Anticipating the Unknowns

2019 Asia Pacific CISO Benchmark Study

cisco

Contents

Regional Overview

Executive overview

About the report

The C-Suite is tasked with accelerating the business. But how do you accomplish that in the digital age where CISOs are in charge of defending against the onslaught of cyberthreats every day on every device, every app, every user, every cloud? For those in charge of information security, we've created this report to educate you on the state of your profession as it relates to keeping your organizations safe.

You generally want to support the business, and not mire it down in bureaucracy. If you're going to be a bit more open, how are you mitigating control? This is going to be different for everyone. CISOs must deal with that balance of organizational culture while combating the most critical threats.

Surveying almost 2,000 security leaders across 11 countries in Asia Pacific, from organizations of 100–499 to large enterprises and the public sector, we gathered data in four areas where security decision-makers carry out their charges:

- **Cybersecurity culture**
- **Security alerts and the impact of data breaches**
- **Cybersecurity trends: Cloud and Operational Technology threats**
- **The defenders' approach on managing vendors**

Each country report has a specific introduction and recommendations section in addition to these topics.

In this regional summary, you'll find the top eight most interesting things to come out of the 2019 Asia Pacific CISO Benchmark Study, key regional trends such as average alert remediation and downtime* and costs of a breach, and finally a comprehensive recommendations section which addresses the key issues outlined in the report. This covers how to simplify your security environment, how to get more investment from the boardroom, and how to address the security skills gap.

Top eight most interesting things from the study

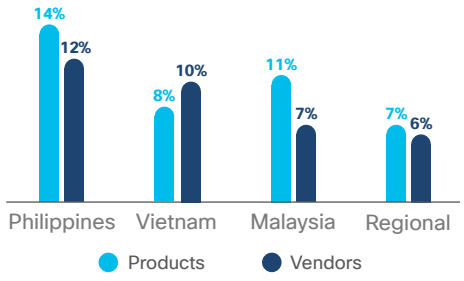
1. Some organizations don't know how many vendors or products exist in their environment

Security teams are facing active adversaries who are well-funded and endlessly patient, and other perennial challenges that never seem to go away, like keeping an accurate inventory of users, applications, and devices.

That's why being aware of what your teams are doing to protect your organization is so crucial, so that you can ensure optimal efficiency and eliminate any wasted effort.

Here are the countries with the highest percentages of organizations who aren't aware of how many vendors or security products they use. There could be a variety of reasons as to why these countries have less visibility of their security environments than others (perhaps there are different teams within the organization, legacy issues, etc.), but the important thing to note is that honesty is the best policy. Knowing that you "don't know" is a good place to start; then you can work to address these issues.

Chart: Top countries who are unaware of the number of security products and vendors used in their security environment

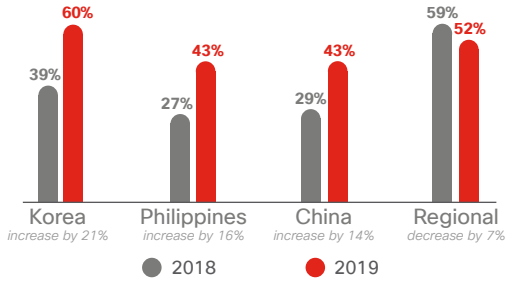


2. The biggest increase in cybersecurity fatigue levels from 2018

Cybersecurity fatigue is defined as defenders essentially giving up trying to stay ahead of malicious threats and actors. It's a sign that security teams have become overwhelmed by the amount of security alerts they receive, and are constantly putting out fires, rather than proactively building an effective security strategy. In the recommendations section, we'll explore some tips on how to reduce burnout.

These are the countries who had an exhausting year, cybersecurity wise, and have increased their levels of fatigue the most:

Chart: Biggest increase in cybersecurity fatigue levels

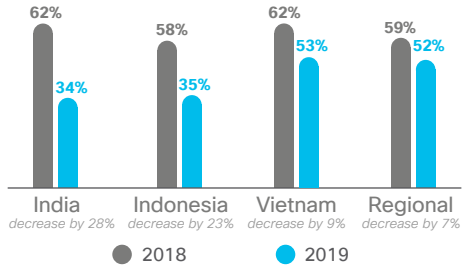


3. The biggest decrease in cybersecurity fatigue

Overall, cybersecurity fatigue levels in Asia Pacific went down by 4% from 2018 to 2019, which is no small feat considering there were some large increases (see above).

Here are the countries who made the most positive strides in their security approaches:

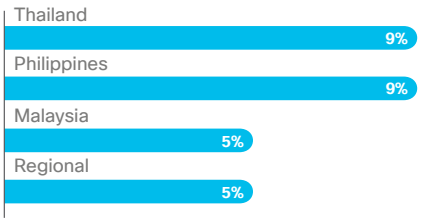
Chart: Biggest decrease in cybersecurity fatigue levels



4. The most significant amount of downtime experienced

The goal in any data breach is to get operations back to normal as quickly as possible, and ensure that the attack has been completely remediated from all systems. These are the countries with the highest percentage of organizations who experienced severe downtime after their most critical data breach:

Chart: Percentage of organizations who experience downtime* of five days or more



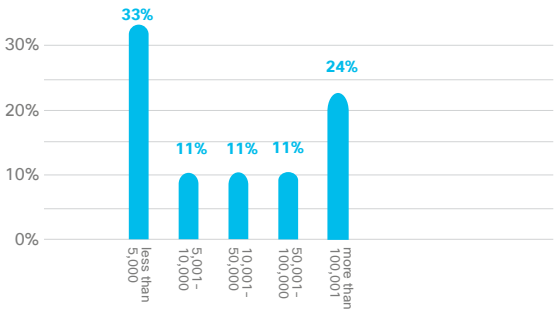
(Note: in each country report we outline recommendations to improve downtime and build an effective cyber resilience plan)

5. The highest percentage of daily alerts investigated

Security practitioners in Asia Pacific are being kept busier than their global counterparts when it comes to receiving security alerts.

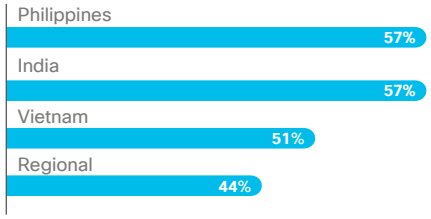
At a worldwide level, 49% of respondents reported receiving fewer than 5,000 alerts per day (some countries are receiving more than 500,000 alerts a day) whereas in the Asia Pacific region, that figure is only 33% (albeit this is a big improvement on last year's average of 25%). Most countries receive far more than 5,000 alerts every single day.

Chart: Regional average of alerts received:



The real challenge, as ever, lies in what comes after the alerts are received: how many are actually investigated. While the regional figure is 44% alerts investigated (which has fallen by 12% in the last year), here are the countries that are pulling that percentage figure up with their investigation abilities:

Chart: Countries with the highest percentage of alerts investigated



6. The highest percentage of legitimate alerts remediated

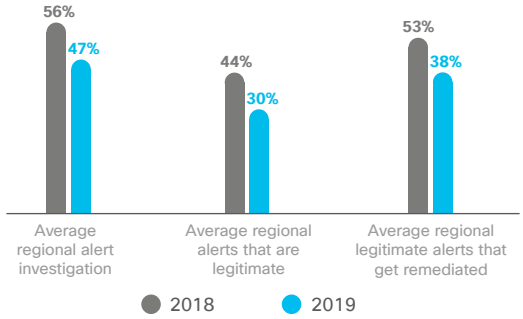
Even more significant than the investigation, is the ultimate remediation of legitimate security incidents. The average remediation level for Asia Pacific is 38%, lower than the global average of 43%.

In 2019, there are significantly fewer legitimate alerts being found among the investigations. This is good news for defenders in that there isn't an actual incident, but it does mean that more false positives are being generated, and could be a potential reason as to why investigation levels are shrinking.

These are the countries that are doing the best remediation work (you'll notice that the Philippines comes top in both investigation and remediation):

Chart: Countries with highest percentage of alerts remediated

Chart: Average percentage of regional alert investigated and remediated and alerts that are legitimate in 2018 and 2019

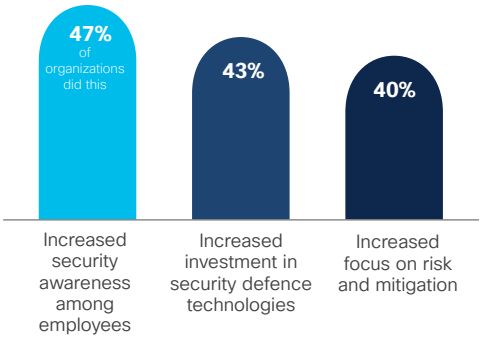


7. Most common areas of improvement after a breach

Asia Pacific organizations drove a significant amount of improvements after they experienced a breach in the past year. The top one by far was to increase security awareness among employees. This makes sense, given that investment in specialized security teams and bridging the talent gap in Asia Pacific is a major obstacle. As a result, organizations will be more reliant on their general employees being able to spot attempted phishing and email spoofing attacks.

Another thing to note is that globally, the top improvement (34%) was to hire a CISO (Chief Information Security Officer)—only 24% of organizations chose to do this in Asia Pacific, preferring to go down the general employee/security tool route rather than invest in a strategic role. This might be having an impact on budget allocation, which we'll explore in the regional trends section.

Chart: Top three most common areas of improvement after a breach



8. The countries with the most amount of different security vendors to manage

As you'll see in the 2019 report, many of the issues facing organizations in Asia Pacific when it comes to cybersecurity (i.e., volume of alerts and huge amounts of downtime) seem to stem mainly from a lack of integration in a multi-vendor environment.

Your security vendors need to be people who aren't thinking about selling their products, but about protecting your business.

The best way to do that is for security to work as a team. Teams communicate in real time, teams learn from each other, and teams respond as a coordinated unit. Your endpoint security has to work with your network security and with cloud security, and you have to have MFA that speaks to identity and access. And you can only get to securing your business with a platform approach.

When that happens, security becomes easier and more effective.

Here are the countries who find working in a multi-vendor environment the most challenging. There is a direct correlation between the countries who use the most vendors on average, and the countries who find this approach more challenging—signalling the need for change and consolidation.

Chart: Countries with highest percentage of organizations who found working in a multi-vendor environment the most challenging

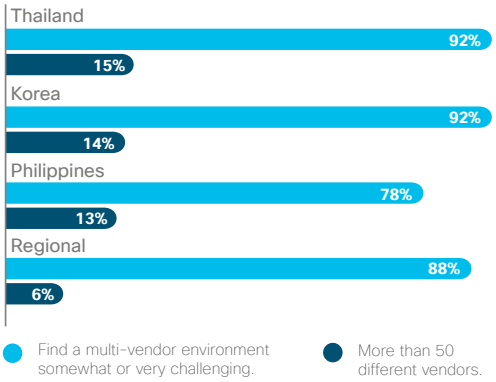
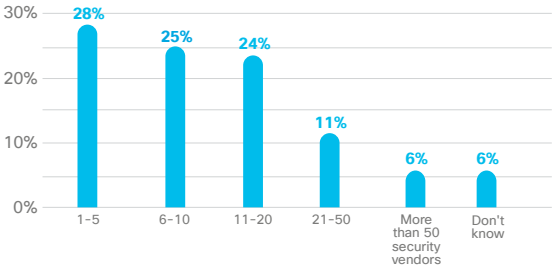


Chart: Average regional rates



Key regional trends

1. Cloud

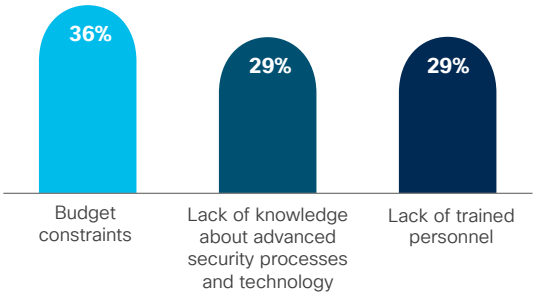
Asia Pacific countries tend to have higher percentages of their infrastructures hosted in the cloud rather than on-premise. 16% have between 80–100% hosted, compared to just 9% in this bracket globally.

When asked for the main reasons as to why the organization embraced cloud technology, ease of use came top (52% of Asia Pacific countries chose this reason), closely followed by "cloud offers better data security" (50% of countries felt this was an important aspect of their decision).

2. The most cited obstacles for adopting advanced security technologies

We asked organizations what were the biggest barriers to increasing their cybersecurity activities, and interestingly, the top three obstacles are all interconnected in a slightly vicious cycle. For example, in order to receive budget for advanced tools, you need the knowledge, skills and the resource to implement them. Since all are significant issues for Asia Pacific, they almost define each other.

Chart: Most cited obstacles for adopting advanced security technologies



3. Operational Technology attacks

OT networks support infrastructure, such as manufacturing, utilities and defence, as well as building infrastructure that operates key facility systems such as lights, elevators, and heating and cooling systems. OT systems monitor and ensure the safety of these operations. An OT network, for example, may monitor a switch and trigger a shutdown if a certain value is exceeded. While OT systems run critical infrastructure, they paradoxically often run on aging software and obsolete hardware, which makes them difficult to patch and highly vulnerable to exploits by malicious actors.

NotPetya (also known as Nyetya) was malware that made its debut via a software update to M.E.Doc, which is an accounting software used extensively in Ukraine. But what began as a software exploit that infected enterprise IT networks spread pervasively to disrupt companies' OT networks. What makes NotPetya and its ilk of cyberattacks all the more concerning is that OT networks are increasingly connected to enterprise IT networks that house critical company data.

We asked organizations to tell us whether they have already experienced an OT attack, and whether they expect OT attacks to gain more prominence.

In Asia Pacific, 25% of organizations had already experienced an OT attack, and 73% expected this trend to increase in the next year. The rest believed cyber attacks to be focused on IT, and not OT.

This is a big shift from last year, when only 50% believed attacks would target OT.

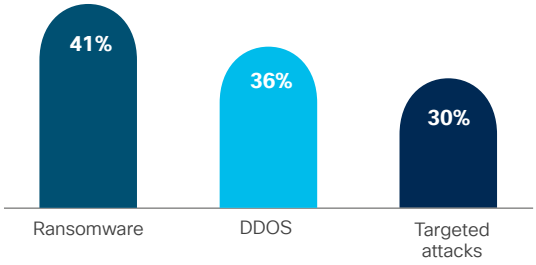
By contrast, 21% of organizations in the rest of the world told us they had already experienced an OT attack, with 64% expecting OT attacks to increase in the next year, and 36% believing that OT attacks are not a growing trend.

This shows us once again how reactive the security industry can be. Often it takes an attack for us to take something seriously, and because organizations in Asia Pacific have already experienced more OT attacks, a higher percentage of this region believe OT attacks to rise.

4. Top three security risks

We asked each survey responder to tell us their three biggest security risks. The top three were Ransomware (41%), DDOS (36%), and targeted attacks (i.e., phishing, email spoofing) (30%).

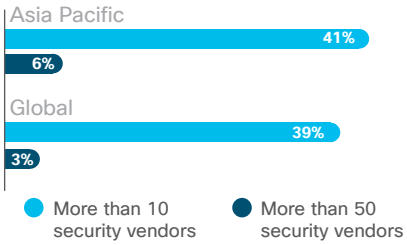
Chart: Top 3 security risks



5. Managing a multi-vendor environment

Organizations in Asia Pacific are managing slightly more vendors per company than their global counterparts. 41% are using more than 10 vendors, compared to 39% globally. 6% are using more than 50 vendors, compared to 3% globally.

Chart: Percentage of organizations with more than 10 or 50 security vendors in their security environment in Asia Pacific and global



When asked how challenging a multi-vendor environment is to manage, countries in Asia Pacific are finding it tougher. 83% said it was either somewhat or very challenging, compared to 79% of organizations across the rest of the world. It seems there is a direct correlation between the higher number of vendors, and the burden it is to manage them.

6. Average alert remediation

Countries in Asia Pacific lag behind the worldwide figure for alert investigation (44% versus 51% globally), and also on legitimate alert remediation (38% compared to 43% worldwide). This is a large drop from last year for the region, when 53% of legitimate alerts were being remediated.

7. Downtime and costs

Downtime* is a particular issue for Asia Pacific countries especially this year. Globally, the average percentage of organizations who experienced downtime of over 24 hours after their most severe breach is 4%.

In Asia Pacific, this is 23%. 13% of organizations in the region were down for more than 48 hours, and 5% had to wait five days before normal business could be resumed.

This is a dramatic increase from 2018, when 9% of organizations suffered downtime of over 24 hours. The fact that this is now 23% indicates several countries had hugely disruptive breaches over the course of the year.

This does mean that the cost of a breach tends to be higher in the region (costs include the cost of the investigations, lost revenue, lost customers, lost opportunities and out of pocket costs). Globally, 33% of organizations paid less than $100,000 after their most severe breach. In Asia Pacific, only 24% are in the sub $100,000 bracket.

In the middle bracket, 33% of organizations in the rest of the world pay upwards of $1,000,000 after their most severe breach. In Asia Pacific, this number was 37%.

For very severe breaches (over $5,000,000) only 8% of global organizations endured these costs, compared to 12% of APJC organizations. The higher costs at this extreme end will likely be caused by the more severe breaches that the region was subjected to this year.

Seven recommendations based on the key findings

1. Achieving simplicity

With the challenges that Asia Pacific countries are telling us they are experiencing from a multi-vendor environment, it might be pertinent to consider a Zero Trust approach.

This approach looks to simplify security by looking at three key areas:

Workforce
Protect your users and their devices against stolen credentials, phishing, and other identity-based attacks

Workload
Managing multi cloud environments and contain lateral movement across the network

Workplace
Gain insights into users and devices, identify threats and maintain control over all connections in your network

To secure the workplace, Zero Trust starts with establishing a level of trust around the identity of the user and what they can access to work within the organization's environment. Having checked the device and authenticated the user, the next fundamental element is controlling what doors to what applications they can enter, and what is considered out of bounds.

The Zero Trust approach is about restricting a user so that they can only enter an area which is approved and relevant to their duties. This all needs to be done with minimal impact on the end user. Introducing difficulty into any security control area just breeds avoidance. What is appealing about the agile and flexible approach is its ability to bring new applications on board wherever they are found–whether running in the cloud, in a local data center or a third-party application. No matter where the doors are, they can be open or shut from a central point based on a policy.

2. Streamlining your existing security tools, and managing complexity

For many organizations, you've been forced to pick individual solutions from an industry that's rife with incompatibility. This has put you on an endless treadmill of stitching up products that don't easily fit together. And that's on top of everything else–new regulations, board mandates, budgets, the revolving door of security talent. The grind never stops.

At the heart of your platform should be a simple idea: 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.

The crucial thing is to "use what you've got" before replacing everything, and making sure that everything comes back to the problem you're trying to solve. At Cisco we're committed to third party integration so that our customers are better protected. The bad guys are working collaboratively and connected, so we need to make sure, as an industry, that we're doing the same. Otherwise we will always be playing the hackers' game, and having the rules dictated to us.

3. Reducing cybersecurity fatigue levels

Overall, the average percentage of organizations in Asia Pacific suffering from cybersecurity fatigue was 52%, which is a small reduction from last year by 4%. So while overall levels are better, the improvement pales in comparison to the worldwide figure of a 30% burnout rate, which is a 16% improvement in the last year.

Some countries, such as Korea, the Philippines and China, have drastically increased their fatigue levels.

Burnout can be a real issue in the security industry, so when it comes to coping with cybersecurity fatigue, here are our tips:

1. Training
Organizations could take advantage of cybersecurity courses from vendors and certification groups to bolster in-house skills and help teams feel more on the front foot. The Cisco Learning Network now offers a new Cisco Cybersecurity Specialist certification for people who want to take on a first-responder role when networks have been attacked. Global Information Assurance Certification (GIAC) has a new Network Forensic Analyst certification that gives security professionals the skills to extract and analyse artefacts and activity left behind from unauthorized activity or network-based attacks.

2. Automating manual processes
This means not having to go on a wild goose chase to stop malware from entering even more of their systems. For example, a network security device spots an infected computer, and has the network automatically quarantine it so it can't do any further harm.

3. Orchestration, via a Zero Trust approach (see above)

4. Keep your software current
Unpatched or outdated software represents an attractive attack surface for adversaries, and increases the pressure on security teams.

4. Building a cyber resilience plan to reduce downtime

Having a cyber resilience plan that is understood and tested regularly, is crucial to alleviate downtime and costs after a breach.

Here are some tips on what should be considered as part of your plan:

- Assign responsibilities – who is doing what? Roles should include analysis, communication with the team/customers/press, and setting up remote working.
- Identify a leader – someone who knows your business and your security strategy.
- Your plan should allow fluidity, to incorporate the latest threats.
- Determine the critical components of your network to replicate in a remote location.
- Have a back-up plan in case a key team member is away.

Ask yourself what the damage will be to your business if corporate data made it onto the internet. Will it only cost you downtime and reputational damage, or will there be greater costs?

5. How to get more budget in the boardroom

The first thing to mention here is that in Asia Pacific, there isn't as much willingness to hire a CISO as there is in other countries. After a breach, the top improvement at a global level was to hire a CISO. In Asia Pacific, not only is there ten percentage points in difference, hiring a CISO was one of the least opted routes. Not having someone on a strategic level, in the C-Suite, could be hindering budget allocation for security.

Secondly, studies show that almost a quarter of boards are dissatisfied with the level of reporting about cybersecurity. The problem is often a lack of benchmarking, a lack of clarity about what risk factors that a particular business is facing, and overall, the reporting is incredibly complicated and difficult to interpret.

The most important thing to bear in mind when asking for more support on cybersecurity, is to keep things simple with a clear call to action. If you don't know exactly what improvements need to be made, not only have you given the cyber criminals a massive head start, but your board is unlikely to be convinced of the value of the investment.

Done right, cybersecurity can actually give you a strong competitive advantage. It's no longer about aiming to contribute "nothing", but instead, security is increasingly being used to differentiate companies from their competition. "We can do this, because we're secure." "We can scale that in the cloud, because we're secure."

Here are some tips to get more budget assigned from the boardroom:

1. Personalise your business' cybersecurity risk factors. Just like employers don't like receiving generic CVs, boards don't like it when they have to look at stuff that is of little relevance. What does risk mean to you? Are you a retail business that is particularly at risk at peak periods? Are your employees more likely to partake in Shadow IT?

2. It's also important to benchmark this against other companies in your industry. Boards like context—it's not just your business that needs to mitigate this risk—everyone needs to.

3. Even better, add a monetary value on the potential cost of a data breach for this particular risk. Don't forget to add legislative fines on top of this.

4. Demonstrate a scenario of a cyber attack. For example, a ransomware attack on an endpoint. Explain how your current security posture would cope with such an attack and, how you could limit the damage with more effective layers of security. Crucially, how quick can you respond? At what point would you know about the threat? What can be done to improve this? Again, put monetary values on the potential downtime/cost to remove the malware.

You could also use high-profile breaches as an opportunity to have a conversation with the board. Describe how that breach can happen in your organization. Then show them how to address vulnerabilities.

6. Getting the right skills

According to industry analysts, there will be a global shortage of two million cybersecurity professionals as early as next year. If not addressed, it could grow to three and a half million by 2021. With the threat landscape as diverse as ever, we'll need to create a global cybersecurity workforce as diverse as ever.

Here are some things we could consider to increase security skills across the region:

1. Open the door to newcomers. Cisco Australia have started a program to encourage more females to join the cybersecurity industry called MentorMe, a six-month program that pairs female university students across Australia with a Cisco mentor (mentors are both women and men). For those of us already in the industry, this is our role to play! Participating in a mentorship is one of the ways we can open the door and introduce newcomers to various cybersecurity career paths.

2 As security discussions move to the boardroom, CISOs and their teams need data science skills to analyse cybersecurity data and business skills to manage trust (company reputation) and risk (costs). The new CISO must communicate not in bits and bytes, but in plain language.

3 Consider using security partners and managed security service providers (MSSPs) who continually invest in security expertise, intelligence, and innovative new technologies—this is a way to keep pace with a dynamic threat environment.

4 Train existing talent. In an effort to train talent that will support Tokyo 2020 and develop the next generation of cybersecurity professionals in Japan, our local Cisco team has launched a Cybersecurity Talent initiative program. Using a combination of Cisco Net Academy curriculum, coupled with on-the-job training opportunities, the program is honing in on creating more female engineering talent in Japan. This same model is also being applied to second career retraining opportunities locally.

The talent shortage numbers may look scary and there is a lot of work to do still. Yet, there are reasons to be hopeful. Since we started teaching cybersecurity courses at the Cisco Net Academy five years ago, nearly half a million students have been served, with 32% of those in just the past year demonstrating an encouraging and growing interest. In fact, we had 238% growth in students participating in cybersecurity courses during the FY17–FY18 fiscal year alone.

7. Increasing security awareness among employees

We often hear that "humans" are the weakest link when it comes to security. While that may be true, it can be a little harsh to label us as such, when we are being actively targeted by cyber criminals at the same time as having day jobs, targets to meet, etc.

The truth is, the bad guys are getting cleverer and cleverer in their schemes to try and persuade us to click on malicious links or attachments, without us spotting anything suspicious. What we need is a greater understanding of the types of threats that involve human interaction in order for them to be successful.

As targeted attacks is a top three risk for organizations in Asia Pacific, here are our tips on what to do with the type of attacks your employees receive every day, such as phishing attempts and email spoofing:

- Look out for a sense of urgency. For example, if they urge you to act now to take advantage of something or prevent something.
- Be wary of an overly generous offer, and/or an email or attachment you weren't expecting/from someone you don't know.
- Hover over links before you click on them. If it looks suspicious, it probably is!
- Do simulation exercises for assessing how your employees react to a staged phishing attack, and then educate them. Duo Insight is a free phishing assessment tool by Duo Security that allows you to find vulnerable users and devices in minutes and start protecting them right away.
- Check the sender's address. Is there a slight misspelling?
- Put a policy in place; always verify wire transfers with a phone call (don't just email back—the scammer can do that too!).
- Filter any messages that have an envelope sender (Mail-From) and "friendly from" (From) header that contain one of your own incoming domains in the email address.

Notes:

1. * Downtime: The set of global data available does not offer a level of detail beyond "More than 24 hours" and the figure of 4% might include data that stretches into multiple days.
2. "Global" refers to a survey published in February 2019 which includes 18 worldwide countries, of which four are in Asia Pacific (Australia, India, Japan and China. Regional data was collected in July 2019 as a response to these figures and is not a subset of the "global" number.

Country Overview

Australia Overview

Introduction

For Australia, the main callout is that **organizations are suffering immensely from cybersecurity fatigue** (defined as virtually having given up on proactively defending against threats). This is strange when security appears to be a high priority at the executive level, but this hasn't translated into a budget allowance. For the first time, budget constraints have become the top obstacle for Australia.

A possible reason for the fatigue levels is that **corporations in Australia now receive twice the amount of daily security alerts than they did last year.** This has affected their ability to investigate alerts and remediate legitimate ones. The **percentage of real security incidents that have been fixed has dropped by a concerning 31%.** Unfortunately, the monetary costs of a breach in Australia are higher than other countries. **84% of organizations in Australia suffered a breach that cost them over $1m.**

On the positive side, Australia is making great strides where it comes investing in people and teams rather than just technology. They are relatively confident in their security tools' ability to deal with adapting threats, and so hopefully this investment in people and processes will bring those fatigue levels down.

The cybersecurity culture in Australia

98% of Australian organizations surveyed also told us that they somewhat or strongly agreed that their organizations take cyber risk into account as a matter of routine. However, when we look at the constraints of investments in advanced security practices, we see a different picture.

Table: The greatest obstacles to adopting advanced security processes and technology in organizations

	Australia	Regional	Global
Budget constraints	37%	35%	35%
Competing priorities	30%	22%	26%
Lack of trained personnel	22%	29%	24%
Lack of knowledge about advanced security processes and technology	21%	33%	22%
Compatibility issues with legacy systems	23%	29%	27%
Certification requirements	27%	20%	24%
Organizational culture/attitude about cybersecurity	32%	27%	21%
Reluctance to purchase until they are proven in the market	23%	18%	20%
Current workload too heavy to take on new responsibilities	26%	23%	22%
Organization is not a high value target for attacks	22%	16%	16%
Security is not an executive level priority	19%	15%	13%

In 2018, the top three obstacles for Australia were certification (33%), organizational culture (30%), and competing priorities (28%).

In our 2019 survey, budget constraints have become the top obstacle (37%) even though it was outside of the top three challenges the previous year. Budget constraints is followed by organizational culture/attitude about cybersecurity (32%) and competing priorities (30%).

The top two obstacles may indeed be linked–organizational culture/attitude about cybersecurity could affect budget decisions. Although the majority of executive leaders see security as a high priority, budget is not necessarily granted to solving cybersecurity challenges within those organizations.

We asked organizations in Australia if they were suffering from cybersecurity fatigue.

Australia is almost the reverse of the global average when it comes to cybersecurity fatigue (Australia 65% vs global 30%). Far more organizations are struggling to defend against threats than those who say they feel as though they are on top of it.

On the positive side, 65% is a decrease from our 2018 study, when 69% of organizations surveyed told us they were suffering from cybersecurity fatigue. There is more to be done before Australian organizations can feel like they have an empowered culture of cybersecurity, rather than an overwhelmed one.

Security alerts and the impact of data breaches

Australian organizations receive a much higher average of daily alerts than the global average. In fact, 69% of organizations surveyed received more than 100,000 alerts every single day. This is more than double last year's figures (33%).

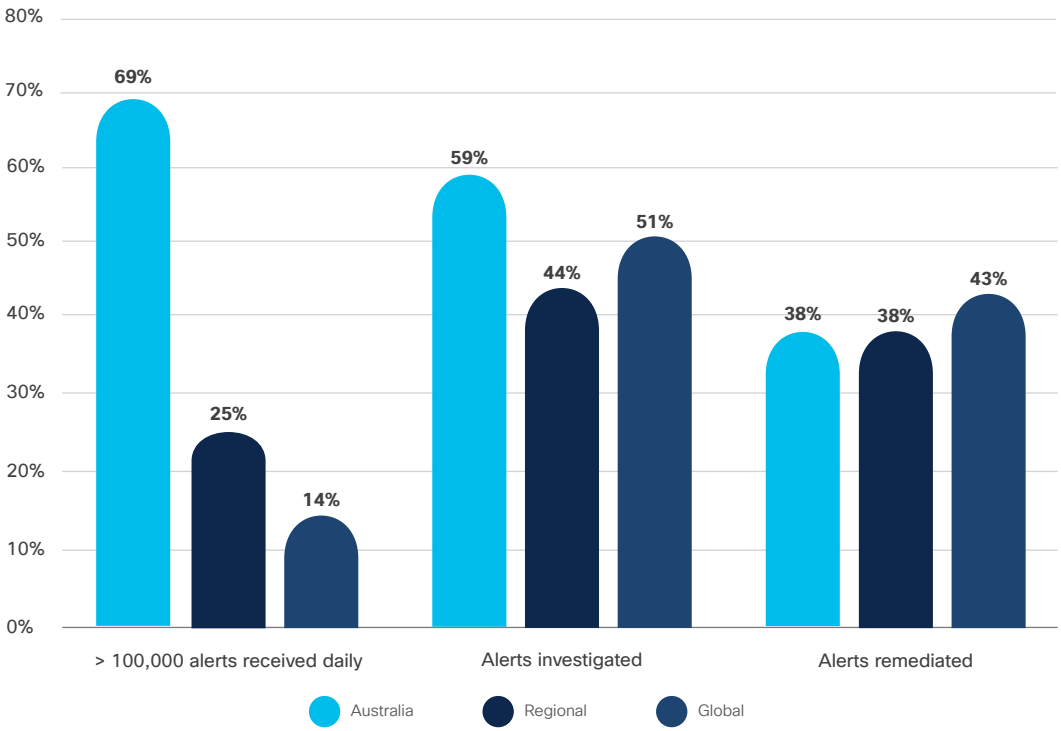
However, even though more alerts are received, Australian organizations are able to investigate a higher percentage of them than in other countries. This suggests that the country may have more dedicated resources to activate investigations.

The fact that Australia is receiving far more alerts last year, seems to be having a direct impact on the number of alerts they can investigate. The percentage is at 59%, down from last year when 72% of alerts were able to be investigated.

Last year, 65% of investigated alerts were legitimate. This is now 33%, suggesting that the vast increase in daily alerts are mostly false negatives/noise.

In our 2018 study, the percentage of remediated legitimate alerts was 69%. This has declined dramatically to 38%.

Chart: Alerts received, investigated and remediated



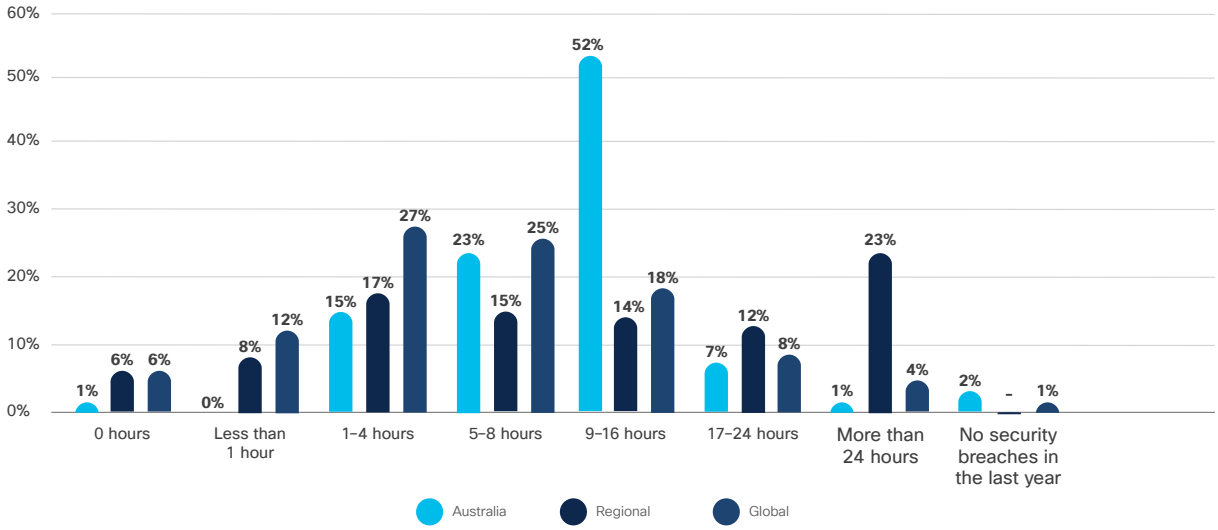
Australia is now below the global average which indicates that perhaps too much resource is going into investigating all alerts, and not enough going into remediating legitimate ones. This could be a reason why cybersecurity fatigue in Australia is so high compared to the global average.

When it comes to data breaches and the improvements that were made following a breach, the top four for Australia were: increased enforcement of data protection laws and regulations (perhaps to avoid another costly fine), hired/ created CISO, established compliance/ risk management office, formed a team that specialises in Security.

Most of these improvements aren't technology/ products related. They are people and roles related, indicating that Australia is choosing to invest in people/ skills to tackle cybersecurity challenges.

We also asked about the organisation's most severe breach, and how long systems were down as a result. 75% of organisations experienced outage of 5-16 hours. This is longer than the global average (43%).

Chart: Downtime* following a data breach in businesses



We also asked about the monetary cost from their most impactful breach. Cost of breach in Australia is vastly higher than the global average. For 84% of organisations in Australia that suffered a breach, it cost them over $1,000,000.

Nearly half of Australian organisations received a monetary cost of $5,000,000 – compared to only 7% globally.

Cloud trends

In general, Australian organizations host more of their networks in the cloud than in any other countries surveyed. This suggests the Australian market is more ready to embrace the opportunities provided by the cloud. When asked why they chose the cloud, the top reason was that cloud offers better ease of use, followed by better security.

Table: Reasons for using cloud to host IT infrastructure among businesses

	Australia	Regional	Global
OpEx preferred over CapEx	28%	33%	26%
Lack of internal IT workforce	37%	22%	25%
Cloud offers better data security	45%	50%	50%
Scalability	41%	43%	40%
Regulation or compliance requirements	41%	29%	27%
Ease of collaboration with external parties	43%	52%	37%
Ease of use	51%	19%	51%
Not core to business so outsourcing is preferable	27%	40%	18%
Other	1%	-	1%

Over a third of Australian organizations have already experienced an Operational Technology attack, 15% more than global. The vast majority expect this trend to continue, indicating that Australian organizations are more tuned to this particular cyber trend than other countries.

The defenders' approach

The number of organizations using more than 50 vendors has gone down from 12% in our 2018 study to only 1% in our 2019 study, indicating a strong move towards consolidation.

However, 78% of Australian organizations use more than 11 vendors, compared to 35% globally. So while it is a promising move, this integrated approach is an ongoing process. It is possible that cyber fatigue in the country could be reduced with a more integrated, consolidated security architecture to enable automated response to cybersecurity breaches.

94% of Australian organizations find it challenging to orchestrate alerts from multiple vendors, with the vast majority selecting "very challenging". This is further underlined by the sheer volume of alerts they are receiving, and the decline in the percentage of remediated alerts.

Recommendations

As the majority of Australian organizations are currently suffering from the challenges of a multi-vendor environment, it might be **pertinent to consider a Zero Trust approach.** This approach simplifies cybersecurity by focusing on three key areas: identity, device, and applications.

To secure the workplace, Zero Trust starts with establishing a level of trust around the identity of the user and what they can access to work within the organization's environment. Having checked the device and authenticated the user, the next fundamental element is controlling what doors to what applications they can enter, and what is considered out of bounds.

The Zero Trust approach is about restricting a user so that they can only enter an area which is approved and relevant to their duties. This all needs to be done with minimal impact on the end user. Introducing difficulty into any security control area just breeds avoidance. What is appealing about the agile and flexible approach is its ability to bring new applications on board wherever they are found—whether running in the cloud, in a local data centre or a third-party application. No matter where the doors are, they can be opened or shut from a central point based on a policy.

Secondly, **managing so many different interfaces seems to be having an abject effect on many Australian organizations' ability to orchestrate alerts.** Having one management console, such as Cisco Threat Response, can automate integrations across products and accelerate key security operations functions: detection, investigation, and remediation.

China Overview

Introduction

Despite a relatively challenging year for China—if their much higher cybersecurity fatigue levels are anything to go by—the country can **still claim to have one of the highest resolution rates of legitimate security incidents in Asia Pacific.**

Challenges wise, **China is still struggling to integrate legacy systems and multi-vendor environments.** In our recommendations section, we'll look at how a Zero Trust approach can help simplify and integrate existing tools to prevent cybersecurity breaches.

The cybersecurity culture in China

The top three obstacles to adopting advanced security processes and initiatives in China hasn't changed since last year. Managing the compatibility with legacy systems remains the biggest issue, followed by budget constraints and a lack of knowledge about advanced security processes and technology.

Table: The greatest obstacles to adopting advanced security processes and technology in organizations

	China	Regional	Global
Budget constraints	32%	35%	35%
Competing priorities	23%	22%	26%
Lack of trained personnel	28%	29%	24%
Lack of knowledge about advanced security processes and technology	30%	33%	22%
Compatibility issues with legacy systems	36%	29%	27%
Certification requirements	21%	20%	24%
Organizational culture/attitude about cybersecurity	19%	27%	21%
Reluctance to purchase until they are proven in the market	25%	18%	20%
Current workload too heavy to take on new responsibilities	23%	23%	22%
Organization is not a high value target for attacks	17%	16%	16%
Security is not an executive level priority	16%	15%	13%

We asked organizations in China if they were suffering from cybersecurity fatigue.

43% declared they were. This is far higher than the global average (30%), although it's lower than other Asia-Pacific countries such as Australia and Japan, where the percentage of companies experiencing cyber fatigue is in the upwards of 60–80%.

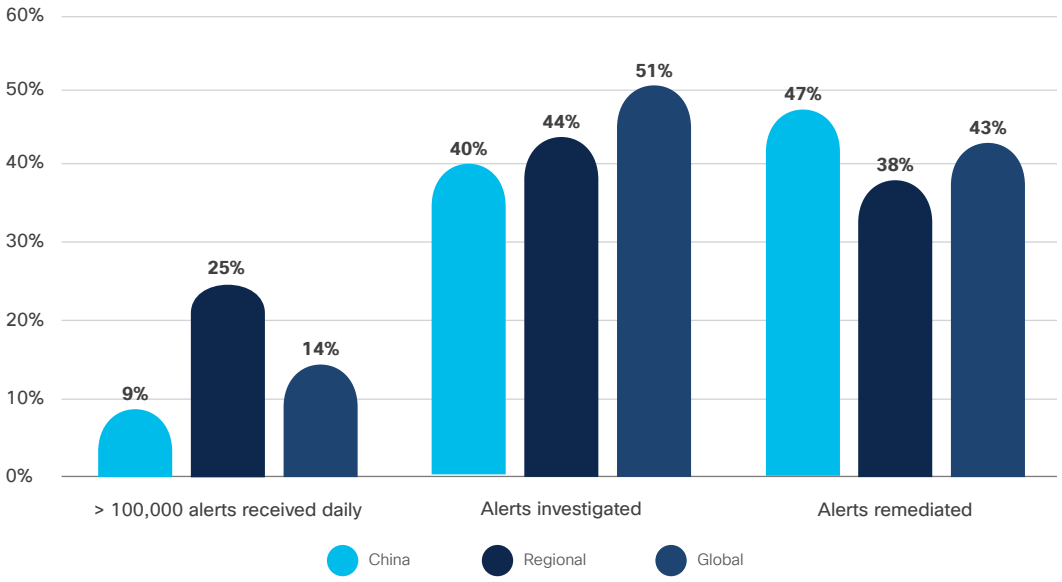
This is a worrying trend. In 2018, this figure was 29%. A year of difficulty seemed to have followed to push this number up by 14 percentage points.

Security alerts and the impact of data breaches

Compared to other countries in Asia, China's record of receiving daily security alerts is rather moderate, in line with the global average. However, when we look at the percentage of alerts that are routinely investigated, China lags behind the rest of the world. The percentage of legitimate alerts is slightly lower in China compared to other countries, which means that many of these alerts are false positives.

On a positive note, China's record of remediating legitimate security incidents is higher than the rest of the world.

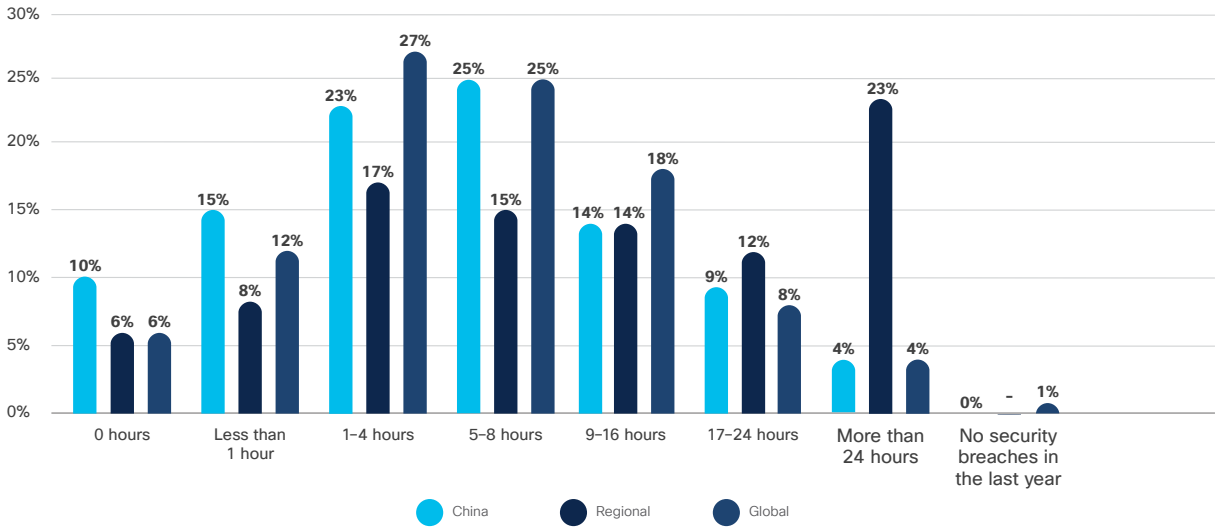
Chart: Alerts received, investigated and remediated



When it comes to data breaches and the improvements that were made following a breach, the top improvement for China was to put higher investments into security defense technologies/solutions. This is followed by an increased focus on risk analysis and risk mitigation, and an increased focus on preventing security breaches caused by employee-owned mobile devices. China's approach differs from its neighbors in Asia Pacific—who typically chose to make improvements in people and teams. China has predominantly chosen to focus on security tools and processes.

We also asked about the organizations' most severe breaches, and how long systems were down as a result. Results in China were slightly better than the global average, with 48% experiencing four hours or less downtime for a severe breach, compared to 45% of global companies who fell into this bracket. The percentage of organizations in China experiencing heavy downtime of nine hours and more is also very similar to the global average.

Chart: Downtime* following a data breach in businesses



Cloud trends

In general, organizations in China host more of their networks in the cloud than other countries. This isn't too surprising for a mature, technology-savvy market.

When asked why they chose the cloud, there were two top reasons: better data security, and ease of use. Scalability is also high on the list.

Table: Reasons for using cloud to host IT infrastructure among businesses

	China	Regional	Global
OpEx preferred over CapEx	37%	33%	26%
Lack of internal IT workforce	23%	22%	25%
Cloud offers better data security	53%	50%	50%
Scalability	50%	43%	40%
Regulation or compliance requirements	23%	29%	27%
Ease of collaboration with external parties	38%	52%	37%
Ease of use	53%	19%	51%
Not core to business so outsourcing is preferable	26%	40%	18%
Other	0%	-	1%

When it comes to operational technology attacks, China very much sees this trend continuing. They experienced a significant level of cyber attacks on OT in the last year, more so than the rest of the world. Most companies in China expect OT attacks to increase. China companies are seeing 9% more cyber-attacks in OT compared to the rest of the world (30% compared to 21%).

The defenders' approach

The increased investment has slightly increased the number of security vendors in Chinese organizations. In our 2018 study, 30% were using more than 10 vendors. This has now increased to 39%. As a consequence, 98% of organizations surveyed find it somewhat or very challenging to orchestrate alerts from multiple vendors, up from last year's 95%.

This could be one of the reasons for China's high levels of cybersecurity fatigue. When you increase the numbers of vendors in your organization without a focus on integration, you tend to be more at risk of reduced accuracy in detection, and slower remediation levels.

Recommendations

As organizations in China struggle with managing a multi-vendor environment with a lack of integration, it might be pertinent to consider a Zero Trust approach.

This approach looks to simplify security by looking at three key areas:

1. **Workforce (protect your users and their devices against stolen credentials, phishing, and other identity-based attacks)**
2. **Workload (managing multi-cloud environments to contain lateral movement across the network)**
3. **Workplace (gain insights into users and devices, identify threats and maintain control over all connections in your network).**

To secure the workplace, Zero Trust starts with establishing a level of trust around the identity of the user and what they can access to work within the organization's environment. Having checked the device and authenticated the user, the next fundamental element is controlling what doors to what applications they can enter, and what is considered out of bounds.

The Zero Trust approach is about restricting a user so that they can only enter an area which is approved and relevant to their duties. This all needs to be done with minimal impact on the end user. Introducing difficulty into any security control area just breeds avoidance. What is appealing about the agile and flexible approach is its ability to bring new applications on board wherever they are found—whether running in the cloud, in a local data center or a third-party application. No matter where the doors are, they can be open or shut from a central point based on a policy.

Secondly, having one management console, such as Cisco Threat Response, can automate integrations across products and accelerate key security operations functions: detection, investigation, and remediation.

India Overview

Introduction

Organizations in India have made significant improvements to their cybersecurity postures in the last year, including increased budget levels and up-to-date infrastructures. 76% of organizations feel their security tools are very or extremely effective in defending against adaptive threats, indicating that India is very well prepared to deal with the ever-changing tactics of cyber criminals.

However, this can be a double-edged sword, as organizations in India have cited high workloads as their biggest obstacle.

On the alerts side, this is a story of two halves. India has dramatically reduced the number of the security alerts received, but its record at investigating those alerts seems to have similarly dropped, as has their remediation record.

Also of note, India has made great strides in integrating their security architectures. In 2018, 57% of organizations in India were using more than 10 vendors. In 2019, that number has gone down to 29%.

The cybersecurity culture in India

In India, there is a strong sense of support for security initiatives. 92% of organizations say that cybersecurity is an executive level priority. However, the biggest hindrance to adopting advanced security processes and initiatives is that people's workloads are currently too heavy to take on any new responsibilities. A potential approach India could take to free up resources may be to increase the level of automation on manual tasks.

Table: The greatest obstacles to adopting advanced security processes and technology in organizations

	India	Regional	Global
Budget constraints	27%	35%	35%
Competing priorities	31%	22%	26%
Lack of trained personnel	22%	29%	24%
Lack of knowledge about advanced security processes and technology	26%	33%	22%
Compatibility issues with legacy systems	31%	29%	27%
Certification requirements	31%	20%	24%
Organizational culture/attitude about cybersecurity	18%	27%	21%
Reluctant to purchase until they are proven in the market	26%	18%	20%
Current workload too heavy to take on new responsibilities	32%	23%	22%
Organization is not a high value target for attacks	18%	16%	16%
Security is not an executive level priority	8%	15%	13%

It's interesting to note that in our 2018 survey, the top obstacle for India was budget constraints at 37%. This has decreased by a whopping 10% in 2019, so much so that it doesn't even make the top three anymore. Security being seen as a higher priority seemed to have shifted budget allocations in favor of it.

We asked organizations in India if they were suffering from cybersecurity fatigue.

India came up at 34%, slightly above the global average (30%). This could be due to the fact that the current workloads were too high. However, this is an improvement on 2018 when 38% of organizations were feeling like giving up on defending against threats. The country also has one of the best fatigue levels in Asia Pacific.

Security alerts and the impact of data breaches

India is close to the average amount of the daily security alerts received overall. The key thing to note is that the percentage of organizations dealing with fewer than 5000 alerts has vastly improved from 38% in our 2018 survey to 54% in 2019.

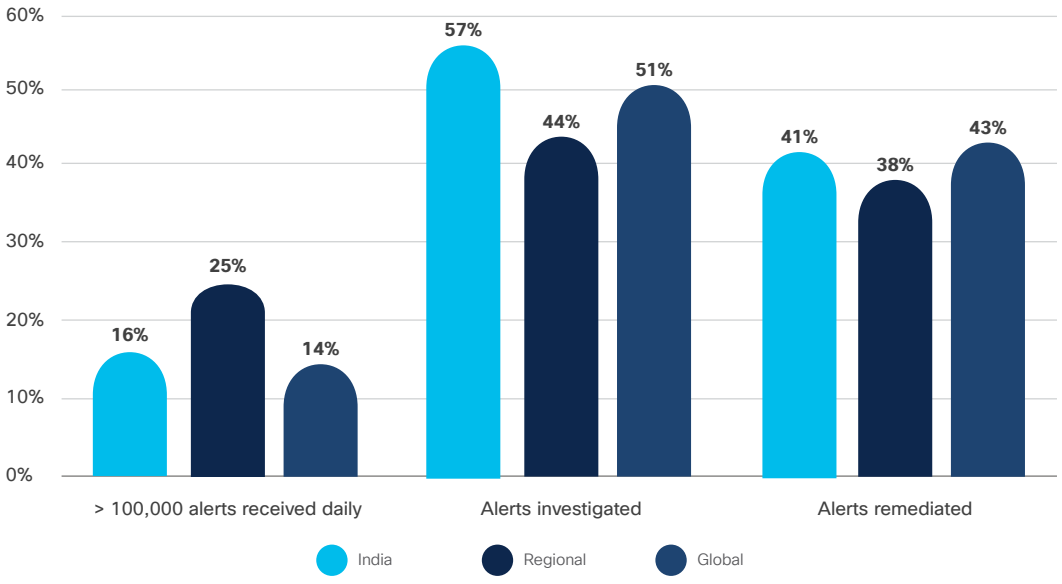
In our 2018 study, we talked about the fact that 17% of defenders were dealing with 250–500,000 alerts per day, way above the regional benchmark. In 2019, this appears to have been brought under control, with only 2% of defenders telling us they are dealing with 250–500,000 alerts every day.

However, even though the number of daily alerts has decreased, India's record at investigating alerts has actually become worse. In 2018, they were able to investigate 61% of all alerts. This has now dropped to 57%. While it remains higher than the global average, it indicates that 43% of all alerts have been left unresolved.

Unfortunately, the number of legitimate incidents in India appears to be higher than the global average. This makes the rate of investigations all the more concerning. What could be getting through the gaps?

The bad news continues. The percentage of legitimate alerts effectively remediated has fallen from 52% in 2018, to 41% in 2019.

Chart: Alerts received, investigated and remediated

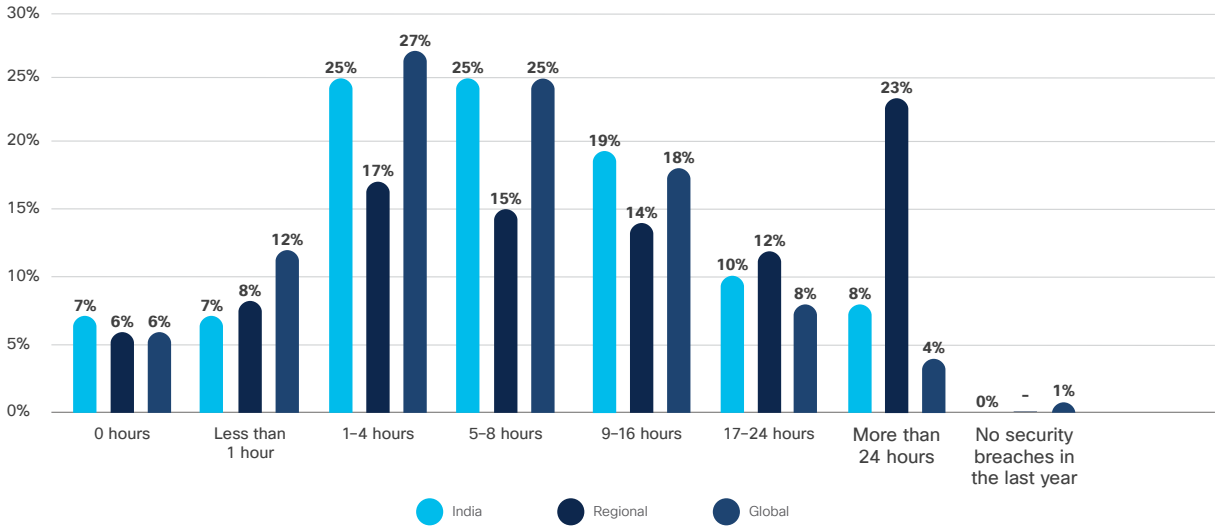


We'll look at some strategies to manage alerts in our recommendations section.

When it comes to data breaches and the improvements that were made following a breach, the joint top improvement for India was to increase enforcement of data protection laws and regulations, and to hire a CISO. This is closely followed by increased security training among employees, and increased investments in the training of security staff. All top improvements are policy or people/training related.

We also asked about the organizations' most severe breaches, and how long systems were down as a result. Results in India were very much on par with the global average, except the more dramatic periods of downtime. 18% of organizations in India experienced downtime for over 17 hours as a result of a severe breach, compared to 12% globally.

Chart: Downtime* following a data breach in businesses



We also asked about the monetary cost from their most impactful breach. Last year, we saw the cost of a breach in India to be either relatively low, or massively high–there was no middle ground. This year, we're seeing less of the "huge" fines, and more moderate costs associated with a breach.

Cloud trends

In general, organizations in India host more of their networks in the cloud than other countries, which suggests the India market is readily embracing the opportunities provided by the cloud.

When asked why they chose the cloud, the top reason for India was that cloud offers better security.

Table: Reasons for using cloud to host IT infrastructure among businesses

	India	Regional	Global
OpEx preferred over CapEx	48%	33%	26%
Lack of internal IT workforce	22%	22%	25%
Cloud offers better data security	60%	50%	50%
Scalability	48%	43%	40%
Regulation or compliance requirements	36%	29%	27%
Ease of collaboration with external parties	50%	52%	37%
Ease of use	54%	19%	51%
Not core to business so outsourcing is preferable	14%	40%	18%
Other	0%	-	1%

Despite the fact that a quarter of organizations in India have already experienced an Operational Technology attack–a rate higher than the global average–not as many organizations expect this trend to continue. In fact, 34% of organizations in India don't expect to be hit by an OT attack in the next year, if at all.

The defenders' approach

We may well have found the reason behind the vastly reduced number of security alerts in India: they are using far fewer vendors on average than in 2018. In 2018, 57% of organizations in India were using more than 10 vendors. In 2019, that has gone down to 29%.

A catalyst for the big move towards consolidation may be just how challenging it is to orchestrate alerts from multiple vendors' security products. 89% of organizations surveyed find it somewhat or very challenging to orchestrate alerts from multiple vendors.

The drive towards consolidation has also dramatically decreased the number of different security products used by organizations in India. In our 2018 study, 67% were using more than 10 products. This is now 41%. In 2018, 24% were using more than 50 products. This is now just 11%.

Recommendations

Things “getting through the gaps” was certainly an issue to highlight for India this year. As such, it might be pertinent to consider a Zero Trust approach.

This approach looks to simplify security by looking at three key areas:

1. Workforce (protect your users and their devices against stolen credentials, phishing, and other identity-based attacks)
2. Workload (managing multi-cloud environments to contain lateral movement across the network)
3. Workplace (gain insights into users and devices, identify threats and maintain control over all connections in your network).

To secure the workplace, Zero Trust starts with establishing a level of trust around the identity of the user and what they can access to work within the organization’s environment. Having checked the device and authenticated the user, the next fundamental element is controlling what doors to what applications they can enter, and what is considered out of bounds.

The Zero Trust approach is about restricting a user so that they can only enter an area which is approved and relevant to their duties. This all needs to be done with minimal impact on the end user. Introducing difficulty into any security control area just breeds avoidance. What is appealing about the agile and flexible approach is its ability to bring new applications on board wherever they are found—whether running in the cloud, in a local data center or a third-party application. No matter where the doors are, they can be open or shut from a central point based on a policy.

Indonesia Overview

Introduction

Indonesia has made hugely positive strides in cybersecurity over the past year in almost every area. Security alert investigation and remediation levels are looking more positive, and cybersecurity fatigue levels have decreased dramatically.

Possible reasons for this could be a drive towards automation to alleviate manual resources, and an overall increased effort towards consolidation and integration within multi-vendor environments.

The cybersecurity culture in Indonesia

Currently, the biggest issue preventing organizations from adopting advanced security processes and technology is a fairly common one: budget constraints. Almost half of the organizations surveyed cited this as their greatest challenge. It is also higher than last year by 8%. The next challenge, selected by just less than a third of organizations, is compatibility with legacy systems.

Table: The greatest obstacles to adopting advanced security processes and technology in organizations

	Indonesia	Regional	Global
Budget constraints	47%	35%	35%
Competing priorities	18%	22%	26%
Lack of trained personnel	22%	29%	24%
Lack of knowledge about advanced security processes and technology	25%	33%	22%
Compatibility issues with legacy systems	30%	29%	27%
Certification requirements	28%	20%	24%
Organizational culture/attitude about cybersecurity	26%	27%	21%
Reluctant to purchase until they are proven in the market	15%	18%	20%
Current workload too heavy to take on new responsibilities	18%	23%	22%
Organization is not a high value target for attacks	16%	16%	16%
Security is not an executive level priority	20%	15%	13%

We asked organizations in Indonesia if they were suffering from cybersecurity fatigue.

Indonesia has one of the best records in Asia Pacific with regards to cybersecurity fatigue levels (Indonesia 35% vs global 30%). In fact, it has decreased from 58% in 2018 to 35% in 2019. This indicates that the country has made significant improvements to its overall cybersecurity culture.

Security alerts and the impact of data breaches

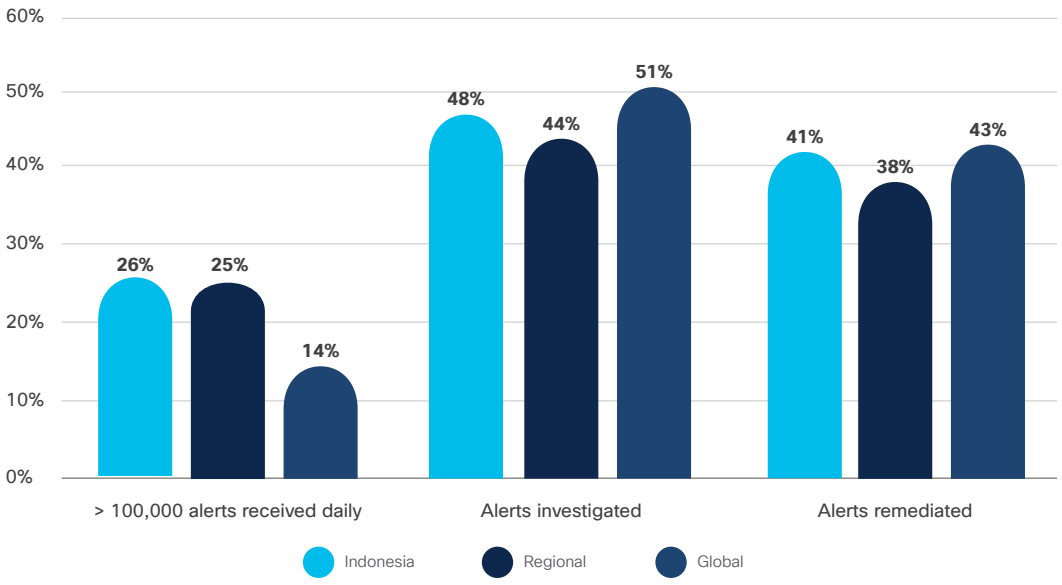
One possible reason for the improved fatigue levels is that organizations in Indonesia have brought their daily security alerts down significantly. In 2018, only 28% were receiving less than 5000 daily alerts. This number has increased to 43%.

On average, organizations in Indonesia were able to investigate 48% of all the alerts received, close to the global average. It's a slight improvement on last year's results, but this does still mean that half of all security alerts are never investigated.

The percentage of legitimate alerts is higher than the global average, which means Indonesia deals with more genuine incidents.

Overall, organizations in Indonesia are fixing 41% of legitimate incidents, which is exactly the same as in 2018.

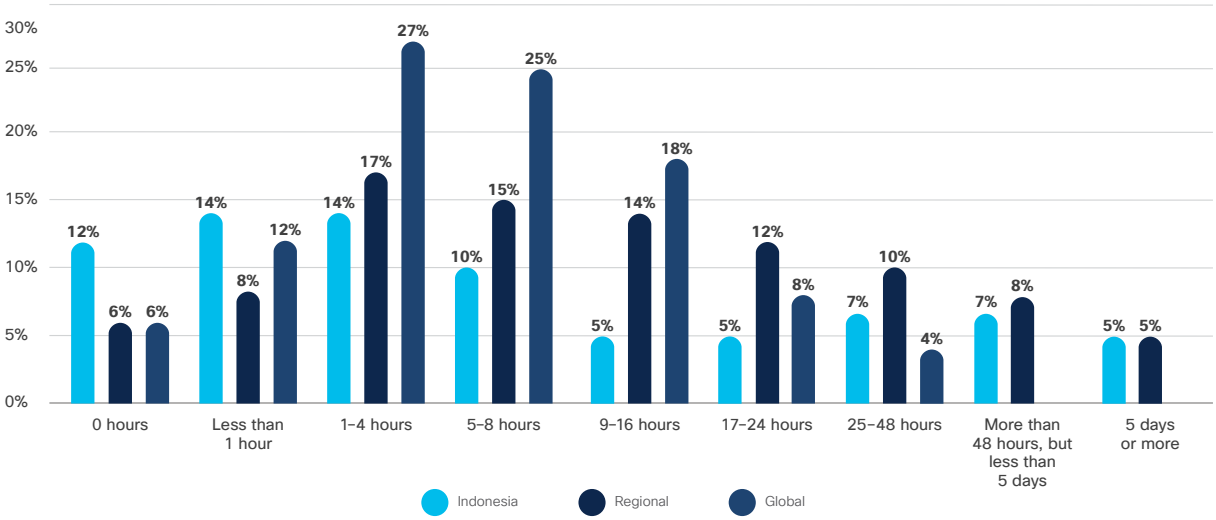
Chart: Alerts received, investigated and remediated



When it comes to data breaches and improvements made following a breach, the top improvement was greater investment in security defense technologies/solutions. Which may be a reason as to why budget constraints are doubly an issue this year – organisations in Indonesia are clearly fighting for more investments, with some being fortunate, and others not so much.

We asked respondents to select every improvement that applied in our survey. It is interesting to note that Indonesian organizations made more improvements in the last year than the global average. This will certainly have helped decrease cybersecurity fatigue levels.

Chart: Downtime* following a data breach in businesses



We also asked about the organizations' most severe breaches, and how long systems were down as a result. This is where Indonesia's experience of dealing with more legitimate security incidents is having an effect, as downtime is a greater issue for severe breaches when compared to worldwide. 19% of organizations were down for more than 25 hours in the last year (compared to 4% globally).

Cloud trends

62% of organizations in Indonesia have more than 40% of its infrastructure hosted in the cloud. Overall, Indonesia embraces the cloud more so than their global counterparts.

When asked why they chose the cloud, the top reason for Indonesia was that cloud offers better security, closely followed by its ease of use.

Table: Reasons for using cloud to host IT infrastructure among businesses

	Indonesia	Regional	Global
OpEx preferred over CapEx	25%	33%	26%
Lack of internal IT workforce	11%	22%	25%
Cloud offers better data security	67%	50%	50%
Scalability	34%	43%	40%
Regulation or compliance requirements	28%	29%	27%
Ease of collaboration with external parties	41%	52%	37%
Ease of use	63%	19%	51%
Not core to business so outsourcing is preferable	20%	40%	18%
Other	0%	-	1%

Just over half of organizations in Indonesia fully expect cyber attacks to extend beyond IT and into Operational Technologies next year.

This is another sign that security remains a reactive industry. In order for organizations to take a breach seriously, they need to experience it. Having witnessed more OT attacks, more organizations in Indonesia expect this trend to stick around.

The defenders' approach

The percentage of organizations in Indonesia who use more than 10 vendors has declined from 41% in 2018 to 35% in 2019. This could be the reason as to why fewer alerts/false positives are being generated.

This also means that the percentage of organizations struggling to orchestrate alerts from multiple vendors' security products has gone down from 87% in 2018 to 66% in 2019.

Recommendations

Indonesia has made huge improvements over the past year, so the main recommendation would be for them to keep doing what they're doing.

As budget constraints are more of the issue today, here are some tips to get more budget assigned from the board room:

1. Personalize your business' cybersecurity risk factors. Just like employers don't like receiving generic CVs, boards don't like it when they have to look at stuff that is of little relevance. What does risk mean to you? Are you a retail business that is particularly at risk during peak periods? Are your employees more likely to partake in Shadow IT?
2. It's also important to benchmark this against other companies in your industry. Boards like context–it's not just your business that needs to mitigate this risk. Everyone needs to.
3. Even better–add a monetary value on the potential cost of a data breach for this particular risk. Don't forget to add legislative fines on top of this.
4. Demonstrate a scenario of a cyber-attack. For example: a ransomware attack on an endpoint. Explain how your current security posture would cope with such an attack and how you could limit the damage with more effective layers of security. How quickly can you respond? At what point would you know about the threat? What can be done to improve this? Again, put monetary values on the potential downtime/cost to remove the malware.

You could also use high-profile breaches as an opportunity to have a conversation with the board. Describe how that breach can happen in your organization. Then show them how to address vulnerabilities.

The trend in Indonesia is to consolidate and integrate their security products, which is clearly having a positive effect on the number of alerts and overall cybersecurity fatigue levels. For anyone who would like to go down a similar route, it might be pertinent to consider a Zero Trust approach.

This approach looks to simplify security by looking at three key areas:

1. Workforce (protect your users and their devices against stolen credentials, phishing, and other identity-based attacks)
2. Workload (managing multi-cloud environments to contain lateral movement across the network)
3. Workplace (gain insights into users and devices, identify threats and maintain control over all connections in your network).

To secure the workplace, Zero Trust starts with establishing a level of trust around the identity of the user and what they can access to work within the organization's environment. Having checked the device and authenticated the user, the next fundamental element is controlling what doors to what applications they can enter, and what is considered out of bounds.

The Zero Trust approach is about restricting a user so that they can only enter an area which is approved and relevant to their duties. This all needs to be done with minimal impact on the end user. Introducing difficulty into any security control area just breeds avoidance. What is appealing about the agile and flexible approach is its ability to bring new applications on board wherever they are found–whether running in the cloud, in a local data center or a third-party application. No matter where the doors are, they can be open or shut from a central point based on a policy.

Japan Overview

Introduction

From the survey results in Japan, we've identified a couple of areas that are cause for concern. Firstly, **cybersecurity fatigue levels are still the highest in the region at 77%.** Secondly, in 2019, there has been **a sharp drop (20%) in the amount of daily security alerts investigated.** Currently, 65% of security alerts in Japan are never seen to, and 80% of true security incidents are never remediated.

However, there are significant improvements being made by organizations in Japan such as separating the security team from the IT department. Even though these won't see immediate improvements overnight, this is a very positive trend.

The cybersecurity culture in Japan

For the second year running, the biggest hindrance to adopting advanced security processes and initiatives in Japan is budget constraints. The number of executive leaders who deem security a priority could be the issue here–it is less in Japan than in other countries.

The second biggest constraint is the lack of knowledge about advanced security processes, followed by the organizational culture/attitude towards cybersecurity. These might be contributing to the budget issues and overall notion that cybersecurity doesn't quite have the same level of priority as in other countries.

Table: The greatest obstacles to adopting advanced security processes and technology in organizations

	Japan	Regional	Global
Budget constraints	33%	35%	35%
Competing priorities	23%	22%	26%
Lack of trained personnel	24%	29%	24%
Lack of knowledge about advanced security processes and technology	31%	33%	22%
Compatibility issues with legacy systems	23%	29%	27%
Certification requirements	25%	20%	24%
Organizational culture/attitude about cybersecurity	30%	27%	21%
Reluctant to purchase until they are proven in the market	25%	18%	20%
Current workload too heavy to take on new responsibilities	26%	23%	22%
Organization is not a high value target for attacks	19%	16%	16%
Security is not an executive level priority	19%	15%	13%

In better news, the issue of a lack of trained staff has decreased for Japan and it is now outside of the top three obstacles.

We asked organizations in Japan if they were suffering from cybersecurity fatigue.

Japan's response here is yet another cause for concern. 77% of organizations are so overwhelmed by security and malicious threat actors that they have virtually given up on staying ahead of them. In comparison, the global average is just 30%.

It's a trend that seems to be continuing from 2018 where 76% of Japanese organizations described themselves as experiencing cybersecurity fatigue. We'll explore some reasons for this in the next section.

Security alerts and the impact of data breaches

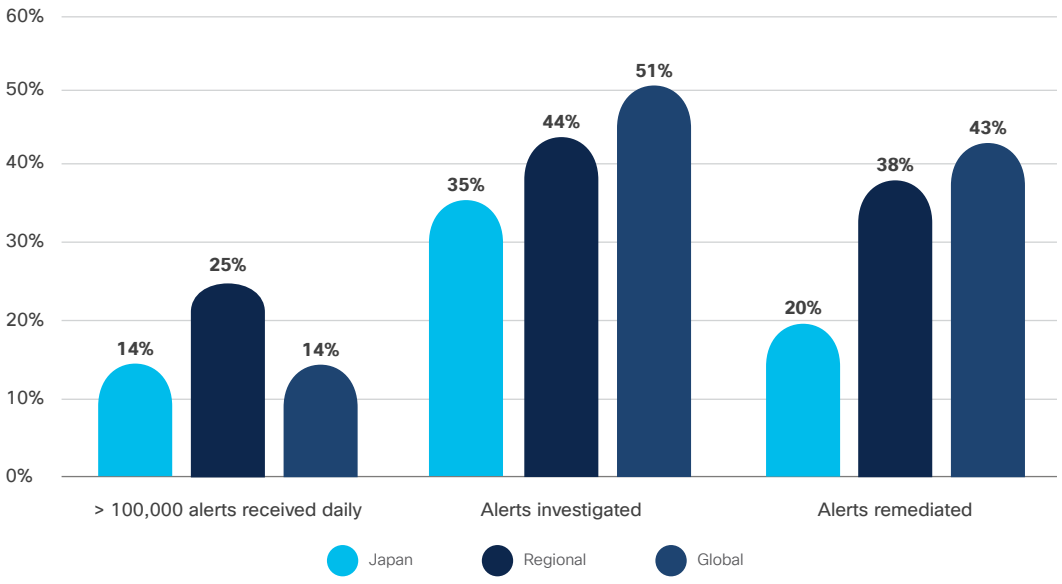
One cause for the cybersecurity fatigue could be the sheer volume of security alerts Japanese organizations receive every day. 45% of organizations surveyed are receiving between 10,000 and 100,000 alerts every single day. That's more than double the global average 21% globally in that bracket.

This high volume of alerts is having a direct impact on how many of these alerts can be investigated. In 2018, organizations in Japan were able to investigate 55% of alerts. It fell sharply by 20% in 2019. Which means that currently, 65% of security alerts in Japan fall through the cracks.

The percentage of legitimate alerts is slightly lower in Japan compared to other countries, so many of these alerts are generating false positives.

Most concerning of all is that 80% of true security incidents never get remediated. This is far higher than the global average. In our 2018 study, 51% of legitimate alerts were being remediated in Japan. This is a huge fall of 31 percentage point over the past year.

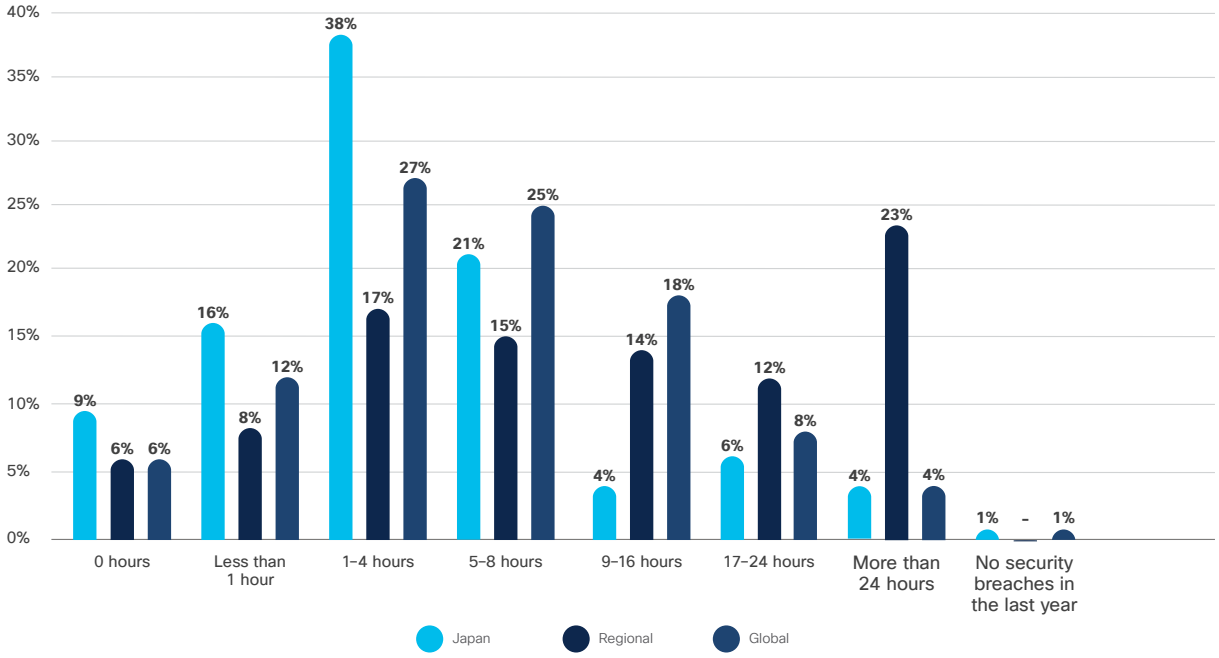
Chart: Alerts received, investigated and remediated



When it comes to data breaches and the improvements that were made following a breach, the top improvement for Japan was to separate the security team from the IT department. This is an important initiative because it means that that cybersecurity is far less likely to be "bolted on". Having a separate security department that is purely focused on protecting people, data and assets, is a great indication that it is embedded in an organizations' ecosystem, rather than it being "a problem for the IT department".

We also asked about the organizations' most severe breaches, and how long systems were down as a result. Results in Japan were much better than the global average, with 63% experiencing four hours or less downtime for a severe breach. Only 45% of global companies fall into this bracket. The percentage of Japanese companies experiencing heavy downtime above nine hours is also lower than the global average – 14% in Japan compared to 30% global average.

Chart: Downtime* following a data breach in businesses



We then asked about the monetary cost from their most impactful breach (i.e. lost revenue/lost customers/lost opportunities/out of pocket costs). Organizations in Japan are experiencing higher losses than the global average, with the most concerning figure being the rise of companies paying more than $10,000,000. In our 2018 study, this affected 1% of Japanese organizations. In 2019 this is now 5%.

Cloud trends

In general, organizations in Japan host more of their networks in the cloud than other countries. This isn't too surprising for a mature, technology-savvy market.

When asked why they chose the cloud, the **top reason for Japan was lack of internal IT workforce.** It's the people issue that we've seen time and time again in this year's report which is having an impact on managing alerts and overall cybersecurity fatigue.

It appears **the solution for Japan is to scale up by using the cloud,** however it's important to remember that organizations must not omit all security responsibility in doing so. It should be a partnership between themselves and their cloud provider.

Table: Reasons for using cloud to host IT infrastructure among businesses

	Japan	Regional	Global
OpEx preferred over CapEx	29%	33%	26%
Lack of internal IT workforce	47%	22%	25%
Cloud offers better data security	42%	50%	50%
Scalability	32%	43%	40%
Regulation or compliance requirements	34%	29%	27%
Ease of collaboration with external parties	35%	52%	37%
Ease of use	39%	19%	51%
Not core to business so outsourcing is preferable	33%	40%	18%
Other	0%	-	1%

When it comes to Operational Technology attacks, **Japan has witnessed more than global (36% vs 21%).** Japan sees this trend to likely continue.

The defenders' approach

Organizations in Japan have been busy streamlining their vendors in the past year. In our 2018 study, 45% of the organizations surveyed were using more than 10 security vendors. This has now gone down to 36%.

A catalyst for the move towards consolidation may be **due to how challenging it is to orchestrate alerts from multiple vendors' security products.** 88% of organizations in Japan find it somewhat or very challenging to orchestrate alerts from multiple vendors.

Recommendations

Burnout can be a real issue in the security industry. When it comes to coping with cybersecurity fatigue in Japan, the country which suffers from the highest burnout rate, here are our tips:

1. Training. Organizations could take advantage of cybersecurity courses from vendors and certification groups to bolster in-house skills and help teams feel more on the front foot. The Cisco Learning Network now offers a new Cisco Cybersecurity Specialist certification for people who want to take on a first-responder role when networks have been attacked. Global Information Assurance Certification (GIAC) has a new Network Forensic Analyst certification that gives security professionals the skills to extract and analyze artifacts and activity left behind from unauthorized activity or network-based attacks.
2. Automating manual processes. This means not having to go on a wild goose chase to stop malware from entering even more of their systems. For example, a network security device could spot an infected computer and immediately trigger an automatic quarantine so it can do no further harm.
3. Orchestration via a Zero Trust approach (see below).
4. Keep your software current. Unpatched or outdated software represents an attractive attack surface for adversaries and increases the pressure on security teams.

Secondly, in order to better manage alerts and simplify your security environment, it might be pertinent to consider a Zero Trust approach.

This approach looks to simplify security by looking at three key areas:

1. Workforce (protect your users and their devices against stolen credentials, phishing, and other identity-based attacks)
2. Workload (managing multi-cloud environments to contain lateral movement across the network)
3. Workplace (gain insights into users and devices, identify threats and maintain control over all connections in your network).

To secure the workplace, Zero Trust starts with establishing a level of trust around the identity of the user and what they can access to work within the organization's environment. Having checked the device and authenticated the user, the next fundamental element is controlling what doors to what applications they can enter, and what is considered out of bounds.

The Zero Trust approach is about restricting a user so that they can only enter an area which is approved and relevant to their duties. This all needs to be done with minimal impact on the end user. Introducing difficulty into any security control area just breeds avoidance. What is appealing about the agile and flexible approach is its ability to bring new applications on board wherever they are found—whether running in the cloud, in a local data center or a third-party application. No matter where the doors are, they can be open or shut from a central point based on a policy.

Korea Overview

Introduction

In the Korea report, a couple of things stand out. Firstly, there has been a **huge increase in the number of organizations who say they are now experiencing cyber fatigue**—defined as virtually giving up on staying ahead of threats. Secondly, the volume of alerts at the larger end of the scale (i.e. more than 100,000 Security alerts received daily) has more than tripled in the last year.

This may be due to more of a multi-vendor and multi-product environment, which by all accounts hasn't been integrated (a startling 92% of organizations are struggling to cope with a lack of integration)—this means **Korea is reporting longer levels of downtime and higher monetary costs**. The general sentiment among security teams in Korea is one of an uphill struggle.

On the positive side, **Korea has made tremendous strides in being able to investigate and remediate legitimate alerts**, despite the odds being against them in terms of the sheer volume of alerts they receive every day.

The cybersecurity culture in Korea

When looking at the obstacles preventing the adoption of advanced security technology, Korea stands out for its higher percentage of their executive leaders not seeing cybersecurity as a priority.

20% of organizations selected this as a significant obstacle. While it is not the most cited reason, it's the one that is most at odds with the rest of the world. Unfortunately Korea, alongside Indonesia, is the country where more work needs to be done to raise the profile of the importance of Security.

Table: The greatest obstacles to adopting advanced security processes and technology in organizations

	Korea	Regional	Global
Budget constraints	34%	35%	35%
Competing priorities	19%	22%	26%
Lack of trained personnel	24%	29%	24%
Lack of knowledge about advanced security processes and technology	32%	33%	22%
Compatibility issues with legacy systems	23%	29%	27%
Certification requirements	15%	20%	24%
Organizational culture/attitude about cybersecurity	26%	27%	21%
Reluctance to purchase until they are proven in the market	12%	18%	20%
Current workload too heavy to take on new responsibilities	8%	23%	22%
Organization is not a high value target for attacks	13%	16%	16%
Security is not an executive level priority	20%	15%	13%

The other call-out is that the lack of knowledge about advanced security processes and technology is a much higher obstacle in Korea than in other countries. Again, this may well come down to lack of executive support for security training budgets.

We asked organizations in Korea if they were suffering from cybersecurity fatigue.

Korea is significantly higher than the global average when it comes to cyber fatigue (Korea 60% vs global 30%), perhaps due to the frustration of not being able to utilize advanced processes effectively. Even more significant is the fact that the percentage of organizations saying that they are suffering from cyber fatigue (60%) has risen dramatically from 2018 (39%). Clearly, the past 12 months haven't been easy for organizations in Korea.

Security alerts and the impact of data breaches

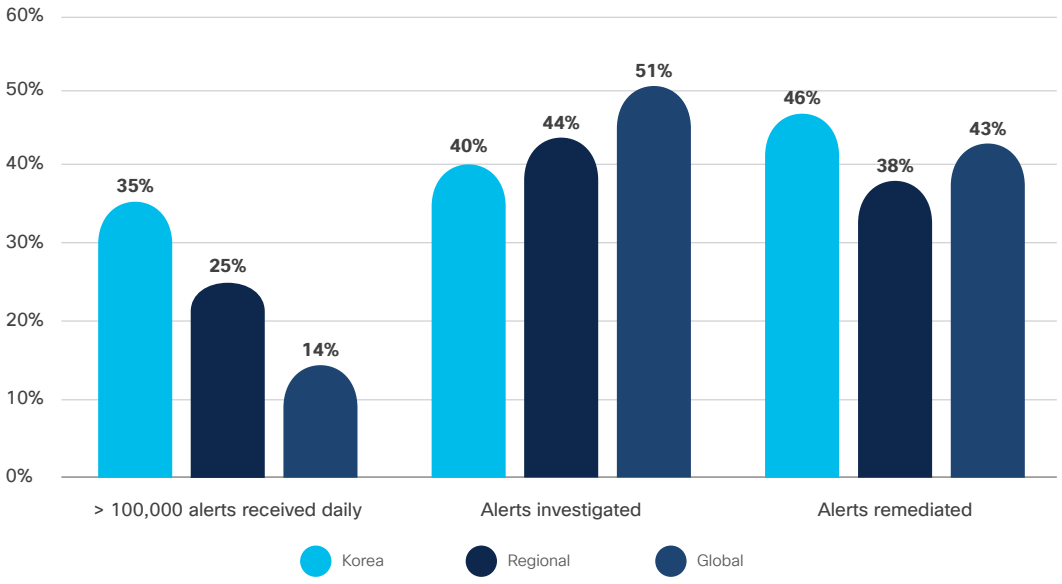
Korea receives over double the average amount of security alerts received overall, with 35% of organizations receiving 100,000 alerts or more during any given day, compared to the global average of 14%. In 2018, this was only 11% for Korea. This could be another reason why cyber fatigue has climbed so dramatically in 2019.

On average, organizations in Korea are able to investigate 40% of all the alerts received. In the context of the rapid rise in the volume of alerts, this should be commended. In 2018, despite there being less alerts being received, organizations were only able to investigate 30% of them. So, despite the enormous challenges facing Korea with security alerts, they have made great strides in the past year at being able to investigate more incidents.

The percentage of legitimate alerts is just under the global average. For Korea, this means a great deal of false positives are being investigated before they are deemed to be illegitimate alerts.

Korea beats the global average of successfully remediating legitimate alerts at 46%, above the global average of 43%. Again, this should be commended since they are receiving far more daily alerts on average. Korea has also improved on 2018's figure of 40% remediated alerts.

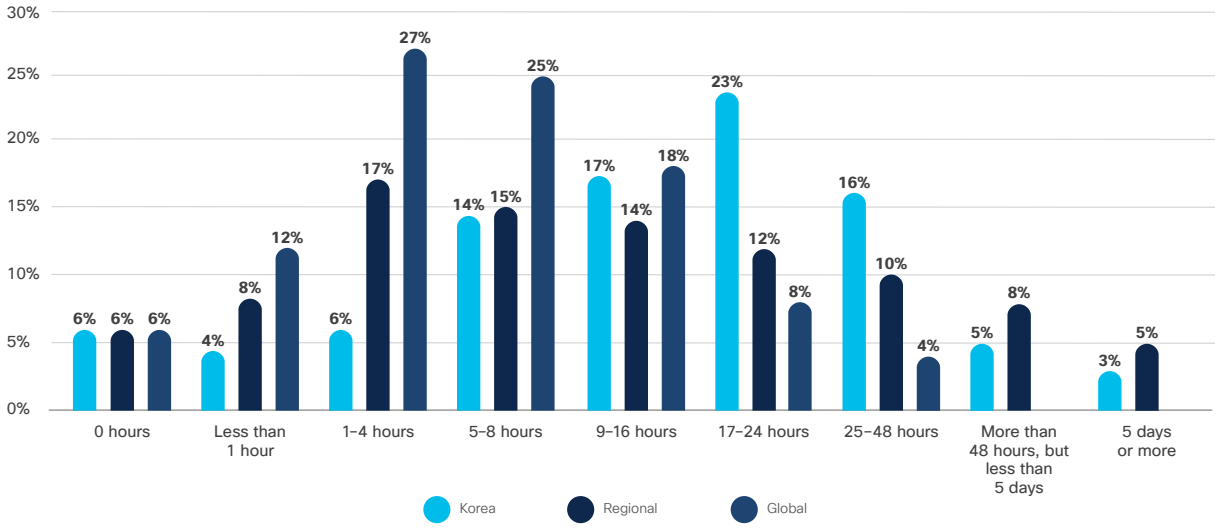
Chart: Alerts received, investigated and remediated



When it comes to the improvements that were made following a breach, the most selected improvement (by far) was to increase security awareness training among employees, in order to thwart attacks such as phishing and email spoofing before they have the chance to enter their way into the network.

We also asked about the organization's most severe breach, and how long systems were down as a result. This will be fairly tough reading for organizations in Korea, as downtime is a much greater issue for the region than other countries. 8% of organizations experienced downtime of more than 48 hours, with almost two thirds (64%) of organizations having to down tools for more than nine hours after a severe breach.

Chart: Downtime* following a data breach in businesses



Cloud trends

Organizations in Korea are very much in line with the global average in terms of percentage of the IT infrastructure hosted in the cloud. The majority have around half of their infrastructures hosted, and the other half on-prem.

When asked why they chose the cloud, the top reason for Korean companies was that cloud technologies are easier to use than on-prem, followed by the scalability that cloud can offer.

Table: Reasons for using cloud to host IT infrastructure among businesses

	Korea	Regional	Global
OpEx preferred over CapEx	30%	33%	26%
Lack of internal IT workforce	30%	22%	25%
Cloud offers better data security	35%	50%	50%
Scalability	37%	43%	40%
Regulation or compliance requirements	27%	29%	27%
Ease of collaboration with external parties	32%	52%	37%
Ease of use	39%	19%	51%
Not core to business so outsourcing is preferable	24%	40%	18%
Other	0%	-	1%

Organizations in Korea are more skeptical than other countries about the increase of Operational Technologies being attacked. 38% of organizations disbelieved that this will happen to their companies in the next year. By comparison, Vietnam and Thailand are much more firmly in the "believe" column—it should be noted those countries have already experienced a higher percentage of OT attacks. This reiterates the reactive nature of the security industry – some organizations only tend to pay attention to a type of attack when it's too late.

The defenders' approach

56% of organizations in Korea use more than 10 vendors in their security environments, which is one of the highest ratios in the region. Unfortunately, this multiple vendor approach is posing a significant challenge. A massive 92% of organizations say that they are struggling with orchestrating alerts within this type of environment.

This struggle is clearly having an effect on cyber fatigue. In our recommendations section we'll discuss the importance of integration in a multi-vendor environment.

Recommendations

A lot of the issues facing organizations in Korea when it comes to cybersecurity (i.e. volume of alerts, and huge amounts of downtime) seem to come down mainly to a lack of integration in a multi-vendor environment. Your security vendors need to be people who aren't thinking about selling their products, but about protecting your business.

The best way to do that is for security to work as a team. Teams that communicate in real time, learn from each other, and respond as a coordinated unit. Your endpoint security has to work with your network security and with cloud security, and you have to have MFA that speaks to identity and access. And you can only get to securing your business with a platform approach. When that happens, security becomes easier and more effective.

Another issue for Korea is a lack of executive buy in. Here are four tips to increase the awareness of security issues at board level:

- Personalize your business' cybersecurity risk factors. Just like employers don't like receiving generic CVs, boards don't like it when they have to look at stuff that is of little relevance. What does risk mean to you? Are you a retail business that is particularly at risk during peak periods? Are your employees more likely to partake in Shadow IT?
- It's also important to benchmark this against other companies in your industry. Boards like context–it's not just your business that needs to mitigate this risk–everyone needs to.
- Even better–add a monetary value on the potential cost of a data breach for this particular risk. Don't forget to add legislative fines on top of this.
- Demonstrate a scenario of a cyber attack. For example, a ransomware attack on an endpoint. Explain how your current security posture would cope with such an attack and, how you could limit the damage with more effective layers of security. Crucially, how quick can you respond? At what point would you know about the threat? What can be done to improve this? Again, put monetary values on the potential downtime/cost to remove the malware.

Malaysia Overview

Introduction

Unlike most countries, budget has become less of a concern for Malaysian organizations in the past year; with more of an appetite to invest in training and talent.

Lack of resource is a large problem in this region. It contributes to high levels of cyber fatigue. With more budget being assigned to recruitment in 2019, we will hopefully see these levels decline over the coming years.

We're also seeing an increasing number of security alerts hitting Malaysian infrastructures, an increasing number of organizations struggling to deal with the challenges posed from a multi-vendor environment, and a lack of integration between products.

The cybersecurity culture in Malaysia

There are three obstacles preventing organizations in Malaysia from adopting advanced security technologies. These are budget constraints, a lack of knowledge about advanced security technologies, and a lack of trained personnel.

This is a bit of a vicious cycle. In order to receive budget for advanced tools, you need a plan and the resource to implement them. Since both are significant issues for Malaysia, they almost define each other.

Table: The greatest obstacles to adopting advanced security processes and technology in organizations

	Malaysia	Regional	Global
Budget constraints	38%	35%	35%
Competing priorities	14%	22%	26%
Lack of trained personnel	38%	29%	24%
Lack of knowledge about advanced security processes and technology	38%	33%	22%
Compatibility issues with legacy systems	25%	29%	27%
Certification requirements	11%	20%	24%
Organizational culture/attitude about cybersecurity	43%	27%	21%
Reluctant to purchase until they are proven in the market	17%	18%	20%
Current workload too heavy to take on new responsibilities	24%	23%	22%
Organization is not a high value target for attacks	14%	16%	16%
Security is not an executive level priority	11%	15%	13%

However, even though it's still the number one obstacle, budget has actually become less of a concern for Malaysia over the past year. In our 2018 study, 55% of organizations struggled with budget. This has gone down to 38%. The training of staff has remained largely the same. Perhaps extra emphasis needs to go towards staff training on advanced security tools, as it appears there is more appetite for these tools to be installed in 2019.

We asked organizations in Malaysia if they were suffering from cybersecurity fatigue.

Malaysia is significantly higher than the global average when it comes to cyber fatigue (55% vs global at 30%), perhaps due to the lack of resources, and frustrations at not being able to utilize advanced processes effectively. Indeed, the number of organizations suffering from cyber fatigue has increased by 6% since 2018. The frustration has clearly been festering over the past 12 months.

Security alerts and the impact of data breaches

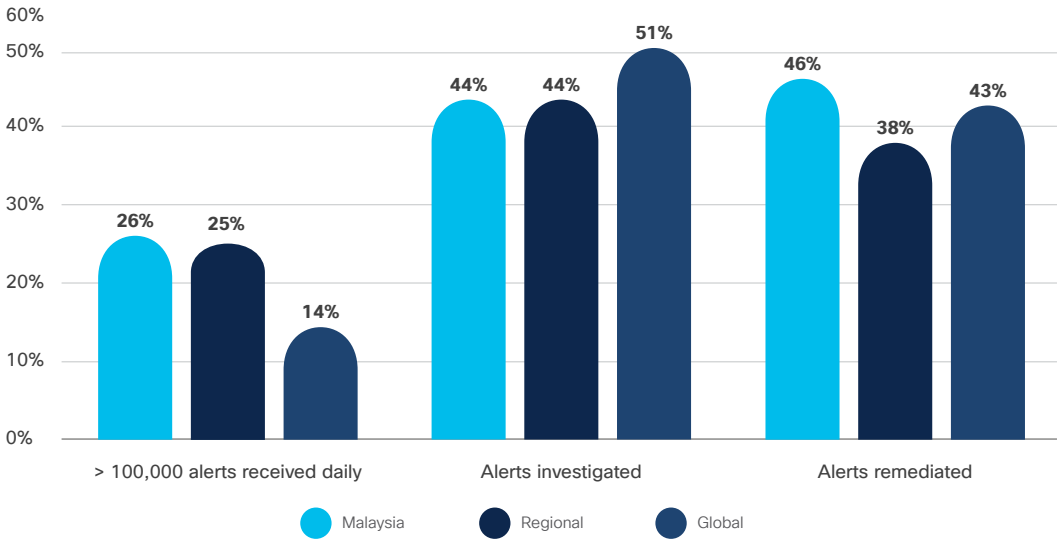
Malaysia receives more than the average amount of security alerts received globally, with a quarter of organizations receiving 100,000 alerts or more during any given day. This is a significant increase from 2018, when only 9% of organizations were receiving over 10,000 alerts a day. This could be another reason why cyber fatigue has climbed in 2019 – they have the same amount of resources, but they are dealing with more than twice the number of alerts.

On average, organizations in Malaysia were able to investigate 44% of all alerts received. The situation is not as bad as it could have been, given the overwhelming amount of alerts a lot of companies deal with. In fact, this is a 4% improvement on last year.

The percentage of legitimate alerts is higher than the global average, which means that more actual incidents are being uncovered from the alerts that are being investigated.

The best news is that despite Malaysia receiving more alerts (with more of a legitimate nature) than other countries, their record on remediating them is better than the global average (46% Malaysia vs 43% global). This is a slight improvement since last year when 42% of legitimate alerts were remediated.

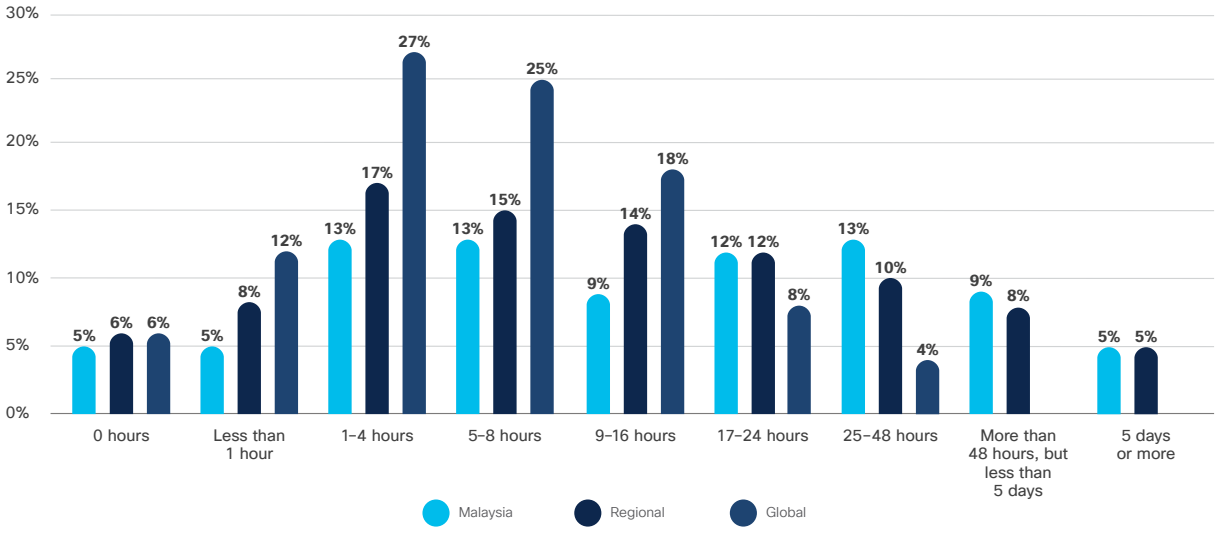
Chart: Alerts received, investigated and remediated in Malaysia vs Global



When it comes to the improvements that were made following a breach, the top improvement was to increase security awareness training among employees, followed by increased focus on risk analysis and risk mitigation, and an increased focus on preventing security breaches caused by employee-owned mobile devices.

We also asked about the organizations' most severe breaches, and how long systems were down as a result. This will be tough reading for organizations in Malaysia, as downtime is a much greater issue for the region than in other parts of the world. 14% of organizations experienced downtime of more than 48 hours, with almost half (48%) of organizations experiencing lights out for more than nine hours after a severe breach. We'll look at some recommendations for managing downtime at the end of this report.

Chart: Downtime* following a data breach in businesses



Cloud trends

The average number of organizations in Malaysia that have over 80% of their infrastructure hosted on cloud is double that of the global average—it stands at 18% compared to the worldwide average of 9%.

There are two main reasons why organizations in Malaysia are moving to the cloud: scalability and ease of use.

Table: Reasons for using cloud to host IT infrastructure among businesses in Malaysia

	Malaysia	Regional	Global
OpEx preferred over CapEx	37%	33%	26%
Lack of internal IT workforce	30%	22%	25%
Cloud offers better data security	38%	50%	50%
Scalability	43%	43%	40%
Regulation or compliance requirements	35%	29%	27%
Ease of collaboration with external parties	38%	52%	37%
Ease of use	43%	19%	51%
Not core to business so outsourcing is preferable	18%	40%	18%
Other	0%	-	1%

Half of organizations surveyed fully expect cyber attacks to extend beyond IT and into Operational Technology next year. This is higher than the global average.

This is another sign that security remains a reactive industry. In order for organizations to take a breach seriously, they need to experience it. Having witnessed more OT attacks in the past year, more organizations in Malaysia expect this trend to stick around.

The defenders' approach

The percentage of organizations in Malaysia that use more than 10 vendors has risen very slightly from 32% in 2018 to 35% in 2019. This is now one of the highest ratios of multi-vendor product environments in Asia Pacific.

Unfortunately, organizations in Malaysia are finding it more challenging than other countries to orchestrate multiple vendor alerts and it is clearly having an effect on cyber fatigue. More focus should be on integration in order to try and combat this. We'll look at possible solutions in the recommendations section.

Recommendations

A lot of the issues facing organizations in Malaysia when it comes to cybersecurity (e.g., volume of alerts and huge amounts of downtime) seems to boil down to a lack of integration and preparedness for an attack.

Firstly, integration between vendors and products is crucial in identifying and stopping threats—automatically and in real time.

This makes our response so much more powerful. For organizations, it means not having to go on a wild goose chase to stop malware from invading even more of their systems. For example, a network security device could spot an infected computer and immediately trigger an automatic quarantine so it can do no further harm. This is automation in action, and it is the one ingredient that could empower organizations with faster detection and response time to security threats.

Secondly, a cyber resilience plan that is understood and tested regularly is also crucial.

Here are some tips on what should be considered part of your plan:

- Assign responsibilities—who is doing what? Roles should include analysis, communication with the team/customers/press, and setting up remote working.
- Identify a leader—someone who knows your business and your security strategy.
- Your plan should allow fluidity to incorporate the latest threats.
- Determine the critical components of your network to replicate in a remote location.
- Identify single points of failure to prepare a back-up plan for (e.g., in case a key team member is away).
- Create a list of the tools, technologies and physical resources that must be in place.
- Consider both internal and external communications. Customers need to be notified accordingly, and your employees need to understand their role in getting the organization up and running again.

Consider the damages your business could suffer if corporate data were to make its way to the internet. Will it only cost you downtime and reputational damage, or will there be greater costs?

Philippines Overview

Introduction

There are two things that set the Philippines apart in this report–one is for a very good reason, and the other one not so good.

On the positive side, the **Philippines can claim the top spot for the greatest number of alerts that get investigated daily,** and also the highest number of legitimate alerts that get remediated. Security teams are clearly mission-centric and closely aligned, but their heavy workload is having a big effect on cybersecurity fatigue.

On the downside, **there is a large number of organizations that are unaware of how many alerts they receive**, or even how many vendors or products they have within their environment. There could be a variety of reasons why organizations in the Philippines have less visibility of their security environments than others (perhaps there are different teams within the organization, legacy issues etc.), but the important thing to note is that honesty is the best policy. Knowing that you "don't know" is a good place to start; then you can work to address these issues.

The cybersecurity culture in the Philippines

Much like many of its fellow Asia Pacific countries, budget constraints are the number one issue for the Philippines, which stop organizations from adopting advanced security technology. The figures are exactly the same as last year.

Interestingly, the Philippines has great executive level buy-in, with only 11% of organizations saying that security is not an executive priority. In our recommendations section, we'll look at how to obtain even more security budget from the boardroom.

One thing that may be hindering more budget being spent is that the Philippines cites a lack of knowledge about advanced systems and processes as their second biggest challenge. We'll also look at how teams can become upskilled, in order to implement new security systems.

Table: The greatest obstacles to adopting advanced security processes and technology in organizations

	Philippines	Regional	Global
Budget constraints	41%	35%	35%
Competing priorities	14%	22%	26%
Lack of trained personnel	32%	29%	24%
Lack of knowledge about advanced security processes and technology	35%	33%	22%
Compatibility issues with legacy systems	31%	29%	27%
Certification requirements	18%	20%	24%
Organizational culture/attitude about cybersecurity	23%	27%	21%
Reluctance to purchase until they are proven in the market	15%	18%	20%
Current workload too heavy to take on new responsibilities	21%	23%	22%
Organization is not a high value target for attacks	11%	16%	16%
Security is not an executive level priority	11%	15%	13%

We asked organizations in the Philippines if they were suffering from cybersecurity fatigue.

An area of concern for the Philippines is that fatigue levels have risen dramatically, from 27% in 2018 to 43% in 2019. This is higher than global (30%). This could be due to budgets not being spent on upgraded tools, and more manual reactive processes having to take the brunt.

Security alerts and the impact of data breaches

The Philippines is now relatively in line with the global average with regard to security alerts received daily. 46% of organizations are receiving less than 5000 alerts a day (which is an 11% improvement on last year), with 19% at the top end receiving more than 100,000 alerts a day (for Korea, 35% of organizations receive this many alerts).

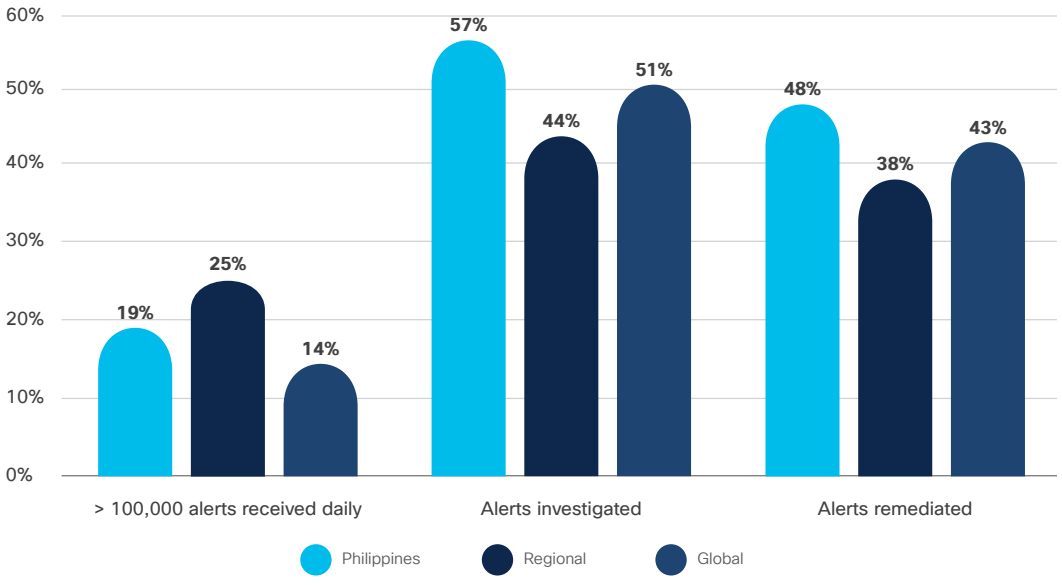
The most worrying statistic, however, is that 16% of organizations don't know how many alerts they receive. This is the second highest percentile in this "don't know" bracket, just behind Malaysia.

On the positive side, the Philippines claimed the top spot in terms of the percentage of alerts (57%) that get investigated among all countries in Asia Pacific that we surveyed. It's also an increase from last year's survey which was 49%.

Due to the percentage of legitimate alerts in the Philippines being higher than the global average, it's a very good thing that organizations do investigations regularly.

While 48% is far from a perfect record for fixing legitimate security incidents, it is higher than the global average.

Chart: Alerts received, investigated and remediated

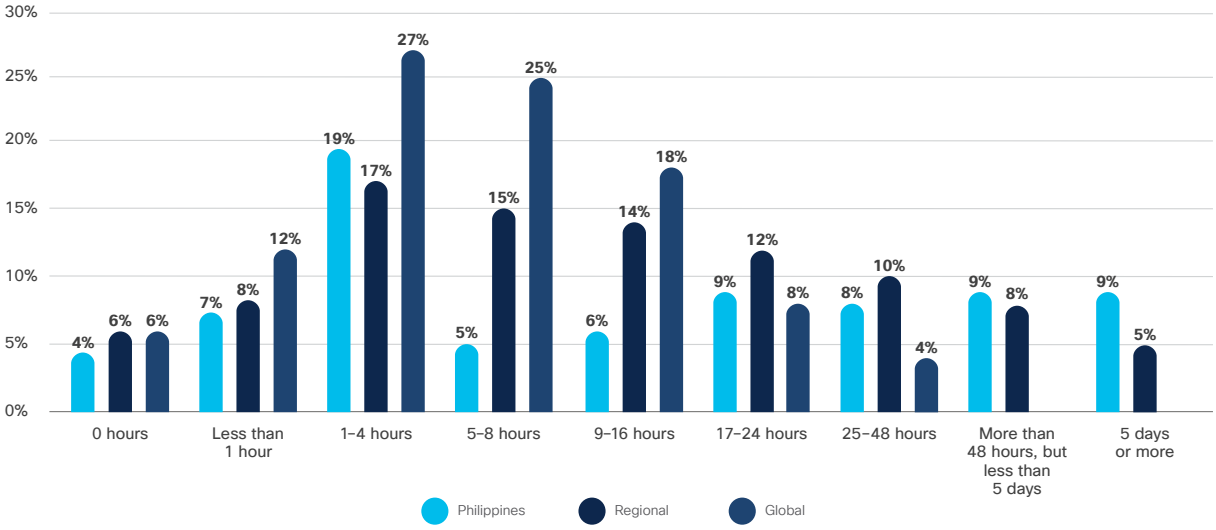


When it comes to the improvements that were made following a breach, the top improvement was to increase security awareness training among employees. This makes sense, given that there are fewer specialized security teams in the Philippines. As a result, organizations will be more reliant on their general employees being able to spot attempted phishing and email spoofing attacks.

However, organizations in the Philippines have gone against the trend of hiring a CISO/ establishing a strategic leader for security—only 20% of organizations went down this route, compared to 34% globally.

We also asked about the organization's most severe breach, and how long systems were down as a result. Much like most of its Asia Pacific counterparts, downtime at the more severe end is more of an issue than other countries across the world. This may be down to the skills gap and an overall reactive posture to dealing with cyber attacks.

Chart: Downtime* following a data breach in businesses



Cloud trends

The Philippines has the highest percentage (10%) of organizations that run their infrastructure entirely in the cloud, with no on-prem at all. Overall, the trend towards placing more infrastructure in the cloud is higher than that of other countries.

When asked why they chose the cloud, the top reason for the Philippines was that it offers better data security, followed by ease of use.

Table: Reasons for using cloud to host IT infrastructure among businesses

	Philippines	Regional	Global
OpEx preferred over CapEx	26%	33%	26%
Lack of internal IT workforce	23%	22%	25%
Cloud offers better data security	51%	50%	50%
Scalability	39%	43%	40%
Regulation or compliance requirements	24%	29%	27%
Ease of collaboration with external parties	42%	52%	37%
Ease of use	45%	19%	51%
Not core to business so outsourcing is preferable	12%	40%	18%
Other	0%	-	1%

Organizations in the Philippines are less convinced about the proliferation of Operational Technology attacks than other countries, with a higher percentage believing this is further away than next year.

The defenders' approach

40% of organizations in the Philippines are managing at least 10 different vendors (10% are managing 50, much higher than the global average). Again, the most concerning fact here is that 12% of organizations in the Philippines aren't sure how many different vendors they are managing (the highest in this bracket). This makes integration, or lack thereof, a real issue.

Unfortunately, the majority (78%) of organizations in the Philippines are finding it challenging to orchestrate multiple vendor alerts, and it is clearly having an effect on cyber fatigue.

Recommendations

With budget constraints a big issue for the Philippines, here are some tips to get more budget assigned from the boardroom:

- Personalize your business' cybersecurity risk factors. Just like employers don't like receiving generic CVs, boards don't like it when they have to look at stuff that is of little relevance. What does risk mean to you? Are you a retail business that is particularly at risk during peak periods? Are your employees more likely to partake in Shadow IT?
- It's also important to benchmark this against other companies in your industry. Boards like context—it's not just your business that needs to mitigate this risk. Everyone needs to.
- Even better—add a monetary value on the potential cost of a data breach for this particular risk. Don't forget to add legislative fines on top of this.
- Demonstrate a scenario of a cyber attack. For example: a ransomware attack on an endpoint. Explain how your current security posture would cope with such an attack and how you could limit the damage with more effective layers of security. How quick can you respond? At what point would you know about the threat? What can be done to improve this? Again, put monetary values on the potential downtime/cost to remove the malware.

On the integration issues, your security vendors need to be people who aren't thinking about selling their products, but about protecting your business.

The best way to do that is for security to work as a team. Teams communicate in real time, teams learn from each other, and teams respond as a coordinated unit. Your endpoint security has to work with your network security and with cloud security, and you have to have MFA that speaks to identity and access. You can only secure your business with a platform approach.

When that happens, security becomes easier and more effective.

Finally, a cyber resilience plan that is understood and tested regularly is also crucial.

Here are some tips on what should be considered part of your plan:

- Assign responsibilities—who is doing what? Roles should include analysis, communication with the team/customers/press, and setting up remote working.
- Identify a leader—someone who knows your business and your security strategy.
- Your plan should allow fluidity to incorporate the latest threats.
- Determine the critical components of your network to replicate in a remote location.
- Identify single points of failure to prepare a back-up plan (e.g., in case a key team member is away).
- Create a list of the tools, technologies and physical resources that must be in place.
- Consider both internal and external communications. Customers need to be notified accordingly, and your employees need to understand their role in getting the organization up and running again.

Ask yourself what the damage will be to your business if corporate data made it to the internet. Will it only cost you downtime and reputational damage, or will there be greater costs?

Singapore Overview

Introduction

For Singapore, there is a greater emphasis on the importance of cybersecurity at the executive level, reflected in the increased budget and investment in personnel and training.

However, we are seeing an increased volume of alerts hitting organizations every day, perhaps caused by an increased number of vendors and security products. This is having a knock-on effect on alert remediation, and an overall increase in cyber fatigue (defined as virtually giving up on staying ahead of threats).

The one thing that distinguishes Singapore from most countries is the amount of downtime experienced after a severe breach. In our recommendations section, we give advice on how to put together a cyber resilience plan, and how to integrate your architecture to improve detection and remediation times.

The cybersecurity culture in Singapore

Currently, the biggest issue preventing organizations in Singapore from adopting advanced security processes and technology is a fairly common one: budget constraints. This is closely followed by a lack of knowledge about advanced security processes. It seems that even if organizations were able to secure the budget for more technology, most wouldn't have the resources or ability to install it effectively.

Table: The greatest obstacles to adopting advanced security processes and technology in organizations

	Singapore	Regional	Global
Budget constraints	34%	35%	35%
Competing priorities	30%	22%	26%
Lack of trained personnel	29%	29%	24%
Lack of knowledge about advanced security processes and technology	33%	33%	22%
Compatibility issues with legacy systems	31%	29%	27%
Certification requirements	15%	20%	24%
Organizational culture/attitude about cybersecurity	25%	27%	21%
Reluctance to purchase until they are proven in the market	17%	18%	20%
Current workload too heavy to take on new responsibilities	31%	23%	22%
Organization is not a high value target for attacks	19%	16%	16%
Security is not an executive level priority	13%	15%	13%

However, even though it is still the number one obstacle, budget has actually become less of a concern for Singapore over the past year. In our 2018 study, 47% of organizations struggled with budget. This has gone down to 34%. The training of staff has largely remained the same. Perhaps extra emphasis needs to go towards staff training on advanced security tools, as it appears there is more appetite for these tools to be installed in 2019.

We asked organizations in Singapore if they were suffering from cybersecurity fatigue.

The country is significantly higher than the global average when it comes to cyber fatigue (Singapore 45% vs global 30%), perhaps due to the frustration of not being able to utilize advanced processes effectively. Indeed, the amount of organizations suffering from cyber fatigue has risen from only 36% in 2018. The frustration has clearly been festering over the past 12 months.

Security alerts and the impact of data breaches

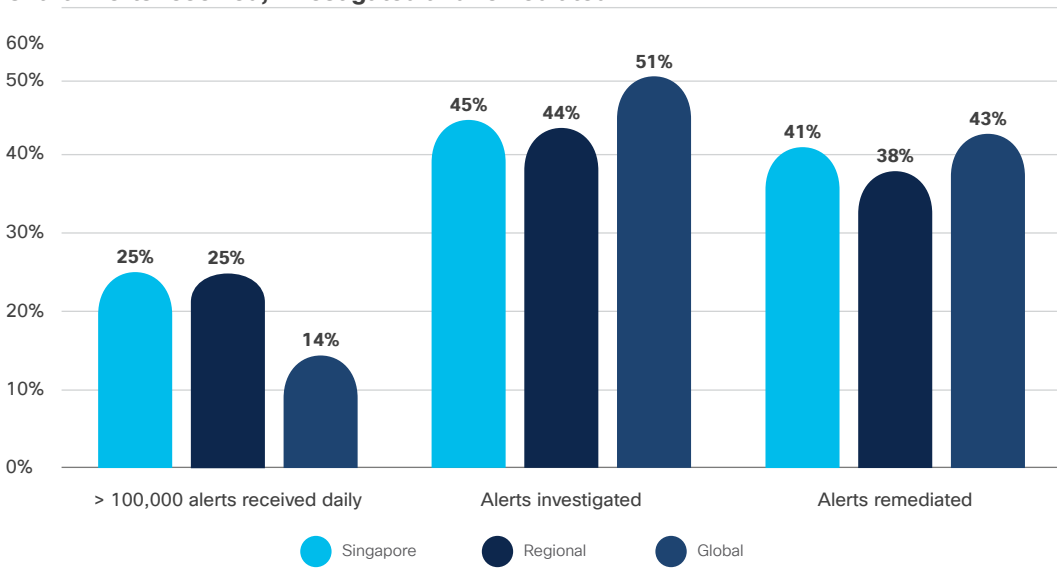
Singapore receives more than the average amount of security alerts received overall, with a quarter of organizations receiving 100,000 alerts or more during any given day. Things were very similar last year, so with no improvements being made, this could be another reason why cyber fatigue has climbed in 2019. This could be another reason why cyber fatigue has climbed in 2019.

On average, organizations in Singapore were able to investigate 45% of all the alerts received. The situation is not as bad as it could have been, given the overwhelming amount of alerts a lot of companies deal with. In fact, this is a 4% improvement on last year.

The percentage of legitimate alerts is virtually the same as the global average, but for Singapore this means a great deal of false positives are happening.

Unfortunately, bad news continues for Singapore's record on coping with security alerts – their record of fixing legitimate incidents has gone down from 50% in 2018, to 41% in 2019, which means more malicious activities may be entering the network.

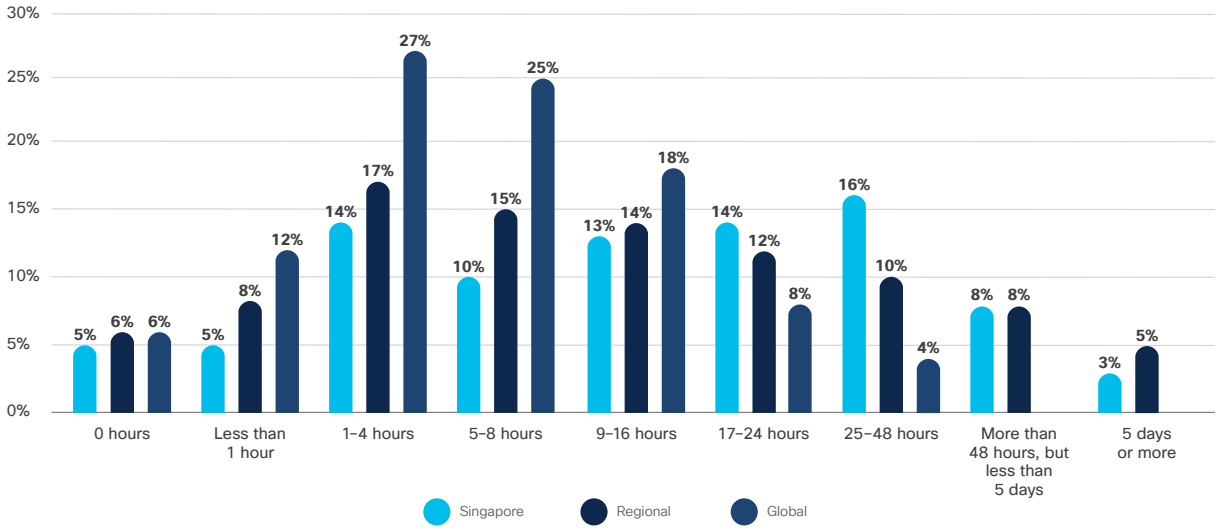
Chart: Alerts received, investigated and remediated



When it comes to data breaches and the improvements that were made following a breach, the top improvement was to increase security awareness training among employees, closely followed by increasing the investment in the training of security staff. If this pays off, we will see "lack of awareness/knowledge" be reduced as an obstacle for Singapore next year.

We also asked about organizations' most severe breaches, and how long systems were down as a result. This will be fairly tough reading for organizations in Singapore, as downtime is a much greater issue for the region than in other parts of the world. 11% of organizations experienced downtime of more than 48 hours, with over half (54%) of organizations being down for more than nine hours after a severe breach.

Chart: Downtime* following a data breach in businesses



Cloud trends

The majority of organizations in Singapore have around half of their infrastructures based in the cloud. A significant 37% of those organizations surveyed have more than 60% of their infrastructure hosted.

When asked why they chose the cloud, the top reason for Singapore was that cloud offers better security, closely followed by the preference of OpEx over CapEx.

Table: Reasons for using cloud to host IT infrastructure among businesses

	Singapore	Regional	Global
OpEx preferred over CapEx	51%	33%	26%
Lack of internal IT workforce	38%	22%	25%
Cloud offers better data security	52%	50%	50%
Scalability	37%	43%	40%
Regulation or compliance requirements	43%	29%	27%
Ease of collaboration with external parties	27%	52%	37%
Ease of use	17%	19%	51%
Not core to business so outsourcing is preferable	17%	40%	18%
Other	0%	-	1%

The defenders' approach

The percentage of organizations in Singapore who use more than 10 vendors has risen from 27% in 2018 to 34% in 2019. This could be the reason why so many more alerts and false positives are being generated.

Unfortunately, organizations in Singapore are finding it more challenging (90%) than other countries to orchestrate multiple vendor alerts, and it is clearly having an effect on cyber fatigue. More focus should be on integration in order to try and combat this.

Recommendations

A lot of the issues facing organizations in Singapore when it comes to cybersecurity (e.g., volume of alerts and huge amounts of downtime) seems to boil down to a lack of integration and preparedness for an attack.

Firstly, integration between vendors and products is crucial in identifying and stopping threats—automatically and in real time.

This makes our response so much more powerful. For organizations, it means not having to go on a wild goose chase to stop malware from invading even more of their systems. For example, a network security device could spot an infected computer and immediately trigger an automatic quarantine so it can do no further harm. This is automation in action, and it is one of the key ingredients that could empower organizations with faster detection and response time to security threats.

Secondly, a cyber resilience plan that is understood and tested regularly is also crucial.

Here are some tips on what should be considered part of your plan:

- Assign responsibilities—who is doing what? Roles should include analysis, communication with the team/customers/press, and setting up remote working.
- Identify a leader—someone who knows your business and your security strategy.
- Your plan should allow fluidity to incorporate the latest threats.
- Determine the critical components of your network to replicate in a remote location.
- Identify single points of failure to prepare a back-up plan (e.g., in case a key team member is away).
- Create a list of the tools, technologies and physical resources that must be in place.
- Consider both internal and external communications. Customers need to be notified accordingly, and your employees need to understand their role in getting the organization up and running again.

Consider the damages your business could suffer if corporate data were to make its way to the internet. Will it only cost you downtime and reputational damage, or will there be greater costs?

Thailand Overview

Introduction

Thailand should be commended for their legitimate alert remediation record, which matches the global average. However they are dealing with a significantly higher percentage of real security incidents, and more alerts that need investigations to begin with.

A real issue for Thailand, particularly in 2019, is a **lack of knowledge about advanced security processes**, which is hindering resource levels and vastly increasing cybersecurity fatigue levels among security staff.

Finally, organizations in Thailand are finding it much more difficult to manage a multi-vendor environment than their regional counterparts. In our recommendations section, we'll look at tips on how to integrate more, as well as how to combat the skills gap and uptrain people within the security team.

The cybersecurity culture in Thailand

From a culture perspective, the highest obstacle for organizations in Thailand is a lack of knowledge about advanced security processes and technology. This issue has been cited 15% more than any other challenge. The next challenge is a lack of trained personnel, followed by compatibility with legacy systems.

In fact, a lack of knowledge about advanced security processes and technology is doubly an issue for Thailand this year (in 2018, 27% of organizations cited it as a main challenge compared to 52% in 2019).

Table: The greatest obstacles to adopting advanced security processes and technology in organizations

	Thailand	Regional	Global
Budget constraints	30%	35%	35%
Competing priorities	13%	22%	26%
Lack of trained personnel	37%	29%	24%
Lack of knowledge about advanced security processes and technology	52%	33%	22%
Compatibility issues with legacy systems	32%	29%	27%
Certification requirements	20%	20%	24%
Organizational culture/attitude about cybersecurity	30%	27%	21%
Reluctance to purchase until they are proven in the market	12%	18%	20%
Current workload too heavy to take on new responsibilities	20%	23%	22%
Organization is not a high value target for attacks	19%	16%	16%
Security is not an executive level priority	19%	15%	13%

We asked organizations in Thailand if they were suffering from cybersecurity fatigue.

Thailand is significantly higher than the global average (Thailand 65% vs global 30%) when it comes to cyber fatigue and has the second joint highest levels (equal with Australia), with Japan being the country with the most cybersecurity fatigue, at 77%.

This could well be due to frustration at a lack of resource and training, and the pressure it can create on current teams.

Security alerts and the impact of data breaches

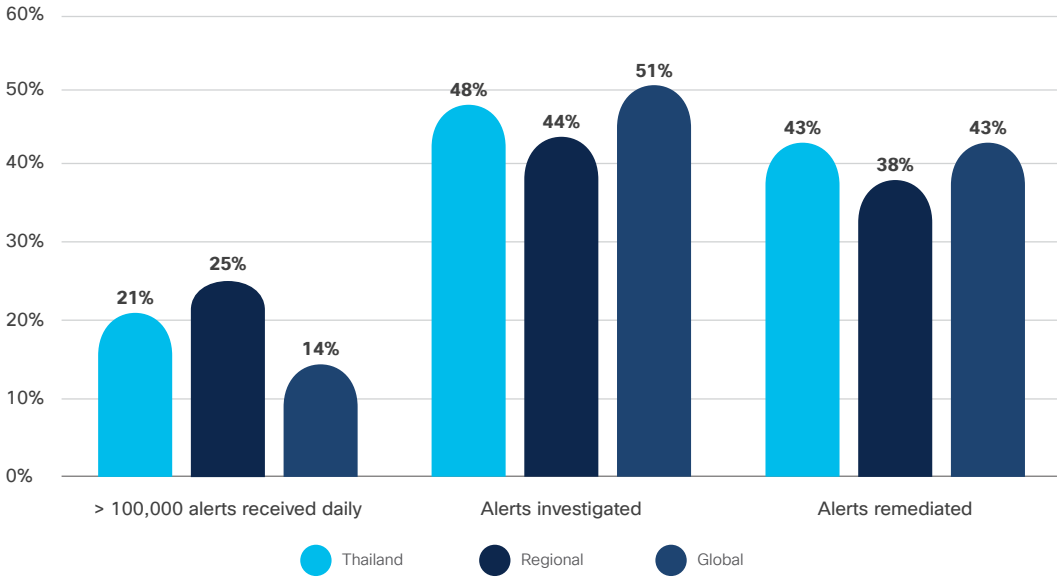
Thailand receives more security alerts compared to the global average, with 45% of organizations receiving 50,000 alerts or more during any given day. Globally, 23% of organizations receive this amount.

Things were very similar last year, and with no improvements being made, this could be another reason why cyber fatigue has climbed in 2019.

On average, organizations in Thailand were able to investigate 48% of all the alerts received, which isn't as bad as it could have been, given the overwhelming amount of alerts a lot of companies are having to deal with. In fact, it's an 11% improvement on last year.

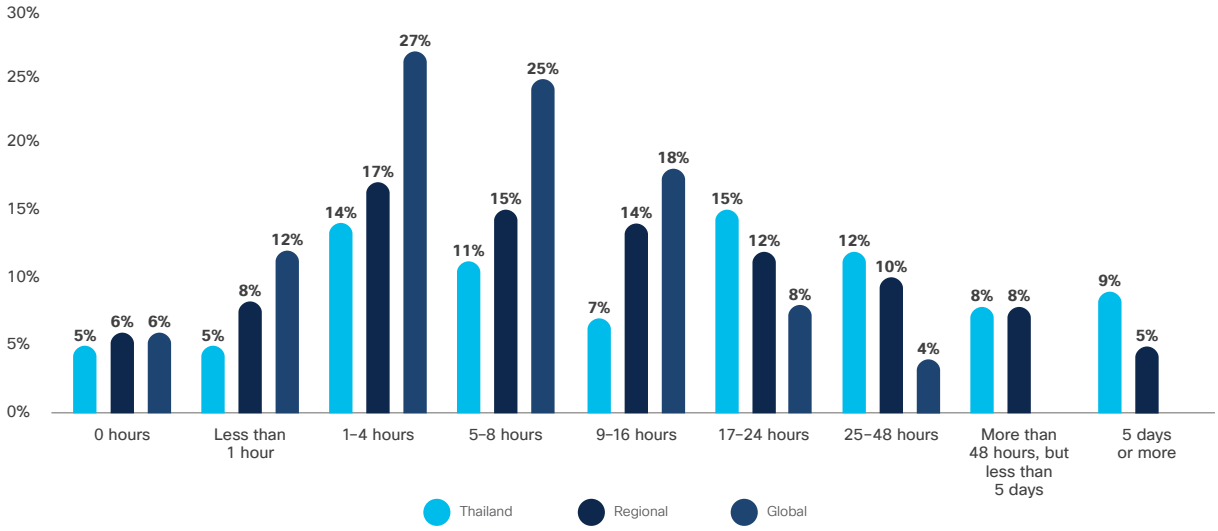
In fact, the percentage of legitimate alerts is significantly higher than the global average. Yet Thailand matches the global average for the percentage of legitimate alerts that get fixed, which should be commended considering they are dealing with significantly higher percentages of incidents.

Chart: Alerts received, investigated and remediated



When it comes to data breaches and the improvements that were made following a breach, the top improvement was to increase security awareness training among employees, closely followed by automating security defenses and putting an increased focus on risk analysis and risk mitigation. If this pays off, hopefully we'll see cybersecurity fatigue levels go down in Thailand, as more responses will be automated.

Chart: Downtime* following a data breach in businesses



Also of interest, is that we asked respondents to select every improvement that applied–overall organizations in Thailand made many more improvements than the global average.

We then asked about the organization's most severe breach, and how long systems were down as a result. This will be tough reading for organizations in Thailand, as downtime is a much greater issue for the region than other countries. 44% of organizations experience downtime for more than 17 hours, compared to the global average of 12% for this time period. Thailand is the most affected region in Asia Pacific for severe breaches, with 9% of organizations experiencing a breach that lasted for five days or more.

Cloud trends

68% of organizations in Thailand have more than 40% of its infrastructure hosted in the cloud. Overall, the trend in Thailand is to embrace the cloud more so than their global counterparts.

When asked why they chose the cloud, the top reason for Thailand was that cloud offers more ease of use, followed by scalability and better data security.

Table: Reasons for using cloud to host IT infrastructure among businesses

	Thailand	Regional	Global
OpEx preferred over CapEx	33%	33%	26%
Lack of internal IT workforce	24%	22%	25%
Cloud offers better data security	57%	50%	50%
Scalability	55%	43%	40%
Regulation or compliance requirements	36%	29%	27%
Ease of collaboration with external parties	42%	52%	37%
Ease of use	71%	19%	51%
Not core to business so outsourcing is preferable	26%	40%	18%
Other	0%	-	1%

Just under half of organizations in Thailand fully expect cyber attacks to extend beyond IT and into Operational Technologies next year.

This is another sign that security remains a reactive industry. In order for organizations to take a breach seriously, they need to experience it. Having witnessed more OT attacks already, more organizations in Thailand expect this trend to stick around.

The defenders' approach

The percentage of organizations in Thailand that use more than 10 vendors has risen slightly from 50% in 2018 to 55% in 2019.

Unfortunately, organizations in Thailand are finding it challenging (82%) to orchestrate multiple vendor alerts. 54% find it "very challenging" (more than double the worldwide figure), and this is clearly having an effect on cyber fatigue. Therefore organizations should focus on integration in order to try and combat this.

Recommendations

As organizations in Thailand told us they were experiencing significant challenges in managing a multi-vendor environment, here are some tips on how to overcome this issue.

Integration between vendors and products is crucial, in order to quickly detect threats and stop them from spreading, automatically and in real time. This enables organizations to respond effectively to threats, which means not having to go on a wild goose chase to stop malware from entering even more of their systems. For example, a network security device spots an infected computer, and has the network automatically quarantine it so it can't do any further harm.

That is automation in action, and it's the one ingredient that can empower organizations to quickly detect and respond to security threats.

Secondly, to help bridge the skills gap, organizations in Thailand could take advantage of cybersecurity courses from vendors and certification groups to bolster in-house skills. The Cisco Learning Network now offers a new Cisco Cybersecurity Specialist certification for people who want to take on a first-responder role when networks have been attacked. Global Information Assurance Certification (GIAC) has a new Network Forensic Analyst certification that gives security professionals the skills to extract and analyse artifacts and activities left behind from unauthorized activity or network-based attacks.

Vietnam Overview

Introduction

With almost no middle ground, Vietnam appears to be either leading the pack for its Asia Pacific counterparts or bringing up the rear, depending on the topic.

Vietnam excels at dealing with alerts and remediating them, which in turn has positively affected cybersecurity fatigue levels.

However with the region experiencing much longer periods of downtime after a severe breach, it is clear that resource levels and finding talent is a major problem for Vietnam. In our recommendations section, we'll look at how to bridge the talent gap, as well as what goes into building a cyber resilience plan.

The cybersecurity culture in Vietnam

Currently, the biggest issue (by far) for Vietnam which prevents organizations from adopting advanced security processes and technology, is a lack of trained personnel. This is followed by a lack of knowledge about advanced security processes. This is somewhat surprising as Vietnam has one of the best records in Asia Pacific in terms of executives seeing security as a high priority. But despite the appetite for security investments, it remains true that finding the right talent is a constant struggle.

Table: The greatest obstacles to adopting advanced security processes and technology in organizations

	Vietnam	Regional	Global
Budget constraints	36%	35%	35%
Competing priorities	19%	22%	26%
Lack of trained personnel	47%	29%	24%
Lack of knowledge about advanced security processes and technology	40%	33%	22%
Compatibility issues with legacy systems	30%	29%	27%
Certification requirements	15%	20%	24%
Organizational culture/attitude about cybersecurity	22%	27%	21%
Reluctance to purchase until they are proven in the market	15%	18%	20%
Current workload too heavy to take on new responsibilities	23%	23%	22%
Organization is not a high value target for attacks	17%	16%	16%
Security is not an executive level priority	10%	15%	13%

We asked organizations in Vietnam if they were suffering from cybersecurity fatigue.

While the number of organizations prescribing themselves with cybersecurity fatigue is higher than the global average (53% Vietnam vs 30% global), it has actually improved a lot since last year, when 62% of organizations in Vietnam were classified as suffering. With an organizational culture that takes security seriously, this percentage should go down even further in 2020, if Vietnam can solve the talent gap problem.

Security alerts and the impact of data breaches

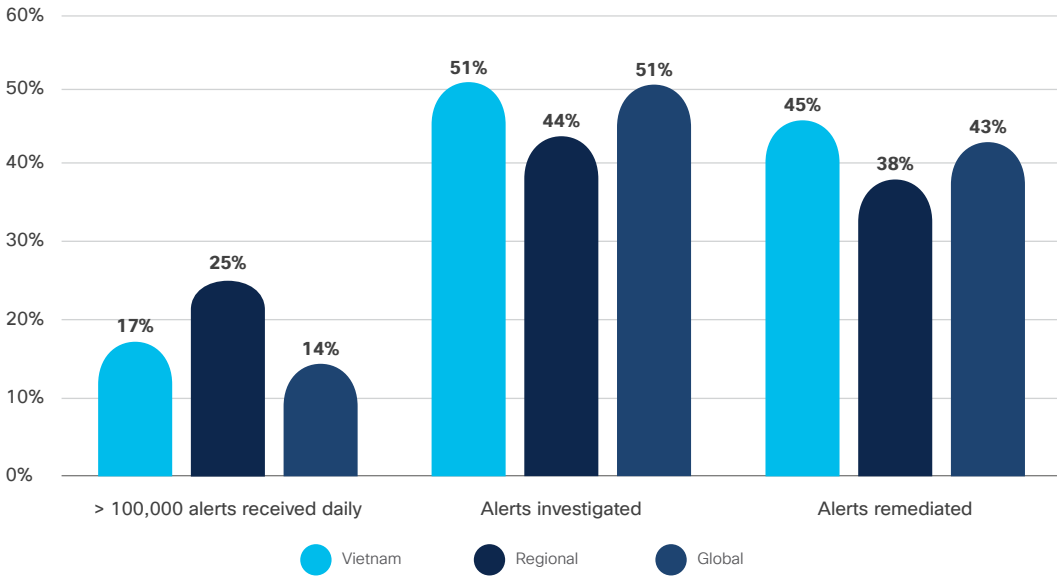
Vietnam has the best record in Asia Pacific when it comes to the volume of security alerts received on a daily basis. The majority are receiving 5000 alerts or less, and only 17% of organizations receive 100,000 or more on a daily basis. When you compare this with somewhere like Korea, 35% of organizations receive this amount every single day.

Vietnam loses its top spot to the Philippines when it comes to the percentage of alerts that are investigated (Philippines investigate 58%) but still, this is much higher than most countries in Asia Pacific.

The percentage of legitimate alerts in Vietnam is more than the global average. This means the region is able to complete more security investigations, because more incidents are in need of being remediated.

While Vietnam's record of remediating 45% of legitimate alerts is less than desirable (55% of actual security incidents are being left alone), it's a slightly better record than the global average.

Chart: Alerts received, investigated and remediated

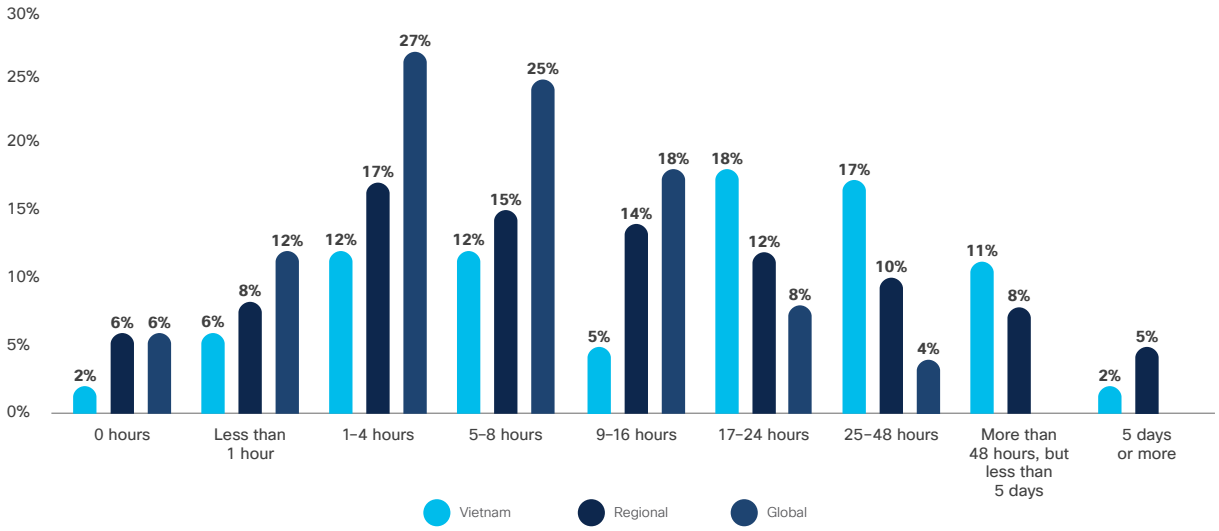


When it comes to improvements that were made following a breach, the top improvement by far was to increase security awareness training among employees. This makes sense, given that there is fewer specialized security teams in Vietnam. As a result, they will be more reliant on their general employees being able to spot attempted phishing and email spoofing attacks.

As impressive as Vietnam's record on dealing with alerts, downtime is a big area for concern. This area is where Vietnam's lack of dedicated personnel hurts the most.

Almost half (48%) of organizations in Vietnam had to down tools for 17 hours or more after their most severe breach. This is the worst record of downtime in Asia Pacific, followed by Korea.

Chart: Downtime* following a data breach in businesses



Cloud trends

Vietnam has more organizations with hosted infrastructures than the global average. Almost half the organizations in Vietnam have more than 60% of its infrastructure hosted in the cloud.

When asked why they chose the cloud, the top reason for Vietnam was that it offers better security, followed by its ease of use.

Table: Reasons for using cloud to host IT infrastructure among businesses

	Vietnam	Regional	Global
OpEx preferred over CapEx	36%	33%	26%
Lack of internal IT workforce	21%	22%	25%
Cloud offers better data security	62%	50%	50%
Scalability	38%	43%	40%
Regulation or compliance requirements	23%	29%	27%
Ease of collaboration with external parties	49%	52%	37%
Ease of use	54%	19%	51%
Not core to business so outsourcing is preferable	14%	40%	18%
Other	0%	-	1%

Significantly more organizations in Vietnam expect cyber attacks to target Operational Technologies in the next year. This might be because, on average, they have already received more attacks than other countries. Since security tends to be a reactive industry, in order for organizations to take a breach seriously, they often need to experience it first.

The defenders' approach

The percentage of organizations in Vietnam who use more than 10 vendors has decreased from 35% in 2018 to 31% in 2019. This could be one of the reasons as to why the number of alerts/ false positives are under better control this year.

The catalyst for a more consolidated approach may well be the number (76%) of organizations who find it more challenging than last year to deal with alerts from multiple vendor's products.

Recommendations

To help bridge the skills gap, organizations in Vietnam could take advantage of cybersecurity courses from vendors and certification groups to bolster in-house skills. The Cisco Learning Network now offers a new Cisco Cybersecurity Specialist certification for people who want to take on a first-responder role when networks have been attacked. Global Information Assurance Certification (GIAC) has a new Network Forensic Analyst certification that gives security professionals the skills to extract and analyse artifacts and activities left behind from unauthorized activity or network-based attacks.

Another recommendation to help with resource, is to consider automating certain processes in real time. This means not having to go on a wild goose chase to stop malware from entering even more of their systems. For example, a network security device spots an infected computer, and has the network automatically quarantine it so it can't do any further harm.

Finally, a cyber resilience plan that is understood and tested regularly is also crucial to alleviate downtime after a breach.

Here are some tips on what should be considered as part of your plan:

- Assign responsibilities—who is doing what? Roles should include analysis, communication with the team/customers/press, and setting up remote working.
- Identify a leader—someone who knows your business and your security strategy.
- Your plan should allow fluidity to incorporate the latest threats.
- Determine the critical components of your network to replicate in a remote location.
- Identify single points of failure to prepare a back-up plan (e.g., in case a key team member is away).
- Create a list of the tools, technologies and physical resources that must be in place.
- Consider both internal and external communications. Customers need to be notified accordingly, and your employees need to understand their role in getting the organization up and running again.

Ask yourself what the damage will be to your business if corporate data made it to the internet. Will it only cost you downtime and reputational damage, or will there be greater costs?

The Cisco Cybersecurity Series

Throughout the past decade, Cisco has published a wealth of definitive security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports provide detailed accounts of threat landscapes and their organizational implications, as well as best practices to defend against the adverse impact of data breaches.

In a new approach to our thought leadership, Cisco Security is publishing a series of research-based, data-driven publications under the banner, Cisco Cybersecurity Series. We have expanded the number of titles to include different reports for security professionals with varied interests. Calling on the depth and breadth of expertise of threat researchers and innovators in the security industry, the collection of reports in the 2019 series include the Data Privacy Benchmark Study, the Threat Report and the CISO Benchmark Study, with more to come throughout the year.

For more information, and to access all archived copies of the reports, visit www.cisco.com/go/securityreports.

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 www.cisco.com/go/offices.

Published March 2019 CISO_01_0319_r1