THE STATE OF CYBERSECURITY IN ASIA-PACIFIC

A new survey reveals that the difficulty of keeping up with rapidly evolving cybersecurity solutions may be hindering the ability of organizations in the Asia-Pacific region to keep their data safe – and tells us what to do about it.

Table of Contents

Introduction

The world is in the midst of massive technological change. Unprecedented breakthroughs are bringing the physical and digital worlds closer than ever before, pushing businesses and governments to rethink production, management and governance systems.

Yet even as newer, more complex technologies, such as big data, analytics, machine learning, artificial intelligence and the internet of things, promise to open up a world of unparalleled growth opportunities, the risk of confidential data being maliciously collected, stored and disseminated is on the rise. Indeed, it is not so much a matter of if private information is secure, but how it is likely to be stolen or misused.

In the Asia-Pacific region, this risk is further compounded by the fact that cybersecurity is still a relatively nascent sector. Very few countries have implemented national cybersecurity strategies, and not many organizations are equipped to keep up with ever-evolving threats and regulations.

Today, more than ever, organizations must arm themselves with knowledge and tools that will keep their information safe.

To find out more about these challenges and opportunities, Palo Alto Networks® recently surveyed more than 500 industry professionals from five key Asia-Pacific markets – Australia, China, Hong Kong, India and Singapore. The results show that, despite increasing resources, decision-makers are finding it difficult to grow their immediate cybersecurity capabilities or plan their long-term cybersecurity strategies. The main barrier? The difficulty of coping with fast-evolving cybersecurity solutions.

This report examines how Asia-Pacific organizations can overcome these obstacles, as well as how they can consolidate their cybersecurity strategies to thrive in this data-driven era.

Assessing Cybersecurity Drivers and Barriers

Home to 60 percent of the world's population,[1] the Asia-Pacific region has a staggering 1.2 billion mobile phone users[2] and nearly half of the world's internet users.[3] As such, the region's digital services market will experience double-digit growth rates thanks to mobile phone and internet use.[4]

Without a major change in mindset, however, many organizations risk losing the potential opportunities that this favorable environment may bring. The survey shows that, despite devoting more resources to cybersecurity, organizations in the region remain confused about the best way to mitigate cyberthreats, a reality that severely hinders their ability to lead in the digital era.

Cybersecurity Resources Are on the Rise

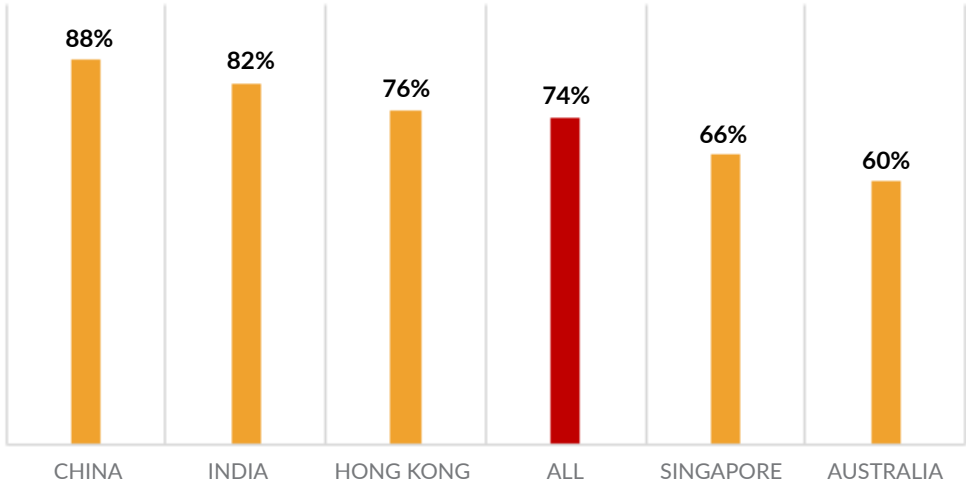
Organizations across the region are paying more attention to cybersecurity. A spate of highly public cyberattacks shook the region these past two years, demonstrating just how destabilizing DDoS (distributed denial of service), phishing and ransomware attacks can be.

The rise of cloud services and BYOD (bring your own device) – two paradigms that essentially decentralize data circulation – has driven organizations to address potential vulnerabilities by increasing the resources devoted to cybersecurity.

Cybersecurity budgets, for instance, are sizeable. Our survey reveals that the majority of Asia-Pacific organizations (74%) devote 5 to 15 percent of their total IT spend to cybersecurity, with China, India and Hong Kong leading the way. At 86 percent, financial organizations with more than 500 employees are the leading segments in this regard.

1. UNESCAP (2016), Population Dynamics, accessed in May 2017.
Available at www.unescap.org/our-work/social-development/population-dynamics
2. eMarketer (2015), Asia-Pacific Boasts More Than 1 Billion Smartphone Users, accessed in May 2017.
Available at www.emarketer.com/Article/Asia-Pacific-Boasts-More-Than-1-Billion-Smartphone-Users/1012984
3. Internet World Stats (2016), Internet Users in the World by Region, accessed March 2017.
Available at www.internetworldstats.com/stats.htm
4. TM Forum (2016), Asia-Pacific a Bright Spot for Digital Services, accessed in May 2017.
Available at https://inform.tmforum.org/internet-of-everything/2016/12/asia-pacific-bright-spot-digital-services

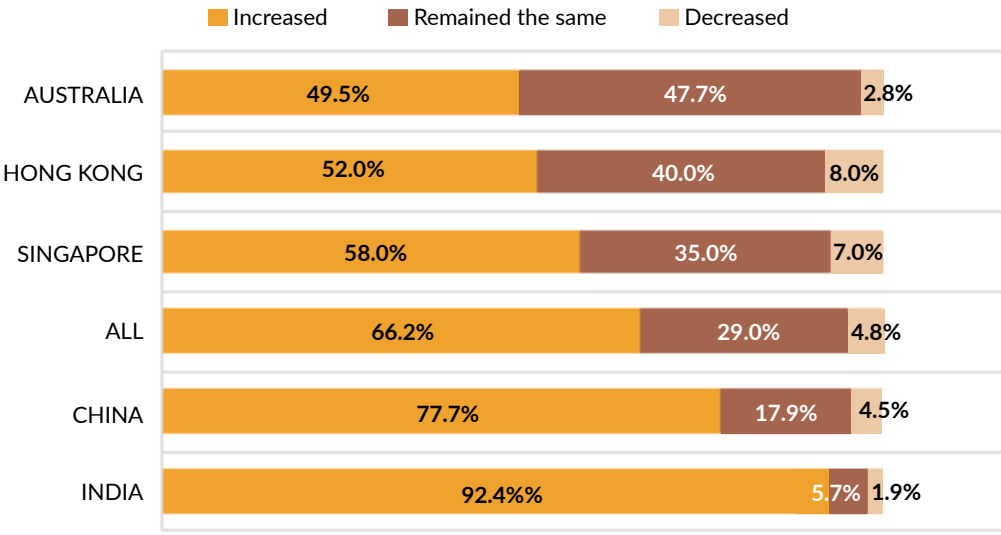
5 to 15 percent of the organization's IT budget is allocated to cybersecurity



Interestingly, cybersecurity budgets are not only consequential – they are also on the rise. For 66 percent of Asia-Pacific organizations, cybersecurity budgets increased from the previous year. This was more marked in India (92%) and China (78%), and much less so in Hong Kong (52%) and Australia (50%).

Here, too, the financial sector outperformed other sectors. 72 percent of surveyed financial organizations saw their budgets increase year-to-year, while one in three (33%) healthcare organizations saw it decrease. Company size also seems to play a role in this regard, as 79 percent of companies with more than 500 employees saw their cybersecurity budgets increase, while 68 percent of companies with 50 employees or fewer saw it remain the same.

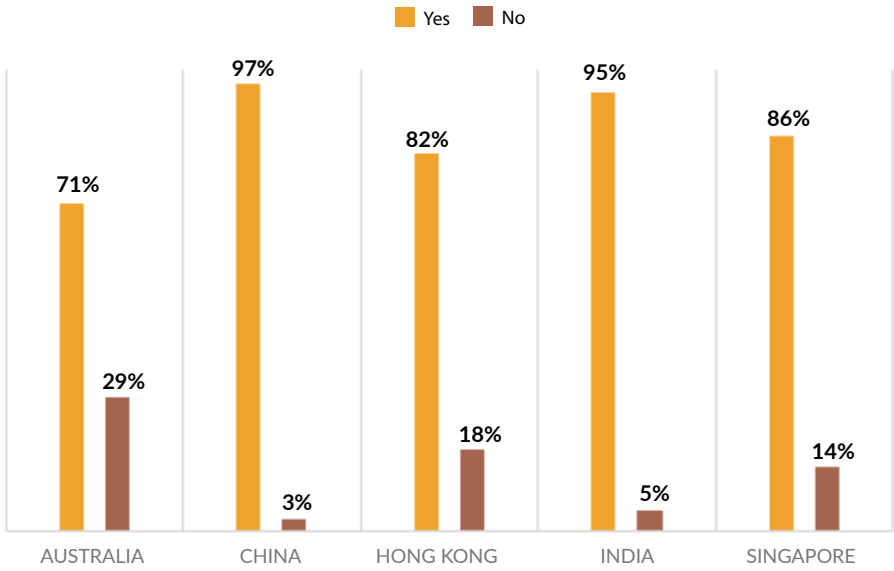
Did your cybersecurity budget increase or remain the same from FY2015–16 to FY2016–17?



As in many other areas, simply throwing money at a problem does not always yield results. Knowledge and expertise are vital components of any coherent cybersecurity response, especially in a world where threats move quickly and stealthily across borders.

China leads the pack in this regard, with 97 percent of surveyed organizations having a dedicated IT security team or department. India (95%) and Singapore (86%) are close behind. At 97 percent and 90 percent respectively, the government and finance sectors take the lead, while a majority of smaller companies (55%) do not have such dedicated teams.

Does your organization have a department or team dedicated to IT security?



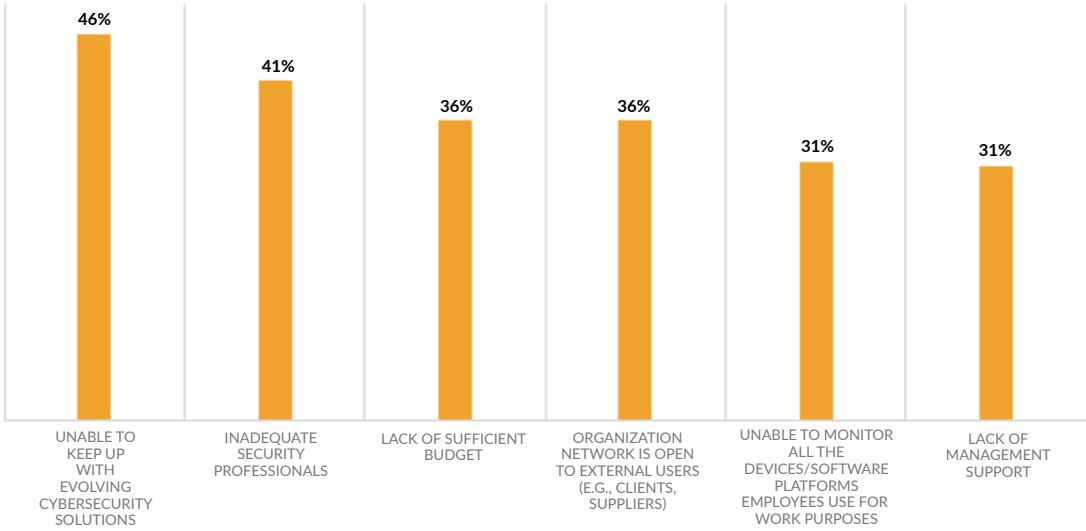
The availability of both a sizeable budget and specialized manpower should give Asia-Pacific organizations the upper hand when it comes to overcoming cybersecurity threats. Yet many of them still report struggling in this area. Why is this the case?

Cybersecurity Is Challenging

The survey shows that cybersecurity is far from being a straightforward challenge for most Asia-Pacific organizations. Investment and skills may have grown in recent years, but longer-term strategies remain out of reach when the cyberthreat landscape changes so rapidly.

Greatly adding to the confusion is the seemingly unstoppable evolution of cybersecurity solutions. For 46 percent of respondents across industries and company sizes, it is the primary barrier to ensuring cybersecurity.

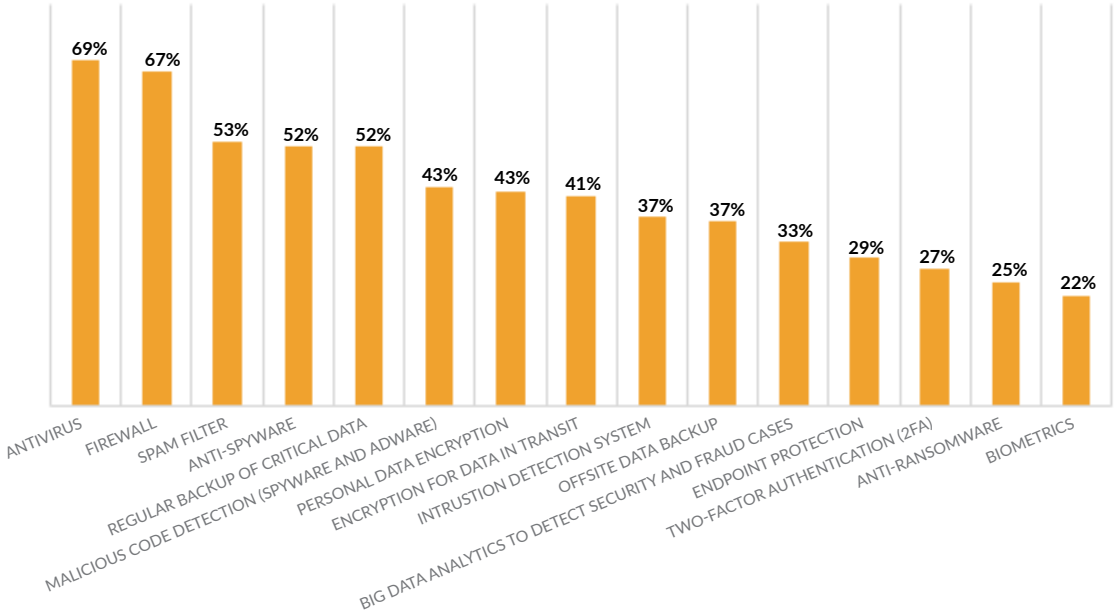
What is the primary barrier to ensuring cybersecurity at your organization?



The disparate security measures adopted by the organizations surveyed illustrate the difficulty of keeping up with constantly evolving cybersecurity solutions. Overall, antivirus solutions remain predominant (69%), closely followed by firewalls (67%). At the other end of the spectrum, two-factor authentication (27%), anti-ransomware (25%) and biometrics (22%) have low levels of adoption.

Antivirus solutions are more predominantly used in the healthcare (74%) and manufacturing (70%) sectors, while the education and government sectors (both 76%) prefer using firewalls. Across all industries, biometrics and anti-ransomware rank relatively low (25% or less). Interestingly, only the healthcare sector is equally unfavorable to endpoint protection, two-factor authentication and biometrics (all 15%).

Which security measure has your organization adopted?



A Major Shift Is Needed

The survey also highlights an important disconnect between respondents' confidence in their ability to counter cyberthreats and the tangible results their methods yield.

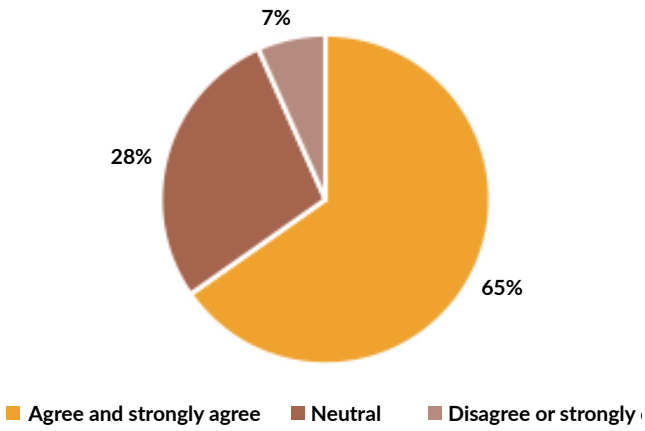
Some 65 percent of surveyed organizations agree or strongly agree that they are well-prepared to handle a cyber-attack. Among the five key markets, China is the most confident (80% of respondents agree and strongly agree), while Hong Kong is the only market in which respondents are more neutral than confident (46% are neutral; 44% agree or strongly agree).

Organizations in the manufacturing sector are more confident than others (69% agree or strongly agree), closely followed by the government sector (66%). Unsurprisingly, companies with more than 500 employees are more confident than those with 50 employees or fewer – 79 percent of larger companies agree or strongly agree, compared to 40 percent of smaller companies.

Despite this confidence, cyberattacks remain a real threat and often cause considerable damage.

Some 61 percent of respondents experienced breaches in FY2015–16, and 52 percent have experienced breaches in FY2016–17, even though the year has not ended. In this regard, respondents in India and China are more affected than those in other markets, but all sectors and company sizes are more or less affected the same.

I am confident that my organization is well-prepared to handle a cyberattack



How many cybersecurity breaches has your organization experienced?

	FY2015–16	FY2016–17
None	40%	48%
1–10	58%	46%
11 or more	3%	6%

Additionally, 47 percent of all respondents lost between US$10,000 and US$250,000 from these breaches in FY2015–16, while a similar proportion (48%) has already lost the same amount in FY2016–17.

What are your organization's estimated monetary damages resulting from cybersecurity breaches?

	FY2015–16	FY2016–17
No impact	12%	16%
US$10,000 and below	22%	16%
US$10,001–US$50,000	15%	17%
US$50,001–US$100,000	17%	16%
US$100,001–US$250,000	15%	15%
US$250,001–US$500,000	6%	9%
US$500,001–US$1,000,000	5%	3%
US$1,000,001 and over	2%	3%
Not sure	5%	4%

Together, these responses show that the primary barrier hindering Asia-Pacific organizations from ensuring cybersecurity is not necessarily related to the budget, expertise or solutions available to them, but rather the way they understand cyberthreats and their ability to effectively counter them.

It is clear a major shift is necessary. Today's organizations must constantly update not just their technologies, but the processes and frameworks with which they tackle new attack methods. So, how can new mindsets and strategies help companies become more resilient against increasingly complex cyberthreats?

Developing Holistic Strategies

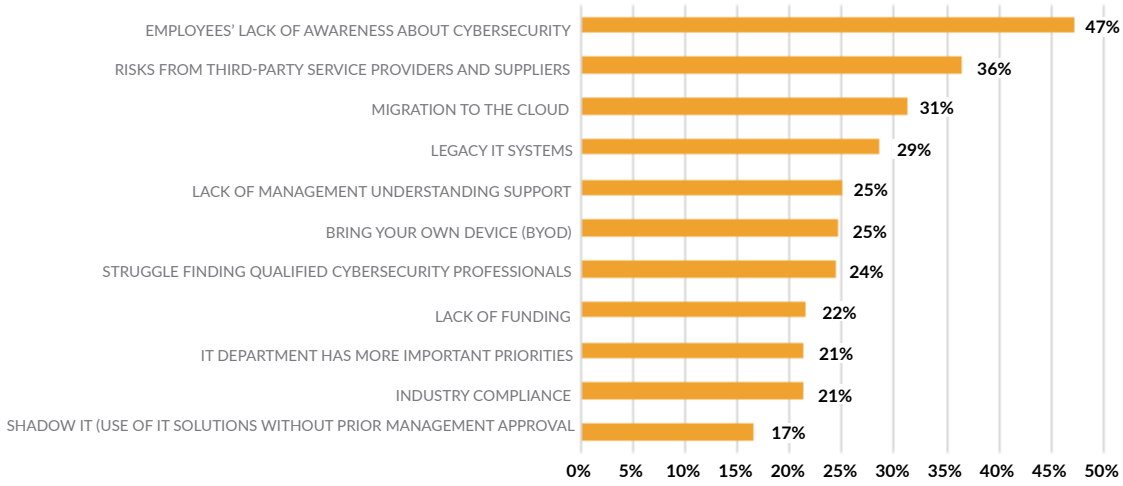
The methods and tactics used by malicious individuals and organizations are evolving so rapidly that even security experts can have a hard time keeping up. The best defense against a nebulous, all-encompassing threat is to put in place a consistent, overarching strategy that empowers everyone – not just IT specialists.

The survey shows that Asia-Pacific organizations want nothing more than to do away with complicated security mechanisms and focus on core cybersecurity foundations: increased awareness, up-to-date training and continuous learning. These are the ingredients for an effective, preventive approach to cybersecurity.

Awareness Is Key

When asked to name the biggest cybersecurity challenge for their organization, Asia-Pacific respondents unanimously point to employees' lack of awareness about cybersecurity (47%), closely followed by risks from third-party service providers (36%) and migration to the cloud (31%).

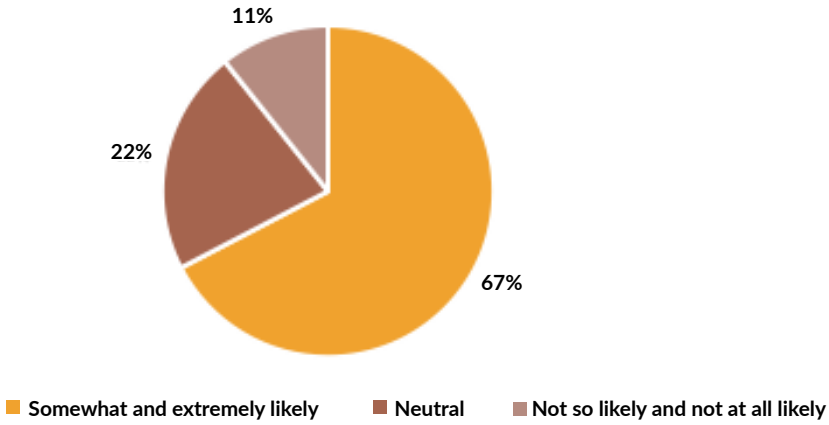
Interestingly, this trend remains roughly similar for companies regardless of market, industry or number of employees. This indicates that, in a world of increased interconnectedness, all businesses worry about the impact their internal shortcomings may have on their external vulnerabilities, and vice versa.



What are the biggest cybersecurity challenges that your organization is facing?

Lack of employee awareness stands out as a major internal threat. When asked how likely it is for an internal threat to pose a cybersecurity risk for the organization, a combined 67 percent of respondents say it is somewhat likely or extremely likely.

How likely are internal threats (e.g., employees downloading unauthorized attachments/software) to pose a cybersecurity threat for your organization?



The same response is found across all industries but is more pronounced in the government sector.

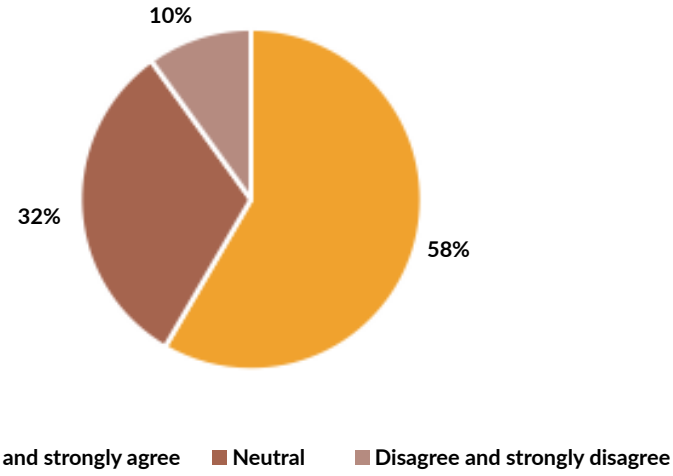
How likely are internal threats (e.g., employees downloading unauthorized attachments/software) to pose a cybersecurity threat for your organization? (by industry)

	All	Financial	Healthcare	Education	Manufacturing	Government
Extremely likely	21%	25%	13%	18%	21%	32%
Somewhat likely	46%	38%	43%	53%	50%	29%
Neutral	22%	23%	28%	22%	20%	26%
Not so likely	8%	7%	11%	4%	9%	8%
Not at all likely	3%	7%	4%	2%	1%	5%

Prevention Trumps All

Perhaps indicative of this lack of awareness is the fact that most organizations in the Asia-Pacific region (58%) believe that the "detect and respond" approach to cybersecurity is more important than prevention.

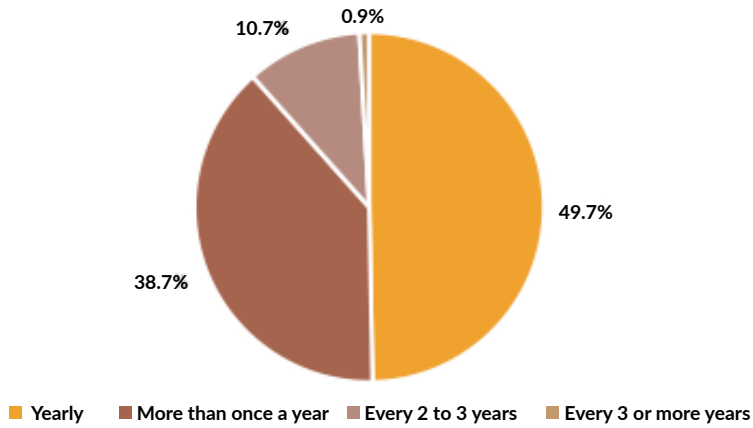
In my organization, detecting and responding to cyberthreats is more important than prevention



Proven preventive measures include implementing training programs for both consumers and businesses, as well as designing comprehensive cybersecurity policies and keeping them up to date.

The survey shows that most organizations (50%) stick to a yearly review of cybersecurity policies and standard operating procedures, while only 39 percent do so more than once a year. At 33 percent, 45 percent and 50 percent respectively, Australia, India and China lead in terms of reviewing policies more than once a year. Conversely, 21 percent of Australian respondents review their policies every two to three years, with some doing so at intervals greater than three years. In terms of industries, manufacturing, government and financial organizations are leading the way in making sure they review their policies more than once a year.

How often do you review your policy and/or standard operating procedure for cybersecurity?



Providing up-to-date training and requiring employees to regularly revisit their knowledge of the cybersecurity environment is critical to a company's holistic security. An effective training program reminds employees of the best practices already in place while ensuring they are aware of the latest traps to avoid. Most importantly, it is generally recommended that training take place more than once a year to prevent and mitigate successful cyberattacks.

Another way to prevent cyberthreats is to share and escalate information. The survey shows that 83 percent of respondents believe it is important to share information with the authorities. At the moment, however, only 44 percent share information with their industry peers, with the healthcare industry leading the way.

	Do you think reporting data breaches to regulators will help prevent cybercrime?	Do you currently share threat information with other companies in your industry?
Yes	83%	44%
No	17%	46%
Not sure	–	9%

Experienced Partners to the Rescue

As the survey shows, effective threat management is an advanced discipline that requires the experience, knowledge and skills to make sense of information coming from multiple interconnected sources.

Working with like-minded technology partners, managed service providers and industry groups that prioritize prevention is the best way to keep your organization out of the headlines associated with cyber breaches.

A robust security platform focusing on prevention helps reduce cybersecurity risk to a manageable level, allowing organizations to compartmentalize the most serious threats and concentrate on business operations.

The benefit of a flexible, natively integrated security platform is the elimination of added complexity and cost of managing a wide array of point products from multiple vendors. Having a simple, coherent and automated security environment makes it harder for security teams to make fatal mistakes. It also makes it faster and easier to share threat intelligence, minimizing the spread of attacks and raising the cost to attackers.

Conclusion

Palo Alto Networks survey shows that cybersecurity is at the center of how organizations can transform to be more agile and responsive to new market paradigms. It also reveals that security is not simply about having the right resources; it further requires organizations to reexamine their strategies in order to tackle unprecedented cyberthreats.

In a world in which agile new entrants are constantly disrupting industries, it is essential for organizations to equip themselves with knowledge, experience and tools that will keep their infrastructure and information safe, as well as compliant with data and privacy regulations.

Those that do not will be less competitive – and even risk becoming obsolete.

Is your organization ready to make the change?

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com