Ignorance is Risk

Hong Kong SAR SME Cyber Preparedness Report 2019

CHUBB®

Contents

Welcome

Mr Andrew Taylor,
Cyber Underwriting Manager,
Chubb Asia Pacific

Following Chubb's inaugural SME Cyber Preparedness Survey for Hong Kong SAR (Hong Kong) in 2018, we are pleased to bring you the second edition of this report.

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 Hong Kong[1] they will be hardest hit without good risk mitigation, incident response planning and the consideration of cyber insurance.

In 2019, three-quarters (76%) of SMEs we surveyed said they had experienced a cyber incident. Despite the increased frequency of cyber incidents, about a third (34%) of SMEs reviewed their security protection but took no further action after a cyber incident, with only 11% making any attempt to recover breached data files. This is compounded by the fact that almost half (47%) of SME leaders say their employees do not recognise the severity of cyber risks to their businesses. As employees are usually the first and best form of cyber defence, this is a significant missed opportunity.

We hope that you find this report useful and the insights will contribute to reducing cyber risk for SMEs in Hong Kong.

[1] http://multimedia.scmp.com/native/infographics/article/3005155/sme-growth-guide/

Ignorance is Risk

Cyber Risk Landscape

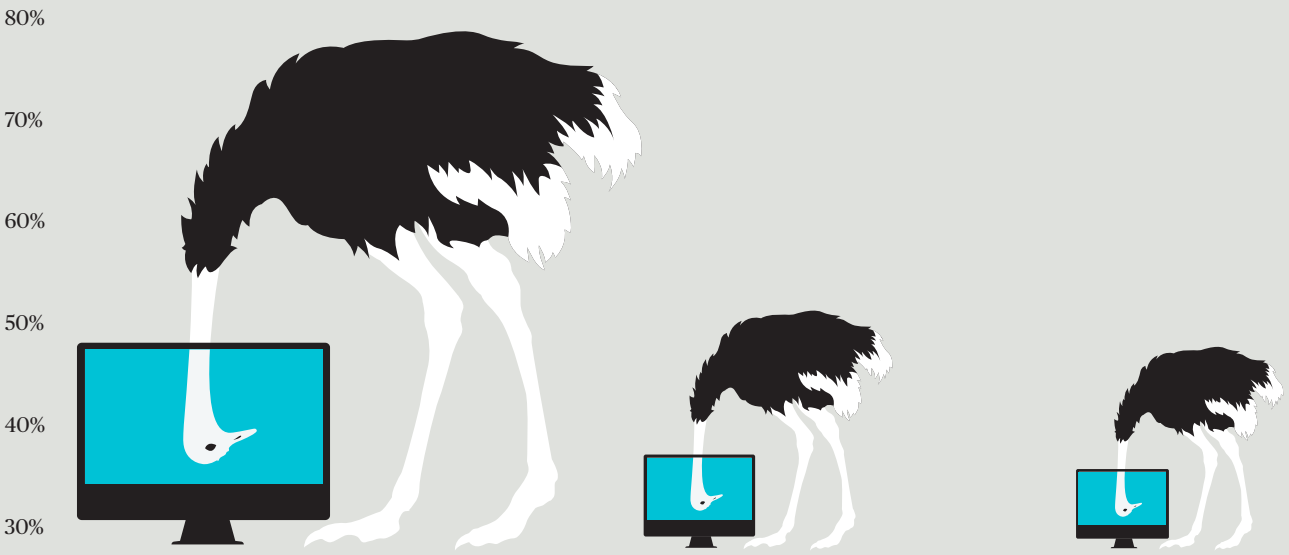
More than 9,000 cyber attacks occurred in Hong Kong, costing companies HK$2.2 billion in 2018.

Hong Kong has launched the Cyber Resilience Assessment Framework (C-RAF) to improve data security in the financial sector[2].

Digital Economy

Hong Kong has a rapidly expanding digital economy forecast to be worth US$5.8 billion by 2022[3].

Key Survey Highlights



76%

76% of Hong Kong SMEs were victims of cyber incidents in the past year.

47%

47% of SME leaders in Hong Kong say that their employees do not recognise the severity of cyber risks to the business.

45%

45% of Hong Kong SMEs do not fully understand the insurance solutions available and the role of insurance in cyber risk management.

[2] https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf

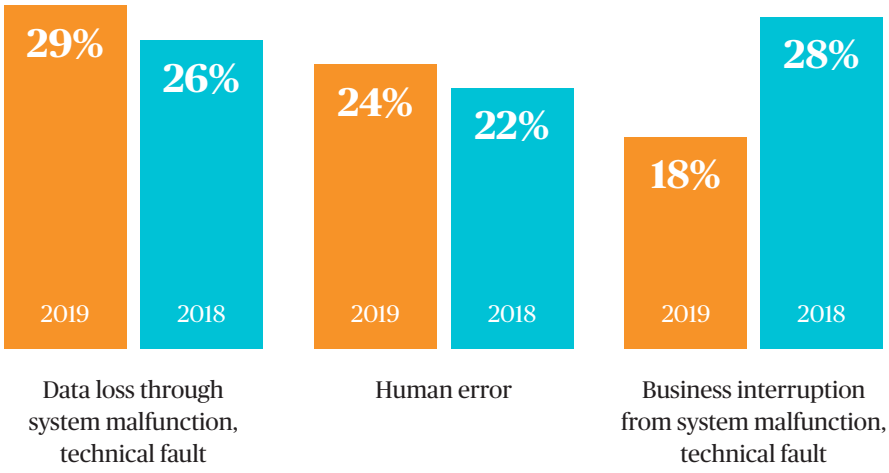
[3] https://www.scmp.com/business/companies/article/2149582/hong-Kong SARs-digital-spending-surge-us58b-2022-consumers-turn

Risky Business

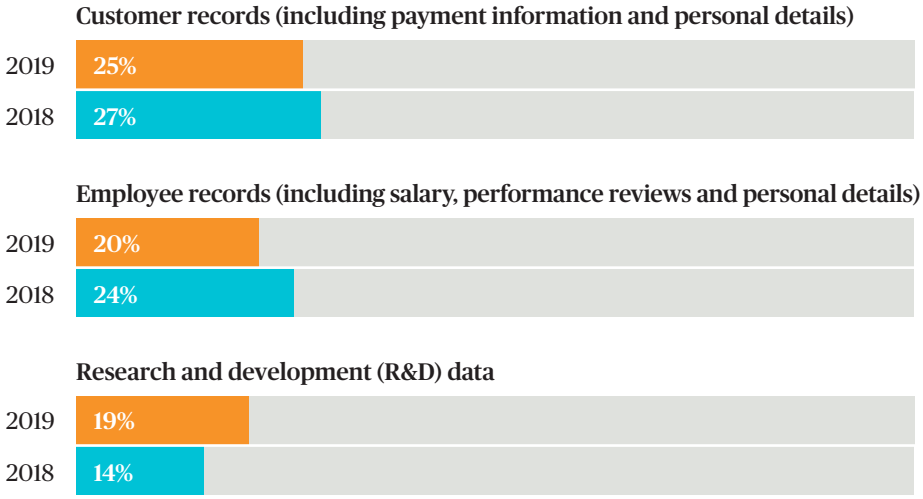
Our 2019 survey found that 76% of SMEs experienced cyber incidents in the past 12 months, a slight increase from 71% in 2018.

The most commonly experienced types of cyber incidents were data loss through system malfunction and technical fault (29%) followed by human error (24%) and business interruption from system malfunction and technical fault (18%).

Alarming Facts:
Most commonly experienced types of cyber incidents in 2019 vs 2018



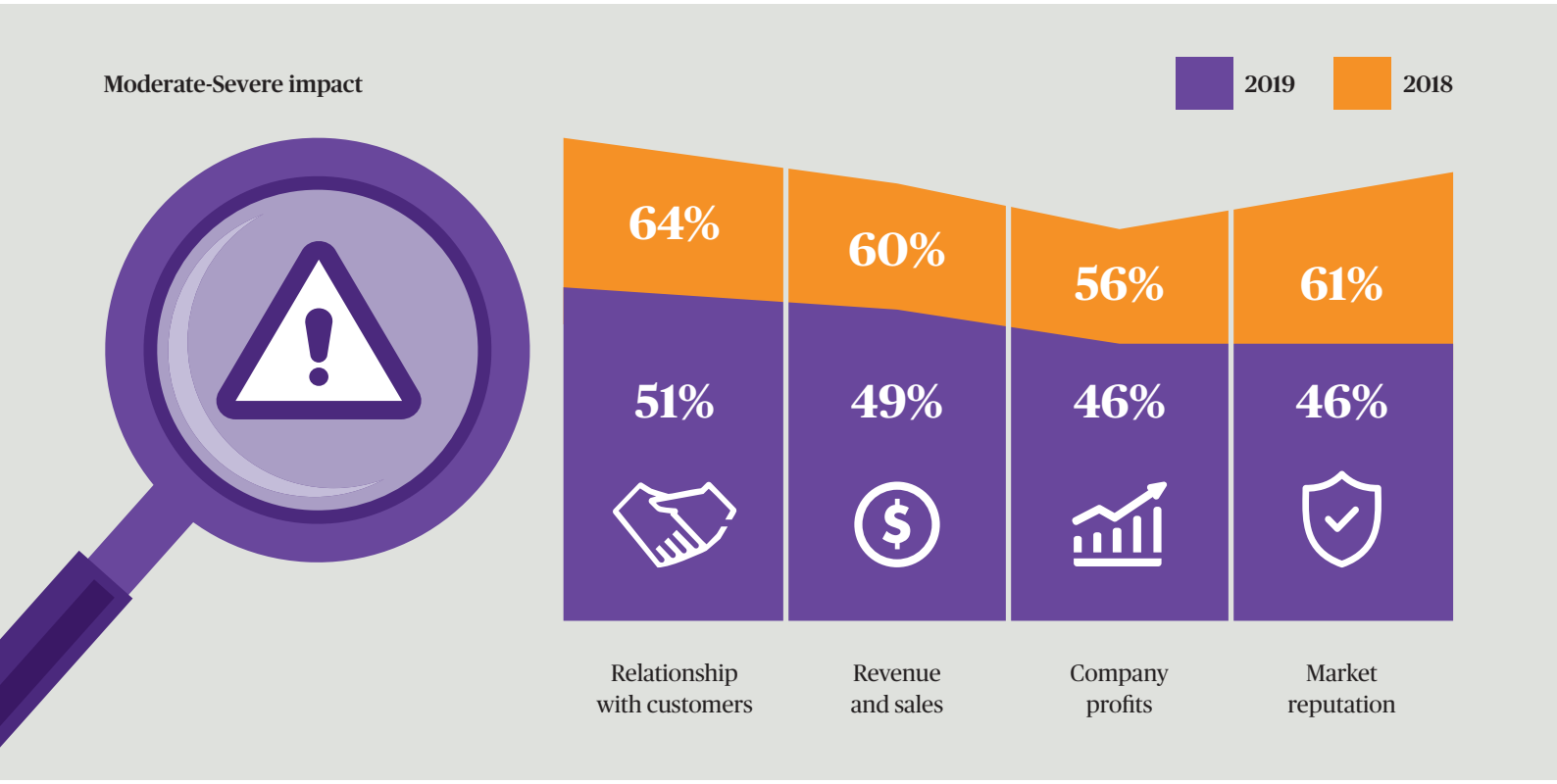
The most commonly breached data files were similar to those in 2018



The Customer Comes Last

In the wake of a major cyber incident, SMEs are most concerned about the effects on their relationships with customers (51%), but less so than in 2018 (64%). This is followed by worries around revenue and sales (49%), company profits (46%) and market reputation (46%).

Despite these concerns, after a cyber incident, more than a third (34%) of SMEs reviewed their security protection but took no further action, with 11% taking no further action beyond recovering the files.



Employ Your Best Defence

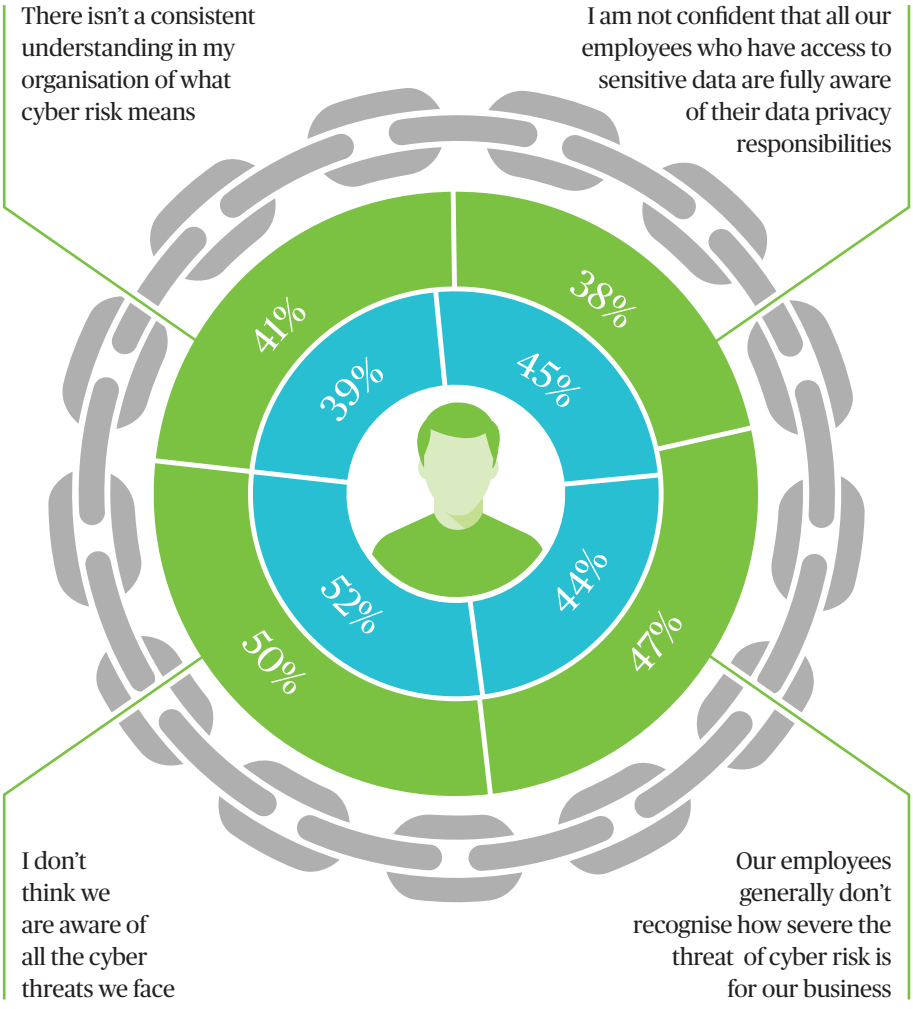
Employees are both the biggest risk and greatest opportunity for SMEs looking to improve their cyber defences. Being the organisation's first line of defence, they play a critical role in detecting and potentially preventing data breaches.

Currently, half (50%) of Hong Kong SME leaders do not think that employees are aware of all the cyber threats they face.

Almost half (47%) say their employees do not recognise the severity of cyber risks to their businesses. 41% say there is no consistent understanding in their organisation of what cyber risk means therefore, building awareness of cyber risks among employees is more important than ever.

Moreover, 38% of SME leaders are not confident that all their employees who have access to sensitive data are fully aware of their data privacy responsibility.

Are employees ready to be the company's best defence?



Case Study: Ransomware attack

Industry:
Construction

Annual revenue approximately:
HK$27.4 million

Costs over:
HK$2.6 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.

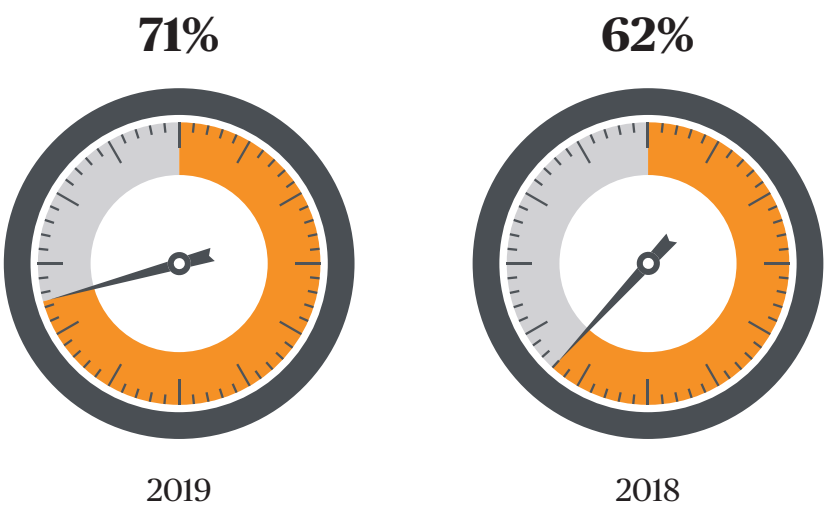
The Need for Speed

SMEs in Hong Kong were faster to respond to cyber incidents compared with a year ago, with 71% of businesses resuming operations within 12 hours following a cyber incident. This is a significant increase from 62% in 2018.

More than two-thirds (69%) of SMEs had communicated to affected stakeholders within 72 hours, compared with 62% in 2018. In the event of a cyber incident, 64% of SME leaders said that employees involved knew the proper contingency plans and the crisis response went ahead as planned, compared with 56% in 2018.

While most would assume having better response rates means having better data breach response plans, this is not always the case. Although the study reveals that Hong Kong businesses have improved incident response times, more than half (54%) still do not have a proper data breach response plan in place.

More businesses resumed operations within 12 hours following a cyber 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.

How Insurance Can Help

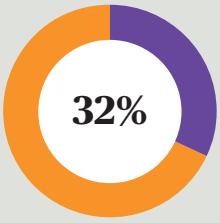
This year's study reveals that more SMEs are beginning to understand the gravity of cyber risks, with 68% indicating that they had learned from past cyber incidents so that similar situations would be less likely to occur in future, compared with 59% in 2018.

59% of SME leaders in Hong Kong also increased security protection and improved processes around these data files following a cyber incident, compared with 46% in 2018.

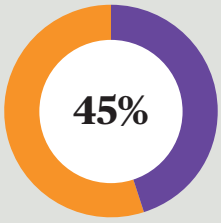
While it is evident that more SMEs in Hong Kong are becoming aware of cyber risks, proactive protection measures remain largely inadequate. Nearly a third (32%) of SMEs did not purchase cyber risk insurance before or after experiencing a cyber breach. Although this is a significant drop from 53% in 2018, close to half (45%) of SMEs do not fully understand the insurance solutions available and the role of insurance in cyber risk management. Following a cyber incident, SMEs most value regulatory advice (60%), followed by speed of incident response (57%) and accessibility to incident response services (57%).

SMEs covered by cyber risk insurance	2019	2018
Yes - we are currently covered by this insurance	33%	26%
Yes - we have taken out this insurance in the past but are no longer covered by it	16%	20%
No - we have never been covered by this type of insurance	47%	48%
Don't know	4%	7%

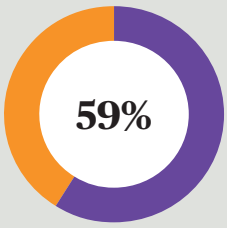
Actions taken following a cyber incident



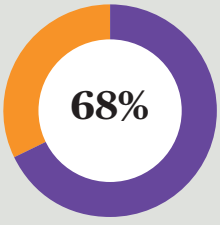
32% of SMEs did not purchase cyber risk insurance before or after experiencing a cyber breach.



45% of SMEs do not fully understand the insurance solutions available and the role of insurance in cyber risk management.



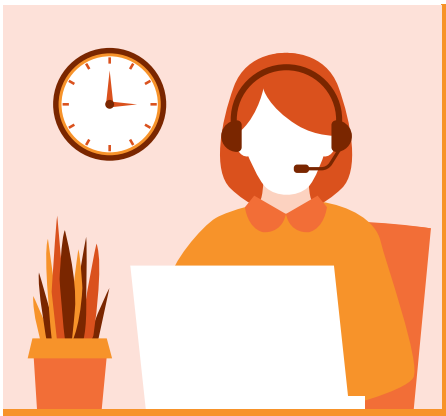
59% of SME leaders increased security protection and improved processes around data files following a cyber incident, compared to 46% in 2018.



68% say they learned from past cyber incidents so that similar situations are less likely to occur in future, as compared to 59% in 2018.

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

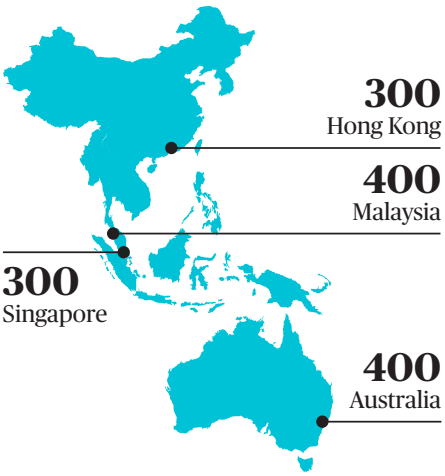
Chubb works with cyber phishing experts to offer phishing awareness assessments. The assessments include two simulated real-life phishing scenarios that are conducted over the course of four months for up to 500 individual email addresses.

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%

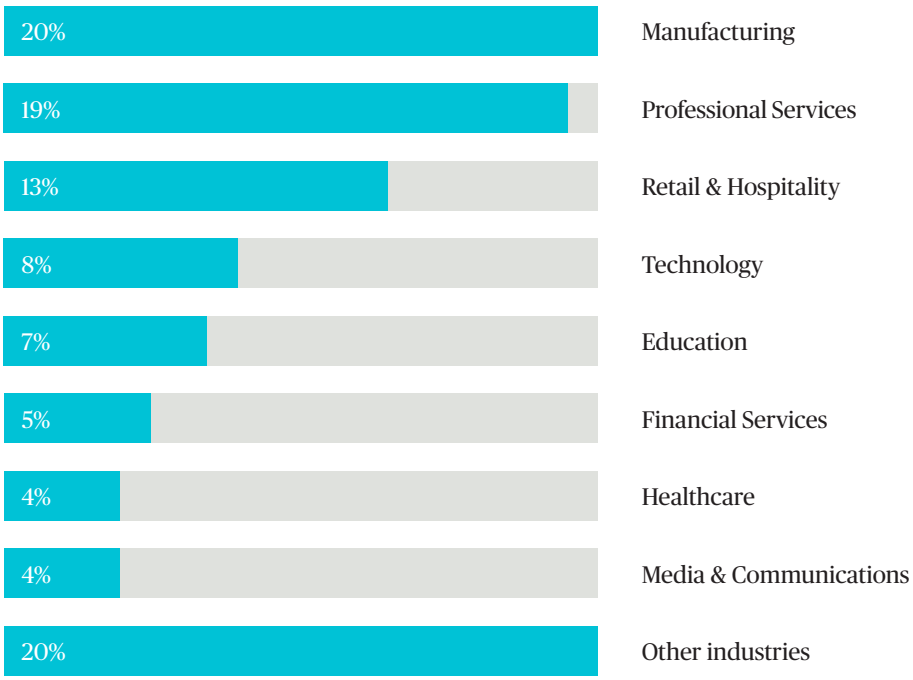
Board-level executive

18%

Senior managers or directors below board level

from SMEs between 2 to 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 - 37% of Hong Kong SMEs admitted their current plan is ad hoc and not documented. Of those that do have a plan in place, only 47% 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 in Hong Kong SAR

Chubb is the world's largest publicly traded property and casualty insurer. With both general and life insurance operations, Chubb has been present in Hong Kong SAR for more than 90 years via acquisitions by its predecessor companies. Its general insurance operation in Hong Kong SAR (Chubb Insurance Hong Kong Limited) is a niche and specialist general insurer. The company's product offerings include property, casualty, marine, financial lines and consumer lines designed for large corporates, midsized commercial & small business enterprises as well as retail customers. Over the years, it has established strong client relationships by offering responsive service, developing innovative products and providing market leadership built on financial strength.

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

Contact Us

Chubb Insurance Hong Kong Limited
39/F, One Taikoo Place,
979 King's Road,
Quarry Bay, Hong Kong
O +852 3191 6800
F +852 2560 3565
www.chubb.com/hk

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.