Ignorance is Risk

Malaysia SME Cyber Preparedness Report 2019

CHUBB®

Contents

Welcome

Mr Andrew Taylor,
Cyber Underwriting Manager,
Chubb Asia Pacific

We are delighted to bring you Chubb's inaugural SME Cyber Preparedness Report for Malaysia.

As one of the world's largest cyber insurers, we believe this report is important for raising awareness of the issues that SMEs face in managing cyber risk. In the coming years, cyber risk is forecast to cost global businesses substantially in lost revenue. With SMEs making up 98% of all businesses in Malaysia, employing 65% of the country's workforce[1] and accounting for 38.3% of its GDP[2], they will be hardest hit without good risk mitigation, incident response planning and consideration of cyber insurance.

We have seen from our survey that 84% of businesses in Malaysia have experienced a cyber incident in the past 12 months. While 61% of them have a data breach response plan in place, we see that preparedness isn't going far enough, leaving businesses exposed. With the proliferation of digitalisation, cyber risks for SMEs will only amplify.

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

[1] https://www.worldbank.org/en/news/feature/2016/07/05/small-is-the-new-big---malaysian-smes-help-energize-drive-economy

[2] https://www.theedgemarkets.com/article/malaysia-sme-contribution-gdp-383-2018

Ignorance is Risk

Cyber Risk Landscape

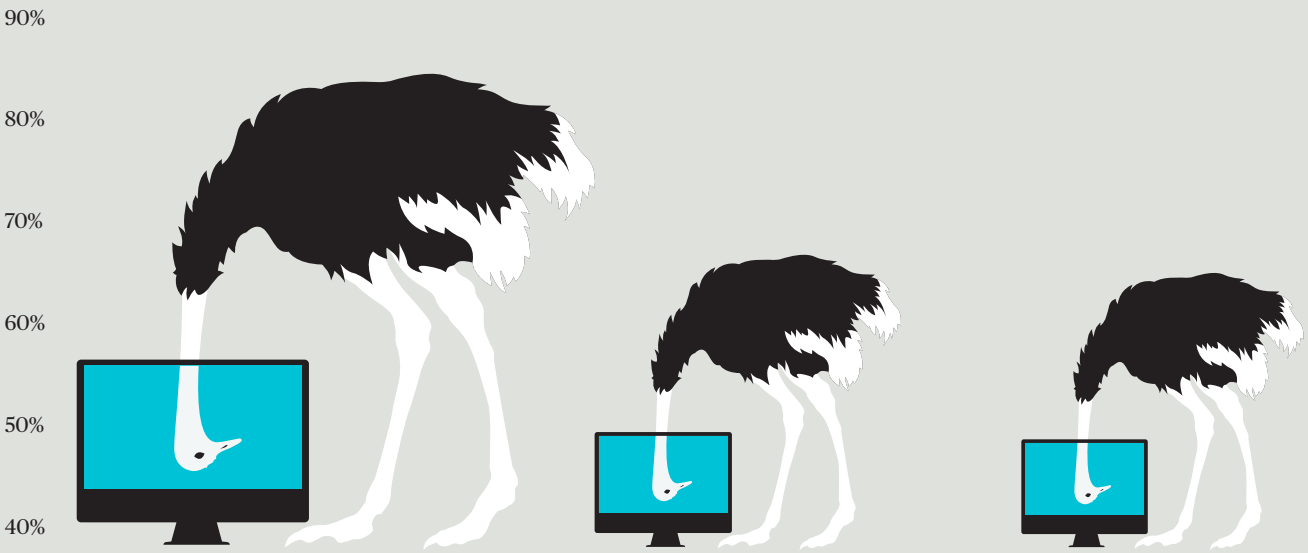
Malaysian businesses are experiencing an average of around 45,000 business email compromises per day[3].

Malaysia's National Cyber Security Agency launched the National Cyber Crisis Management Plan to combat cyber threats through resource mobilisation and infrastructure development[4].

Digital Economy

Malaysia has a rapidly expanding digital economy forecast to be worth US$5.3 billion by 2020[5].

Key Survey Highlights



84%

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

67%

of Malaysian SMEs believe that large corporations are more at risk of cyber attacks than small businesses.

64%

of Malaysian SMEs believe that cyber risk is an IT concern rather than a shared responsibility.

[3] https://www.digitalnewsasia.com/digital-economy/cyber-security-threats-cost-malaysian-organisations-us122bil-economic-losses

[4] https://www.nst.com.my/news/nation/2019/04/475821/national-cyber-security-strategy-be-implemented-middle-year-dpm

[5] https://www.thestar.com.my/business/business-news/2017/12/19/booming-digital-economy-to-raise-malaysias-profile/

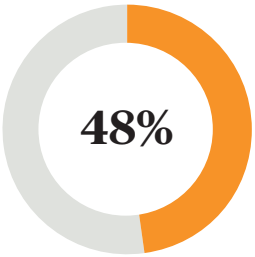
Prepared to be Unprepared

The recent implementation of the National Cyber Crisis Management Plan by Malaysia's National Cyber Security Agency to combat cyber threats[6] is a clear demonstration that local regulators increasingly recognise the need for greater cyber protection.

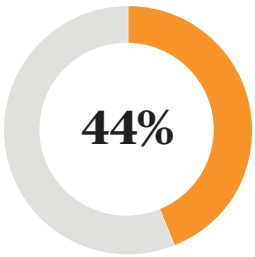
Our survey reveals an overall misconception about the threats of cyber risks to SMEs, with more than two-thirds (67%) believing that large corporations are more at risk of cyber-attacks than small businesses. Yet 84% of SMEs have experienced cyber incidents in the past 12 months, demonstrating that this misconception certainly does not hold water. In fact, smaller companies face a larger degree of exposure to cyber risk owing to their size and resources, as well as the lack of capital to invest in cyber risk management tools.

Human error accounted for the highest proportion of cyber incidents for Malaysia's SMEs, with customer records being the most commonly breached data - with 40% of businesses facing a breach of customer files in the past 12 months.

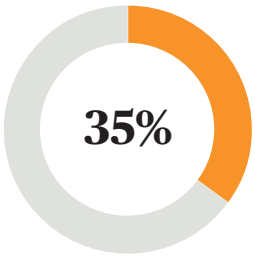
Most commonly experienced types of cyber incidents:



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

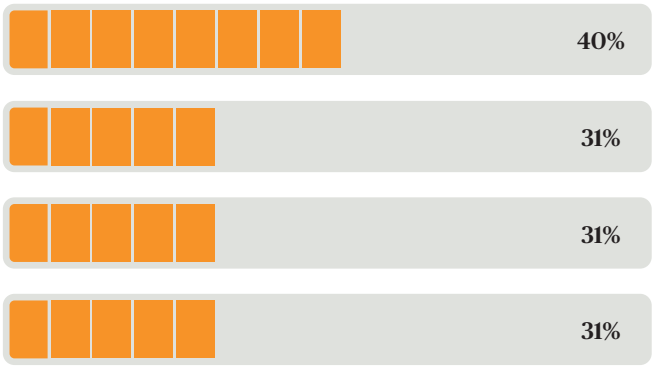


Disruption to computer network



Ransomware attack and phishing compromise whereby employees clicked a malicious email link

Most commonly breached data files:



Customer records (payment information and personal details)

Research and development (R&D) data

Intellectual property (IP) data

Financial performance data

[6] https://www.nst.com.my/news/nation/2019/04/475821/national-cyber-security-strategy-be-implemented-middle-year-dpm

Man vs Machine – Where's the Greatest Risk?

With human error the greatest cause of cyber incidents, it is unsurprising that more than one third (37%) of SME leaders in Malaysia say their employees' poor understanding of potential cyber threats is challenging their ability to protect their business from associated risks.

In addition, 20% of SMEs believe employees are the weakest link in their cyber defence.

While leaders recognise the importance of protecting themselves through cyber training, 41% believe that employees are neglecting their responsibilities around data protection.

This can lead to a situation where employees are neither cognizant nor capable of proper contingency methods in the event of a cyber attack.

This stems from a lack of understanding, with more than half saying there is no consistent understanding within their organisation of what cyber risk means, and 64% believing that cyber risk is largely a concern for IT – rather than a shared responsibility.

20% of SMEs believe employees are the weakest link in their cyber defence.

Case Study:
Employee breaches internal governance

Industry:
Retail

Annual Revenue approximately:
RM 21 million

Costs up to:
RM 715,000

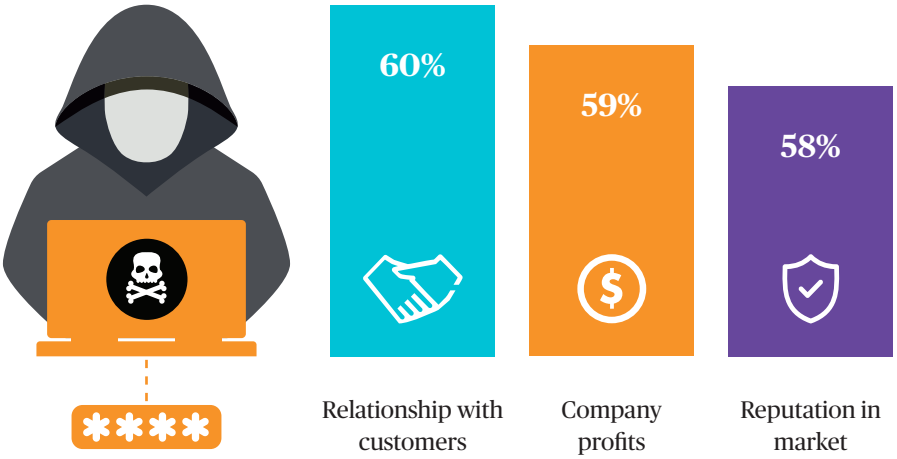
An employee at a hardware store ignored internal policies and procedures and opened a seemingly innocuous file attached to an email. The next day, the hardware store's stock order and cash registers started to malfunction, and business trade was impaired as a result of the network failure.

The hardware store incurred over RM 420,000 in forensic investigation and restoration services. They also had additional increased working costs of RM 85,000 and suffered a business income loss estimated at RM 210,000 from the impaired operations.

Customers Have Most to Lose

In the event of a major cyber incident, businesses indicated that customers followed by company profits and reputation in the market would be most affected - with around three in five SMEs saying these areas would be severely to moderately impacted.

Key impacts SMEs expect to face following a major cyber incident



Case Study: Ransomware attack

Industry:
Construction

Annual revenue approximately:
RM 14.7 million

Costs up to:
RM 1.4 million

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.

The Best Laid Plans...?

Three out of five (61%) of Malaysia's SMEs say they have a data breach response plan. However, there is a clear difference in cyber preparedness among SMEs of different sizes. When the data is broken down by the number of employees, 77% of SMEs with 100-249 employees have a data breach contingency plan compared with 53% in smaller SMEs with fewer than 50 employees.

Malaysian SMEs were faster to respond to cyber incidents than other markets, with 67% resuming operations within 12 hours of a cyber incident. Two-thirds (66%) indicated that everyone involved knew the proper protocol and crisis response went ahead as planned.

Despite these positive indications, many of these incidents could have been avoided. 61% of respondents said that the cyber incidents they suffered stemmed from a previously identified risk. 16% took no action following a data breach beyond recovering affected files, and 60% of respondents said they were unaware of all the cyber threats they face.

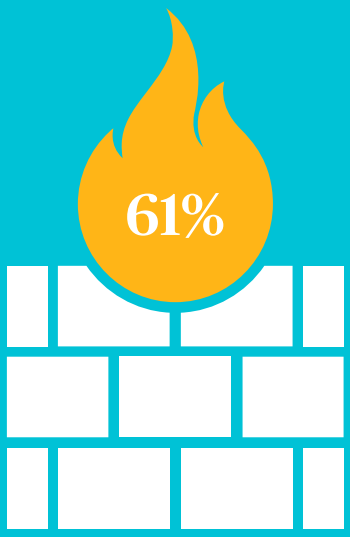
Actions following a data breach

63% increased security protection and processes around the data

55% notified affected parties of the data breach

44% reviewed security protection following a cyber incident but took no further action

16% took no actions beyond recovering the files



"61% of respondents said that the cyber incidents they suffered stemmed from a previously identified risk."

How Insurance Can Help

Insurance does not figure prominently as part of the risk mitigation tool-kit for SMEs in Malaysia. From our sales data, the uptake of cyber insurance is low perhaps either because SMEs do not understand the benefits of a stand alone cyber insurance policy or that they are under the mistaken assumption that their existing basic business insurance covers cyber incidents, when the majority of such policies do not.

70% of SMEs agree that the insurance industry has an important role to play in helping businesses protect themselves against cyber risk. However, 60% also believe that the industry is not moving fast enough to keep up with the rapidly evolving nature of cyber risk. 73% feel that insurance providers should do more to develop solutions to meet business needs.

Following a cyber incident, SMEs in Malaysia most value legal advice (70%) and regulatory advice (69%) provided by the insurer.

SMEs with cyber risk insurance to mitigate cyber risk

32%

purchased cyber risk insurance before an incident

38%

purchased cyber risk insurance only after experiencing an incident

Dwelling on the Downside

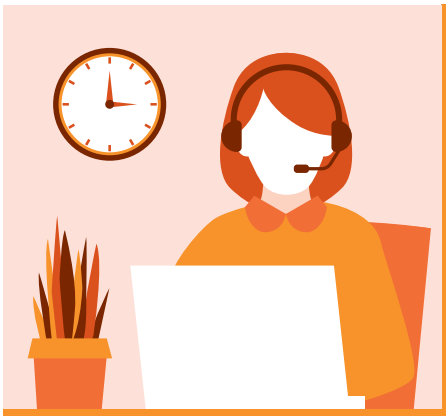
Persistent threats can last inside SME networks for years. Dwell time – the amount of time a threat spends inside of a network before an organisation discovers and removes it – has become a significant problem for SMEs, according to a U.S. report released by Infocyte in July 2019. Dwell time for attacks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

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

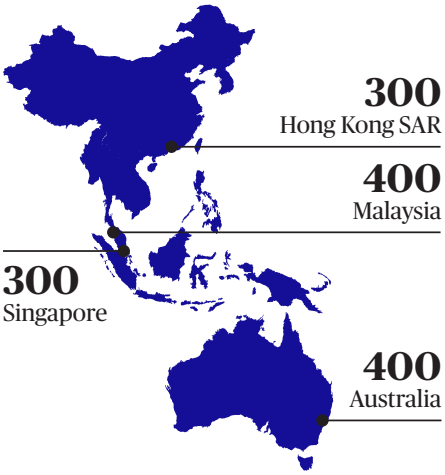
Chubb works with cyber phishing experts to offer phishing awareness assessments. The assessments include two simulated real-life phishing scenarios that are conducted over the course of four months for up to 500 individual email addresses.

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.

About the Research

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



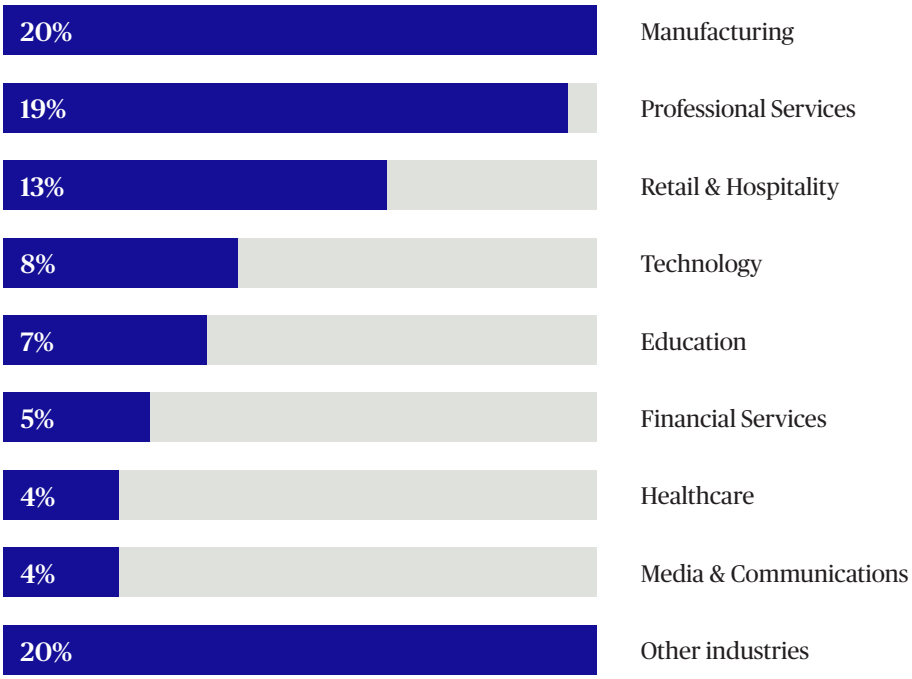
Respondents comprised of;

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 - Over half of SMEs admit their current plan is ad hoc and not documented. Of those that do have a plan in place, just about half 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's operation in Malaysia (Chubb Insurance Malaysia Berhad) provides a comprehensive range of general insurance solutions for individuals, families and businesses, both large and small through a multitude of distribution channels. With a strong underwriting culture, the company offers responsive service and market leadership built on financial strength. Chubb in Malaysia has a network of 23 branches and more than 2,600 agents.

Contact Us

Chubb Insurance Malaysia Berhad (9827-A)

(Licensed under the Financial Services Act 2013 and regulated by Bank Negara Malaysia)

Wisma Chubb 38 Jalan Sultan Ismail
50250 Kuala Lumpur Malaysia

O +60 3 2058 3000
F +60 3 2058 3333

www.chubb.com/my

Chubb. Insured.℠

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.