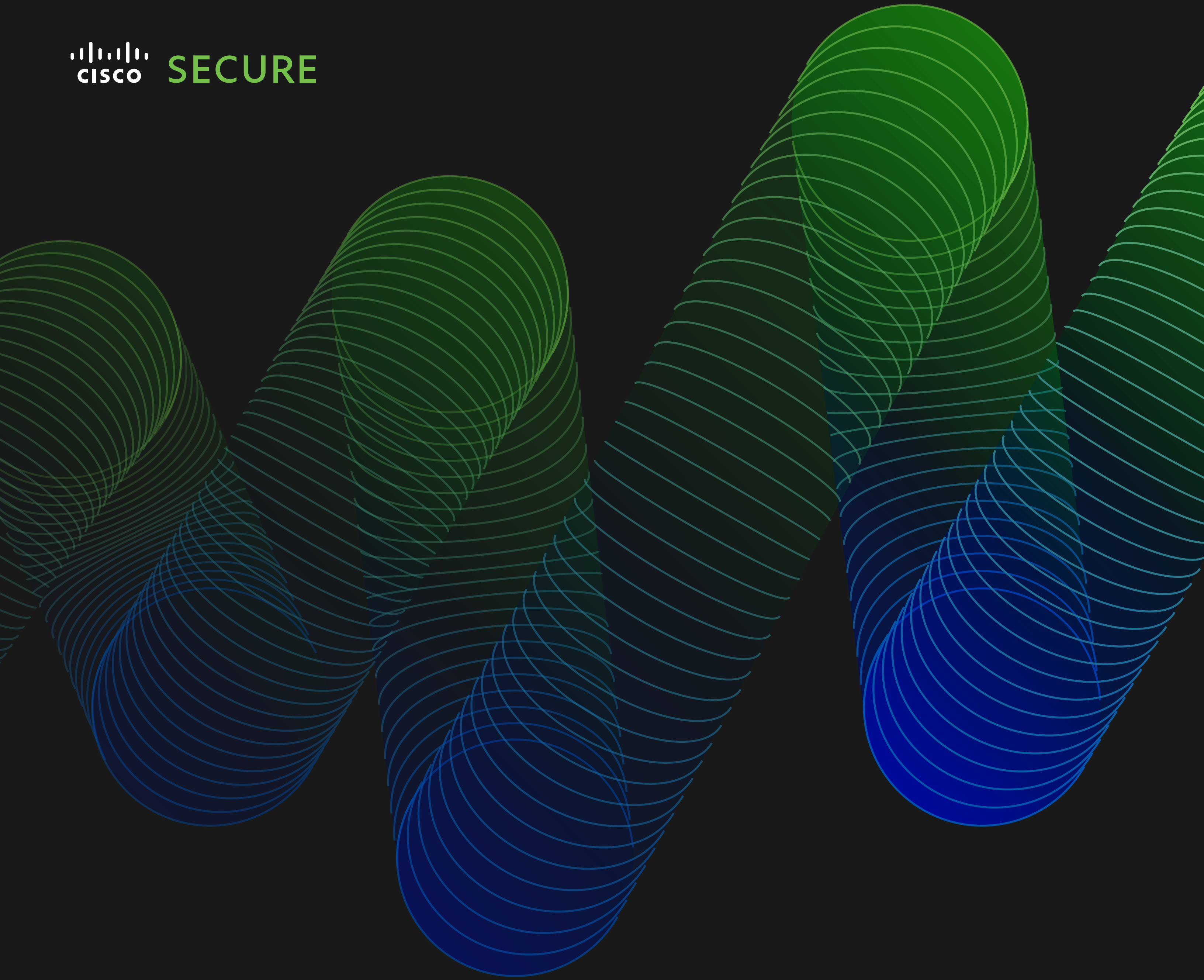
CISCO SECURE



The State of Security Resilience in APJC

Findings from the Security Outcomes Report, Volume 3

CISCO The bridge to possible

What is security resilience, why is it so important, and how can organizations measurably improve it? Those are the questions we sought to answer in our recently released third volume of the Security Outcomes Report. The report analyzes data collected from over 4,700 security leaders and professionals across the globe. This snapshot focuses on the responses from over 1,400 participants working in the Asia-Pacific, Japan, and China (APJC) region.

Assessing security resilience

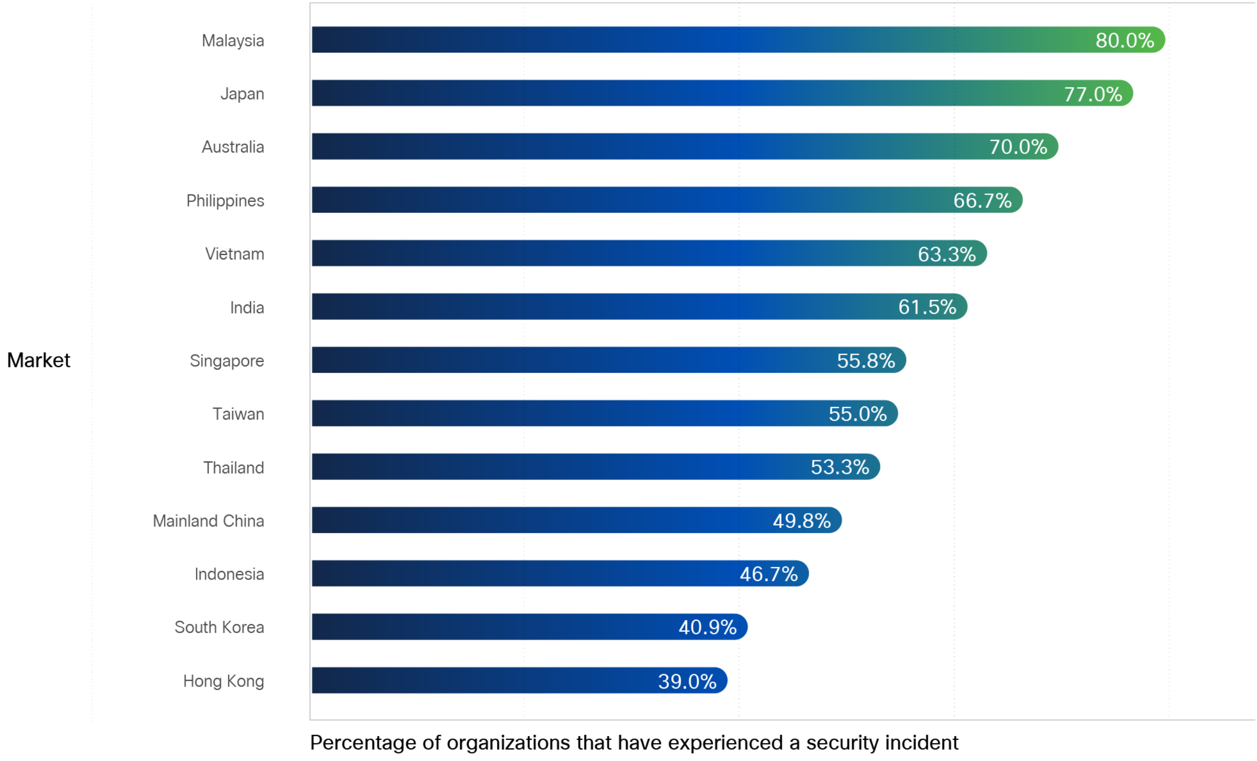
Is resilience on executives' radar?

Yes! We asked respondents about the level of interest and importance top executives place on security resilience. The message couldn't be clearer. A full 97% of APJC execs consider security resilience highly important and that statistic varies little across the region.

Do cyber events impact resilience?

Globally, 62% of organizations (and 58% in APJC) report experiencing major security incidents that jeopardized business operations, the majority of which occurred in the last few years. The rate of resilience-impacting events differs quite a bit across APJC. Reported incident frequencies are lowest in Hong Kong (39% of organizations) and highest in Malaysia (80% of organizations), with other markets falling at regular intervals between those extremes.

Figure 1: Rate of reported security incidents that impacted resilience

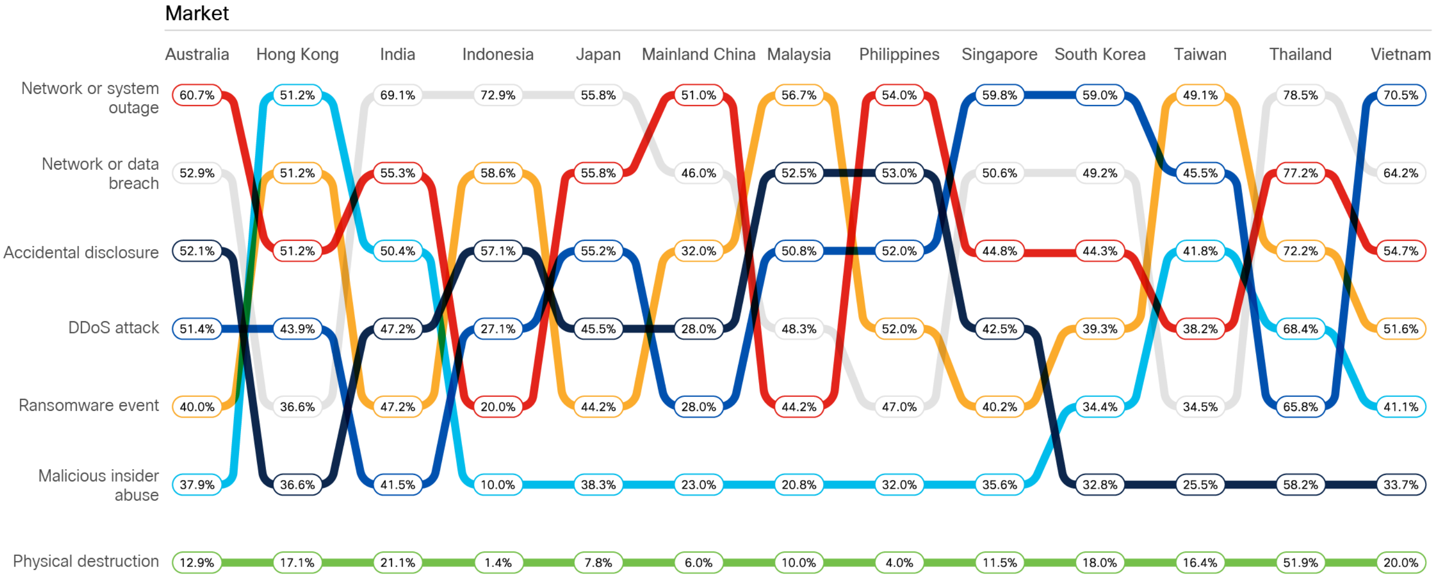


Source: Cisco Security Outcomes Report

What types of cyber events impact resilience?

We asked respondents to elaborate on the types of resilience-impacting incidents they experienced. The chart below ranks common incident types based on the percentage of organizations reporting them in each market. For example, DDoS attacks were the most common among firms in Singapore (60%) and South Korea (59%) but ranked next to last in India (37%). Incidents involving physical destruction were the least common in all markets.

Figure 2: Types of security incidents that impacted resilience

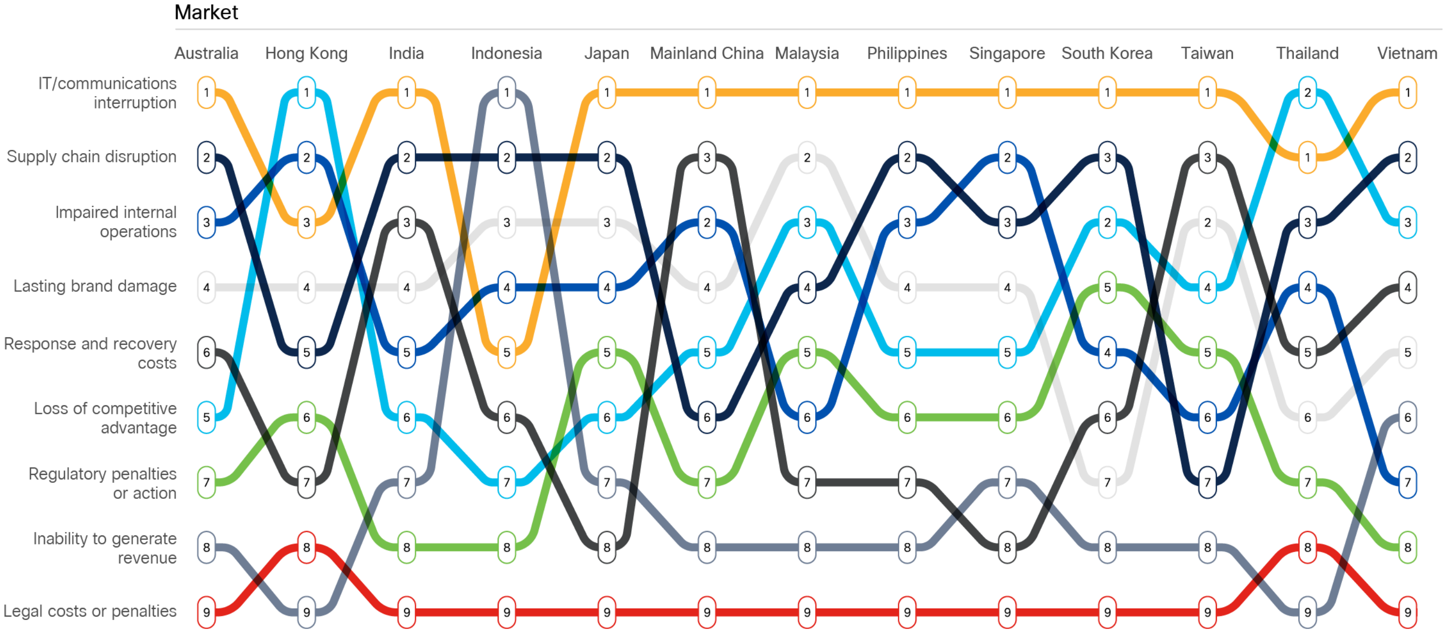


Source: Cisco Security Outcomes Report

What business impacts do incidents cause?

We asked respondents how these major security incidents impacted their organizations. The following chart compares the ranking of impact types based on the percentage of organizations in each APJC market that reported experiencing them. For example, IT interruptions were the most common across most markets, while legal costs or penalties typically landed last. The inability to generate revenue after an incident varied from #1 in Indonesia to #9 in Hong Kong and Thailand.

Figure 3: Types of resilience impacts caused by security incidents



Source: Cisco Security Outcomes Report

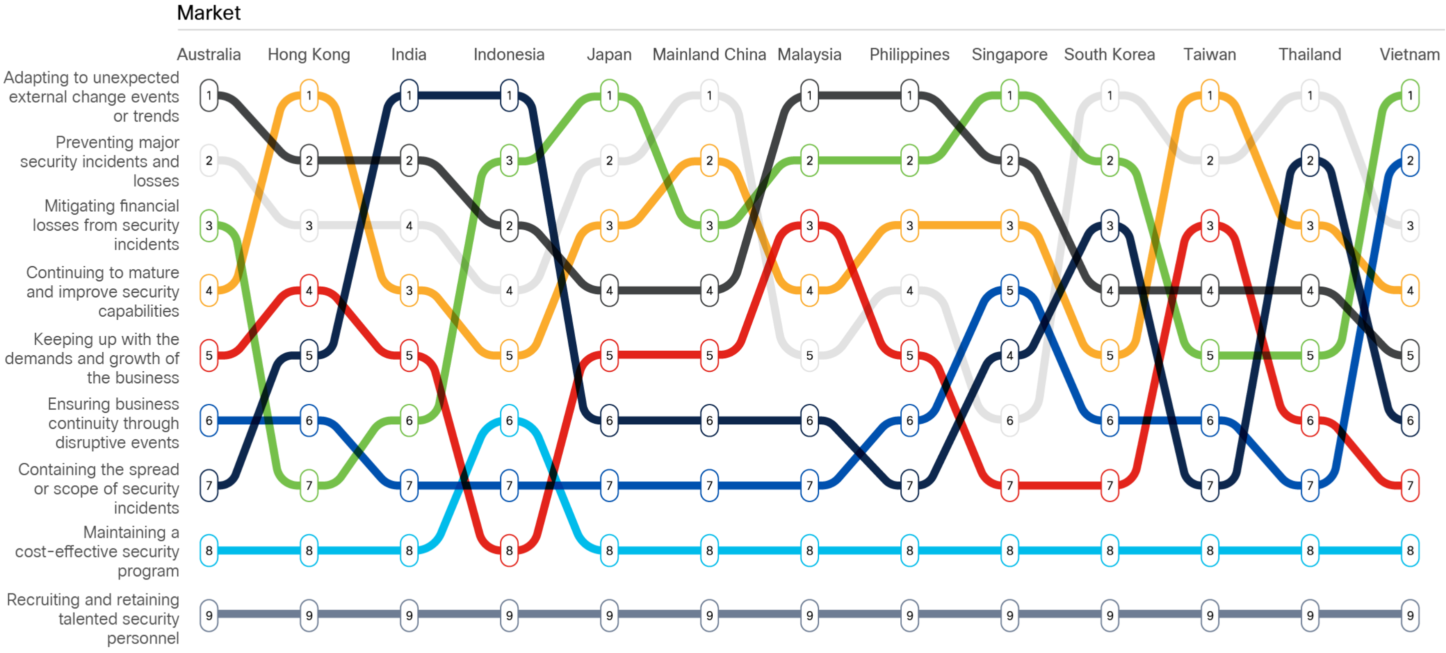
Possible reasons behind the variation in incident rates, types, and impacts among markets include differences in regulatory and compliance pressures, geopolitical factors, prevalent business models, incident detection capabilities, and security program maturity to name but a few.

> “Many organizations struggle with initial policy creation and instantiation to protect assets. Without proper security containment, malware or other threats may be able to spread unchecked throughout an organization’s network, causing widespread infection by way of lateral movement.
>
> A lack of security containment can also make it difficult to identify and isolate the source of an infection, which can prolong the time it takes to resolve an issue, potentially engulfing an organization into a full on server interruption as mentioned in the article as “IT/Communications disruptions” and “impaired internal operations.”
>
> – Timothy Snow,
> CISO Advisor and Architect, APJC, Cisco

Which resilience outcomes are highest priority?

The main report presents nine core objectives or outcomes related to security resilience. We asked participants which of those nine outcomes their organizations considered to be the most important, and rankings for APJC markets are shown below. Maintaining cost-effective programs and recruiting/retaining security talent rank as the lowest priorities across nearly all markets. But there's quite a bit of variation among the other outcomes. For instance, mitigating financial losses from security incidents is the highest priority outcome in Japan and Singapore but falls to #7 and #6 in Hong Kong and India, respectively.

Figure 4: Ranked importance of security resilience outcomes

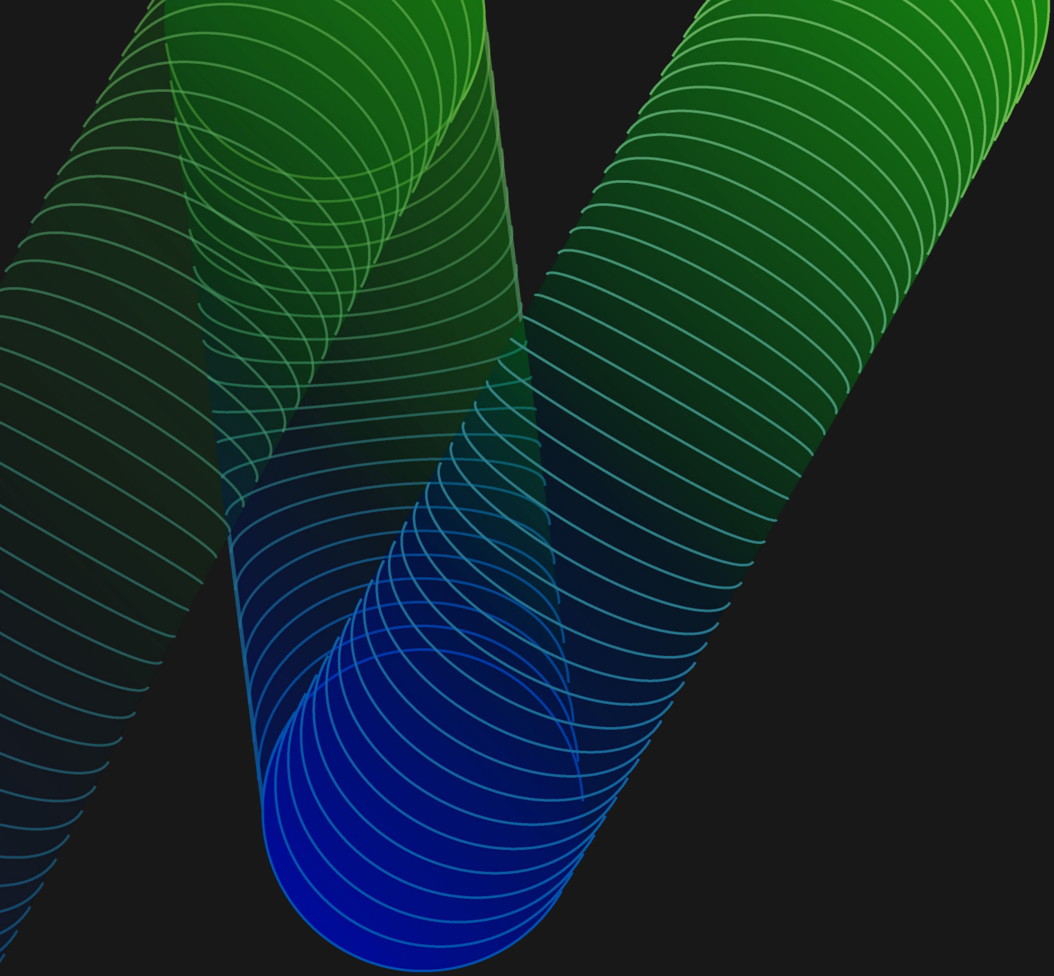


Source: Cisco Security Outcomes Report

Customer spotlight

Hear from Chatchawat Asawarakwong, CISO at **Kasikorn Bank and Business-Technology Group (KBTG)**, on how the financial services organization secured its digital transformation journey with Cisco CX. Watch video.

On a mission to protect its 25,000 users, Australia's largest domestic and international airline **Quantas** deployed Cisco SASE to reduce friction in hybrid work and increase worker satisfaction. Read the case study.



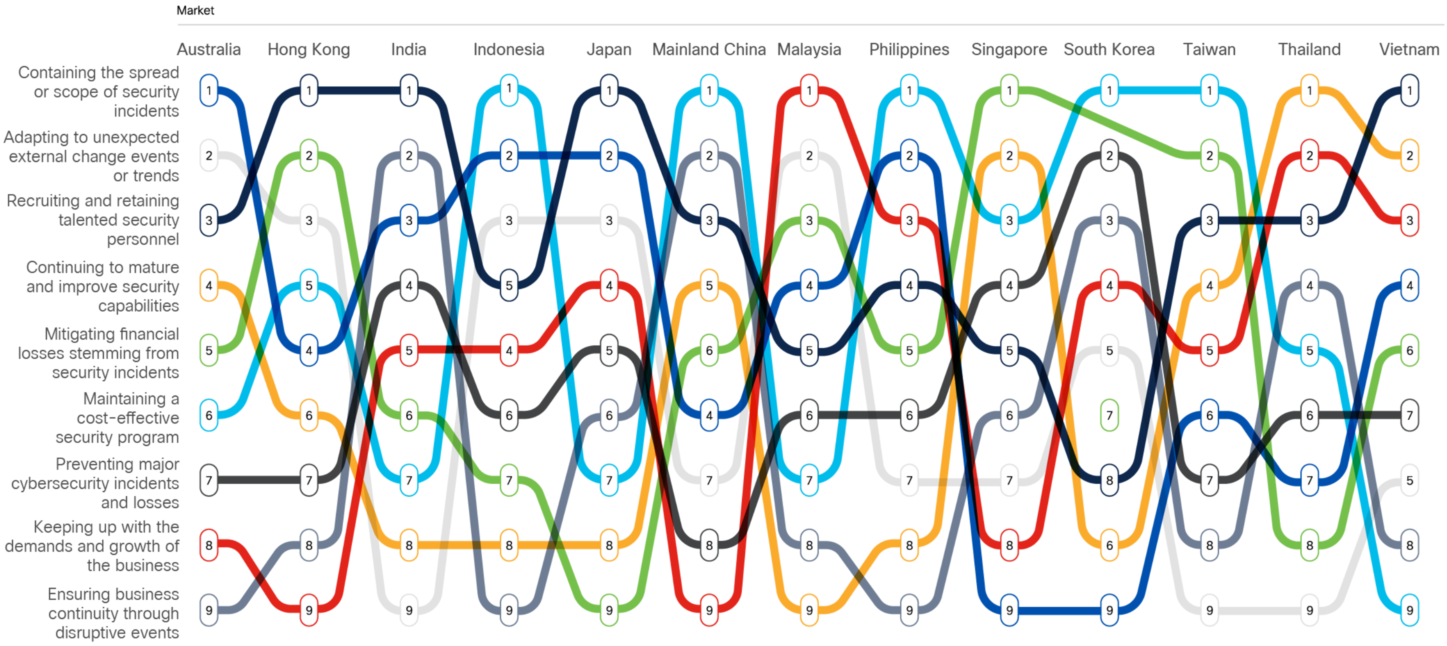
> “It’s surprising to see how low on the scale organizations ranked ‘recruiting and retaining talented security personnel,’ since we’re seeing organizations struggle with adopting new technologies simply because they don’t have the experts and their existing teams are already stretched thin. This is more prevalent in small to mid-size organizations but even large enterprises have retention issues. This directly impacts the consumption of new technology to expand and protect the business.”

– Timothy Snow,
CISO Advisor and Architect, APJC, Cisco

Which resilience outcomes are hardest to achieve?

We also asked respondents to rate how well their organizations actually achieve each of the resilience outcomes. The chart below ranks the relative challenge associated with each outcome and traces how that ranking changes across APJC. It's interesting to see how each market faces difference challenges. By way of example, containing the scope and spread of incidents is the biggest challenge for organizations in Australia but the least challenging to those in Singapore and South Korea. Firms in Malaysia struggle most to ensure security programs keep up with the business, but those in Hong Kong and Mainland China rank that as the lowest among their resilience challenges.

Figure 5: Ranked difficulty of achieving security resilience outcomes



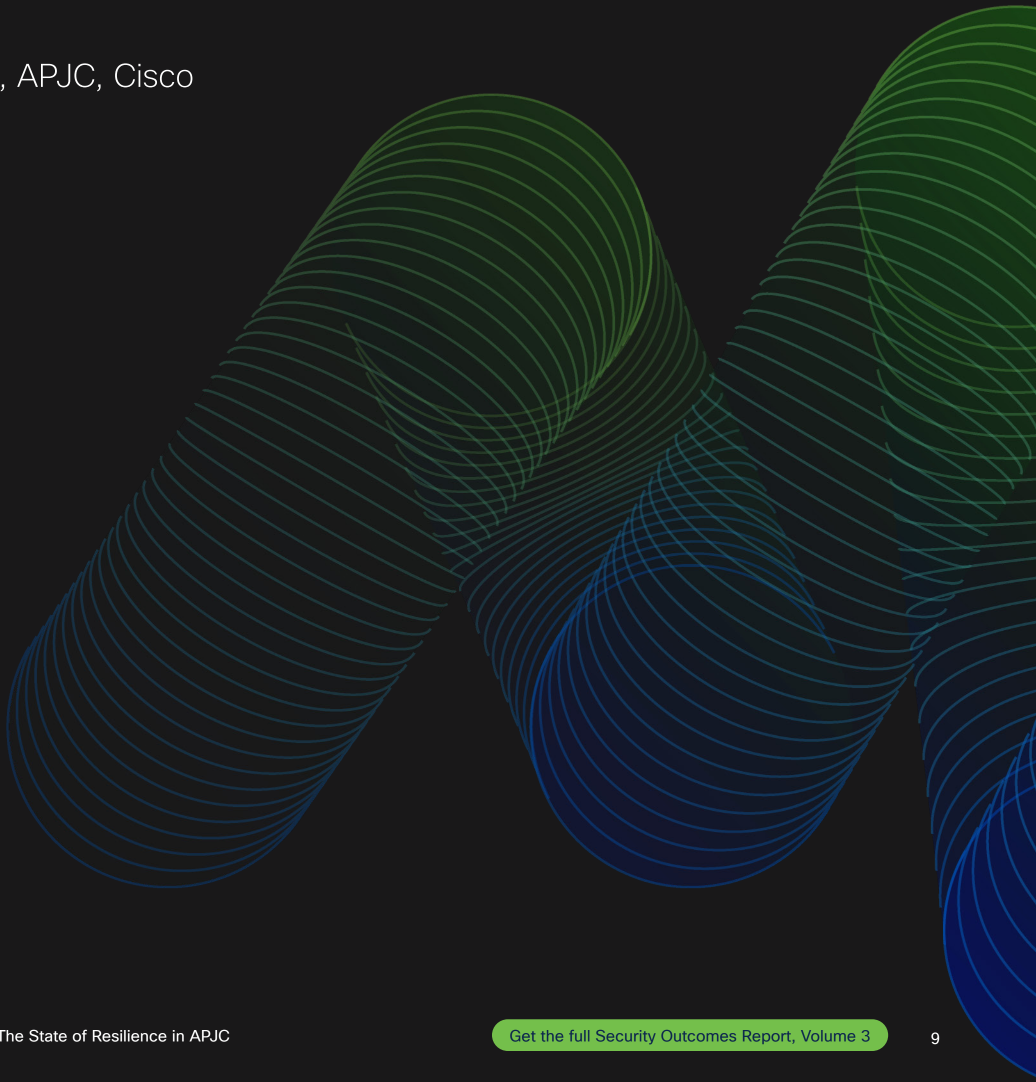
Source: Cisco Security Outcomes Report

Adapt and overcome with security resilience

A seamlessly integrated security stack can lower actual product costs and reduce resources spent on deployment, management, and maintenance. From cloud-first solutions to managed services, Cisco Secure allows your security team to focus on more business-critical initiatives. Learn more about how to build security resilience while reducing both risk and costs: Read the eBook

> “The APJC region is very cost-conscious, with several markets ranking ‘maintaining a cost-effective security program’ at the top. Cost is not only the acquisition of a product or service but the installation, licensing, training, and upkeep of that technology. This may also be a representation of the region struggling with building a comprehensive security architecture.” As seen in the previous edition of the Security Outcomes Report (Volume 2), we saw a direct correlation between security staffing ratios to better threat response with organizations with the highest ratios reporting stronger capabilities than those with lower ratios.”

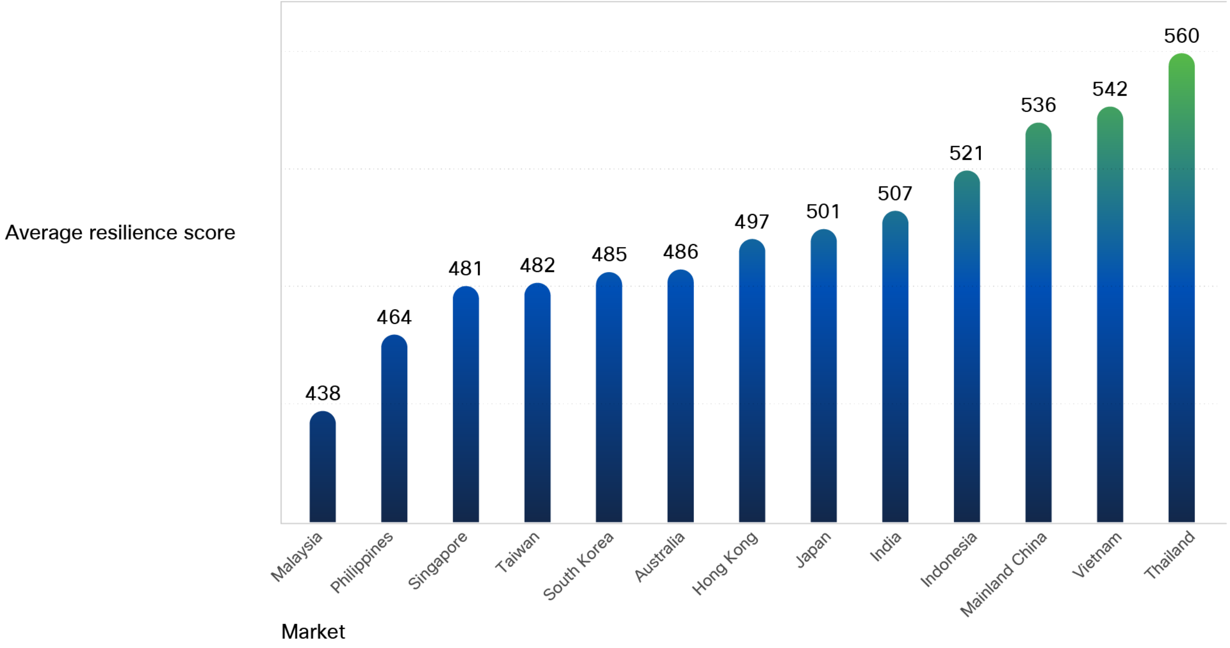
– Timothy Snow,
CISO Advisor and Architect, APJC, Cisco



Can we measure overall security resilience?

Based on ratings across the nine outcomes, we created an aggregate security resilience score for each organization. These scores were normalized such that the global average stands at 500. Overall, six of thirteen APJC markets outperformed that global average. Organizations in Malaysia exhibit the lowest average security resilience score (438), while Thailand achieved the highest (560).

Figure 6: Average security resilience score for organizations in each market



Source: Cisco Security Outcomes Report

Improving security resilience

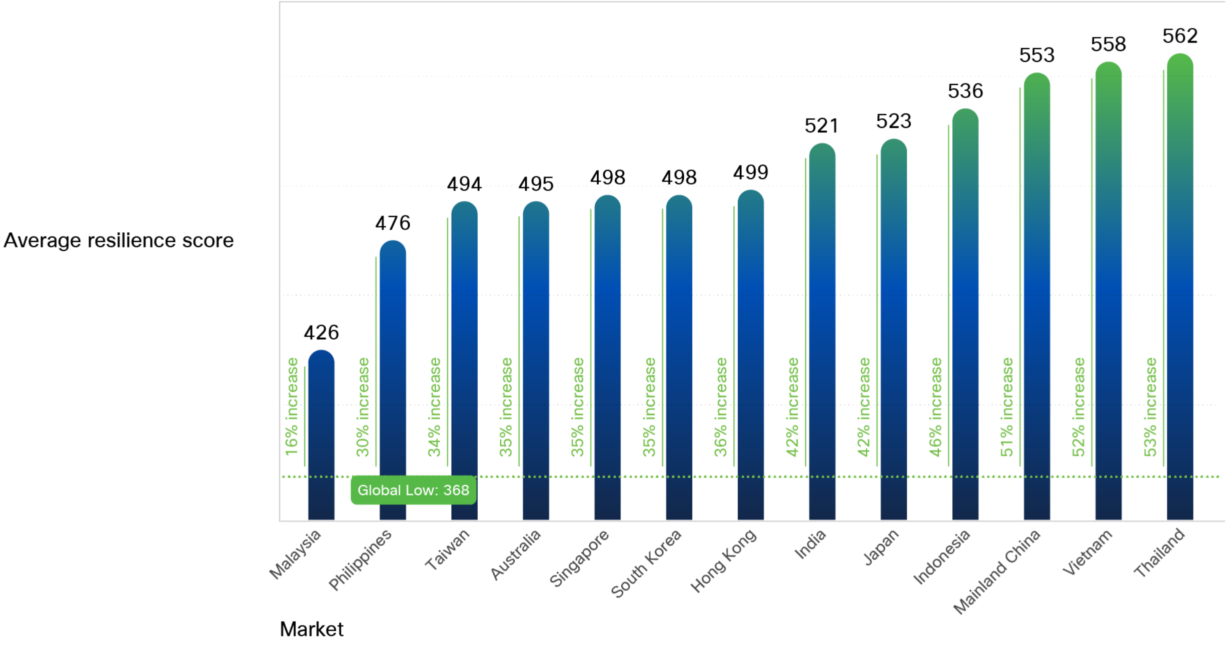
With a score representing overall security resilience across nine outcomes for each organization in the APJC region, we tested numerous factors and identified seven that measurably improve those outcomes. We now show the range of potential improvement to overall security resilience scores associated with a few of these factors specific to APJC.

Establish executive support

Globally, we observed that organizations reporting poor support from top executives exhibit security resilience scores that are 39% lower than those with strong C-suite backing. We offer a few clues from the data in the main report on how to garner such support. Here, we're interested in determining whether markets in APJC exhibit similar effects.

The following chart presents the average security resilience score (blue bar) among organizations in each market with strong executive backing for their security program. The percentage increase on the side of those bars measures the total potential range of improvement over organizations lacking exec support. This enables us to observe that, for example, organizations in Malaysia do benefit from strong executive support (+16% to average security resilience scores), but the increase is not as prominent as the global average of +39%. Those in Thailand, however, experience relatively greater boost of +53% when they're backed with strong executive support.

Figure 7: Potential effect of executive support on security resilience



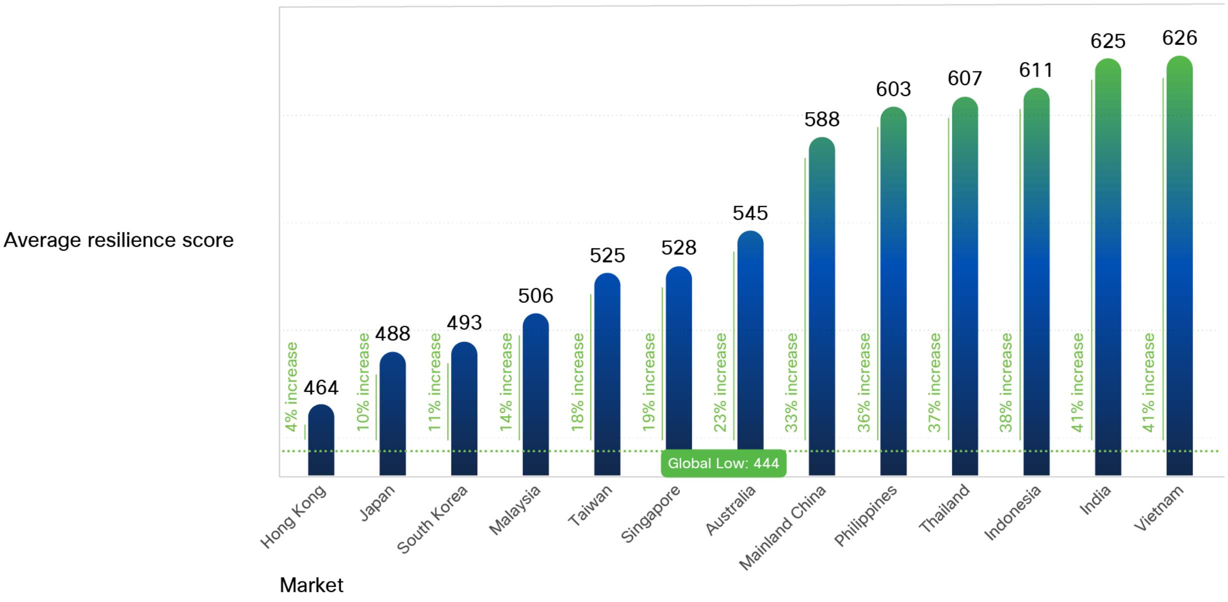
Source: Cisco Security Outcomes Report

Maximize zero trust adoption

The main report measured a 30% difference in average resilience scores between organizations that have made no progress toward implementing zero trust principles and those that have mature implementations (they have MFA, continuous validation, and micro-segmentation with adaptive policies, extensive monitoring, and orchestration of user workflows).

For the most part, APJC markets show similar resilience improvements tied to zero trust. Firms in Hong Kong see a substantially lower margin of increase (+4%) compared to the global average, while those in Vietnam experience a much bigger boost to security resilience (+41%) associated with mature zero trust implementations.

Figure 8: Potential effect of zero trust adoption on security resilience



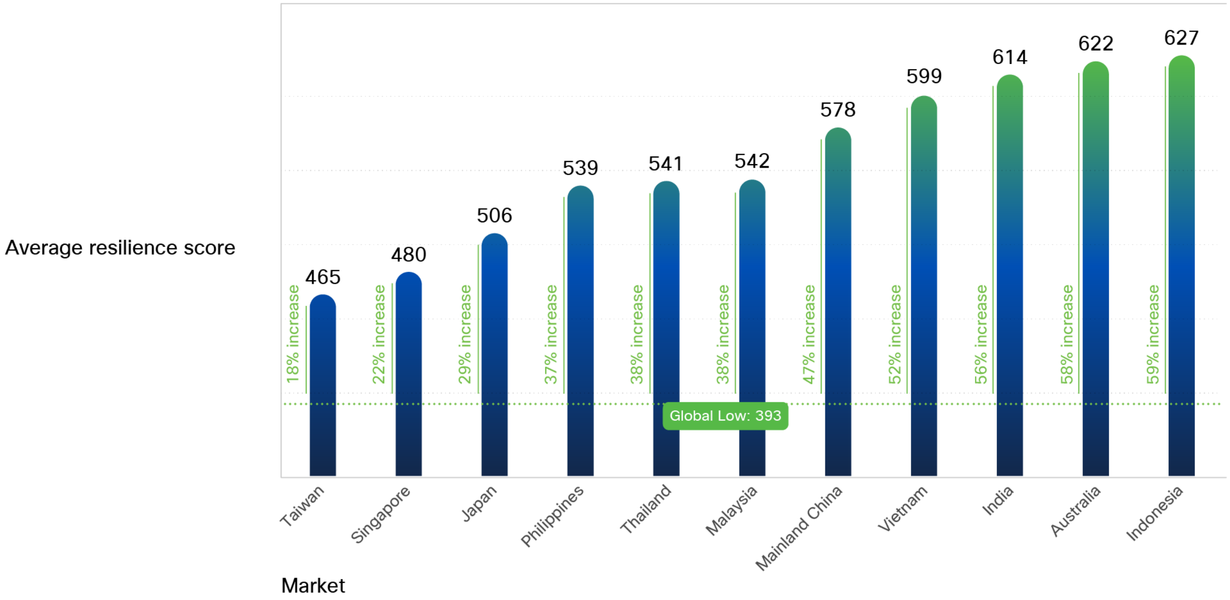
Source: Cisco Security Outcomes Report

Extend detection and response capabilities

Modern cyber threats come at you from a multitude of vectors. It makes sense, then, that having multiple vantage points across those vectors would be an advantage for cyber defenses. Offering visibility into data across networks, clouds, endpoints, and applications while applying analytics and automation to detect, analyze, hunt for, and remediate threats is the core value proposition of extended detection and response (XDR) solutions.

Our data suggests that XDR delivers on that proposed value. Organizations with mature XDR implementations boasted overall resilience scores that were 45% higher than those without XDR capabilities. Per the figure below, average gains in key APJC markets fall fairly evenly above (CN, VN, IN, AU, ID) and below (TW, SG, JP, PH, TH) that mark.

Figure 9: Potential effect of XDR adoption on security resilience



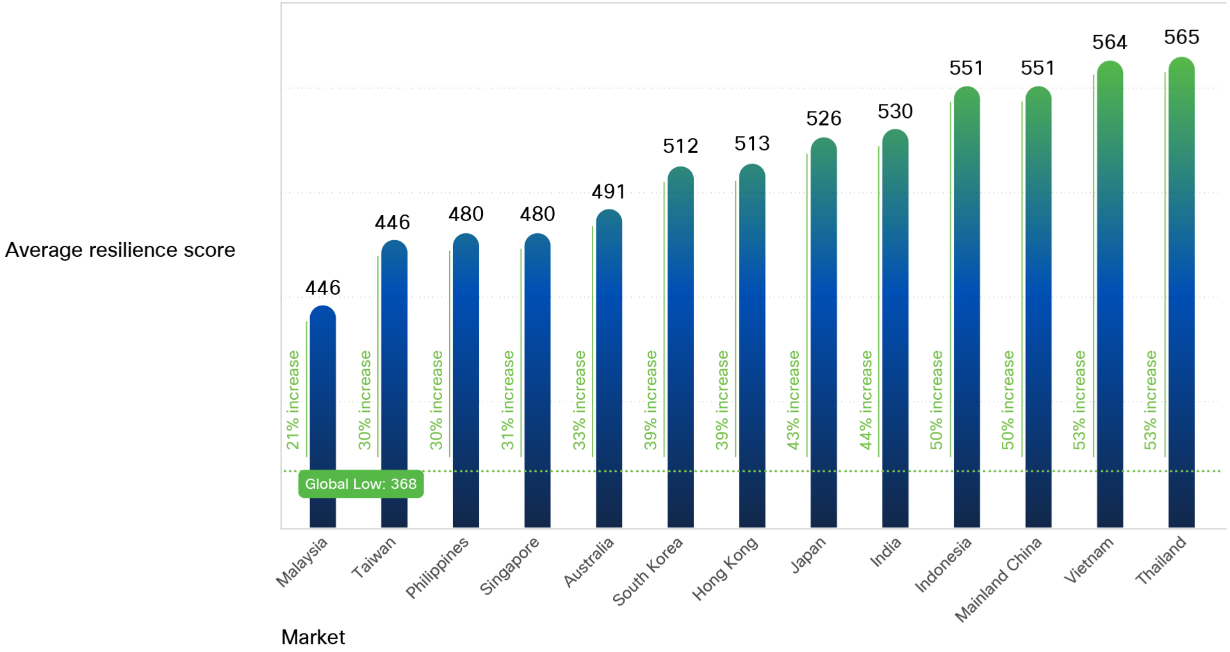
Source: Cisco Security Outcomes Report

Take security to the edge

The acceleration in hybrid work – including a mobile workforce, the proliferation of devices, and the hyper-distribution of applications over multiple cloud providers – has resulted in growing challenges to securing this widespread, fragmented interconnectivity. Secure access service edge (SASE) offers a strategy to converge networking and security into a cloud-delivered service, simplify operations, and remain resilient in the face of ever-changing business demands. What's more, the latest Security Outcomes Report offers compelling evidence in support of SASE's efficacy.

Worldwide, we observed a 27% difference in average resilience scores between organizations with non-existent versus more mature SASE implementations (see what that includes here). All except one market in APJC (Malaysia) show even larger gains of up to +53% (Thailand) over the baseline of firms that haven't started rolling out SASE.

Figure 10: Potential effect of SASE adoption on security resilience



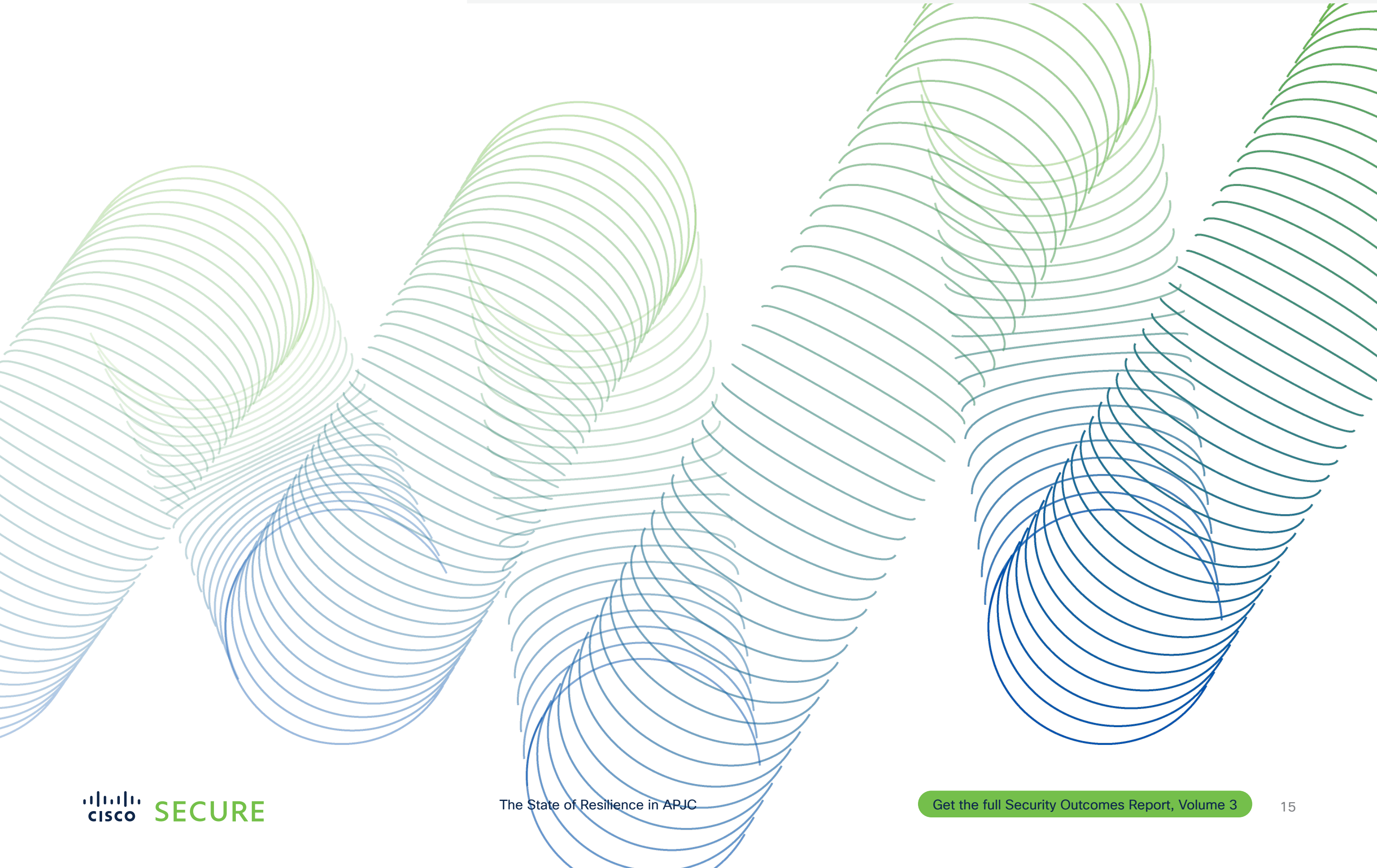
Source: Cisco Security Outcomes Report

Conclusion

While there is certainly some variation in responses across different countries and markets within the APJC region, there were also a few consistencies that are worth exploring. Executives across the region consider security resilience highly important. So what can be done within organizations to address concerns around security resilience? The data clearly points to enhanced XDR capabilities, increased zero trust adoption, and mature SASE implementation as critical pathways to achieving greater resilience. Of course, optimizing each of these areas is a journey and requires planning and collaboration among IT and security operations teams.

Learn more:

To learn more about how teams can collaborate to reach their resilience goals, download the full Security Outcomes Report, Volume 3: Achieving Security Resilience.



CISCO
SECURE

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

Published March 2023

CISCO The bridge to possible