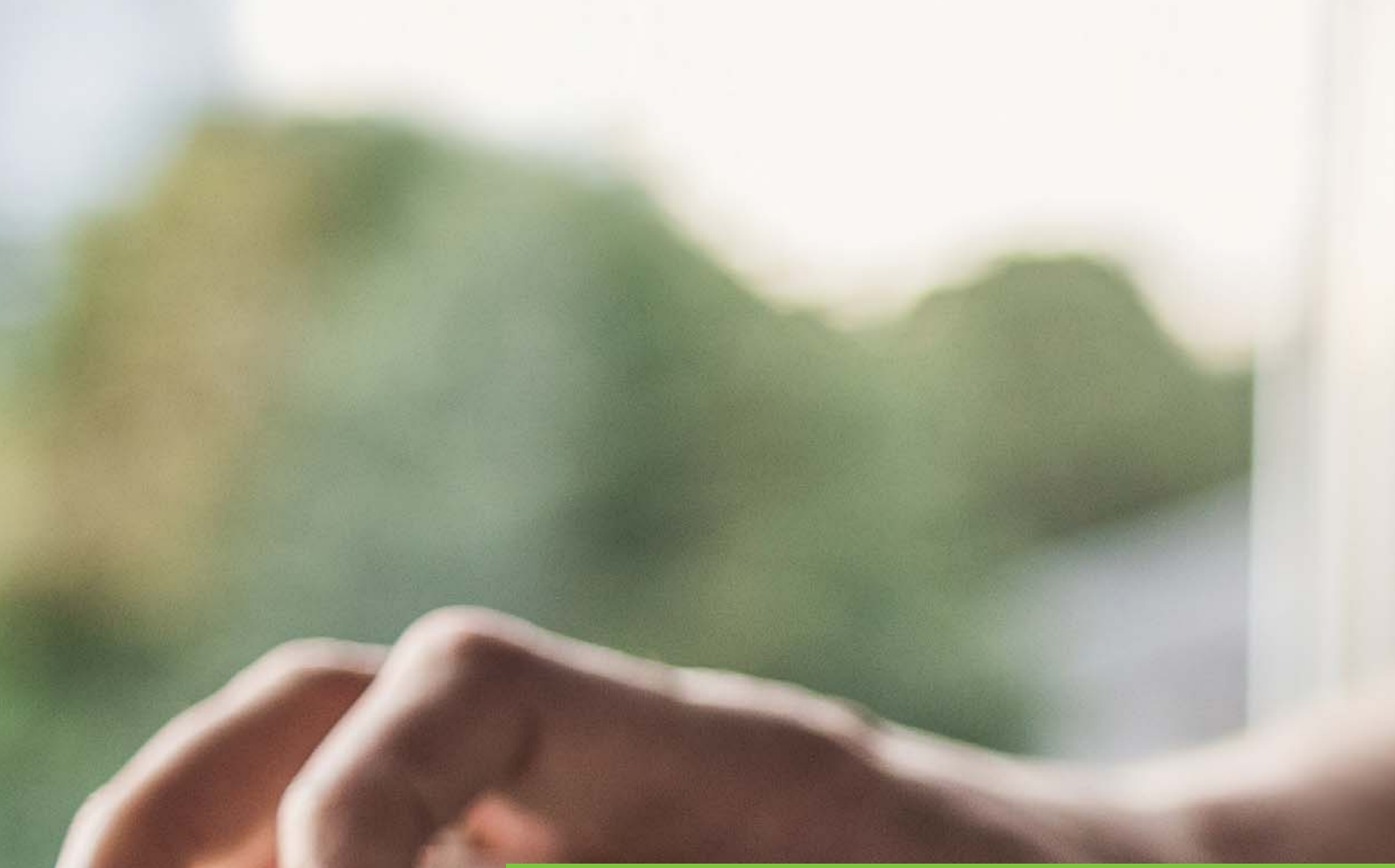


Took no action at all

"Cyber risk is an enterprise risk and not a risk that sits in just one business unit or cost centre. To manage the risk, there should be enterprise-wide controls, and this needs boardroom or business owner oversight.

Cyber risk is an important part of a board officer's fiduciary duties."

Andrew Taylor
Cyber Underwriting Manager, Chubb Asia Pacific



Case Study:
Ransomware hides personal information theft

Retail
Industry

US$105,000
Claim Amount

US$150 million
Annual Revenue

A national retail chain suffered a cyber loss when an employee at one of its franchise stores clicked an email link from an unknown source. The email link contained malware that encrypted a "back-office" computer.

After forensic investigations, it was uncovered that attackers used the ransomware in an attempt to mask their previous breaches on the company's network. Months before the ransomware attack, the computer had been accessed multiple times by threat actors using remote access from an exposed port to the Internet. The criminals targeted the retailer's unencrypted customer database. Over 70,000 customer records were stolen comprising names, postal addresses, email addresses, phone numbers and other sensitive data.

External legal counsel, forensics experts, public relations consultants and a call-centre were required to mitigate the damage caused by the attack.

Data - a need for protection

Protecting data is not just good for business, it is the law. In Australia, small businesses earning more than AU$3 million annually must comply with the Notifiable Data Breaches Scheme that came into effect in February 2018[3].

If a data breach involving customer or employee information has occurred which would likely result in serious harm to the customer or employee, small businesses must by law report the incident to the Office of the Australian Information Commissioner and notify individuals affected[4].

"From 400+ cyber incidents we have recently managed, the majority of the organisations impacted were SMEs. The resources required to respond to data breaches and other cyber incidents can be significant and the impacts are often unexpected. We see some SMEs being caught-out by data breach reporting regimes across jurisdictions and when incidents arise through a business partner. These factors can place additional pressure to an already stressful scenario for the SME business owner."

John Moran
Partner,
Clyde & Co

[3] *https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme*
[4] *Businesses can find out more about cyber security regulations on the Australian government website: https://www.australia.gov.au/information-and-services/security-and-defence/national-security/cyber-security*

Biggest concerns of SMEs following a cyber incident

SMEs are certainly aware of the impact of a cyber incident on their business. From our research, we found that the biggest concern to SMEs following a cyber incident is their relationship with customers (51%). This ranks alongside concerns about profits (51%), the sheer cost of the incident (51%) and their public reputation (47%).

Despite this - or maybe because of this - only 31% of the respondents said they have notified the parties impacted following a cyber incident.

The very foundation of SMEs is more at risk when it comes to cyber security incidents than larger organisations because they have limited resources to respond and recover. The business interruption and financial impact can be catastrophic. The risk to the overall business is what Chubb calls the 'Domino Effect.'

Chart 6: Key concerns of SMEs following a cyber incident

51%
Relationship with customers

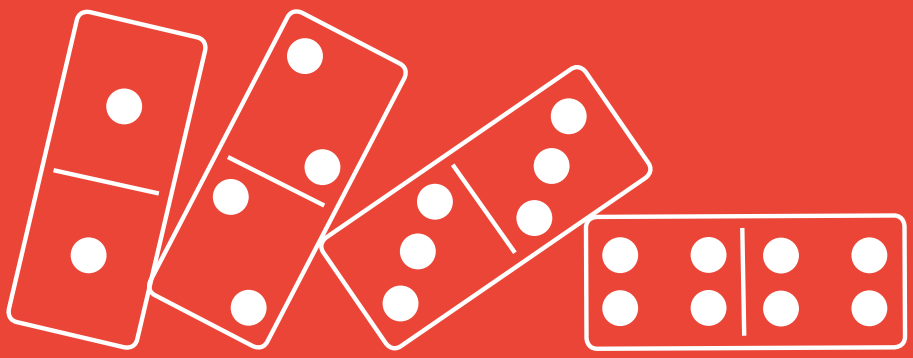
51%
Revenue and sales

47%
Public reputation

51%
Cost of the incident

31%
Had notified the parties impacted following a cyber incident

The catastrophic domino effect on small businesses



The First Domino Cascade

Websites or computer systems of SMEs are attacked and their virtual storefronts and ability to process transactions are destroyed. It's as if the SME has gone out of business and as a result, many customers go elsewhere and a large percentage never return.

The Second Domino Cascade

When attacks involve stolen personal information such as credit card numbers, a downward spiral of negative press and shaken customer confidence can lead to crippling brand damage and further customer attrition can become stampede-like.

The Third Domino Cascade

Restoring digital data, software, and computer systems can require such a large investment of time and money that it can precipitate business bankruptcy. Couple that with a potential ransom payment, and the SME faces financial ruin.

The Fourth Domino Cascade

The last possible outcome is that SMEs may be sued for liability when an attack impacts customers, vendors, suppliers, or others. These lawsuits are often extremely costly and time consuming to defend and that's another way that a cyber attack can become an endgame event.

Case Study:
Business email compromise and stolen customer data

Professional Service
Industry

US$52,000
Claim Amount

US$25 million
Annual Revenue

The business email inbox of a partner in a mid-sized professional service firm was compromised when the partner fell victim to a phishing attack. The partner unwittingly provided his Office 365 log-in details to the attacker. These details were then used to log into his Office 365 account from an international location. The attackers had full access to the partner's contacts, business attachments, confidential client information and calendar. The information the attackers compromised also included European client data.

The attackers used the Office 365 access to delete emails and further compromise the partner's LinkedIn account, perpetuating the phishing scam and information harvesting from the partner's Linkedin followers.

Privacy lawyers, PR consultants and computers forensics experts were required to assist, stop and mitigate the damage caused.

The role of insurance

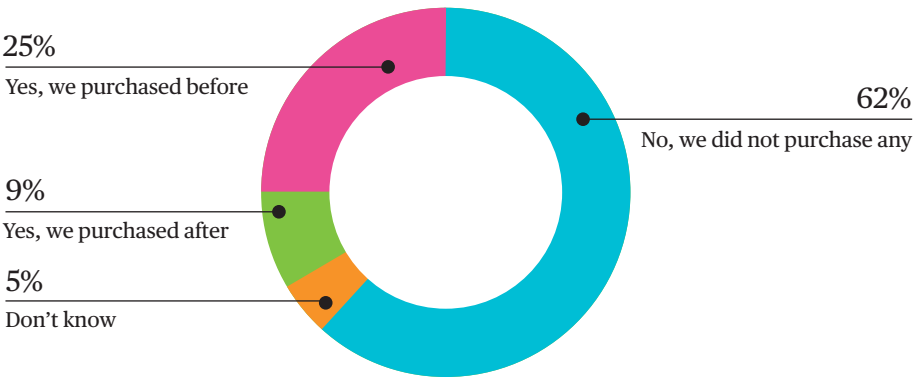
Covering the cost of a cyber incident is critical for companies of all sizes; but particularly for SMEs. Since insurance transfers financial risk from the SME to the insurer, this relieves the burden on the SME in the event of a cyber incident. However, 62% of SMEs surveyed have never purchased cyber insurance before. This may be due to their lack of awareness about the insurance solutions available, with 59% of SMEs polled agreeing to that statement. In addition, 54% would value the ability to identify and minimise the impact of a cyber incident and 53% would value having a hands-on response service.

This is why insurers are responding to the growing challenges of cyber risk to help secure the business world. In line with the OECD's report to the G7 in May 2017, Chubb is working to promote awareness about exposure to cyber losses, share expertise on risk management and encourage investment in risk reduction.

We also maintain the Chubb Cyber Index℠ which provides real time access to our proprietary data. Chubb has been handling cyber claims for nearly 20 years, and these metrics, along with public trend data, offer useful insights to partners and policyholders to help manage and reduce their exposure to future losses.

Chubb further assists clients by providing an Incident Response Platform to help contain threats and limit potential damage to a client's business and, importantly, learn from the incident.

Chart 7: When asked if SMEs had purchased insurance before or after a cyber incident:



"Clearly, there is a need for more broker and client education about the value of cyber insurance. At Chubb, our value proposition is more than just the traditional 'promise to pay' - we offer enterprise-wide support solutions for the benefit of our Insured. That's why we place emphasis on our preventive advice as well as our global incident response support."

Tim Stapleton
Senior Vice President,
Cyber & Technology,
Chubb Overseas General

How SMEs can protect themselves from cyber risks

As modern technology interacts across multiple environments, we will always be faced with the potential for change which could expose a previously unknown risk. However, there are five simple measures that SMEs can take to create their own cyber risk programs and limit their exposure and ensure they are not "too small to fail". These tips are in line with the Australian government's 'Essential 8' mitigation strategies.

Develop and enforce a strong password policy

One of the easiest ways for cyber criminals to access SME assets is by walking through the virtual "open door" that employees provide when using weak passwords. To correct that situation, it is a good idea for SMEs to establish a written password policy requiring strong passwords (e.g., a mix of letters, numbers, and symbols) that are frequently changed. Passwords should also be changed automatically, or accounts marked inactive when employees leave the company.

Conduct regular training about cyber security vigilance

SMEs should inform employees of the role they play in preventing a cyber incident. It is all too easy for malicious software to hitch a ride into the company server when company laptops or other devices are used offsite and later connected to the internal network. The best way to establish positive and secure habits within the company's workforce is with regularly scheduled training and education. It should also restrict access to sensitive information by only allowing management or those who require that information for company operations, to have access.

Update IT equipment and deploy security software

Outdated operating systems and computers can be a risk as they are vulnerable to more sophisticated hacking techniques and newer forms of malware. At the same time, it is important for SMEs to monitor those who have legitimate access to their computer network, as well as to monitor the network itself. Although SMEs do not typically have information security experts within their organisation, they can access basic downloadable software that deploy some of the same technology solutions used by major companies within minutes.

Create a Cyber Incident Response Plan

Establish a dedicated and prepared team of cyber incident responders consisting of both employees and outside service providers who can work toward a resolution for certain incidents quickly.

Purchase Cyber Insurance

SMEs can more fully protect their assets and cash flow by purchasing cyber insurance. The cost of insurance will always be far less than the cost of shutting down a business in the wake of one or more cyber attacks. Cyber insurance, such as Chubb Cyber Enterprise Risk Management (ERM) can be pre-packaged with some of the services mentioned above.

Commonly used cyber terms

Cyber attack	Malicious activity aimed at affecting the availability, confidentiality or integrity of computer systems for data.
Data breach	When sensitive, protected or confidential data is either intentionally or unintentionally copied, transmitted, viewed or used by an individual unauthorised to do so.
Cyber incident	When computer systems or data are compromised as a result of unintentional error or malicious activity.
Malware	Any form of malicious software (including viruses and Trojan Horses) that infects a network, servers, devices or end user computer, including ransomware, remote access tools, network sniffing software and botnet software.
Phishing	Communications via email, messaging, telephone that, though the guise of legitimacy, seeks information or places misinformation in a system environment through a benign-looking link or file.
Ransomware	Computer software that installs covertly on a device and locks the system until a sum of money is paid.
Spear phishing	While phishing is a generally exploratory attack that targets a broader audience and tends to stop once certain information is stolen, spear phishing is more targeted. In spear phishing, the successful theft of credentials or personal information is often only the beginning of the attack, because it is only used to gain access to the target network – a move that ultimately leads to a targeted attack.

About this research

This report has been produced by Chubb in collaboration with YouGov. It is based on a survey of 1,000 respondents from Small and Medium Enterprises (SMEs) in three markets; 400 from Australia, and 300 each from Hong Kong and Singapore.

Respondents comprised board-level executives (77%) and senior managers or directors below board level (23%) from SMEs with 2 to 249 employees.

The industries respondents belonged to are: Professional Services (22%), Manufacturing (17%), Retail & Hospitality (13%), Education (6%), Financial Services (6%), Healthcare (5%), Technology (5%), Media & Communications (3%); and other industries (23%).

For more information about Chubb's Cyber Enterprise Risk Management (ERM) policy, please contact us at AP.Cyber@chubb.com

About Chubb in Australia

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 almost 100 years. Its operation in Australia (Chubb Insurance Australia Limited) provides specialised and customised coverages include Marine, Property, Liability, Energy, Professional Indemnity, Directors & Officers, Financial Lines, Utilities as well as Accident & Health, for a broad client base, including many of the country's largest companies.

More information can be found at www.chubb.com/au

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.℠

Chubb10-575-0219