State of Cybersecurity in APAC:

Small Businesses, Big Threats

ENJOY SAFER TECHNOLOGY™

BACKGROUND

The business security landscape in Asia Pacific

Cybersecurity used to be regarded solely as an IT issue; a concern discussed only by experts in the field. Today, terms such as 'hacking', 'ransomware' and 'data breach' commonly grab headlines in mainstream media, a testament to the scale of the problem these have become. According to Juniper Research, the **cost of data breaches globally is expected to skyrocket to US$2 trillion by 2019**[1], quadrupling in only four years.

Fortunately, businesses have begun stepping up their efforts in battling this growing threat. A recent report by IDC estimated that **businesses worldwide spent US$73.7 billion on security technology in 2016**[2], with this spending likely to exceed US$100 billion by 2020. Against a backdrop of rapid digitalisation – particularly among emerging economies – the Asia Pacific region is expected to be the fastest growing region with an annual growth rate of 13.8% over the 2016-2020 forecast period.

The costs associated with cybersecurity often deter small and medium-sized businesses from making serious considerations about security solutions, owing to limited budgets and lack of expertise. However, the rate of adoption of digital technologies by both consumers and businesses is making the region an ever more attractive target of cybercrime. Furthermore, contrary to popular beliefs, small businesses can be big targets for cybercriminals, who may use them as conduits to target larger corporations. For example, the hack of Target in 2013 – which cost the company US$39 million in settlements – was **later traced to credentials stolen from its HVAC subcontractor**[3].

1 Juniper Research: Cybercrime will cost businesses over $2 trillion by 2019, 12 May 2015

2 IDC: Worldwide Revenue for Security Technology Forecast to Surpass $100 Billion in 2020, According to the New IDC Worldwide Semiannual Security Spending Guide, 12 October 2016

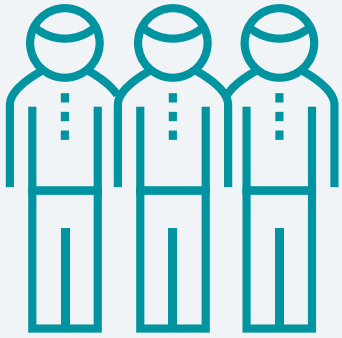
3 KrebsonSecurity: Target hackers broke in via HVAC company, 14 Feb 2014

Cybersecurity is a necessity for small businesses

Most companies understand cybersecurity solutions bring about benefits such as better control over data and services, and higher reliability, but are less confident about its impacts on deliverables such as sales and resource savings. With the costs of breaches to SMBs averaging more than US$35,000 in damages, the financial loss from a cyberattack can truly hurt a business.

However, there is more to it than just financial loss. Consumer awareness of, and demand for, improved security in the products and services they purchase continues to grow. As a result, businesses with a better security focus should see a positive impact on sales.

By ensuring that its information is well protected, a business can build on customers' confidence and trust to bring about more sales that will have positive impacts on the bottom line. The reality is that businesses today cannot just view cybersecurity as a nice-to-have, it is a must-have.



SUMMARY OF KEY FINDINGS

What SMBS in APAC need to know

This report summarises the findings in a recent survey that ESET conducted in the Asia Pacific region, focused on small and medium-sized businesses.

One heartening finding identified in the results was that companies in the region appear to be stepping up efforts in the fight against cybercrime. A majority of companies, regardless of size or market region, reported utilising antivirus software and firewalls. Similarly, most SMBs (81%) were noted to have applied encryption to at last one type of device/ information in their systems.

However, the data also showed that there is still some way to go for businesses in the APAC region in terms of information and communication. While more than half of the companies surveyed **(54%) reported experiencing a cybersecurity breach in the past three years**, only 56% had policies in place to inform their employees about cyber breaches.

Where it came to clients, the number was even lower, with only 49% overall having a communication plan to inform clients. Larger firms appeared to be more responsible in this regard, with about three in five having such plans to fall back on, as compared to about a third of micro SMBs.

Overall, the results indicated a need for micro and mid-sized SMBs to do more to protect their digital assets. While close to half (47%) of companies in this range had experienced cyber breaches in the past three years, few had basic preventive measures such as cybersecurity awareness programs for employees in place.

INTRODUCTION & METHODOLOGY

This report summarises the most important findings in a recent survey that ESET commissioned for SMBs in Asia Pacific. The objective of the survey was to get a better understanding of the perceptions and activities related to cybersecurity of small- and medium-sized businesses in the region. In particular, it sought to uncover what high-level business executives and IT professionals in Asia Pacific thought about issues such as the importance of cybersecurity to business operations, the existing policies and procedures they had in place, as well as their opinions on the need for advanced cybersecurity technologies such as 2FA and encryption.

The survey was conducted during September and October 2016, and gathered responses from over 1,500 stakeholders in five markets – Singapore, Hong Kong, India, Thailand and Japan.

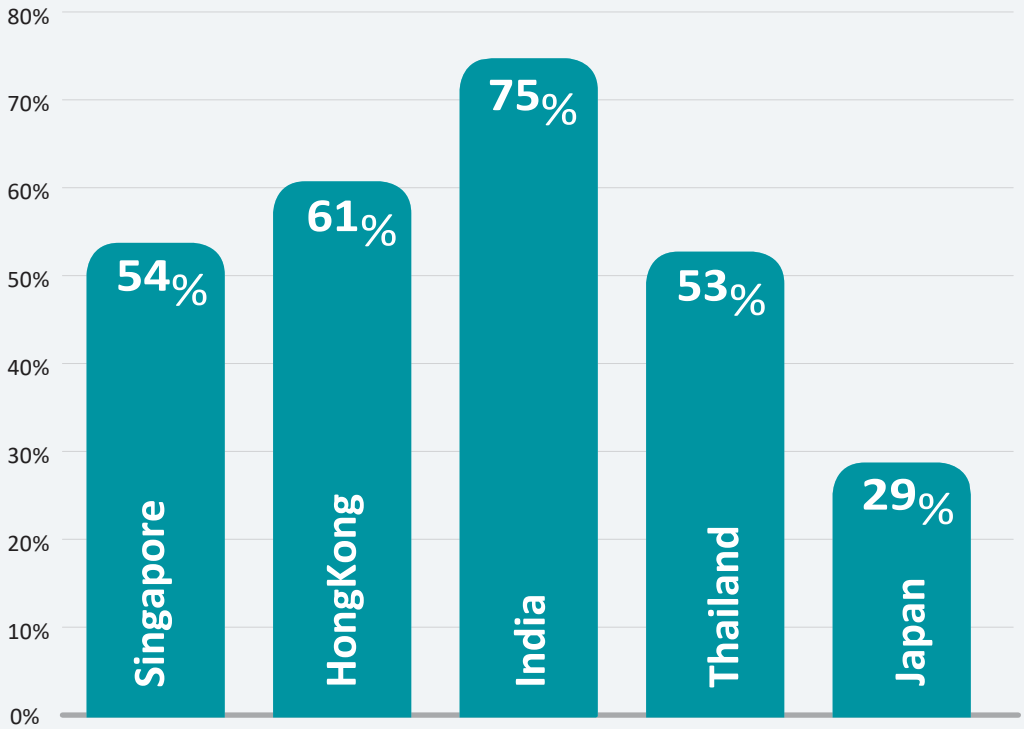
Risk of cyber breach

Asia Pacific is no stranger to cyber threat. These problems have become especially pertinent as economies in the region become increasingly digitalised. Just recently, we witnessed several high-profile attacks such as the massive DDoS attack on Starhub, a major telco in Singapore, as well as the hacks on Mitsubishi Heavy Industries, Japan's largest defence contractor.

While these attacks were directed at large enterprises, SMBs in the region were not spared. **Perhaps surprisingly, more than 50% of companies in all markets surveyed, except Japan, reported having experienced a cyber breach in the past three years.** India was the worst affected, with 75% of companies surveyed hit by a breach in the specified time period. This was followed by Hong Kong, at 61%. The situation appeared rosier in Japan, with only 29% having experienced a breach in the three years prior.

The choice of target by cyberattackers also appeared to be influenced by size of company. **Seven in ten large SMBs indicated that they had been hit by at least one cyber breach** in the past three years, compared to only **37% of micro SMBs**. However, there is a possibility that smaller organisations may become prime targets for cybercriminals attempting to find a backdoor for infiltrating larger organisations. Organisations, regardless of their size, should be vigilant and take the necessary precautions to fend off any malicious threats.

SmBs experiencing Cybersecurity Breaches in the Past 3 years

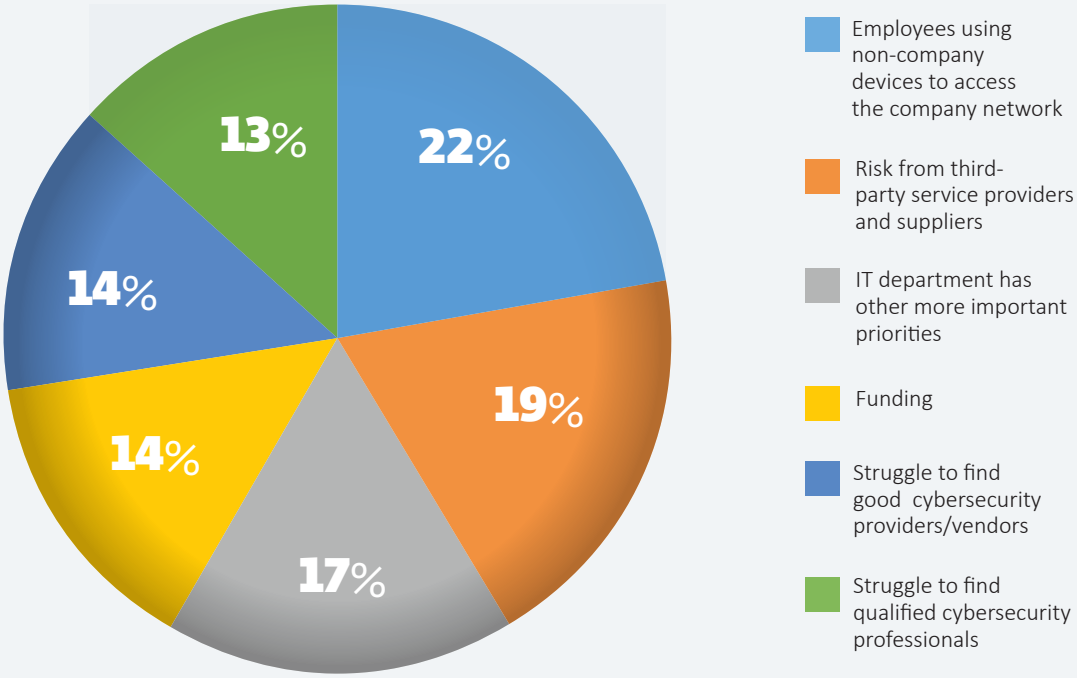


Causes of breach

Given the recent spate of cyberattacks, cybersecurity is receiving heightened interest in the region, bringing scrutiny to the reasons behind these attacks. From the cyber heist at the Bangladesh Central Bank to the large Yahoo! credential theft, it is evident that cyberattacks can impact any industry at any time.

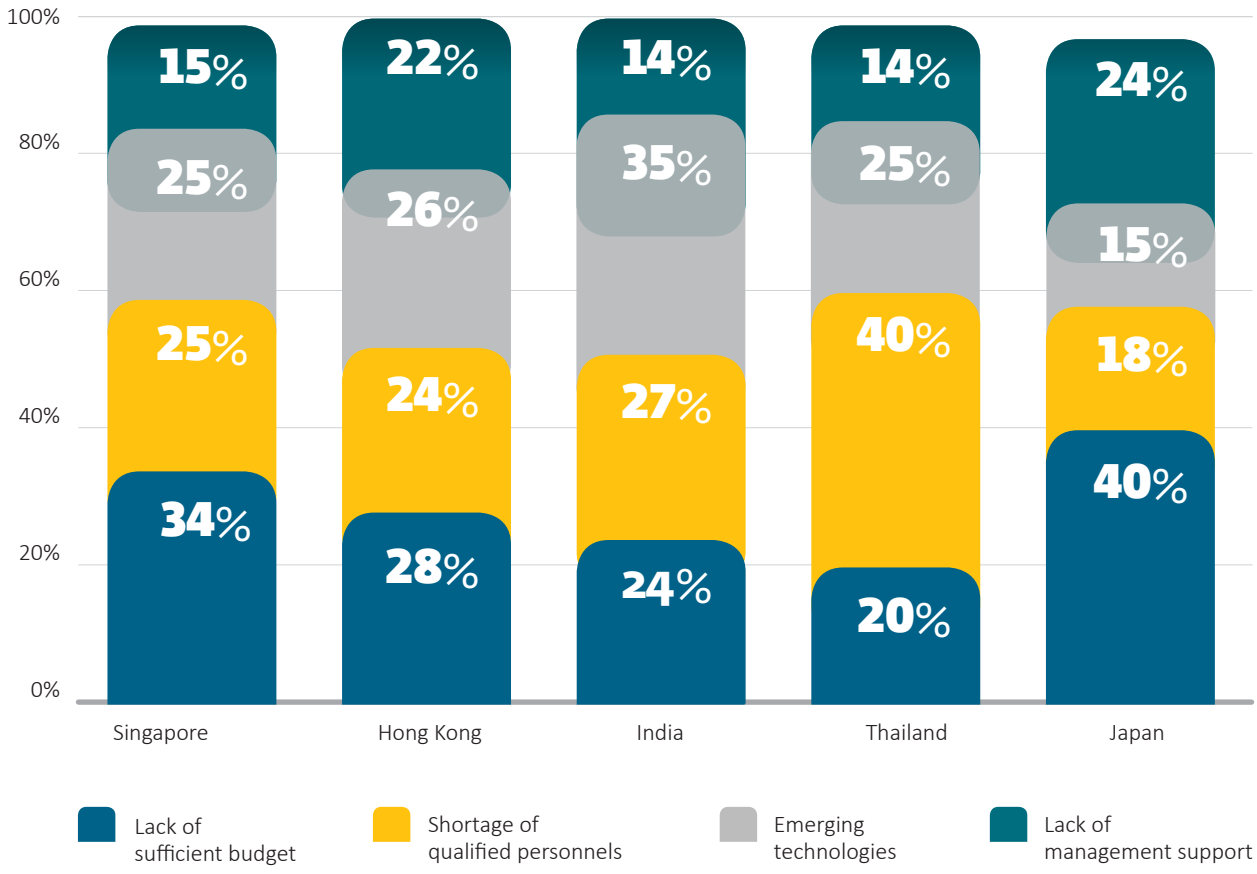
Cybersecurity measures are the first line of defense for companies when it comes to protecting themselves against external threats. However, there are roadblocks that stand in the way of adopting these measures for organisations. **22% of SMBs in general cited employees using non-company devices to access the company network** as being the biggest cybersecurity challenge, with **risks from third-party service providers and suppliers (19%)** following closely behind. It appeared that **smaller businesses also had smaller budgets for cybersecurity,** as funding was most often cited as the key challenge they faced. On the other hand, mid- and large-sized SMBs were less likely to share this concern, with only 12% and 10% respectively highlighting this as the key challenge they experienced.

Biggest Cybersecurity Challenges Faced by SMBs



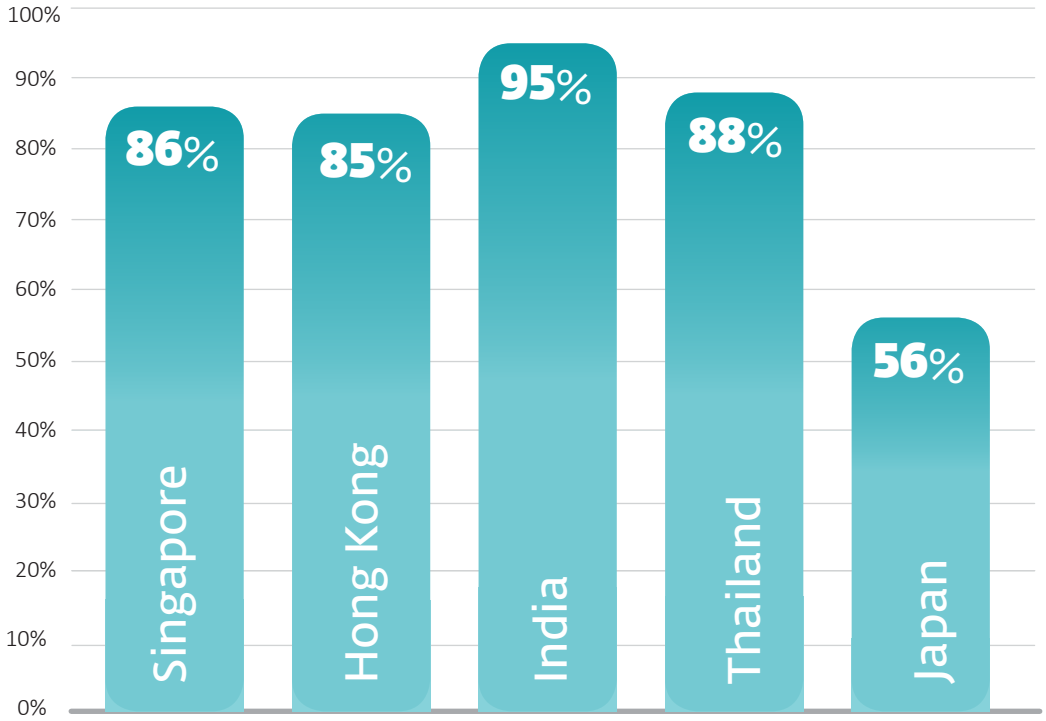
Within countries, **shortage of qualified security personnel** seems to be a big challenge for Thailand (40%). On the other hand, **Indian companies are more worried about emerging technologies (35%)**.

Barriers to Ensuring Cybersecurity by Country



With a rise in the 'Bring Your Own Device' (BYOD) culture in the workplace, SMBs are exposed to a larger attack surface, especially if they do not restrict access to the organisation's network to only authorised devices. Whether it is wired or wireless access to the network, only slightly more than half of SMBs in **Japan (56%) monitor their networks**, a significantly lower number compared to other markets in Asia Pacific such as **India with 95% monitoring access to their network**. Network monitoring is essential for organisations in reducing the mean time to detect potential malware attacks. SMBs need to be able to react quickly in order for them to take proactive measures which can either prevent problems from occurring or reduce the impact of the damage.

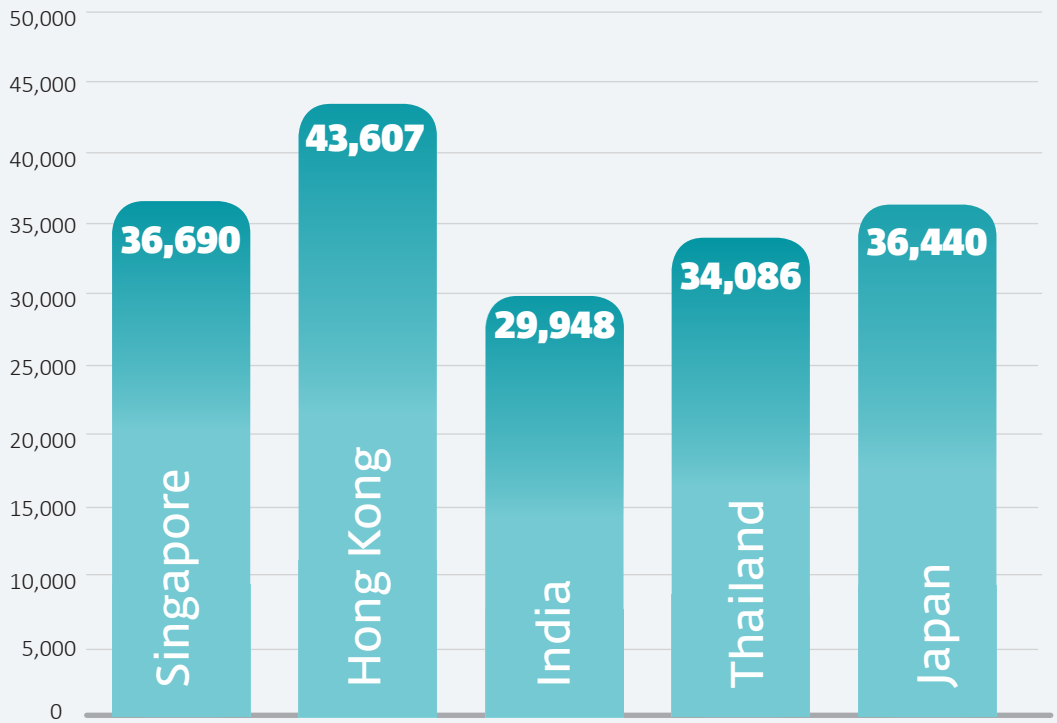
SMBs which Monitor the Computer Network



Cost of breach

When organisations suffer from breaches, more often than not, the biggest drawback is the cost involved which can have a great impact on business continuity. Overall, larger organisations incurred greater losses (averaging US$42,543) as compared to mid-sized SMBs (US$34,464) and micro SMBs (US$22,996), taking into account the time, consultation and hard cost involved in the cybersecurity breaches. Within countries, **cybersecurity breaches cost SMBs in Hong Kong the most, averaging US$43,607 per breach**, higher than the average cost across APAC countries of US$35,439 per breach. This is followed closely by Singapore at US$36,690 per breach and **Japan at US$36,440 per breach**.

Cost Incurred by SMBs per Cybersecurity Breach

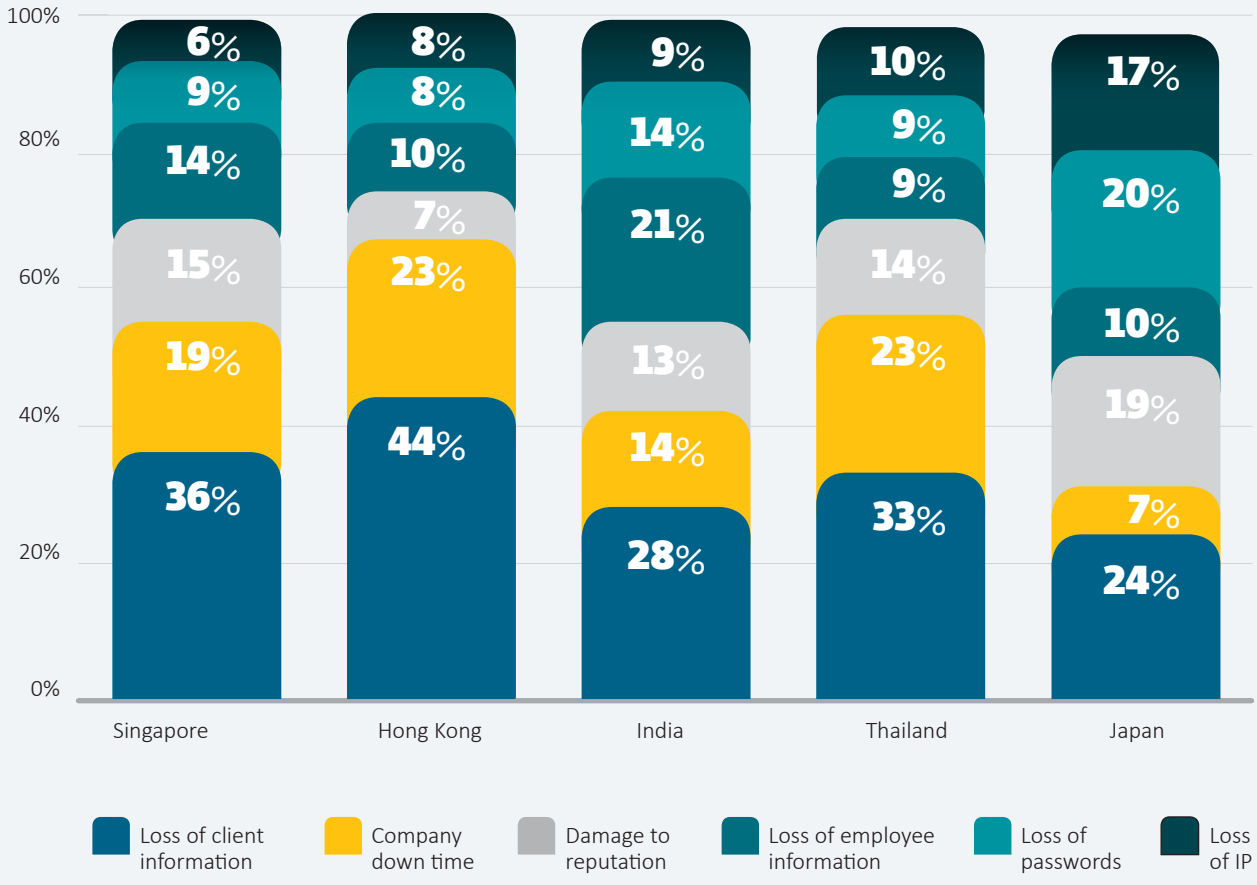


Business concerns

As data breaches rise, businesses are faced with the alarming impact on their day-to-day operations while they recover from a cyber breach. **One third of all companies**, regardless of their size, cited the **loss of client information as their biggest fear** during a cyberattack.

In **Hong Kong**, the impact to business productivity was a key concern to SMBs, with **44% citing loss of clients' contacts and financial details** as the biggest worry and **23% concerned about company downtime** while the breach is being fixed. Across countries, there were some key differences in business concerns that were worth noting – **19% of Japanese SMBs were concerned about the damage to reputation and 21% of Indian SMBs were worried about loss of employee information**.

Concerns About Cyber Breaches by Country



How protected are companies?

Current measures taken by SMBs

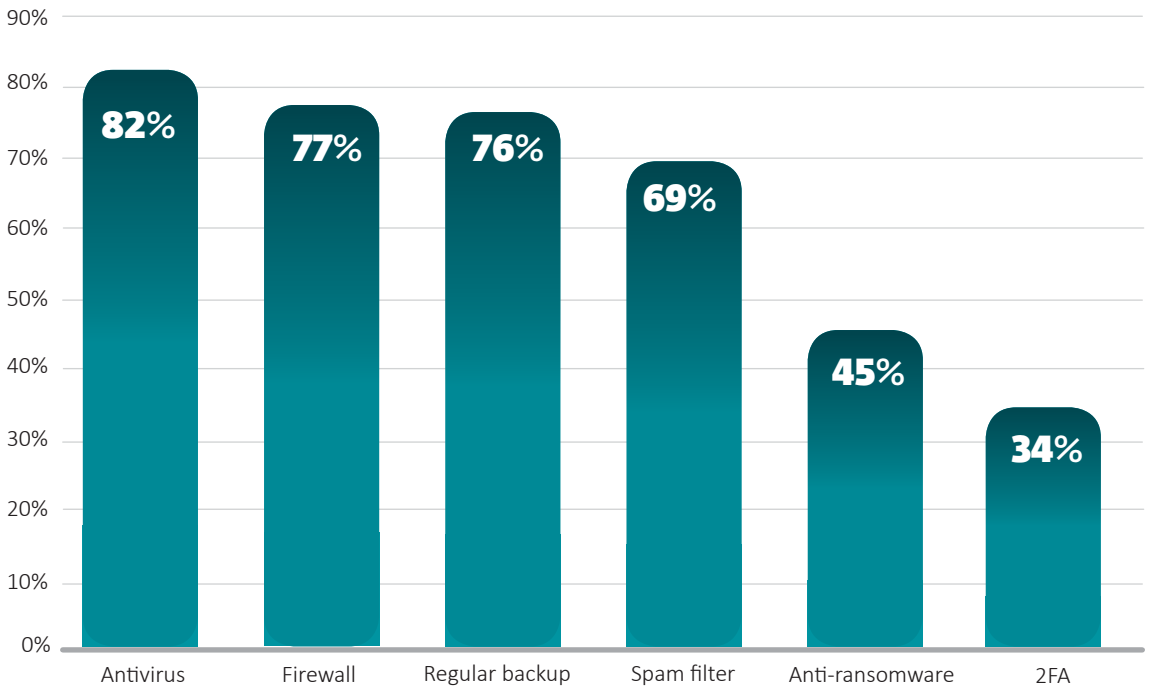
With ransomware and large-scale DDoS attacks hogging headlines in the past year, SMBs of all sizes have begun stepping up efforts to protect themselves from cybercrime. A majority of companies surveyed had some level of security measure within their organisations. The most common tools to combat cyber threats that companies in APAC reported using were **antivirus (82%)** and **firewalls (77%)**.

Companies in Thailand were the most proactive in installing antivirus, with 89% of SMBs already having this measure in place. On the other hand, 86% of SMBs in Hong Kong had already adopted firewalls, the most among APAC markets surveyed.

The situation was similar in terms of more advanced security solutions such as encryption and 2FA. Adoption rates for 2FA were much lower across the board and even in Singapore, where firms were most likely to have implemented 2FA solutions, **only 42% of companies had done so**. However, SMBs should also look into proper execution of these measures as well, given the majority of SMBs in Thailand adopted encryption as cybersecurity measures (80% adopted personal data encryption and 73% adopted encryption for data in transit), yet an overwhelming proportion of SMBs in Thailand that reported suffering cyber breaches claimed these breaches were related to encryption (92%)

In general, large SMBs (defined as SMBs with over 100 employees) were more likely to have adopted cybersecurity measures than their smaller counterparts. **46% of large SMBs had adopted 2FA solutions to protect their systems, as compared to only 18% of micro SMBs**.

SMBs and the Cybersecurity Measures Adopted



Policies for communicating breaches

Cybercriminals often spend weeks or even months planning a single cyberattack, studying the vulnerabilities and possible entry points at companies. Unfortunately, businesses do not share the same luxury in having time to respond to cyber breaches as they hit. IT departments and professionals must respond swiftly if and when breaches occur.

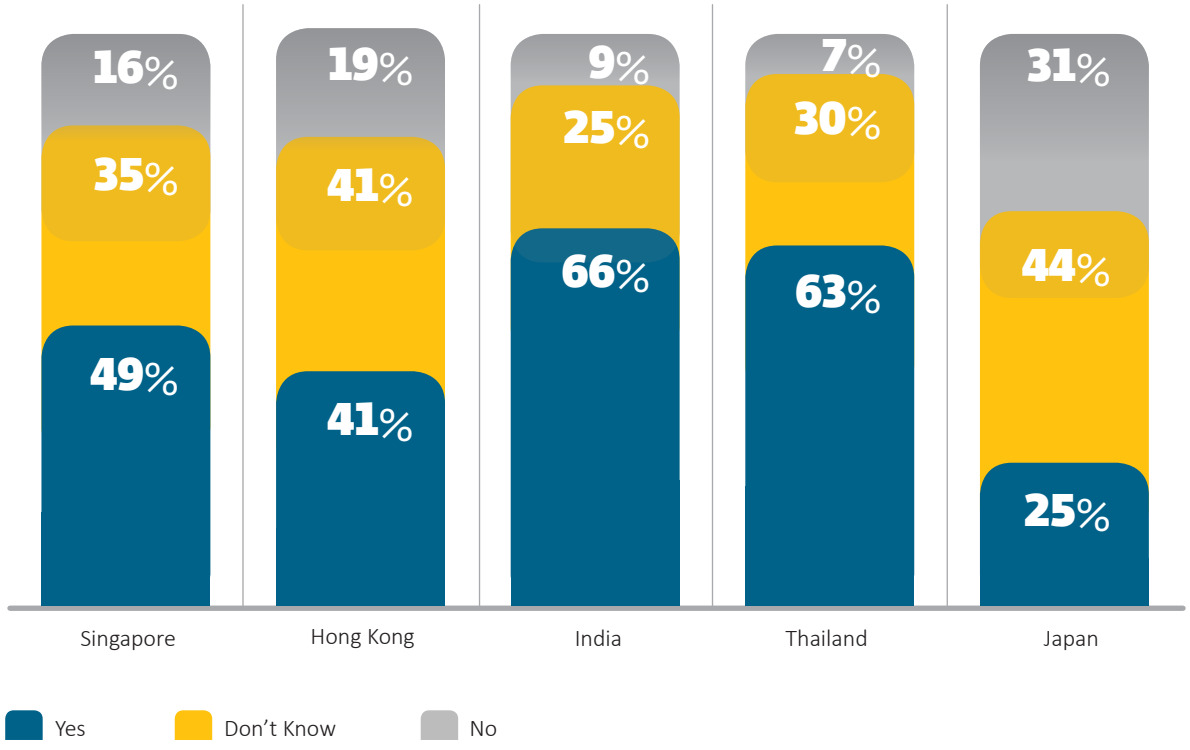
ESET's survey showed that better communication with stakeholders, both internal and external, was needed in the wake of a cyber breach at SMBs.

While most large SMBs had a policy for informing employees about a breach, fewer companies had policies to inform clients. Only 59% of large SMBs had policies in place to inform clients of cyber breaches. With micro SMBs, this proportion shrank further to 34%. Companies working with Indian and Thai SMBs stood a better chance of being informed in case of cyber breach, with 66% and 63% respectively noting that they had policies to inform their clients, the most out of the APAC SMBs surveyed. Japanese SMBs, on the other hand, were less likely to have set practices in place to share information on breaches with their clients, with only 25% of companies noting that they already had such policies in place.

Policies to inform clients about breaches were influenced by a number of factors. Only one in four companies would let their clients know immediately in case of breach, regardless of situation. Conversely, **21% of SMBs surveyed would wait until the issue was fixed before telling their clients**. Most worryingly, **19% of companies indicated that they would not tell their clients at all unless asked**, reflecting a need for businesses in the region to regularly conduct their own backup exercises and proactively take steps to address their own security needs.

Employees factored a bit higher on SMBs' priorities post-cyber breach. More than half of all SMBs surveyed had policies in place to inform employees about cyber breaches. As with informing clients, companies in **India (77%)** and **Thailand (71%)** had cybersecurity awareness programmes in place to educate employees, whereas **Japan (24%)** fared the lowest. Large SMBs also fared better in this respect, with seven in ten having policies already in place to communicate cyber breaches to employees. Micro SMBs, however, had some way to go in catching up, with only 40% ready to do so.

Policies to Inform Clients About Cyber Breach



Barriers and challenges to a secure cyberspace

It is very encouraging that **71% of companies in Asia Pacific agree that there is a need to invest more in cybersecurity solutions**, especially in India (83%) which has the highest rate of companies in the region who feel so. It is not surprising to see that the larger the business, the more aware they are of spending on cybersecurity solutions. However, it is rather worrying that the smaller businesses are slightly more uncertain. The economy in this region, particularly Southeast Asia, is largely driven by SMBs and there is a need to highlight the importance of investing adequately to combat the increasingly rampant cyberattacks.

While there is an acknowledgement of a need to invest more, there are barriers and challenges in ensuring that businesses are well protected against cyberattacks. These challenges and barriers differ depending on the size of the business.

The challenges and barriers that SMBs are facing are certainly not insurmountable. **Only 18% of SMBs felt that management support was an issue** which shows that business leaders in the region understand the need for cybersecurity measures in their organisations.

For businesses with currently no measures in place, this will ensure that they will at least take the first step to implement the very basic protective measures such as antivirus and firewall. For those that are more matured in their cybersecurity measures, greater management support will see better funding to upgrade existing measures and hiring of experts to ensure that tools are maximised effectively.

Main challenges – Difficulties in implementing current cybersecurity solutions

Bring-Your-Own-Device (BYOD) is so common these days that employees assume that it is safe and acceptable to use their own devices to access the network at their own workplace. In fact, this is a nightmare for most SMBs with 22% highlighting that it is their biggest challenge. While companies can ensure that their own devices are well-protected, they do not have control over personal devices. This is why education and creating awareness internally have to remain as one of the key priorities for any business today.

To remain nimble and agile, SMBs work with multiple third-party vendors and suppliers. These vendors and partners may hold sensitive information about them but may not have the necessary cybersecurity measures to prevent an attack. 19% have identified this risk as a challenge to implement their own cybersecurity solutions. While it is a valid concern, SMBs should not wait until their partners are on-board before implementing their own measures. If they are concerned about the safety of the information when it sits with their third-party vendors, then they will need to consider options such as authentication and network monitoring.

As SMBs scale and grow, cybersecurity may not be the top priority when there are other more pressing requirements. This is one of the main challenges when the same team looking at cybersecurity is tasked with other growth projects that are considered more important. This is a bigger challenge seen in large SMBs (24%) when they are scaling up. Micro SMBs on the other hand don't see this as a huge challenge but are instead faced with a challenge in funding.

Main barriers – Difficulties in implementing future cybersecurity solutions

Close to one third of the companies surveyed said that funding remains the biggest barrier when it comes to cybersecurity. Smaller SMBs (35%) are finding it particularly difficult to justify the investment needed especially when such funds can be used for other aspects of running the business. The lack of sufficient budget is more apparent in developed markets such as Japan (40%), Singapore (34%) and Hong Kong (28%) compared to emerging markets such as India (24%) and Thailand (20%). This could mean that SMBs in emerging markets could leapfrog those in the developed markets when it comes to cybersecurity solutions.

Shortage of qualified personnel also ranked highly on the list of challenges in cybersecurity adoption. 27% of companies surveyed believe that there is a lack of experienced professionals in the space that they can hire. This is not surprising considering that cybersecurity only became a major consideration in the last few years. Demand for cybersecurity experts currently outstrips the supply of such individuals. Unlike enterprises, SMBs do not necessarily have the funding to outsource the role to a managed service provider.

Another barrier to the adoption or upgrade of cybersecurity solutions is the constantly changing landscape. SMBs are unsure where and when they should invest in a solution as they are afraid that they are not investing in the latest technology. They are also unsure if the technology suits their organisation. Companies in India face this dilemma the most, with 35% of SMBs in the country citing emerging technology as a barrier to ensure cybersecurity.

What can businesses do?

Businesses, particularly the small- and medium-sized ones, must start looking at cybersecurity seriously. They recognise that they are being targeted, with more than half of the companies experiencing a security breach in the past three years. This is highest in India (75%) and Hong Kong (61%). These breaches not only result in financial loss, they also erode trust and cause reputational damage.

It is understandable that growing the business takes priority but they cannot ignore the threat of cyberattacks in our increasingly digital age. Here are the focus areas they should look at for cybersecurity moving forward:

Explore more sophisticated cybersecurity solutions

The majority of SMBs in the region have basic cybersecurity solutions in place. 82% of businesses have antivirus software installed and 78% have firewalls to stop unauthorised access to their network. However, 54% of businesses are still experiencing a breach.

While it is important that the basic building blocks against cyberattacks are in place, SMBs in the region need to look beyond the basics. Cyberattacks are evolving every day and it is no longer enough to just rely on the bare minimum. They need to start looking at different solutions such as intrusion detection systems or multi-factor authentication, such as 2FA, in order to protect their data and control access to the network. Currently, only a third of businesses in the region implement 2FA to access sensitive information in the company.

Impose better security for personal devices

Other than Japan, the BYOD culture is accepted and sometimes even encouraged in most markets across the region. In fact, this is one of the main challenges that SMBs are facing. Unfortunately, only 59% have a cybersecurity awareness program to educate employees. This is a bigger challenge in smaller SMBs as only 35% have such programs.

When businesses allow their employees to use their own devices to access sensitive information without warning them of the dangers, they run the risk of being breached as the attack surface grows with every employee in the company. Therefore it is important that businesses not only have cybersecurity solutions that are able to monitor unauthorised or abnormal access, it is important for them to implement and educate their employees about cybersecurity best practices.

Set up communications policies in event of breach

While financial loss is always a worry in the event of a breach, damage of reputation to the business cannot be overlooked. This is of particular importance to Japanese businesses where reputation and pride are important aspects for a company.

It is important to look at how to prevent breaches from happening but it is equally important to deal with the aftermath of a breach. 34% of businesses in the region are still looking only at informing customers if they felt that the information was at risk. More alarming is that 19% wouldn't even inform their customers unless asked.

This lack of transparency can be particularly damaging as it can erode customers' trust in a business. SMBs need to reconsider their communication policies and see how they can be improved. Successfully recovering from a breach with transparent communications can help bolster trust and improve relationships with customers.