CISCO
SECURE

The bridge to possible

Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense

September 2021

Contents

Foreword

Cybersecurity is Foundational in Our New Digital Normal

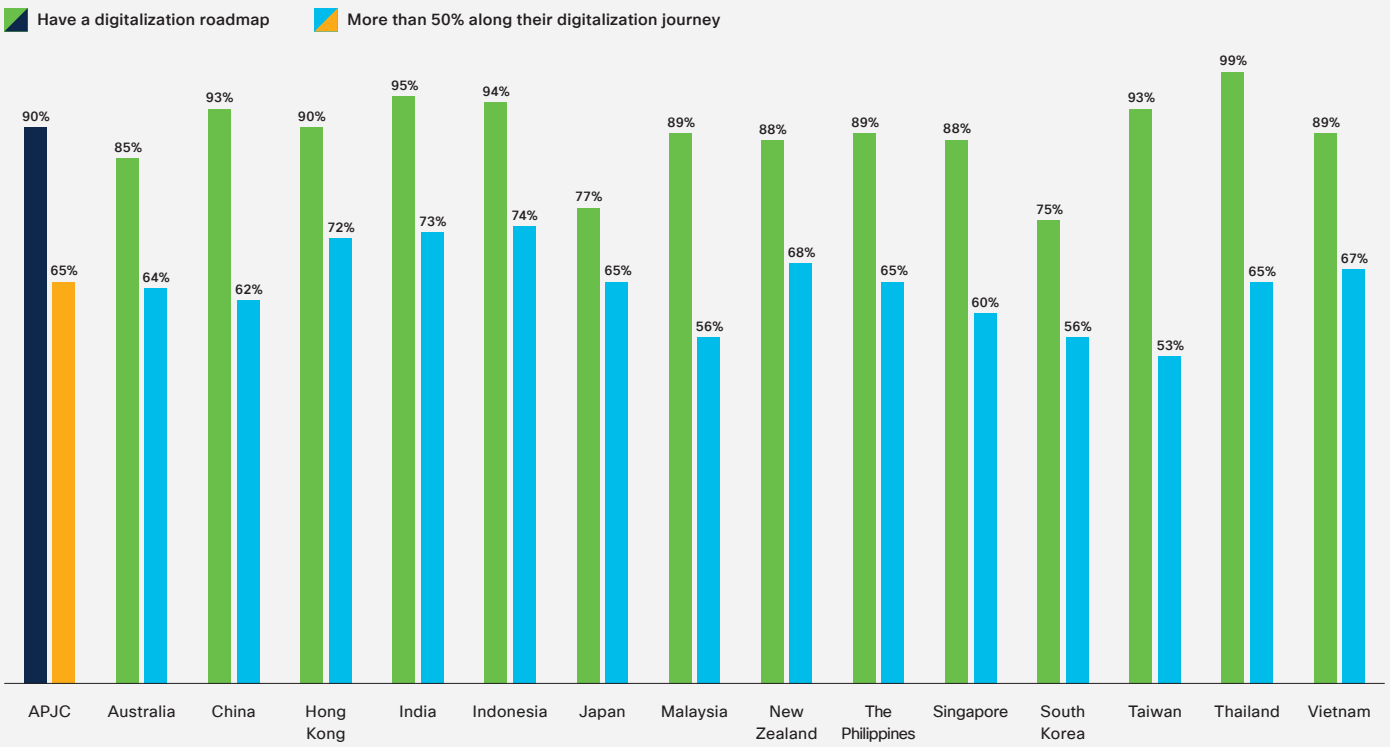
The COVID-19 pandemic has fueled a critical need to invest in technology solutions and capabilities among organizations of all sizes. At the start of the pandemic, businesses turned to technology for survival. The aim was to operate and continue to serve customers even as entire economies went into lockdowns, and the majority of the workforce transitioned to remote working arrangements. Having witnessed first-hand the positive impact that technology can have, and with countries now looking to gradually re-open economies, all organizations are keen to leverage it to thrive in the new normal.

This is especially true for small and medium sized businesses (SMBs) across Asia Pacific. We commissioned independent research to better understand technology trends, especially in relation to cybersecurity, among SMBs.

The research finds that 94% of SMBs in the region have adopted some form of technology. Even more encouraging is that the vast majority (90%) have a digitalization roadmap. This is accentuated in Thailand where 99% have a roadmap, and in India where 95% of SMBs have one. The numbers are slightly lower in mature economies like Japan and Korea though, where 77% and 75% of SMBs respectively said they have a digitalization roadmap or strategy.

When it comes to implementation, 65% of SMBs are well-along their digitalization journey, having deployed more than 50% of their digitalization plans. SMBs in Indonesia, India and Hong Kong SAR are at least half-way along their journey. By contrast, Taiwan, Malaysia, and South Korea have the furthest to go.

APJC SMB DIGITALIZATION PROGRESS BY MARKET



As digitalization among SMBs in the region has picked up pace, there is an increased focus on cybersecurity, not least because the increase in attack surface available to hackers and malicious actors mirrors the pace of digitalization. It is not a surprise that three-quarters of SMBs said they are more concerned about cybersecurity today than they were 12 months ago. This is significant. But it is also encouraging because it demonstrates increased levels of awareness of cyber risk among SMBs.

The fears are well grounded. Our research shows more than half (56%) of Asia Pacific SMBs have experienced a cyber incident in the past year with many falling victim to cybercrime – 85% suffered a malware attack. As a result of these incidents, malicious actors are getting their hands on valuable data ranging from customer information (75%), internal emails (62%), employee data (61%) to intellectual property (61%) and, financial details (61%).

This is having a tangible impact on SMBs with 62% of respondents saying a cyber incident disrupted their operations and 61% noting that it resulted in a loss of revenue.

In addition, 57% saw a loss of trust with customers, while 66% said that a cyber incident affected the company's reputation negatively. Though unquantifiable, a decline in reputation and erosion of trust can have disastrous consequences for any business.

On the positive side, SMBs are aware of the challenge. In fact, many are taking a more planned approach to battle it out with strategic initiatives to understand and improve their security posture. Our research shows 81% have carried out scenario planning and/or simulations for potential cybersecurity incidents in the past 12 months. The majority (81%) have a response plan in place while 82% have a recovery plan ready to roll-out if needed. We will be taking a deeper dive to measure what cadence on this front has a more positive effect on security in the upcoming Security Outcomes Study.

We hope this report will offer useful insights into the cybersecurity challenges faced by SMBs in Asia Pacific. As SMBs across the region gear up for a hybrid work future, with employees straddling between work at the office and remotely, which adds another layer of complexity to tackling cybersecurity, we hope that all those who read it can benefit from the practical suggestions provided to improve cyber preparedness and resilience.

In an increasingly digital world, it highlights the critical importance for all SMBs to apply time and resources to manage and overcome their cybersecurity barriers to build a resilient, future-proof, and ultimately successful business.

Kerry Singleton
Managing Director, Cybersecurity, Asia Pacific, Japan and China, Cisco

Michiko Kamata
Head of Small Business Growth Office, Asia Pacific, Japan and Greater China, Cisco

Bidhan Roy
Managing Director, Commercial Enterprise & Mid-market Segment, Asia Pacific, Japan and Greater China, Cisco

Introduction

This report presents and analyses the findings of a survey of business and IT leaders with cybersecurity responsibilities at over 3,700 SMBs across Asia Pacific. The field work was undertaken between April and July 2021.

It aims to provide a deeper understanding of the evolving cybersecurity challenges facing SMBs in the region, how SMB leaders are approaching cyber preparedness, and recommendations for improving it.

The survey respondents are from 14 markets in the region, including Australia, China, Hong Kong, India, Indonesia, Japan, New Zealand, Malaysia, Singapore, South Korea, Taiwan, Thailand, the Philippines, and Vietnam.

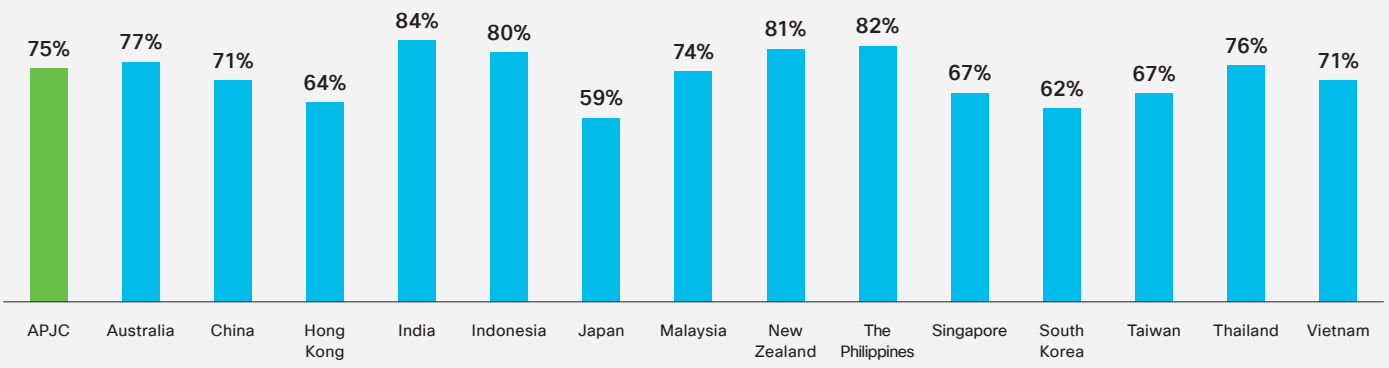
The SMBs surveyed represent a broad range of industries including Business Services; Construction; Education; Engineering; Design and Architecture; Financial Services; Food and Beverage; Healthcare; Manufacturing; Media and Communications; Natural Resources; Personal Care Services; Professional Services; Real Estate; Retail; Technology Services; Travel; Transportation; and Wholesaling.

(IN)secure about security

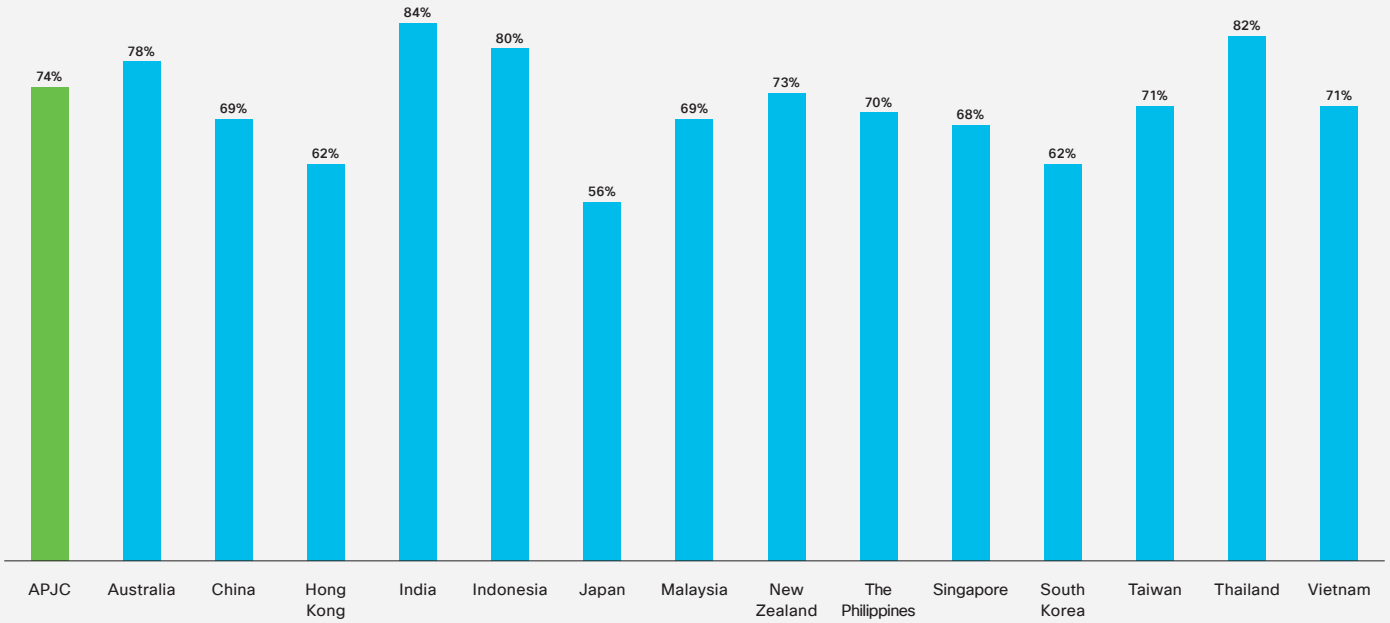
With the business environment evolving rapidly, the cyber threat landscape has also changed significantly over the past year. This is making SMBs across the region more apprehensive about cybersecurity risks. Three quarters (75%) of SMBs in the region said they are more worried about cybersecurity now than 12 months ago, with the greatest concerns being among SMBs in India (84%), the Philippines (82%), New Zealand (81%), Indonesia (80%), and Australia (77%).

The worries are being driven in part by a growing realization of the implications that a serious incident could have on their business. Three quarters (74%) of the SMB leaders surveyed said a major cyber incident could spell the end of their organization.

% OF SMBS MORE WORRIED ABOUT CYBERSECURITY NOW THAN 12 MONTHS AGO



% SMBS THAT BELIEVE A SERIOUS CYBER INCIDENT COULD END THEIR BUSINESS



SMBs are also increasingly aware of where the biggest threats come from. The research highlights that phishing is seen as the top threat by SMBs across the region, with 43% ranking it first. Phishing is a tactic where hackers masquerade as a trustworthy entity to try and get the user to open a specific digital communication sent to them, such as an email, hyperlink, or instant message. Though this is an old tactic, it remains popular due to its simplicity and effectiveness.

At the same time, the rapidly evolving environment, triggered by the pandemic, has seen a huge change in the way SMBs operate. With a mass shift to remote working, a sizable proportion of employees are connecting to companies' networks and accessing information from outside the office. Many are using personal devices to do so as well. SMBs highlighted that unsecured laptops (20% ranked #1), targeted attacks by malicious actors (19% ranked #1) and personal devices (12% ranked #1) are among the top threats to their overall security.

WHICH OF THE BELOW DO YOU BELIEVE POSES THE BIGGEST RISK OF CYBER ATTACKS FOR YOUR ORGANIZATION?

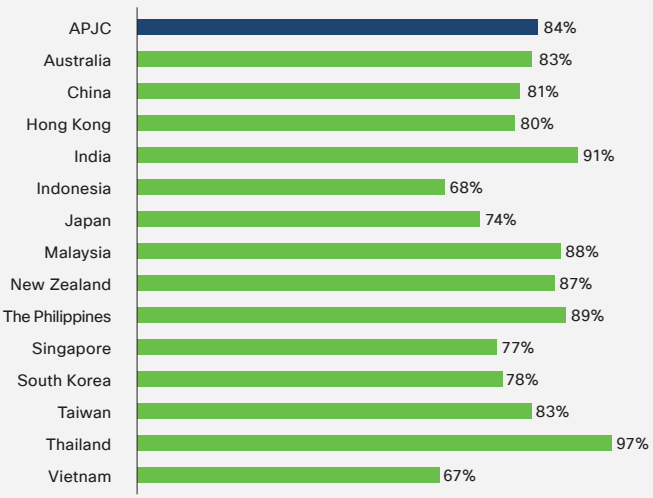
Exposed and under attack

The fears SMBs expressed are well founded. More than four out of five (84%) SMBs across Asia Pacific feel exposed to cyber threats, with one third feeling very exposed. This is not least because many SMBs have experienced a cyber incident. Our research shows 56% of Asia Pacific SMBs have suffered a cyber incident in the past 12 months.

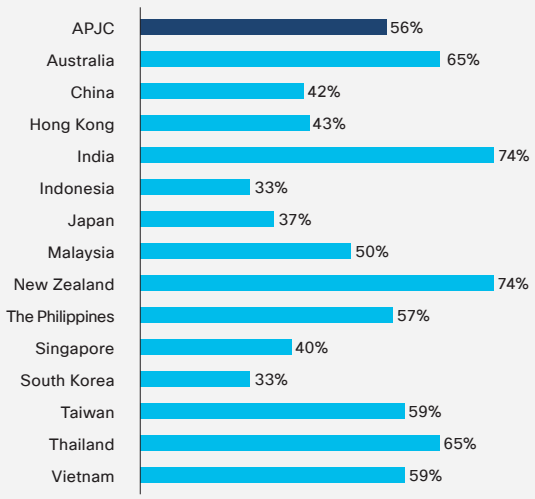
The numbers vary across the region, though, with 74% of SMBs in India and New Zealand experiencing an incident, while only 33% in Indonesia and South Korea and 37% in Japan said they suffered incidents.

In addition, nearly half said the cyber incidents they have experienced have increased during the pandemic with India (70%) and New Zealand (61%) experiencing the biggest uplift followed by the Philippines (53%), Vietnam (53%) and Australia (50%).

% SMBS THAT FEEL EXPOSED TO CYBER THREATS



% SMBS THAT SUFFERED A CYBER INCIDENT IN PAST 12 MONTHS

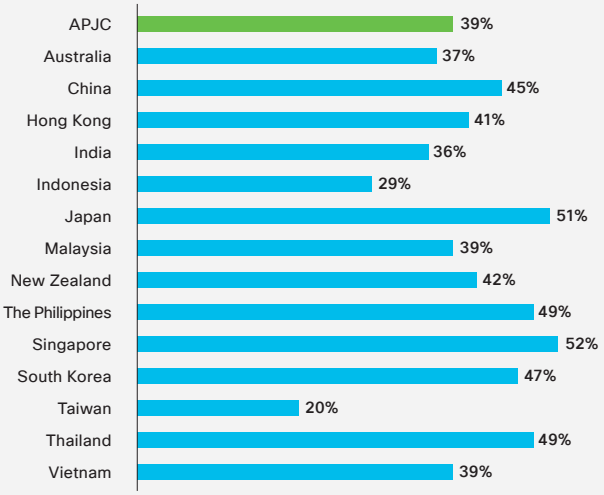


Among those that suffered a cyber incident, a third (33%) ranked not having a cybersecurity solution as the top reason. What was telling though, is that an even greater number of SMBs (39%) said the number one factor was that their cybersecurity solutions were inadequate to detect and prevent an attack. This highlights the fact that having the right technology is critical to building a strong security posture. This was also a key finding of Cisco's *Security Outcomes Study* which also took a deeper dive into the SMB sector.

Of those that experienced incidents, SMBs saw a myriad of different ways in which attackers tried to infiltrate their systems. Malware attacks, which affected 85% of SMBs, led the charts.

The increased adoption and usage of devices such as computers, tablets and smartphones has seen attackers increasingly trying to deploy malware on these systems.

% THAT RANKED CYBERSECURITY SOLUTIONS BEING INADEQUATE TO DETECT AND PREVENT AN ATTACK AS TOP FACTOR FOR SUFFERING CYBER INCIDENTS



SMBs are especially being targeted by attackers looking to deploy malicious software with the intention of either disrupting, damaging, or gaining unauthorized access to the devices being targeted.

The attackers' interest in SMBs can be attributed to a few key aspects. Firstly, there is a perceived notion amongst the hacking community that SMBs are relatively weaker on the cybersecurity front compared to large organizations making them an attractive target. Second, SMBs are increasingly working with larger corporations in some form or the other. The hope hackers have is that if they are able to infiltrate a particular SMB's network, they may be able to use that as a launch pad to then access the network of a larger corporation that this SMB may be working or carrying out digital transactions and digital communications with.

According to the respondents, malware attacks were followed by phishing, with 70% saying they experienced such attacks. Other leading forms of attacks that respondents reported include DNS Tunneling (68%), Denial of Service (64%), SQL Injection (62%), Man-in-the-Middle (61%) and Zero Day Exploit (60%).

Definitions

Denial of Service Attack: attempts to shut down a machine or network, making it inaccessible to its intended users, often web servers of banks, media companies, or government organizations

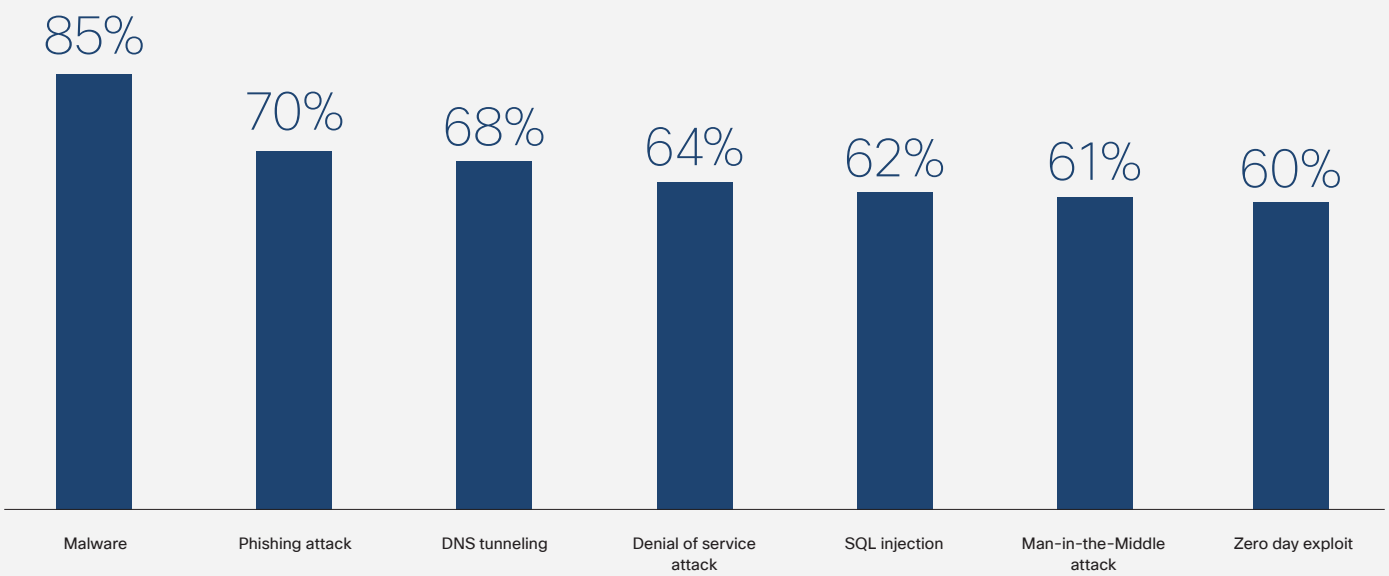
DNS Tunneling: encodes the data of other programs or protocols in DNS queries and responses

SQL Injection: used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker)

Man-in-the-Middle Attack: when a perpetrator positions himself in a conversation between a user and an application making it appear as if a normal exchange of information is underway with the goal of stealing personal information

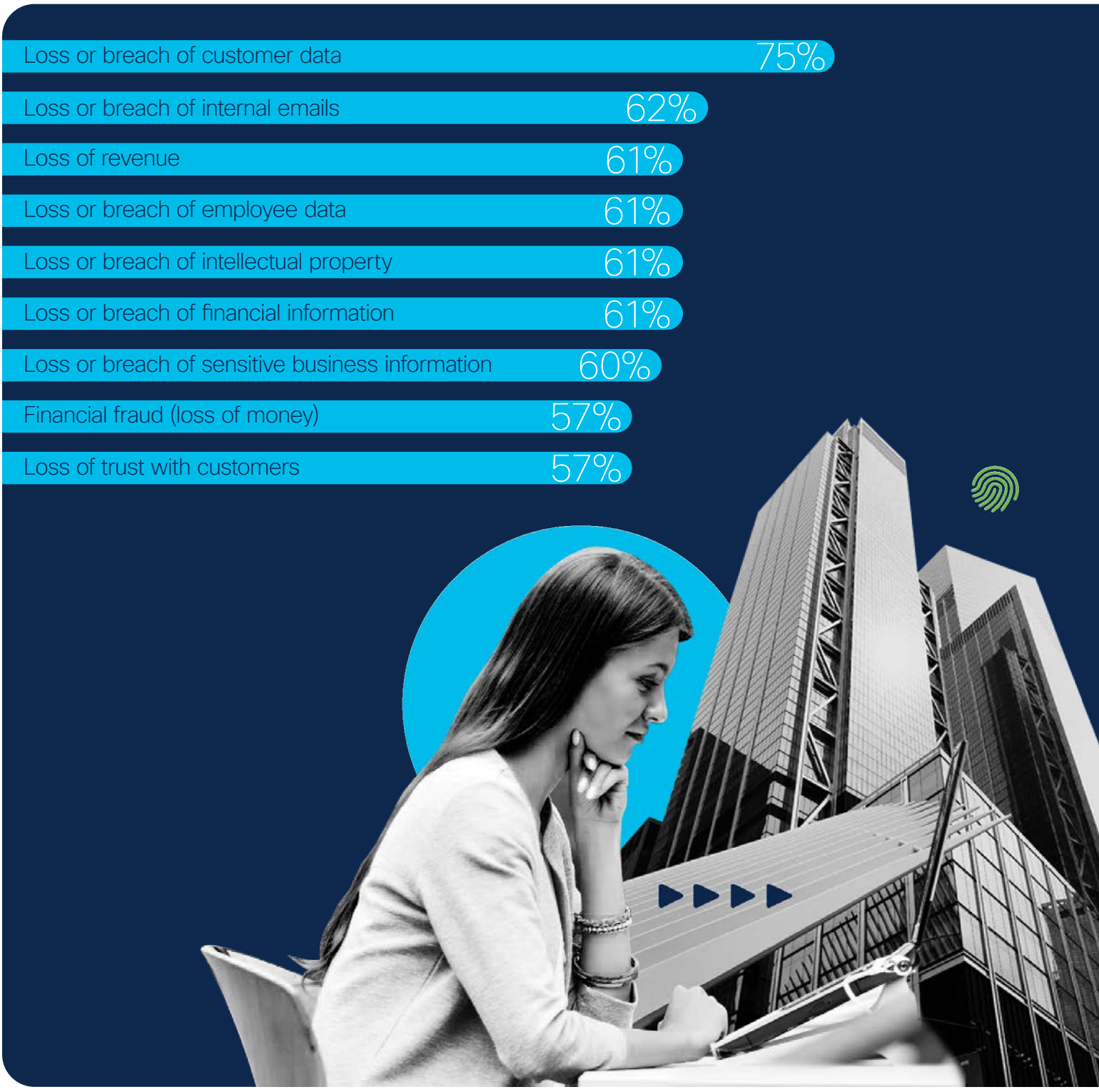
Zero Day Exploit: an attack on a recently-discovered software vulnerability to steal data or cause damage

TYPES OF CYBER INCIDENTS APJC SMBS HAVE EXPERIENCED IN PAST 12 MONTHS



Counting the costs

The majority of SMBs that suffered an incident experienced losses of some kind. A whopping 75% of SMBs that experienced an incident said it resulted in loss of customer data. Six in 10 SMBs that suffered an incident said it negatively impacted their revenue.



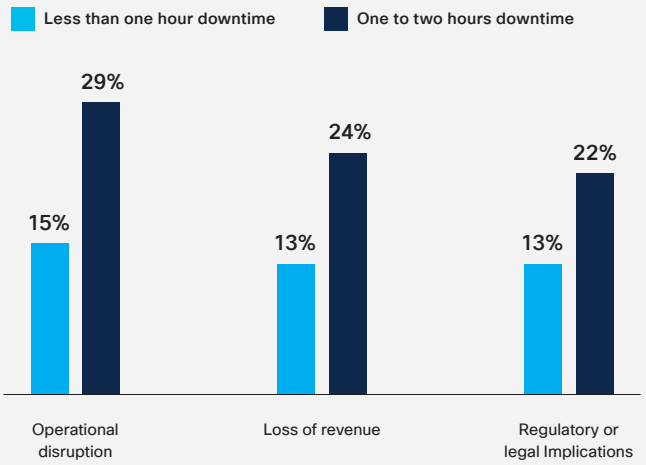
Every second counts when it comes to implications on business

Cybersecurity is a game of odds. The reality, though, is that the odds are tilted in favour of the malicious actors. They are constantly attacking their targets. Those under attack need to win every single time. The attackers on the other hand need to get through the defenses just once to win.

Add to the mix the fact that it does take some time for companies to detect, investigate and remediate a cyber incident. This often gives malicious actors a kind of a head start to be able to cause damage.

The challenge that SMBs are now facing is that we are living in a hyper-connected, digital-first world where customers want instant gratification. This means they have little leeway, if any, for a cybersecurity incident to disrupt their operations. They need to be able to detect, investigate, and block or remediate any cyber incident as quickly as possible.

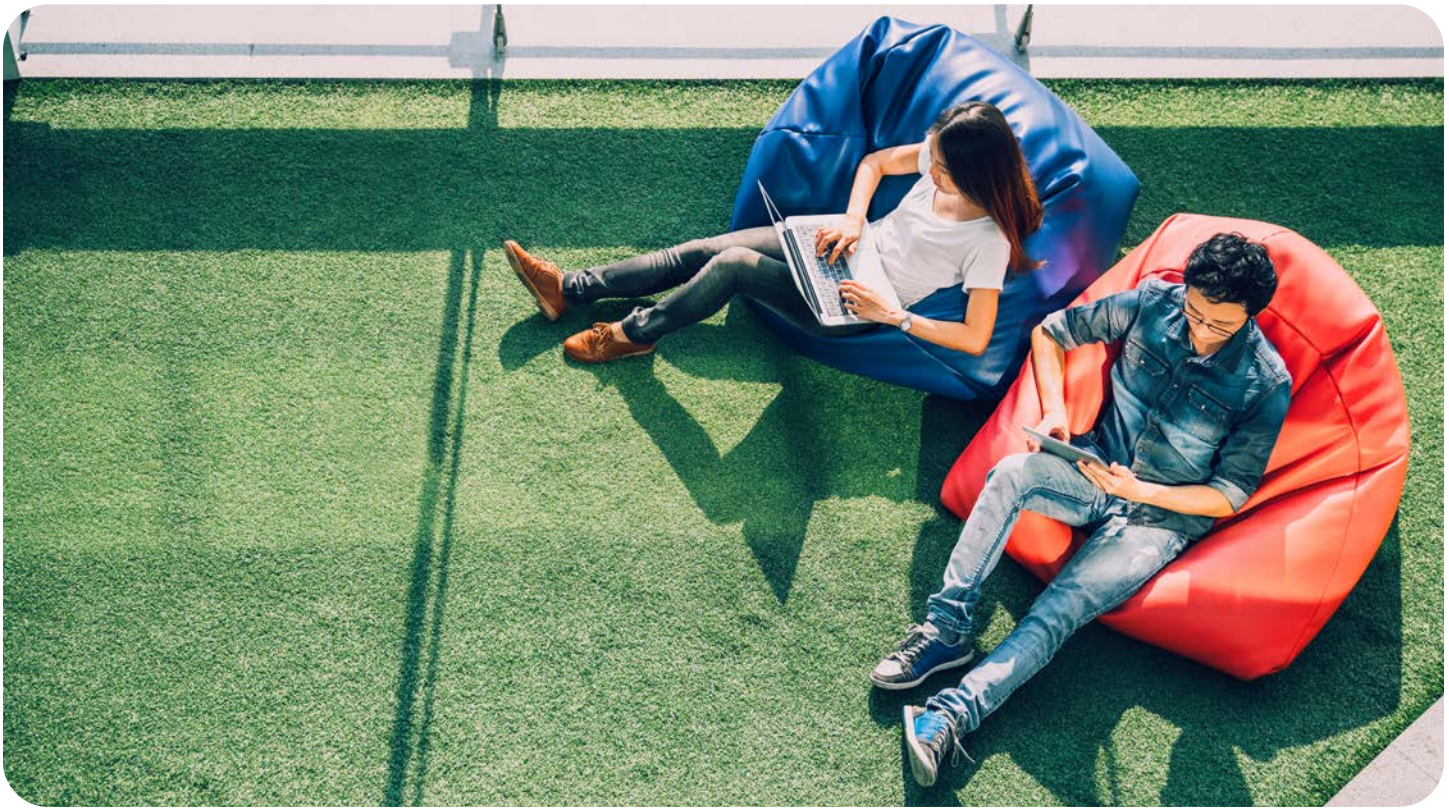
ESCALATION OF IMPACT DUE TO LENGTH OF DOWNTIME*



* For market-wide breakdown of each of these metrics, please refer to the charts in Appendix A

The research highlights that 15% of SMBs in Asia Pacific said that a downtime of even less than an hour results in operational disruption, while 29% said a downtime of between 1 to 2 hours can cause the same. The impact can be quantified as 13% of respondents said a downtime of anything less than an hour will severely impact revenue, while 24% said a downtime of 1 to 2 hours can cause the same.

What is most telling is the fact that one in 10 SMBs said a downtime of one day will result in a closure of their organization.



At the same time, as countries start to introduce and implement cybersecurity guidelines and regulations, downtime caused by cyber incidents also results in legal implications. This trend is already starting to emerge, with 13% of SMBs saying a downtime of less than an hour will have legal implications for them, while 22% said a downtime of between 1 to 2 hours can cause the same.

Just how big a challenge this is for SMBs is highlighted by the fact that only 15% of the respondents to the research said they can detect a cyber incident within an hour. The number of those that can remediate it within an hour is even lower at 10%.

% SMBS AND LENGTH OF TIME TAKEN TO DETECT AND REMEDIATE AN INCIDENT

	APJC	Australia	China	Hong Kong	India	Indonesia	Japan	Malaysia	New Zealand	The Philippines	Singapore	South Korea	Taiwan	Thailand	Vietnam
The average length of time it took to detect an incident															
Under one hour	15%	8%	13%	11%	17%	17%	16%	17%	24%	9%	8%	11%	25%	13%	8%
One to two hours	30%	28%	36%	28%	34%	31%	18%	32%	28%	28%	16%	34%	16%	33%	33%
The average length of time it took to remediate the incident															
Under one hour	10%	6%	8%	3%	12%	12%	9%	12%	11%	9%	5%	4%	16%	7%	3%
One to two hours	23%	20%	31%	26%	23%	27%	13%	21%	17%	22%	21%	18%	21%	26%	24%

Speed of reaction to an incident becomes critical given the impact a sluggish response can have on a business.

It is not just loss of revenue that SMBs are having to grapple with. Cyber incidents are also having an overall monetary impact. More than half (51%) of SMBs in the region that suffered cyber incidents in the past 12 months said that these cost the business US$500,000 or more, with 13% saying that the cost was more than US$1 million.

In fact, the majority of those that suffered an incident saw a monetary impact. Overall, 83% said the cost of incidents was more than US$100,000.

There is also the intangible cost. Of those that suffered an incident in the past year, 57% said it resulted in a loss of trust with customers, while 66% said it affected their reputation negatively. Though unquantifiable, a decline in reputation and erosion of trust can have disastrous consequences for any business.

FINANCIAL IMPACT OF CYBER INCIDENTS OVER PAST 12 MONTHS (US$)

	APJC	Australia	China	Hong Kong	India	Indonesia	Japan	Malaysia	New Zealand	The Philippines	Singapore	South Korea	Taiwan	Thailand	Vietnam
$500,000 or more	51%	64%	41%	39%	62%	43%	49%	32%	62%	28%	51%	58%	27%	47%	30%
$1 million or more	13%	33%	3%	10%	13%	12%	6%	6%	18%	10%	11%	10%	2%	28%	4%

Conquering fear with preparedness

Despite their fears and the tangible impact of cyber incidents, SMBs across the region are not simply giving up and are prepared to battle it out. They are starting with planning and training, with 81% of respondents saying they had completed scenario planning and/or simulations.

Realistic scenario planning and simulation is a key feature in cyber preparedness, not least because it helps SMBs uncover weaknesses in their security posture before the attackers can exploit them. Of those SMBs in the region that carried out simulation exercises, 85% said they uncovered weak points or issues in cyber defenses.

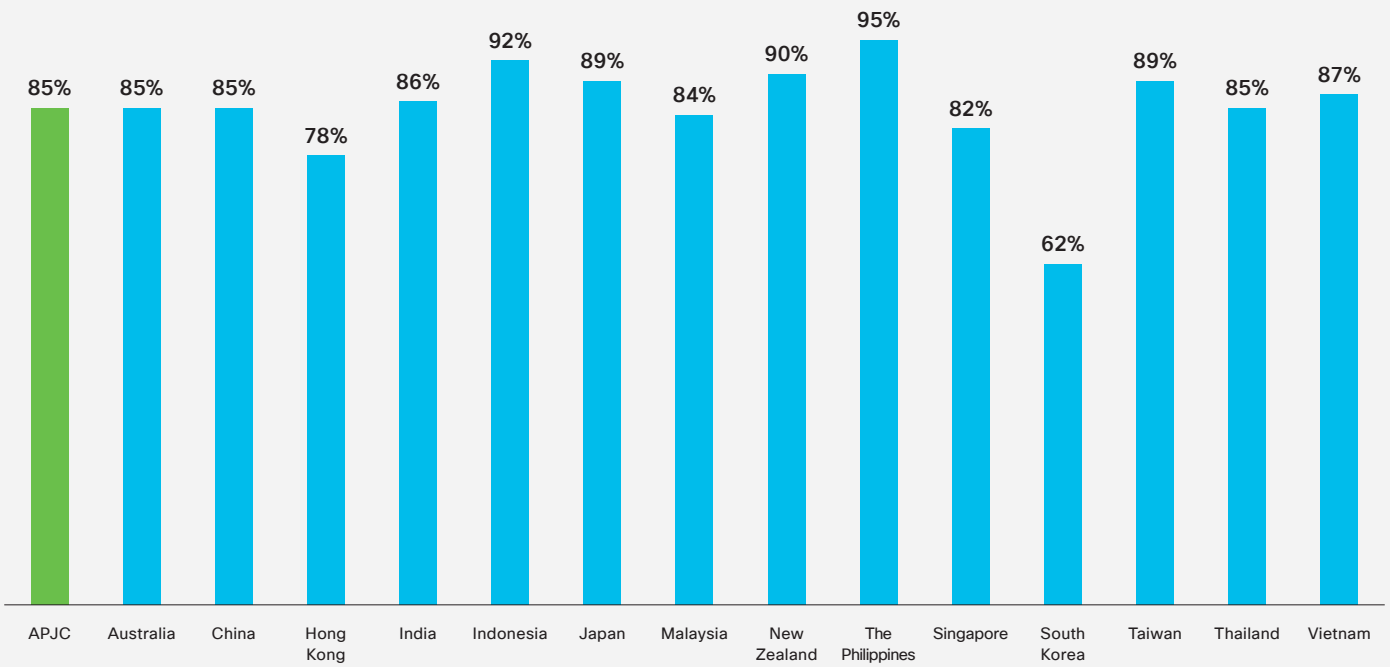
Of those that identified weaknesses, 95% said the exercises revealed issues with not having the right technology solutions in place to detect a cyber attack or threat. The same number found they had too many technologies and struggled to integrate them together, while 96% discovered they did not have the right technology solutions to block an attack.

A high proportion also recognized their processes for responding to a cyber attack were unclear (94%). Meanwhile, 95% said that while they had the right technologies, they did not have enough employees with the right skills to leverage them.

Encouragingly, around half of SMBs were able to address the identified gaps or issues from their scenario planning within two weeks. The sole exception was SMBs that found issues with not having the right technology to detect an attack or threat, which for most took longer to address.

While SMBs across the region are taking the right steps with scenario planning to become more resilient on the cybersecurity front, there is still work to be done in other areas. Top among those is educating all stakeholders. Nearly one in five (17%) said their leaders only have a limited understanding of local cybersecurity legal and regulatory requirements. This knowledge gap is considerably more prominent in New Zealand (30%), Hong Kong (29%), Japan (28%), and South Korea (27%).

DID YOUR CYBERSECURITY SCENARIO PLANNING AND/OR SIMULATIONS UNCOVER ANY WEAK POINTS IN YOUR CYBER DEFENSES (% YES)



Aligning investments and making them count

SMBs are also ensuring that they support their preparedness plans with investment. In fact, the research shows that the level of investment in cybersecurity is strong across the region.

Two-thirds (63%) of SMBs in the region spend at least 4% of annual revenue on cybersecurity on average, with 30% spending at least 6%, and 9% spending over 10%.

In fact, across the board around three quarters of Asia Pacific SMBs have increased their investment in cybersecurity since the start of the pandemic, with around two in five raising this by more than 5%.

An encouraging point to note is that increased spending has been distributed evenly across key areas, which suggests a strong understanding of the need for a multi-faceted and integrated approach to building a strong cyber posture.

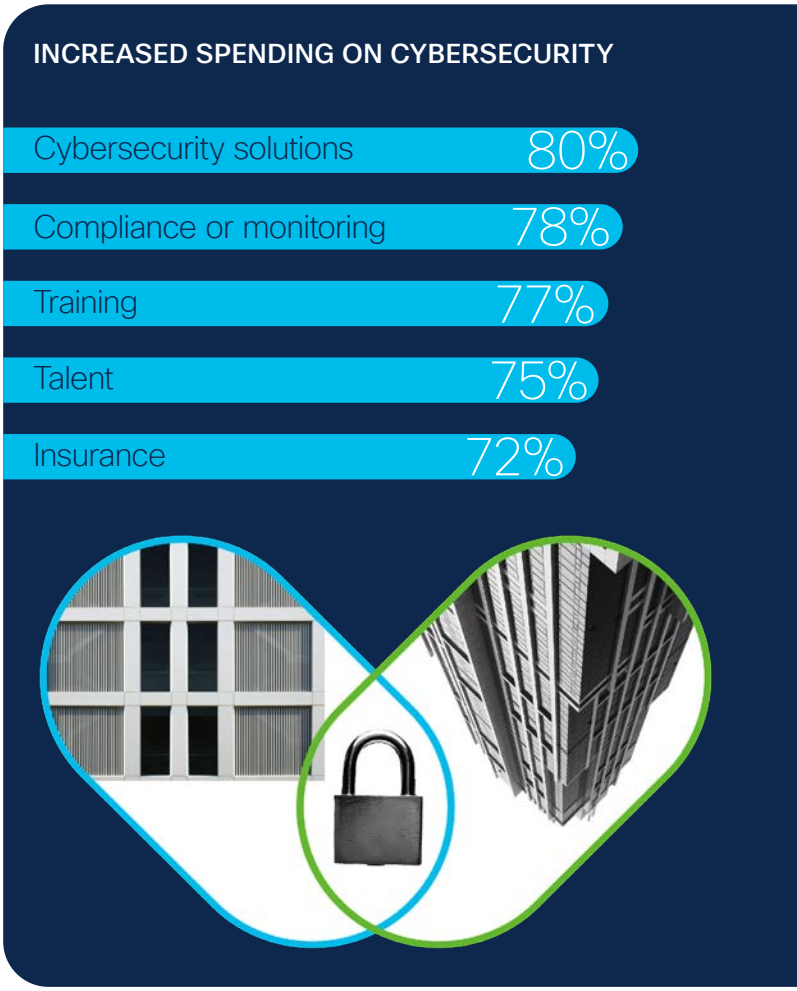
AVERAGE % OF ANNUAL REVENUE SPENT ON CYBERSECURITY

	APJC	Australia	China	Hong Kong	India	Indonesia	Japan	Malaysia	New Zealand	The Philippines	Singapore	South Korea	Taiwan	Thailand	Vietnam
None	1%	1%	0%	2%	1%	1%	8%	0%	0%	1%	2%	3%	0%	1%	0%
Less than 1%	8%	11%	4%	7%	6%	5%	18%	13%	17%	7%	9%	15%	13%	6%	2%
1-3%	27%	27%	30%	38%	20%	14%	33%	28%	26%	32%	29%	37%	42%	19%	18%
4-5%	33%	34%	45%	40%	30%	37%	29%	23%	24%	32%	36%	28%	24%	32%	53%
6-10%	21%	15%	15%	9%	30%	34%	9%	24%	21%	14%	17%	15%	17%	27%	16%
More than 10%	9%	11%	6%	3%	13%	9%	3%	12%	11%	15%	7%	2%	4%	15%	11%

In terms of challenges, SMBs said keeping pace with continually evolving technologies and security requirements (77%); keeping pace with constantly evolving cyber threats (76%); challenges with engaging employees around responsibilities (75%); too much complexity in the industry (75%); and the ability to recruit (73%) are the top barriers they face to increasing cybersecurity resilience.

As highlighted on the right, increased investments in areas such as solutions, compliance, talent, and training are a step in the right direction for SMBs across the region to build a proper cybersecurity posture.

The growing maturity in SMBs' understanding of cybersecurity is perhaps best highlighted by the fact that they are looking at preparedness holistically. However, even with investments in solutions, talent, and training, SMBs do find themselves at the wrong end of a cyber attack. It's just the nature of the industry. With a growing understanding of the potential impacts of a cyber incident on business, and increased legal implications, SMBs are turning towards cybersecurity insurance as a key investment area. This provides them with a cover to cushion the financial impact any such incident might have on their business.



% THAT SAW THE FOLLOWING FACTORS AS BARRIERS TO INCREASING CYBERSECURITY RESILIENCE

	APJC	Australia	China	Hong Kong	India	Indonesia	Japan	Malaysia	New Zealand	The Philippines	Singapore	South Korea	Taiwan	Thailand	Vietnam
Keeping pace with evolving technologies and security requirements	77%	82%	63%	73%	87%	53%	69%	84%	83%	89%	79%	75%	72%	71%	80%
Trying to keep up with evolving cyber threats	76%	80%	59%	71%	87%	50%	66%	87%	81%	88%	82%	74%	74%	77%	81%
Challenges with engaging employees around their responsibilities	75%	76%	61%	65%	86%	55%	70%	81%	82%	81%	75%	67%	68%	73%	81%
Too much complexity in the industry	75%	77%	61%	63%	85%	57%	65%	80%	87%	82%	82%	69%	65%	74%	79%

Five habits of secure SMBs

This report reveals challenges that are common among SMBs in dealing with the ever-changing cybersecurity landscape. Outlined in this section are five habits that SMBs of all sizes can employ to improve cybersecurity posture.

1 **Talk is good:** The cybersecurity environment is constantly evolving, so SMBs need to stay on top of the threats, and potential impact on their organizations. Scheduling frequent, regular meetings among senior leaders and all stakeholders will ensure the threat landscape is incorporated into business planning. SMBs that are well equipped to meet a cybersecurity event talk about the issue frequently. Over 90% discuss the issues and risks weekly and more than two-thirds (68%) talk daily. SMBs less well-organized to face the threats discuss cybersecurity less frequently, with around a third (31%) discussing issues less than monthly.

2 **Simplicity is key:** The traditional approach to handling cybersecurity has been to buy point security products and solutions to address a given concern at that moment in time. However, it has resulted in many SMBs having a myriad of products and solutions in their infrastructure which in many cases do not integrate with each other creating complexity in operations and unwanted delays in the event of a cyber incident. Evaluating how the various parts of the cybersecurity stack work together is critical to the speed and outcome of dealing with an attack. To connect disparate pieces of products and solutions, SMBs need an integrated, platform approach to ensure they have clear visibility on their entire security infrastructure, and that when the system is tested in a real-world situation it works seamlessly.

3 **Fail to prepare; prepare to fail:** One way of ensuring SMBs are prepared for the real world is to simulate the situations and outcomes in a more controlled environment. This can help SMBs get a realistic understanding of where any weaknesses may lie and provide an opportunity to address these and be better prepared for a real-world scenario should it happen. In fact, our research finds that a common trait among better prepared SMBs is that more than 98% had conducted scenario planning or simulations within the last 12 months. Almost all these SMBs, 96% have recovery plans in place to ensure they can get the business up and running as quickly and efficiently as possible. By contrast, among SMBs that did not plan effectively, over half (58%) had not carried out scenario planning and nearly two thirds (63%) did not have recovery plans.

4 **Train, train, train:** It is critical to understand that among all the technology and solutions that an SMB can deploy, it's often that humans can turn out to be the weakest link. This can well be judged by the fact that despite all the advancement in the sector, phishing (which is basically enticing a human to click on a link in a digital communication sent to them) continues to remain the #1 threat vector. SMBs need to ensure that every employee, irrespective of their role, has a basic understanding of cybersecurity and the role they can play in keeping the business safe.

The data from our research on this front is staggering. Among SMBs that are well set to manage the cybersecurity landscape, 96% agree or strongly agree that employees understand cybersecurity in general, and 95% understand the seriousness of a potential attack, and their role. By contrast, those underprepared for an event have much less faith in their employees, with just 15% agreeing that employees understand cybersecurity.

5 **Better together:** Working with the right technology partner is critical to achieve overall success on the cybersecurity front. SMBs should keep in mind a few things. Firstly, the partner they work with should have the capability to provide them with end-to-end protection across their business. In most cases, it will require integrating different products and solutions into one platform to provide simplicity and visibility across the entire infrastructure. Second, as SMBs embark on their digitalization journeys, their business will eventually grow, and they will expand their operations. The partner they choose to work with should have the capability to secure their operations irrespective of their scale. Finally, the partner should have the capacity to provide different consumption models on how the SMB wants to deploy technology.

About this research

3,748 respondents in **14** markets

MARKETS

- Australia
- China
- Hong Kong
- India
- Indonesia
- Japan
- Malaysia
- New Zealand
- The Philippines
- Singapore
- South Korea
- Taiwan
- Thailand
- Vietnam

AUDIENCE

IT and business leaders with cybersecurity responsibilities

THESE ORGANIZATIONS INCLUDE:

- Small (between 1 and 249 employees)
- Medium (between 250 and 999 employees)

INDUSTRIES

- Advertising or Market Research
- Business Services (e.g. Accounting, Consulting)
- Construction
- Education
- Engineering, Design, or Architecture
- Financial Services
- Healthcare
- Manufacturing
- Media and Communications
- Natural Resources (e.g. Oil, Mining, Forestry)
- Personal Care and Services
- Professional Services
- Real Estate
- Restaurant Services
- Retail
- Technology Services
- Transportation
- Travel Services
- Wholesaling
- Others

Appendix A

ESCALATION OF IMPACT DUE TO LENGTH OF DOWNTIME

	APJC	Australia	China	Hong Kong	India	Indonesia	Japan	Malaysia	New Zealand	The Philippines	Singapore	South Korea	Taiwan	Thailand	Vietnam
Amount of downtime before your organization's operations are severely impacted															
Under one hour	15%	10%	21%	11%	17%	18%	10%	13%	17%	16%	7%	10%	21%	18%	8%
One to two hours	29%	25%	28%	21%	32%	35%	18%	32%	39%	28%	23%	29%	28%	31%	30%
Amount of downtime before your revenue is severely impacted															
Under one hour	13%	8%	16%	12%	12%	25%	7%	16%	9%	15%	10%	14%	14%	14%	9%
One to two hours	24%	20%	26%	21%	24%	27%	17%	23%	19%	27%	20%	19%	34%	28%	20%
Amount of downtime before you may face regulatory or legal implications															
Under one hour	13%	7%	16%	14%	13%	19%	6%	17%	8%	13%	11%	13%	18%	14%	12%
One to two hours	22%	19%	24%	18%	24%	32%	15%	23%	20%	19%	24%	21%	25%	22%	17%

About Cisco Secure

Cisco has long established itself as the networking leader, while building an open, integrated portfolio of cybersecurity solutions along the way. We believe that security solutions should be designed to act as a team. They should learn from each other.

They should listen and respond as a coordinated unit. When that happens, security becomes more systematic and effective. Our customers have trusted us for years as both the world's largest provider of IT infrastructure and networking services and the world's largest B2B cybersecurity business.

Cisco Secure is built on the principle of better security, not more. It delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, easy to manage, and easy to use – and that it all works together. We're driven by the fact that people and our customers are at the heart of what we do. We understand that customers want to cut through the complexity and noise and feel confident in their security; focusing on outcomes. This requires simplification without being simplistic. Our cloud-native platform is a giant leap forward in that.

We empower the security community with the reliability and confidence that they're safe from threats now and in the future with the Cisco SecureX platform. We help 100 percent of the Fortune 100 companies protect what's now and what's next with the most comprehensive, integrated cybersecurity platform on the planet. Learn more about how we simplify experiences, accelerate success, and protect futures at cisco.com/go/secure.

The Cisco Security Outcomes Study

For a deeper dive, we invite you to read the 2021 Security Outcomes Study for Small to Midsize Businesses (SMBs), and to visit our dedicated page for more Cisco Secure thought leadership content.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**


CISCO