Executive Summary

Asia Pacific is an exciting region where great strides are being made in digital transformation. It is home to significantly diverse economies and is remarkably leading the charge in developing connected cities of the future—smart cities. Many economies are seeing the benefits of these rapid developments, and as the Internet of Things (IoT) becomes commonplace in organizations and workers continue to work remotely and flexibly, more devices are becoming connected to the Internet.

While this has opened up greater avenues for growth and development, it provides more opportunities for threats to get through and risks for businesses and individuals. Along with this, attackers are getting increasingly sophisticated and are employing cutting-edge techniques to breach organizations.

2017 saw an unprecedented wave of cyber attacks, yet cybersecurity measures are too often reactive responses instead of cornerstones of a sound digital infrastructure. To put this into perspective, in the Asia Pacific region, companies receive 6 threats every minute but only **50% of alerts are being investigated**.

The Cisco 2018 Asia Pacific Security Capabilities Benchmark Study—conducted by independent third-party researchers—offers insights on security practice from more than 2,000 respondents across 11 countries. This includes China, Korea and Japan in North Asia, the Southeast Asian nations of Singapore, Thailand, Malaysia, Vietnam, Philippines and Indonesia, Australia in the south, and India.*

In this report, we highlight the potential economic loss across Asia Pacific due to cybersecurity incidents and the fact that defenders have a lot of work to do and challenges to overcome. Our research and insights are intended to help organizations respond effectively to today's rapidly evolving and sophisticated threats.

The key findings from this report are:

1. **Breaches**

   In Asia Pacific, many companies receive up to 10,000 threats a day according to our study. That means 6 threats are received every minute. **69% of companies surveyed receive more than 5,000 threats a day.** However, only 50% of the total numbers of alerts are investigated.

2. **Lack of security readiness**

   Our study asked 2,000 respondents, **about the digital security infrastructure they have in place**. As many as 9% of respondents said that they do not have any dedicated cybersecurity professionals at their organizations, while 13% do not have executives who have direct responsibility and accountability for the cybersecurity of their organizations.

   Amongst the respondents only 42% said that executive leadership considers cybersecurity a high priority, and just 44% strongly agree that security roles and responsibilities within organizations should have a clear chain of command.

3. **Economic and reputational fall out**

   Cyber attacks are having far-reaching ramifications that include financial and reputational losses to companies. **In Southeast Asia, 51% of all cyber attacks resulted in a loss of more than USD$1 million.** Nearly 10% of respondents said that cyber attacks cost them more than USD$5 million. 33% of respondents in the study said a security breach can cost them anywhere between USD$1 - 5 million.

4. **Multi-pronged attacks**

   The form of cyber attacks is also changing. Attackers are now not just targeting IT infrastructure, but are now also targeting operational technologies (OT) that impact the day-to-day functioning and running of a business.

   30% of organizations have already seen cyber attacks along those lines, while 50% said they expect this to be the case moving forward. In addition, **41% of Asia Pacific respondents said their businesses would be affected if their operational infrastructure is compromised.**

Note: Japan, China, India, Australia respondents were interviewed in 2017. Singapore, Indonesia, Thailand were interviewed in a later phase of the study in June 2018.

5. Increased scrutiny from stakeholders

In addition to financial losses, cybersecurity incidents are also undermining Asia Pacific organizations' ability to gain confidence with their consumers and other stakeholders, with **72% remarking that greater privacy concerns from their customers** is adding more time to their sales cycle. Nearly half say their sales cycle is delayed by more than a month.

In the coming year, executives also believe that scrutiny from stakeholders such as investors, insurance companies, regulators, business partners, executive leadership, watchdog/interest groups, the media, and employees will start to rise.

Recommendations for defenders

When adversaries inevitably strike their organizations, will defenders be prepared, and how quickly can they recover?

Even so, defenders will find that making strategic security improvements and adhering to common best practices can reduce exposure to emerging risks, slow attackers' progress, and provide more visibility into the threat landscape. They should consider:

- Implementing first-line-of-defense tools that can scale, like cloud security platforms.
- Confirming that they adhere to corporate policies and practices for application, system and appliance patching.
- Employing network segmentation to help reduce outbreak exposures.
- Adopting next-generation endpoint process monitoring tools.
- Accessing timely, accurate threat intelligence data and processes that allow for that data to be incorporated into security monitoring and eventing.
- Performing deeper and more advanced analytics.
- Reviewing and practicing security response procedures.
- Backing up data often and testing restoration procedures processes that are critical in a world of fast-moving, network-based ransomware worms and destructive cyberweapons.
- Reviewing third-party efficacy testing of security technologies to help reduce the risk of supply chain attacks.
- Conducting security scanning of microservice, cloud service, and application administration systems.
- Reviewing security systems and exploring the use of SSL analytics and, if possible, SSL decryption.

Defenders should also consider adopting advanced security technologies that include machine learning and artificial intelligence capabilities. With malware hiding its communication inside of encrypted web traffic, and rogue insiders sending sensitive data through corporate cloud systems, security teams need effective tools to prevent or detect the use of encryption for concealing malicious activity.

About the report

The ***Cisco 2018 Asia Pacific Security Capabilities Benchmark Study*** presents our latest security industry advances designed to help organizations and users defend against attacks. We also look at the techniques and strategies that adversaries use to break through those defenses and evade detection. The report also highlights major findings from the **Cisco 2018 Security Capabilities Benchmark Study**, which examines the security posture of enterprises and their perceptions of their readiness to defend against attacks.