Anticipating the Unknowns

2019 Asia Pacific CISO Benchmark Study
Regional Overview

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

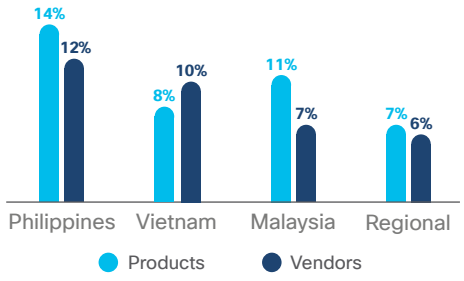
1. Some organizations don't know how many vendors or products exist in their environment

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

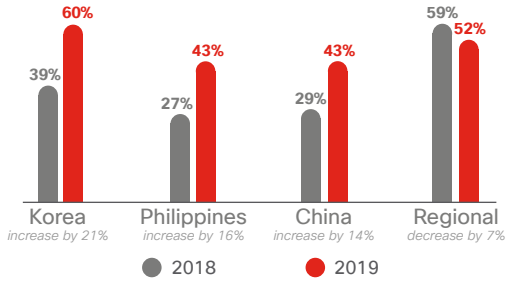


2. The biggest increase in cybersecurity fatigue levels from 2018

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

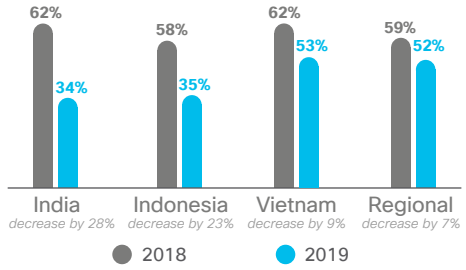


3. The biggest decrease in cybersecurity fatigue

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:

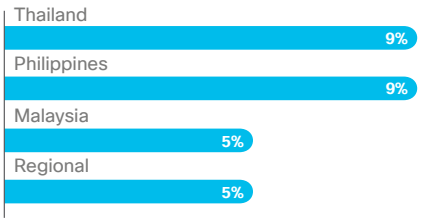
Chart: Biggest decrease in cybersecurity fatigue levels



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



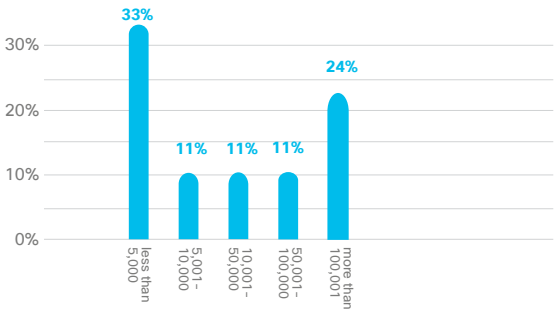
(Note: in each country report we outline recommendations to improve downtime and build an effective cyber resilience plan)

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.

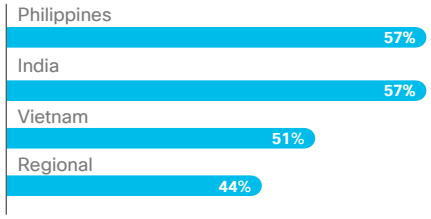
At a worldwide level, 49% of respondents reported receiving fewer than 5,000 alerts per day (some countries are receiving more than 500,000 alerts a day) whereas in the Asia Pacific region, that figure is only 33% (albeit this is a big improvement on last year's average of 25%). Most countries receive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

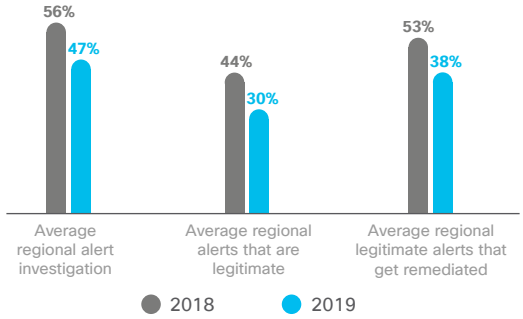
Even more significant than the investigation, is the ultimate remediation of legitimate security incidents. The average remediation level for Asia Pacific is 38%, lower than the global average of 43%.

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

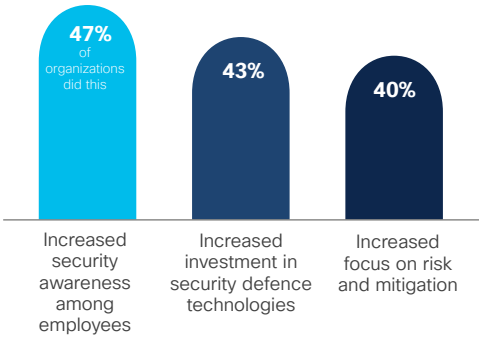


7. Most common areas of improvement after a breach

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

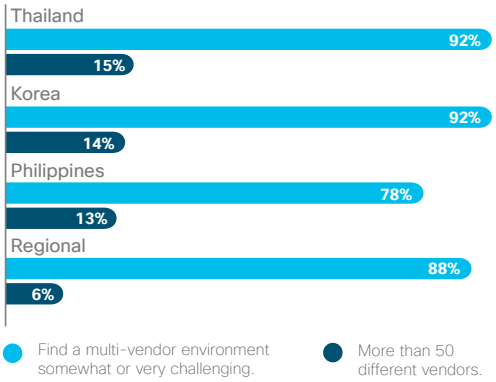
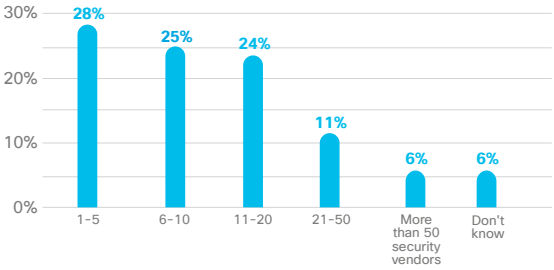


Chart: Average regional rates



Key regional trends

1. Cloud

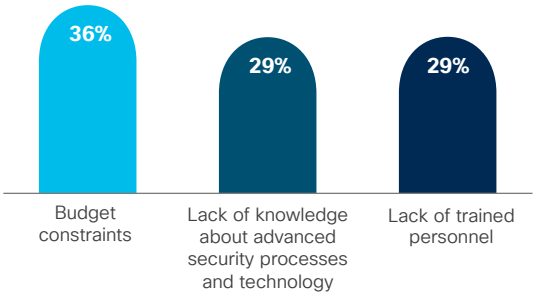
Asia Pacific countries tend to have higher percentages of their infrastructures hosted in the cloud rather than on-premise. 16% have between 80–100% hosted, compared to just 9% in this bracket globally.

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.

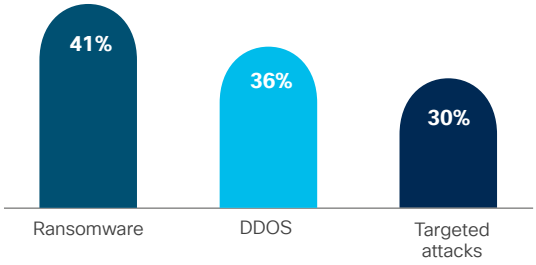
By contrast, 21% of organizations in the rest of the world told us they had already experienced an OT attack, with 64% expecting OT attacks to increase in the next year, and 36% believing that OT attacks are not a growing trend.

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%).

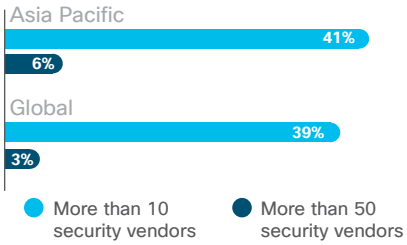
Chart: Top 3 security risks



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.

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