Ignorance is Risk

Regional SME Cyber Preparedness Report 2019

CHUBB®

Contents

Welcome

Mr Andrew Taylor,
Cyber Underwriting Manager,
Chubb Asia Pacific

Following the release of Chubb's inaugural SME Cyber Preparedness Report in 2018, we are delighted to bring you the second edition of this report. In 2019, we have expanded this study to include four locations in Asia Pacific - Australia, Hong Kong SAR, Malaysia and Singapore.

As one of the world's largest cyber insurers, we believe it is important to raise awareness of the issues that small and medium-sized enterprises (SMEs) face in managing cyber risk.

In the past 12 months, more than two-thirds (68%) of SMEs in Australia, Hong Kong, Singapore and Malaysia have experienced a cyber incident. Amid a rising digital economy globally, the number of businesses affected will only increase.

Despite this, many SMEs in the markets studied remain unconcerned by this clear and present danger to their business, choosing to gamble their business on what is - at best - a 50:50 chance of being involved in a cyber incident. The odds are only half the story here though. Cyber resilience needs to be seen as a business' competitive advantage or a unique selling point and not just business as usual. Greater recognition of the downside could mean further costly litigation, or even worse, the end of the business itself.

So why then are so many SMEs prepared to risk so much for so little? The rate at which cyber threats are evolving is certainly a contributing factor. It is difficult to keep up and, as such, there is a disconnect between perceived risk and actual risk. There also remains a certain level of optimism bias - a belief that "it won't happen to me" or that cyber criminals only target larger businesses. As you will see in our reports, the numbers do not support this view.

SMEs can and must be doing more to protect the interests of their business, their partners and their customers. Governments, regulators and insurers also have an important role to play in cyber risk reduction.

Rather than seeing it as a chore or expense, there is also an opportunity for SMEs to view cyber resilience as a potential competitive advantage or unique selling point.

We hope that you will find this report useful and the insights can contribute towards reducing cyber risk for SMEs across the region.

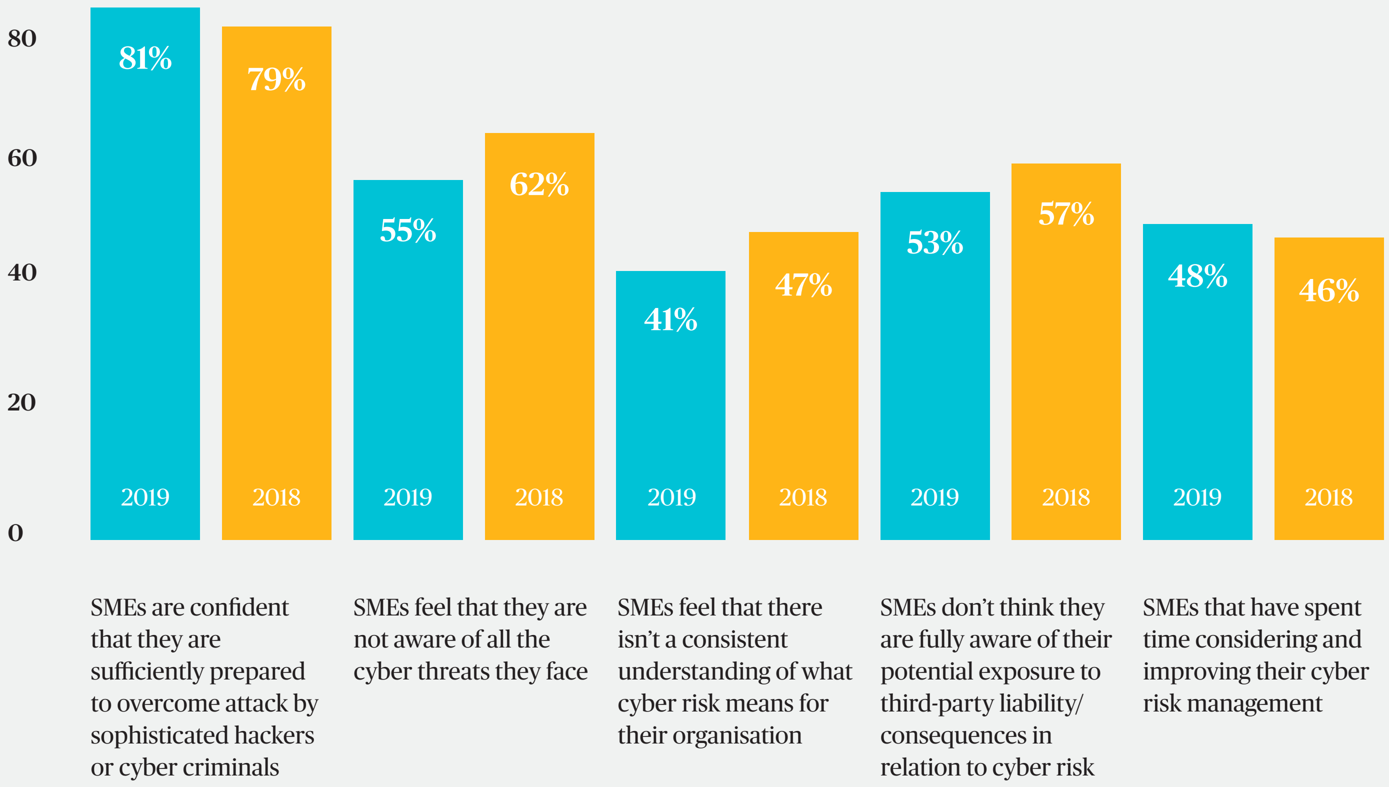
Risky Business

At the core of our results this year is that SMEs remain ignorant when it comes to cyber risk and are risking it all by not investing in improving their defences. A disconnect between perceived and actual risk was apparent in our 2018 report, and it continues to persist in 2019.

On one hand, 81% of SMEs are confident that they are sufficiently prepared to overcome a surprise attack by sophisticated hackers or cyber criminals. On the other, more than half (55%) SMEs concede they are not aware of all the cyber threats they face. 41% also agree that there isn't a consistent understanding of what cyber risk means for their organisation.

There is a lack of understanding, too, about the potential for exposure through third-party partners, with 53% saying they are not fully aware of the risks in this area. Looking back over the past two years, less than half (48%) said their company had spent time considering and improving their cyber risk management. The numbers show this is a dangerous game.

How prepared are SMEs?

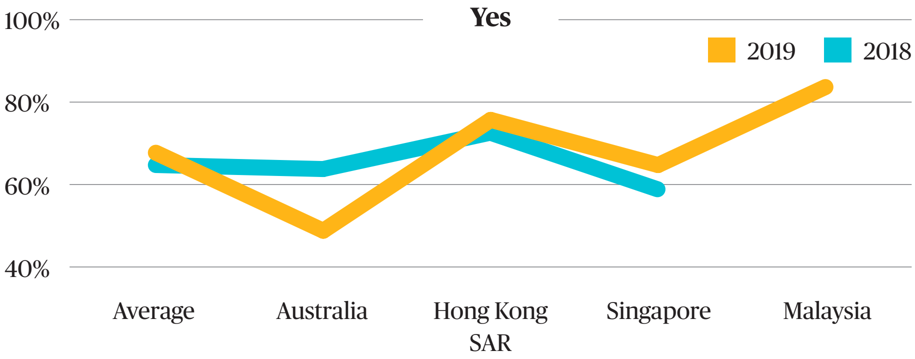


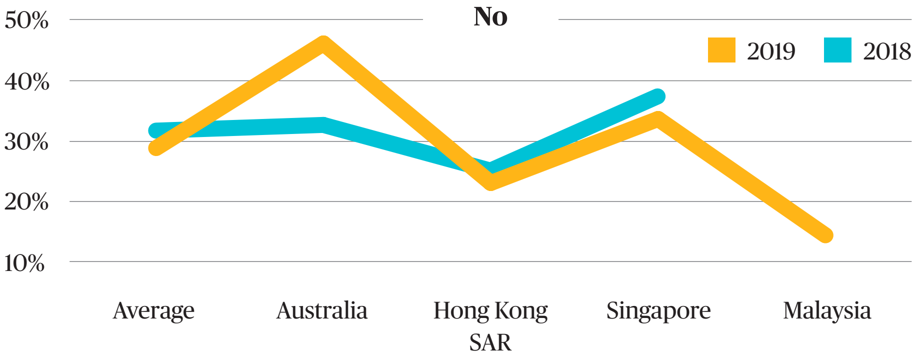
On average, 68% of SMEs across Australia, Malaysia, Hong Kong SAR and Singapore experienced a cyber incident in the past 12 months. Australia was the least affected, with 49% of respondents suffering an incident. This rose to 65% in Singapore and 76% in Hong Kong. Malaysia was most affected, with 84% of businesses suffering a cyber incident in the past year.

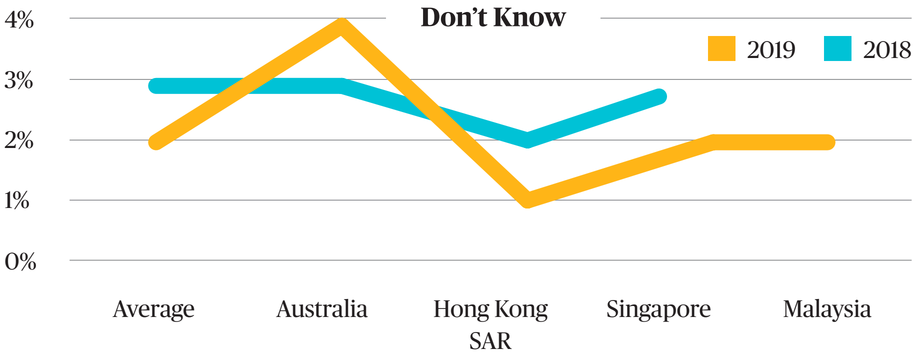
So, while many may believe they are safe from harm, the reality is very different.

At best, an SME in one of these locations has a roughly 50:50 chance of experiencing a cyber incident. What is surprising, is how many business leaders seem comfortable with this level of risk.

Have you suffered a cyber incident in the past 12 months?







No Lessons Learnt

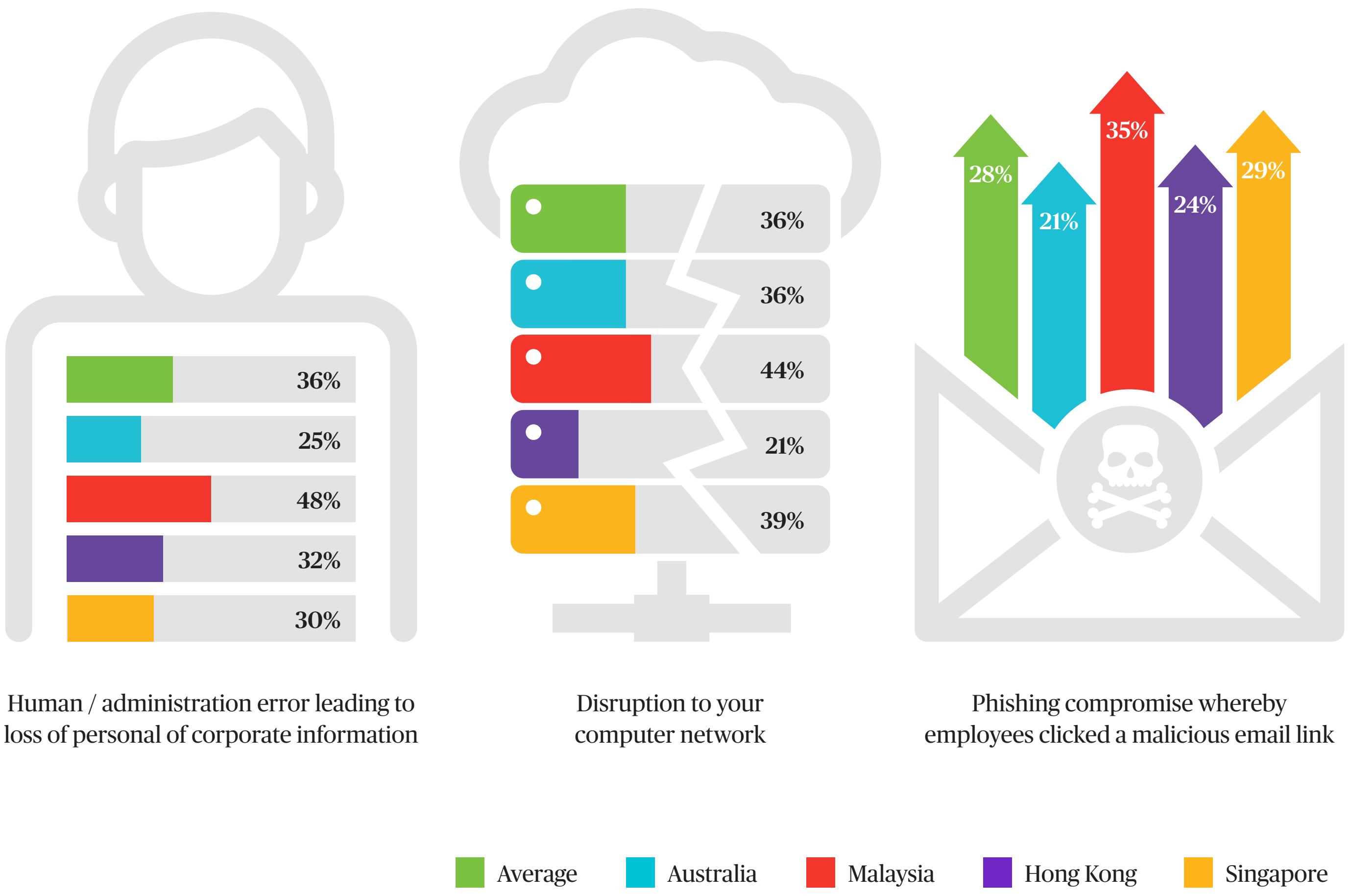
The survey looked at nine incident types, ranging from system malfunctions and technical faults to malicious activity including ransomware and phishing scams.

Tied for the most common factors contributing to a cyber incident are human error and system faults or malfunctions leading to network disruption.

These played a part in more than one-third (36%) of incidents across the markets surveyed in 2019.

Malicious activity was also the cause of a significant number of the reported incidents. Most prevalent were phishing scams where employees are tricked into clicking on seemingly innocent links that led to their accounts being compromised. This occurred in 28% of incidents across the region.

Types of cyber incident experienced in the past 12 months



Human / administration error leading to loss of personal of corporate information

Disruption to your computer network

Phishing compromise whereby employees clicked a malicious email link

*Note: Percentages may not add up to 100% as survey respondents were able to select more than one option for questions with multiple answers.

Employing Your Best Defence

Employers have a clear idea of where they see their weaknesses lying and, for the most part, it is with their employees.

Nearly half (48%) of respondents are not confident that employees with access to sensitive data are fully aware of their data privacy responsibilities. For close to a quarter (23%) of respondents, the biggest challenge in protecting against a cyber incident is their employees.

Additionally, 29% see their employees' poor understanding of the threat as the principal challenge they face in relation to cyber risk. To a degree, this is understandable. As we have seen, 36% of incidents across the region included an element of human error.

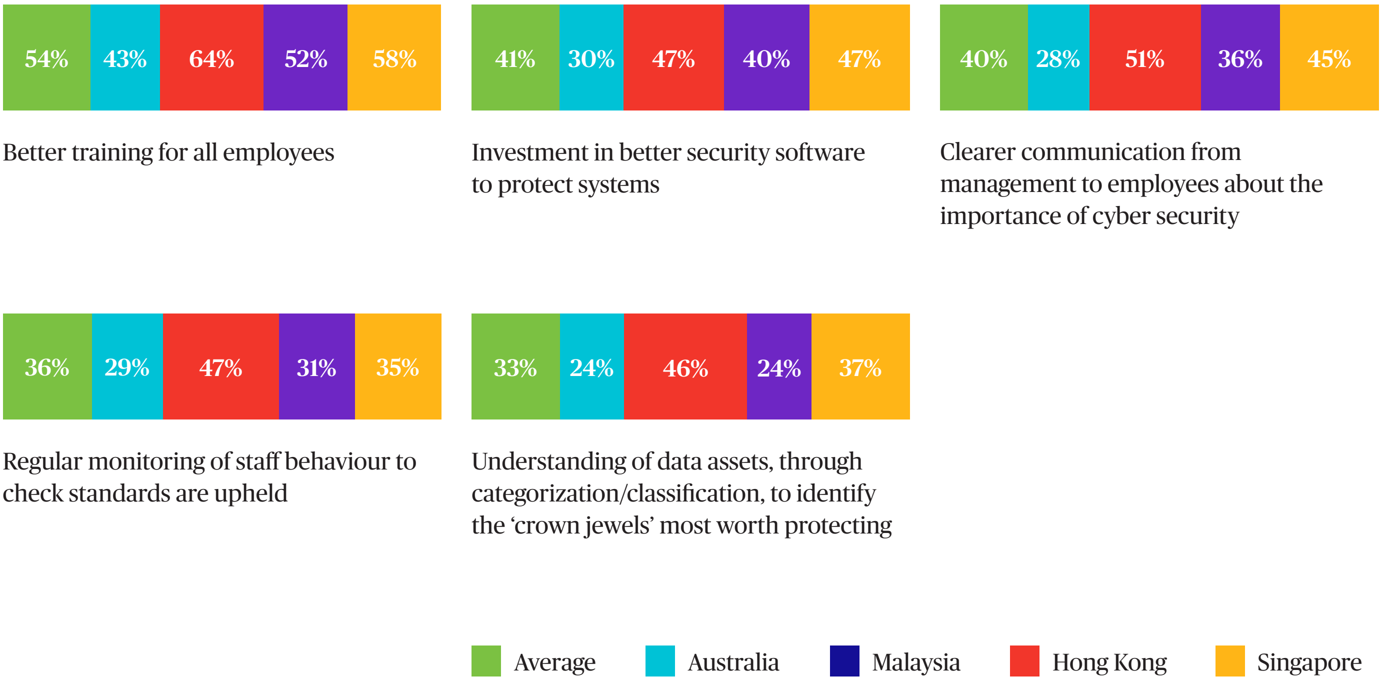
Better training and education could help reduce this high level of human error-related incidents. The majority of SMEs identify "softer" people-centric solutions as a core focus in their organisational approach to cyber risk management.

The key focus is better training for all employees (54%), followed by investment in better security software to protect systems (41%). Such training is important because employees can also be a company's best defence against cyber risks if they are well trained to spot and rectify potential cyber threats. "Hard" solutions are also being considered by many SMEs, with investment in better security software being the primary focus.

Another area ripe for improvement to better equip SME employees is risk management. More than half (56%) of incidents stemmed from a risk the business had already identified. These were essentially accidents waiting to happen.

Only 46% of SMEs have a data breach response plan, while 45% stated that their response plan was ad hoc and not documented.

Where do SMEs think they should focus their efforts to improve their overall cyber risk management activity?



Better training for all employees

Investment in better security software to protect systems

Clearer communication from management to employees about the importance of cyber security

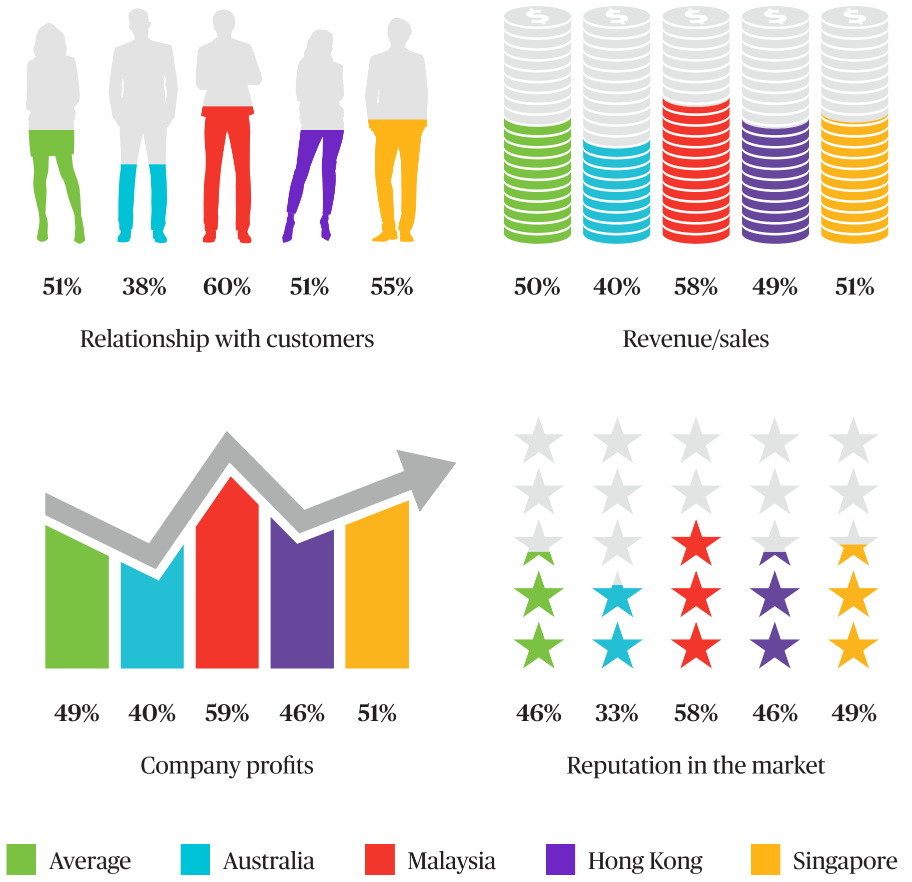
Regular monitoring of staff behaviour to check standards are upheld

Understanding of data assets, through categorization/classification, to identify the 'crown jewels' most worth protecting

The Customer Comes Last

Overall, SMEs are most concerned about the impact of a data breach on their relationship with customers. Following closely behind are revenue/sales, company profits, and reputation in the market. Of the four locations studied, Australian respondents are consistently the least concerned about the impact of a breach, often by a significant margin.

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



Despite these findings, on average, SMEs across all markets performed poorly across a variety of indicators in their cyber incident response. Fewer than half (48%) of SMEs notified all affected parties of a data breach. 59% of affected SMEs did increase protection and enhance their processes around their data files, but a worrying number did little or nothing to recover from an incident or help defend against future incidents.

Fewer than two out of five (38%) reviewed their processes and protection and took no further action, and 14% simply recovered their files and took no further action. 5% of SMEs took no action at all following a cyber incident. This was skewed higher by Australian respondents – with 16% of Australian SMEs taking no action at all.

Case Study:

Employee breaches internal governance

Industry:
Construction

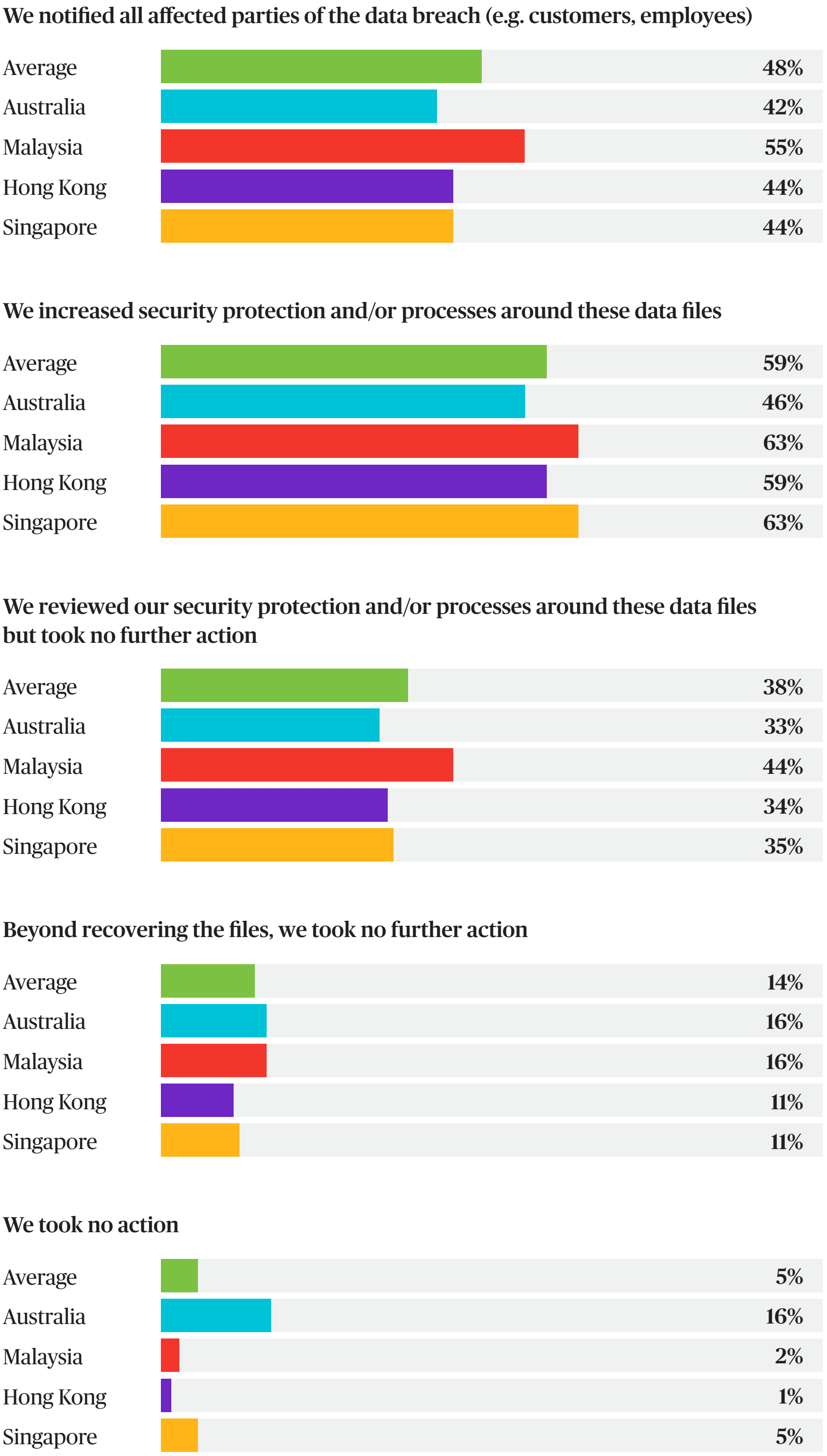
Annual revenue approximately:
US$3.5 million

Costs up to:
US$340,000

A construction company that outsourced its IT operations suffered a ransomware attack because an employee clicked a malicious email link, causing the company's customer and project data to be encrypted. The ransomware infected local hard drives and data that was backed up online.

Without access to the digital records, the company could not operate its business as usual. Due to the failed attempts to negotiate with the extortionist, additional costs were incurred to re-construct and re-enter customer project records. This resulted in significant down time and major loss incurred to the business.

What action did you take following a data breach?


We notified all affected parties of the data breach (e.g. customers, employees)

We increased security protection and/or processes around these data files

We reviewed our security protection and/or processes around these data files but took no further action

Beyond recovering the files, we took no further action

We took no action

Case Study:

Credential Stuffing

Industry:
Retail

Annual revenue:
US$ 215million

Costs over:
US$475,000 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 informed 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.

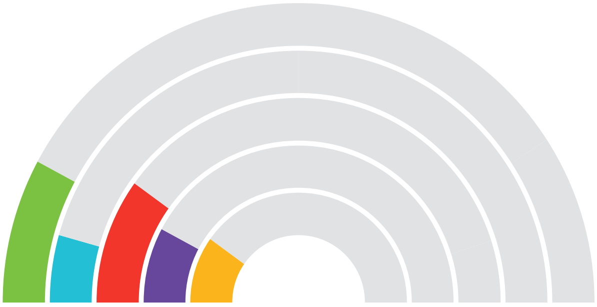
The Role of Insurance

Managing the fallout from a cyber incident can be costly, time-consuming and difficult. Having insurance to fall back on can ease this burden in terms of both cost and resources. The majority (57%) of SMEs recognise insurance has an important role to play in managing their cyber risk profile.

However, despite this, most SMEs are uninsured. Across the markets, 40% of SMEs have never had cyber risk insurance, and worryingly, 16% have let previous cover lapse. 7% of respondents do not know if they had cover or not, which was skewed higher by 14% in Australia.

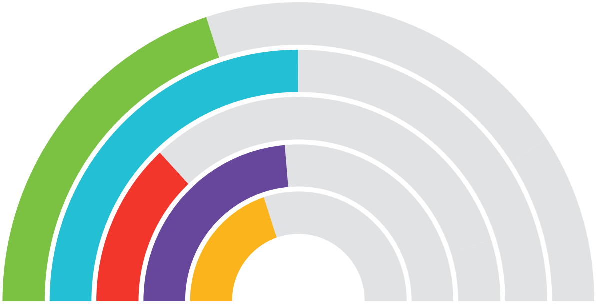
Yes - we have taken out this insurance in the past but are no longer covered by it

16%	Average
9%	Australia
20%	Malaysia
16%	Hong Kong
20%	Singapore



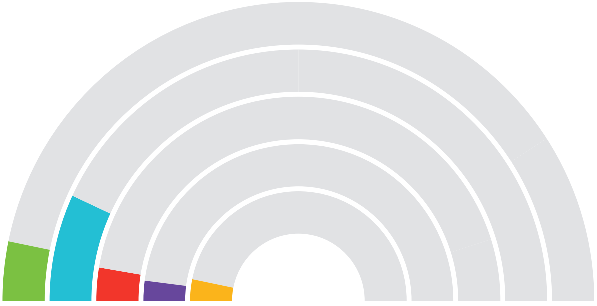
No - we have never been covered by this type of insurance

40%	Average
50%	Australia
26%	Malaysia
47%	Hong Kong
40%	Singapore



Don’t know

7%	Average
14%	Australia
5%	Malaysia
4%	Hong Kong
6%	Singapore



The most valued services for SMEs offered by insurers

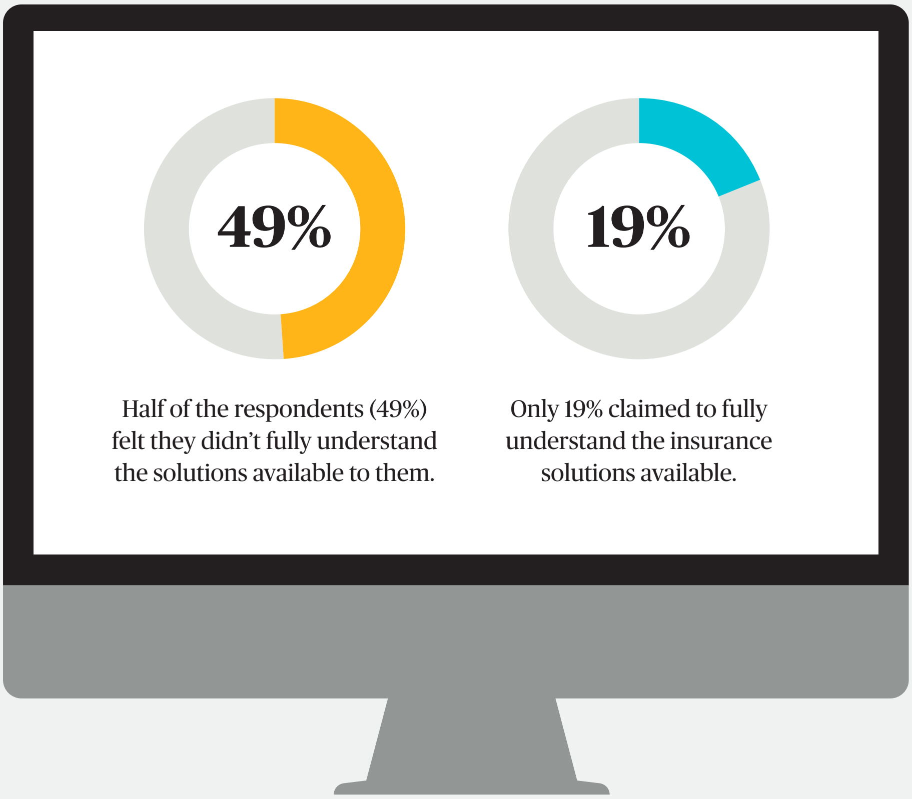
Regulatory advice - being able to steer SMEs through the process of reporting and managing a data breach with their local regulators

Speed of response - being able to quickly and decisively deal with a cyber incident

The ability to identify and minimise the impact of a cyber incident

Just as significant, is that half (49%) of the respondents felt they didn't fully understand the solutions available to them. In fact, only 19% claimed to fully understand the insurance solutions available.

This is an important learning for us at Chubb, and we are committed to improving the way we communicate our solutions to existing and potential clients.



Half of the respondents (49%) felt they didn't fully understand the solutions available to them.

Only 19% claimed to fully understand the insurance solutions available.

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 the threat and limit potential damage. It includes an on-call crisis response available 24/7/365 days; supported by contractual service level agreements. These agreements require a 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.

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 organisation.

Create a Cyber Incident Response Plan - 45% of SMEs across the region admitted their current plan is ad hoc and not documented. Of those that do have a plan in place, only 35% test it regularly. Prepare 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.

Dwelling on the Downside

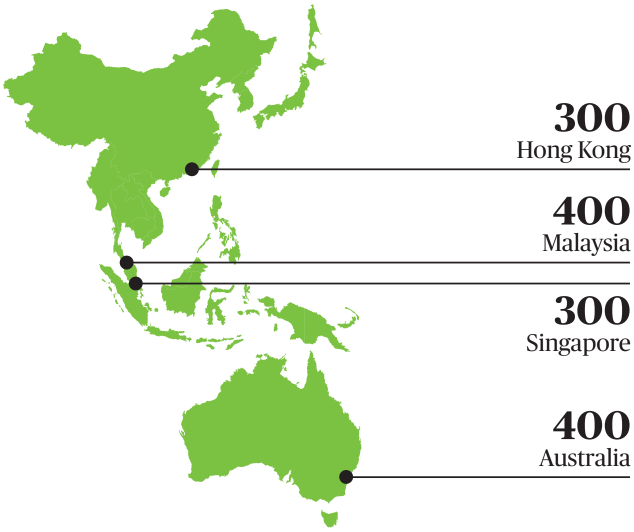
Persistent threats can last inside SME networks for years. Dwell time – the amount of time a threat spends inside of a network before an organisation discovers and removes it – has become a significant problem for SMEs, according to a U.S. report released by Infocyte in July 2019. Dwell time for attacks 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.

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%

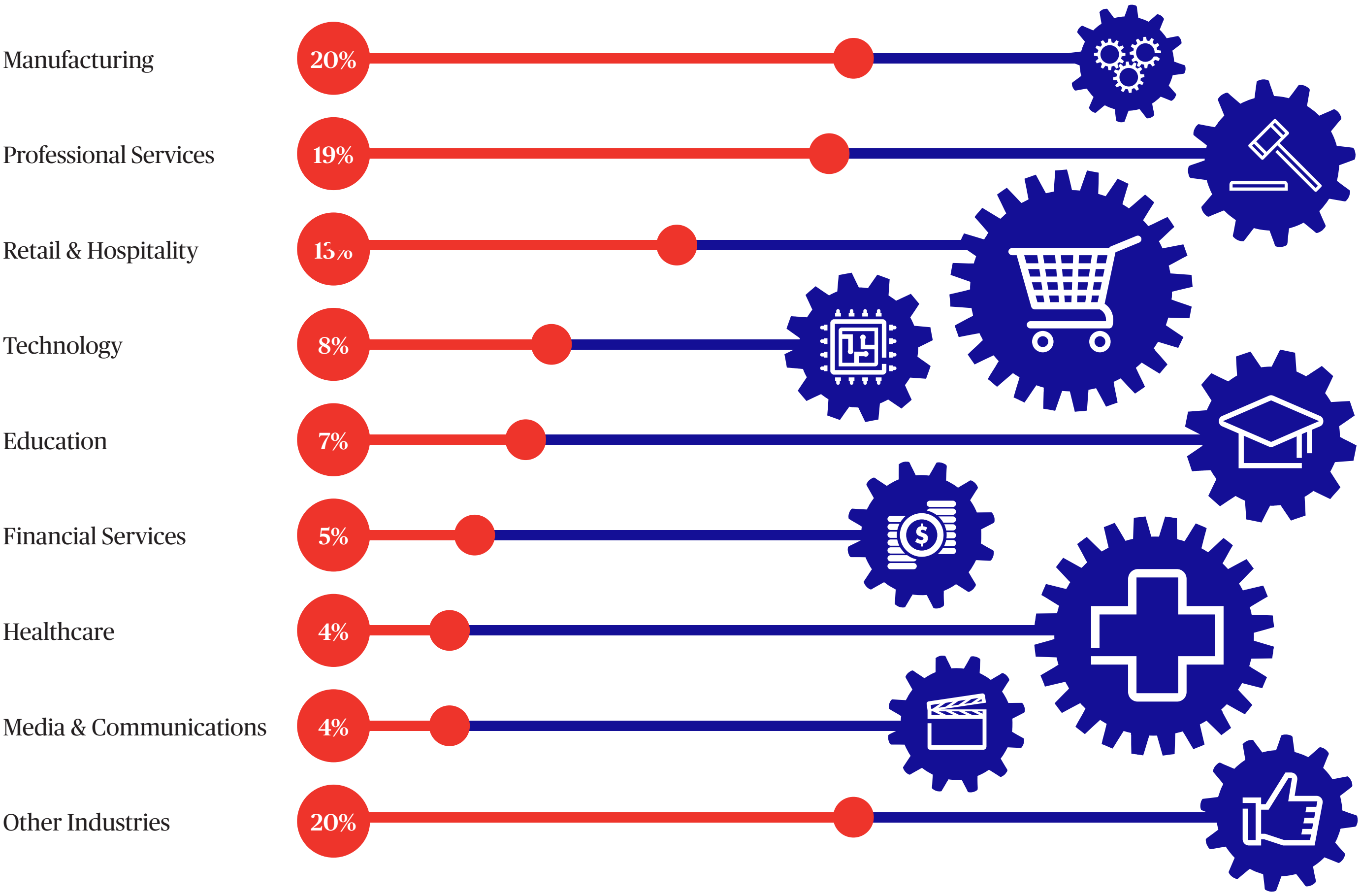
Board-level executive

18%

Senior managers or directors below board level

from SMEs between 2 to 249 employees.

The industries respondents belonged to are:



Glossary of Frequently Used Cyber Risk 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.

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 of 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 Chubb

Chubb is the world's largest publicly traded property and casualty insurance company. With operations in 54 countries and territories, Chubb provides commercial and personal property and casualty insurance, personal accident and supplemental health insurance, reinsurance and life insurance to a diverse group of clients. As an underwriting company, we assess, assume and manage risk with insight and discipline.

We service and pay our claims fairly and promptly. The company is also defined by its extensive product and service offerings, broad distribution capabilities, exceptional financial strength and local operations globally.

Parent company Chubb Limited is listed on the New York Stock Exchange (NYSE: CB) and is a component of the S&P 500 index. Chubb maintains executive offices in Zurich, New York, London, Paris and other locations, and employs more than 30,000 people worldwide.

Chubb's franchise in Asia Pacific comprises an extensive network of operations serving Australia, China, Hong Kong SAR, Indonesia, Korea, Macau SAR, Malaysia, New Zealand, Philippines, Singapore, Taiwan, Thailand and Vietnam.

Contact Us

Australia
www.chubb.com/au

Hong Kong SAR
www.chubb.com/hk

Malaysia
www.chubb.com/my

Singapore
www.chubb.com/sg

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.