Exploring Cyber Security Maturity in Asia

A study of Enterprise Corporate Executives, IT Executives & IT Practitioners’ Perceptions towards Cyber Security Readiness in Asia-Pacific

A Frost & Sullivan Whitepaper Commissioned by LogRhythm
# TABLE OF CONTENTS

Introduction ............................................................................................................................... 3  
Identifying Cyber Security Maturity in Asia-Pacific ................................................................. 4  
Methodology of Research ......................................................................................................... 6  
Understanding the Current State of Cyber Resiliency and its Challenges ......................... 8  
Confidence Levels in Securing Corporate Data ........................................................................ 8  
Weakness in Proactive Cyber Risk Assessments ...................................................................... 10  
Manpower Challenges – Skilled Professionals and Staff Retention ........................................ 12  
Investigating the Efficacy and Investment in Cyber Security Tools ....................................... 14  
Security Intelligence and Analytics .......................................................................................... 14  
Factors Driving Adoption of Real-time Cyber Threat Monitoring ........................................ 15  
Current State of Cyber Security Maturity in Asia-Pacific Organizations ............................ 17  
Other Insights on Asia-Pacific Countries ................................................................................ 19  
Singapore ................................................................................................................................ 19  
Malaysia .................................................................................................................................. 19  
Hong Kong ............................................................................................................................... 19  
Australia ................................................................................................................................. 19  
The Last Word .......................................................................................................................... 20
INTRODUCTION
This whitepaper explores the current state of cyber maturity in Asia-Pacific to indicate the readiness of enterprises in responding effectively to cyber attacks. Organizations today face an ever-evolving cyber threat landscape, ranging from state-sponsored cyber espionage campaigns, hacktivism from disgruntled hacker communities, and criminal activities including extortion using ransomware to selling stolen data on the dark web.

The consensus these days is that cyber attacks are inevitable. It is not a question of if, but when, and how frequent and significant the impact. The focus is not just to prevent, but to detect and respond promptly to such attacks.

Wee Ee Cheong, The Association of Banks in Singapore

Cyber attackers employ some of the most sophisticated attack techniques that are harder to detect and mitigate, emboldened by the fact that they cannot be prosecuted easily, especially when the breach is conducted remotely. What’s more, some enterprises are becoming more risk averse to adopting digital transformation to safeguard against these attacks, making them less competitive and more vulnerable to threats. It is important for organizations to ascertain the appropriate level of cyber maturity to become truly cyber resilient and adopt more digital transformation initiatives to gain a competitive edge. In essence, to disrupt the industry with innovative business models through digital means and not be disrupted by cyber attacks.
IDENTIFYING CYBER SECURITY MATURITY IN ASIA-PACIFIC

Enterprises today are subject to different threat levels ranging from general malware to more advanced attacks. It is of paramount importance for enterprises to assess their current ability to respond to varying levels of attacks and pursue the right steps towards achieving the goal of a resilient enterprise.

**Figure 1: Cyber Security Maturity Model**

In plotting the graph to evaluate cyber resilience, the Y-axis represents the threat level, while the X-axis depicts the ability of the enterprise to respond effectively to a cyber attack. The curve in the center indicates the different maturity levels an organization may attain based on its capabilities to address the various threat levels:

**Level 1: Reactive & Manual**

This security setup is primitive and consists of minimum controls, such as firewalls and anti-virus software at the endpoint, that are signature-based and ineffective in mitigating sophisticated attacks. The threat level is also characterized by the lack of dedicated network security staff and frequent “firefighting” to eradicate malware and restore business operations using manual processes.
Level 2: Tools based
The organization has invested and implemented a variety of security tools. However, the solutions are usually adopted on a piecemeal basis rather than as a fully integrated approach. Adoption of security processes and ensuring the skill sets of security professionals remain weak as well. As a result, the threat mitigation level is only slightly better due to the usage of more tools providing a greater degree of automation to detect and respond to cyber attacks. There is also ample room for improvements in integration for better threat mitigation.

Level 3: Integrated Picture
The organization has a series of aligned security operations, capabilities and processes that begins with the ability to “see” broadly and deeply across the IT environment, and ends with the ability to quickly mitigate and recover from a security incident. There is a tighter integration with security controls alongside the stringent adoption of security processes and dedicated security staff trained to handle common cyber attacks. There is also greater emphasis on interoperability among security controls, and adoption of standards-based data exchange of threat intelligence.

Level 4: Active Defense
These organizations are predictive and agile; establishing fully-equipped Cyber Security Operations Centers leveraging security intelligence and analytics tools to illuminate potential threat events, assisting the operator in detecting threats and remediating the cyber attack promptly. However, its lack of sophisticated capabilities in mitigating advanced targeted attacks using new threat vectors or social engineering techniques could still result in adverse effects on enterprise operations.

Level 5: Resilient Enterprise
Organizations attaining this security level have a tightly integrated set-up of efficient security tools that are empowered by full visibility of threats across Information Technology (IT) and Operational Technology (OT) systems. It will also have the right processes and skill sets which are continually updated to combat advanced attacks and all possible types of threat scenarios. These organizations adopt cyber security best practices and emphasize security awareness as a shared responsibility among all employees, by regularly providing training on how to stay safe online to prevent any disruptions to their business.
METHODOLOGY OF RESEARCH
Frost & Sullivan carried out the Asia-Pacific Cyber Security Readiness Study to evaluate cyber attack readiness and assess the level of cyber maturity among 400 enterprise IT decision-makers in Australia, Singapore, Malaysia and Hong Kong (100 each), comprising different vertical and horizontal markets. The survey aimed to examine two major areas: 1) understanding the current state of cyber resiliency and its challenges; 2) Investigating the efficacy and investment of cyber security tools.

Number of Employees Managed Under IT Security Portfolios within Asia-Pacific

- 123 employees (250 to 499 employees)
- 136 employees (1000 or more employees)
- 141 employees (500 to 999 employees)

Survey Respondents by Role in the Organization

- CTO/CSO/CIO/CISO: 12.5%
- IT Governance, Risk & Compliance: 8.3%
- IT Security Architecture Design: 9.5%
- IT & Security (Operations, Administrators, Others): 25.5%
- IT & Security (Management): 27.3%
- CEO/CFO/COO/CMO: 17.0%
Exploring Cyber Security Maturity in Asia

Survey Respondents by IT Decision-Making Status

- I am the key decision-maker for my organization’s overall IT security budget: 67%
- I have some involvement in the decision-making of my organization’s IT security budget: 33%

Survey Respondents by Industry

- Banking, Financial Services and Insurance (BFSI): 86%
- Manufacturing: 57%
- Government & Public Sector: 59%
- Education: 35%
- Retail & Hospitality: 39%
- Service Provider (Telco or Data Center Operators): 46%
- Healthcare: 35%
- Utilities (e.g., Mining, Oil & Gas, Water, Energy): 43%

Source: Frost & Sullivan Asia-Pacific Cyber Security Readiness Study
UNDERSTANDING THE CURRENT STATE OF CYBER RESILIENCY AND ITS CHALLENGES

CONFIDENCE LEVELS IN SECURING CORPORATE DATA
The survey asked respondents to indicate how confident they are that their corporate data has not been compromised in recent months and to rate the probability that their corporate data could be compromised in the next 12 months on a scale of 1 to 10. The overall results were then plotted on a quadrant that takes the X-axis as the level of confidence, attaining a mean of 7.4, and the level of probability on the Y-axis, achieving a mean of 6.1. The industries were then plotted on the Probability-Confidence Quadrant based on the actual mean scores they attained, falling into the following sections: 1) High Probability / Low Confidence; 2) High Probability / High Confidence; 3) Low Probability / Low Confidence; and 4) Low probability / High Confidence.
From this chart, it is evident that respondents from the healthcare sector in Asia-Pacific are facing a critical situation where they believe they have a high probability of a data breach, and show lower confidence than other industries that their corporate data has not already been breached.

**Healthcare: Anxious realists prone to business disruptions from cyber attacks**

Survey findings indicate an urgent need for the healthcare industry to proactively improve cyber security measures as the majority of respondents from this sector acknowledged that their networks have been breached before and are at high risk of future cyber attacks. Today, healthcare records fetch a higher value than credit card information in the dark web as cyber criminals could exploit the data for financial gains, such as insurance fraud. In 2016, several hospitals in the US and UK were hit by ransomware attacks disrupting their operations and forcing them to divert emergency cases to other hospitals while conducting remediation work.

In future, the proliferation of smart medical devices in clinics and hospitals could expose critical systems such as drug infusion pumps to greater risk of cyber vulnerabilities. The healthcare vertical has less than 7% share of the overall network security market in Asia-Pacific, an indication of inadequate investments in cyber security. Building a resilient
healthcare enterprise starts with greater security awareness at the board level and elevating that security posture across the organization as any level of cyber attack could severely impact outcomes in curing and saving lives.

**WEAKNESSES IN PROACTIVE CYBER RISK ASSESSMENTS**

Importance of cyber health checks

While organizations continue to invest heavily in improving their security defense as part of becoming a resilient enterprise, they should perform regular cyber risk assessments to discover possible lapses in security processes. Conducting cyber health checks encompassing vulnerability assessments and penetration tests are necessary to uncover unpatched systems and the resiliency of cyber defenses in place.

*Figure 3: Cyber Risk vs Frequency of Risk Assessment*

Figure 3 displays several scenarios from one organization that rarely performs cyber risk assessments, such as once a year, to another that frequently conducts risk assessments at four times per year. The organization is subjected to an increase in risk level and inherent threats such as new vulnerabilities in applications and/or operating systems, or external sources into the enterprise, such as when employees bring in their own devices for work. The cyber risk assessment provides enterprises with an opportunity to review and improve their security tools, processes, and employee awareness, ultimately reducing the possibility of a cyber attack to an acceptable level. However, the longer the timeframe between risk assessments, the higher the threat of a data breach, increasing the window of attack opportunity. By performing frequent cyber risk assessments, enterprises could suppress their risk levels with consistent improvements against unforeseen vulnerabilities and new attack vectors, as illustrated in Figure 4.
Absence of cyber risk assessment = lower confidence, higher probability of cyber attacks

30.8% of enterprises surveyed revealed that they would only perform a cyber risk assessment after a breach or on an ad-hoc basis when they suspect irregularities or malicious behavior in the network, and 24.8% had not done so in the last 12 months. For enterprises that did not conduct any cyber risk assessment, the perception of the earlier survey correlates where the average mean of respondents has a higher probability of data breach from 6.1 to 7.6 – an increase of 24.6%, and the confidence level in not encountering data breaches drops from a mean of 7.4 to 6.9.

Enterprises without cyber risk assessments or those that do it on an impromptu basis acknowledged that they are more likely to be attacked. Having proactive assessments are critical for enterprises in achieving a resilient strategy as their systems will be harder to infiltrate and have a smaller attack surface than peers that do not conduct any assessments. Cyber-resilient enterprises could benefit from savings on unnecessary costs wasted on remediating a data breach, lower cyber insurance premiums, legal liabilities, and fines by the authorities.
IT enterprise security risk assessments are performed to allow organizations to assess, identify, and modify their overall security posture and enable security, operations, organizational management and other personnel to collaborate and view the entire organization from an attacker’s perspective.

*Ron Schmittling, ISACA*

**MANPOWER CHALLENGES – TRAINED PROFESSIONALS AND STAFF RETENTION**

**Figure 5: Ranking of Challenges in Maintaining Security Teams and Tools in an Organization**

Source: *Frost & Sullivan Asia-Pacific Cyber Security Readiness Study*
As identified above, enterprises today face challenges primarily in employing skilled professionals, 24.5% of respondents rated shortage of qualified talent as the highest concern followed by staff retention at 23.5%.

Hong Kong enterprises ranked staff retention as their top-most challenge at 35%, which aligns with local government projections that the labor force would decline after 2018. The limited pool of qualified security staff could adversely influence the security posture of an organization. In a separate survey, 75% of Australian CIOs and 85% of Singaporean CIOs anticipate a rise in cyber threats in the next five years due to a shortage of skilled security professionals. Frost & Sullivan estimates that the shortfall in the global information security workforce is forecast to reach 1.5 million in five years. With the severe shortage of cyber security talent anticipated, achieving a resilient enterprise becomes even more daunting. Learning to use security intelligence and analytics tools are considered essential by respondents as they grapple with cyber attacks without sufficient knowledge and experience of using Security Incidents and Event Management (SIEM) tools to handle indicators of compromise effectively.

Enabling security teams with security automation and crowdsourcing threat intelligence

In light of manpower challenges, the need for user-friendly features coupled with automation empowered by machine learning will be key features resilient enterprises need to consider to get their security analysts up to speed quickly to combat cyber attacks. Security analytics tools are essential to make sense of the big data logs and packets, turning them into actionable intelligence and comprehensive forensic capabilities to assist in incident response situations.

Organizations should also consider contributing and tapping on a crowdsourced threat intelligence platform that obfuscates all private data of contributors yet is able to share the necessary intelligence effectively. The sharing of information among enterprises on how to manage and adapt to the threat landscape could hasten the blocking of an attack indicator discovered by another contributor, effectively reducing the mean time to response.

1 “A Study of Trends and Challenges Facing Hong Kong”, The Hong Kong Management Association, 2016
2 “Cyber-Security Threats Increase as Australian CIOs Face Talent Shortage”, Robert Half, Sept 6, 2016
3 “2015 (ISC)² Global Information Workforce Study”, Frost & Sullivan, 2015
INVESTIGATING THE EFFICACY AND INVESTMENT OF CYBER SECURITY TOOLS

SECURITY INTELLIGENCE AND ANALYTICS ARE PARAMOUNT

Respondents were surveyed on 13 commonly adopted cyber security tools in the enterprise and asked to rate the effectiveness of each solution on a scale of 1 to 10. It turns out that respondents across all countries view network intrusion and prevention tools, mainly the use of network security gear such as firewalls and IDS/IPS systems, as their top-most effective solutions. Enterprises surveyed also recognized security intelligence and analytics tools as being of paramount importance and highly effective in mitigating attacks alongside the perimeter defense. Conversely, the increase in phishing emails and business email compromise attacks have reduced respondents’ perception on the effectiveness of email security tools. Enterprises surveyed mostly recognize the effectiveness of anti-APT
solutions to mitigate advanced malware and web assets protection using Anti-DDoS and Web Application Firewalls.

**Relatively weak investments in Security Intelligence and Analytics**

The Asia-Pacific cyber security market is estimated to be worth US$17 billion in 2015 with the network security segment (network firewall, IDS/IPS, and SSL VPN) attaining US$2.76 billion in security investment dollars; while Security Incident and Event Management (SIEM) tools attaining only US$76.0 million, just 2.8% of what enterprises would spend on perimeter defense. More enterprises need to shift from a reactive model that heavily relies on perimeter security tools to a resilient one that has the right security intelligence and analytics platform / SIEM, to enable the transformation towards monitoring, detecting and responding to cyber threats in real-time. The next section studies the factors encouraging enterprises to adopt real-time threat monitoring.

**FACTORS DRIVING ADOPTION OF REAL-TIME CYBER THREAT MONITORING**

*Figure 7: Drivers to Monitor Threats 24/7 by Ranking*

Driven by high number of sophisticated attacks

Driven by compliance requirements

Initiated by government authorities

Recommended practices adhering to recognized standards (e.g. SANS, ISACA)

Highly recommended as best practices by peers

Source: Frost & Sullivan Asia-Pacific Cyber Security Readiness Study
Respondents were asked if they employed 24/7 or “round-the-clock” monitoring of cyber threats at their organizations, and requested to rank the key factors driving their decision to adopt 24/7 monitoring. Of the 79.8% of respondents doing so, only 34.5% operate an in-house Cyber Security Operations Center (CSOC) locally, 22.0% run the CSOC from their headquarters remotely, while 23.3% currently outsource the function to a Managed Security Service Provider (MSSP). Findings suggest that most respondents deploy a CSOC based on best practices recommendations from peers or security certification chapters. Respondents also gave a relatively high rating to CSOC as an effective tool to respond to sophisticated attacks swiftly. Meeting compliance standards does not appear to offer sufficient motivation among respondents to establish a CSOC. Regulatory authorities can play an important role here by working closely with the private sector to strengthen measures promoting the adoption of real-time monitoring among enterprises, given the rising number of cyber attacks that can hit anytime, anywhere.

Targeted attacks are increasingly sophisticated, and can hide malicious traffic and hack multiple systems in an enterprise from laptops to cyber-physical systems. It is essential to ensure that 24/7 monitoring is fully functional to detect indicators of compromise on both endpoint and network monitoring, as well as in IT and Operational Technology (OT) assets. Approximately 94.5% of respondents across all industries agree that it is necessary to mitigate threats targeting OT environments.
CURRENT STATE OF CYBER SECURITY MATURITY IN ASIA-PACIFIC ORGANIZATIONS

When asked to rate their organization’s cyber security maturity level, only 4.3% of respondents cited that they are a resilient enterprise against cyber attacks. Approximately 30% of enterprises invest in multiple tools to help their staff react to an attack faster. However, the approach to implementing the security tools is usually done piecemeal. This deters proper development of threat mitigation processes in the organization due to the lack of integration and minimal focus on developing the right competencies in using the security tools.

Ideally, there should be more organizations in Asia-Pacific attaining Level 5 cyber maturity where they face minimal impact from cyber attacks to their business operations, and fewer organizations at Levels of 1 and 2. From this research, it is evident that 56% or at least 1 out of 2 organizations are either reactive towards threats or invest in several security tools that are poorly integrated limiting optimum utilization. Figure 8 also show that only 4.3% of enterprises polled have the capability to be cyber resilient.

Source: Frost & Sullivan Asia-Pacific Cyber Security Readiness Study
This study surmised that 95.7% of enterprises surveyed in Asia-Pacific will be disrupted by advanced cyber attacks, even though 79.8% employ 24/7 threat monitoring. The survey showed that 138 enterprises run their own CSOCs, with operation costs estimated at an average US$300,000, amounting to US$41.4 million for the sample involved in this study. As examined from earlier surveys, although security intelligence and analytics tools / SIEM, primarily used in CSOCs, are viewed as efficient in combating cyber attacks, there are inherent challenges in using them effectively. This was evident when respondents were asked to select gaps or areas of improvement in their security analytics tools / SIEM. Enterprises surveyed chose better dashboards and user interface, better integration with other security solutions, and ability to process massive data sets/logs in real-time as the top 3 improvement areas. Enterprises should evaluate these areas when selecting or replacing their security intelligence and analytics solutions / SIEM as these attributes could shift their approach from a tools-based structure to an integrated picture, enabling them to advance towards cyber resiliency.

OTHER INSIGHTS ON ASIA-PACIFIC COUNTRIES

SINGAPORE
Enterprises surveyed in Singapore possess a high level of confidence in their security set-up, although they attribute a low probability to breaches occurring. Banking and finance, service providers, and the government sector generally score higher in their confidence level compared to the healthcare, retail, and hospitality industries. Approximately 4 out of 10 enterprises in Singapore currently operate an in-house CSOC, with more expected as the government increases its focus on cyber resiliency and advocates 24/7 monitoring for critical infrastructures.

MALAYSIA
Enterprises surveyed in Malaysia are least likely to view compliance as a key driver for adopting 24/7 monitoring services. This could spur authorities to step up its efforts in developing cyber security standards and mandate adoption, especially for critical infrastructures. Nearly 36% of respondents consider their current cyber security set-up as being reactive and manual, hence, more awareness about investments into holistic and efficient cyber defense tools that can automate their response towards threats is needed. System integrators also play an important role in enabling enterprises to create an integrated platform for their cyber security set-up instead of just implementing a tool to block attacks by itself.

HONG KONG
In Hong Kong, 3 in 10 enterprises cite a preference to outsource CSOC functions, which could rise in the future, as it correlates with findings that Hong Kong enterprises view staff retention as their biggest challenge in maintaining a security team and managing security tools. Hong Kong enterprises also recorded the lowest usage of security analytics tools across all organizational functions compared to other countries. More investments in the right security intelligence and analytics solutions, as well as focus on continual training on how to utilize analytics to make actionable decisions against threats, will be useful.

AUSTRALIA
Approximately 16% of Australian enterprises do not have an action plan in place in the event of a data breach, which is the highest compared to the other countries in this study. More awareness about the need to develop a proper incident response plan is critical as currently, most enterprises surveyed react to a data breach based on previous experience. Australian enterprises are also most likely to adopt SIEM tools integrated into other security solutions such as firewall and endpoint security. The survey also suggests that more integration of threat intelligence is expected in the future to improve enterprises’ response to cyber attacks.
In exploring the maturity of enterprises in Asia-Pacific, the study has derived interesting insights on respondents’ perceptions of cyber maturity. It is also important to consider the steps to achieving the final objective in becoming resilient and preventing any business disruptions from cyber attacks.

To help enterprises operationalize the requirements for attaining the status of a resilient enterprise, Frost & Sullivan introduces the Cyber Resilience Framework that provides guidance on the phases of Defend, Prepare, Absorb, Recover, and Adapt in any cyber attack incident.
A cyber resilient organization strives to achieve the highest level of organizational readiness against any given cyber or cyber-physical security outcomes. It does this by cultivating the ability to manage, recover and learn from any security episode through the reengineering of sociobehavioral tendencies, security expertise, and operational protocols.

*Frost & Sullivan*

**DEFEND: Investing in effective security tools, people, and processes, or just maintaining the status quo?**

Organizations should stop adopting security technologies as a bolt-on requirement. Instead, these technologies should be integrated into the end-to-end design of systems from the start. Security solutions should be evaluated for their efficacy and capability in preventing the latest cyber attacks. Several enterprises surveyed have invested heavily in security intelligence and analytics tools. However, they found these tools to be difficult to use, hard in deciphering the indicators of attacks, and ineffective in eradicating an attack. Remaining status quo could cripple an organization and lead to resource wastage, by continuing to pay for existing equipment that is inefficient in safeguarding it from cyber attacks. Organizations can also consider implementing the Threat Lifecycle Management (TLM)\(^5\) workflow in a unified way, with strong automation in the areas of advanced security analytics and incident response, where security staff can work more efficiently to detect and respond to threats.

---

\(^5\) "The Threat Lifecycle Management Framework", Chris Petersen, 2016
PREPARE: What is your organization’s cyber health, and are you ready for the next cyber battle?
As highlighted in the study, proactive cyber risk assessments to detect unpatched vulnerabilities and penetration tests to detect lapses in security controls can keep cyber risk levels low and deter cyber attackers. Practicing cyber drills with internal incident response teams and testing employees with phishing email campaigns are recommended exercises for organizations. The ANZ Banking Group and Australian Securities Exchange conduct simulated phishing email attacks on staff at all levels to test their vulnerability to cyber attacks.

ABSORB: Is your organization capable of detecting and absorbing threats, even when working in an infected environment?
With defend and prepare in place, security teams should always be on their guard for the next possible attack. With new vulnerabilities being discovered within operating systems and applications on a regular basis, it is more daunting than ever for organizations to maintain a full-patched and 100% safe environment with zero risks of attacks. Employees could be working on systems infected with advanced persistent threats that are programmed to perform malicious activities in stealth mode, such as exfiltrating data to an unauthorized server or encrypting files maliciously using ransomware. Security solutions must be capable of detecting the earliest occurrence of these attack symptoms to prevent it from spreading damage to more systems.

RECOVER: How will your organization respond to a network compromise or a data breach?

A resilient organization will imply that it will have the ability to detect and respond swiftly to a network compromise, thereby avoiding a material data breach. However, for a non-resilient organization, it is imperative to focus on restoring business operations as soon as possible when a data breach occurs. The effort requires the organization-wide involvement of stakeholders beyond the IT department, such as marketing, public relations, and the CEO, to ensure consistent communication both internally and externally to minimize the impact of a breach. For example, after the NHS Trust in the UK was hit by a major malware attack, the national healthcare provider immediately changed the homepage on its website and social networking sites, issuing an alert to the public on the shutdown of its systems, and informing patients that their appointments would be cancelled until the incident was resolved.  

ADAPT: How can an organization learn from past missteps to prevent future recurrence?

Performing cyber forensics to understand the cause of a breach and uncover vulnerabilities, and using that insight to strengthen cyber security defenses is viewed as critical to achieving a truly resilient enterprise. Learning and adapting to new cyber attack techniques should also be established to forge a constant feedback loop across the organization to become more resilient to the possibility of future attacks.

---
