

The state of cybersecurity in Asia-Pacific - blueAPACHE

Canonical: <https://www.blueapache.com/blog/the-state-of-cybersecurity-in-asia-pacific>

Details:

Summary

This blog post, "The state of cybersecurity in Asia-Pacific", is a blueAPACHE article from 2017 covering security. Whilst cybersecurity has gained the attention of company boards, the struggle to keep up with the rapidly evolving cybersecurity technologies, products and solutions is the primary barrier hindering Asia-Pacific organisations from ensuring secure cyber environments. It is written for readers evaluating emPOWER Security, Managed Detection and Response. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2017
Topic	The state of cybersecurity in Asia-Pacific
Services referenced	emPOWER Security, Managed Detection and Response, emPOWER Core Network & DC Interconnect
Named products or vendors	Palo Alto Networks
Cited statistic	Furthermore, 30 per cent have reported financial losses of over US\$100,000 from those breaches.

Article

Whilst cybersecurity has gained the attention of company boards, the struggle to keep up with the rapidly evolving cybersecurity technologies, products and solutions is the primary barrier hindering Asia-Pacific organisations from ensuring secure cyber environments. This is according to 46 per cent of respondents across the Asia-Pacific region surveyed by Palo Alto Networks for its report – The state of cybersecurity in Asia-Pacific. The struggle to combat increasingly sophisticated cyber threats and the search for appropriate solutions to address them have been underscored by the following observations based on the survey:

More money does not mean better solutions – Amongst the spectrum of cybersecurity offerings available, antivirus (69 per cent) and firewalls (67 per cent) have the highest take-up rates in the region. On the other hand, far fewer companies have adopted more advanced solutions, such as two-factor authentication (27 per cent), anti-ransomware (25 per cent) and biometrics (22 per cent). This is despite two-thirds of APAC organisations having increased cybersecurity budgets from the last financial year, with up to 74 per cent getting sizeable budgets (5 to 15 per cent of total IT spend) dedicated to

cybersecurity.

There is a need to change the mindset towards cybersecurity – A majority of organisations in APAC (58 per cent) believe a 'detect and respond' approach is more important than prevention. However, this mindset towards cybersecurity might require re-evaluation, given the continued prevalence of data breaches in the region. In financial year 2016-17, 52 per cent of organisations have reported a cybersecurity breach. Furthermore, 30 per cent have reported financial losses of over US\$100,000 from those breaches.

Different markets, different challenges – Organisations in each market noted a range of challenges they faced in ensuring cybersecurity. Lack of employee awareness stands out as a major internal threat for 47 per cent of those surveyed. Risk from third-party vendors was the second most prominent concern (36 per cent). With the rapid adoption of digital technologies – especially in developing markets – migration to cloud followed as the third-biggest pain point (31 per cent). In particular, governments displayed a need to be more agile in adapting to technology trends, with updating legacy IT systems being their largest hurdle.

As the survey shows, effective threat management requires 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. To view the full report, [click here](#) . For practical strategies to keep up with rapidly evolving cybersecurity technologies, contact the blueAPACHE security team .

Related

emPOWER Security

emPOWER Security (pillar hub)

Managed Detection and Response

emPOWER Core Network & DC Interconnect

emPOWER Connectivity (pillar hub)

Frequently asked questions

What percentage of APAC respondents named keeping up with evolving cybersecurity technology as their primary barrier, per this Palo Alto Networks survey?

The post says 46 per cent of respondents across the Asia-Pacific region surveyed by Palo Alto Networks named the struggle to keep up with rapidly evolving cybersecurity technologies, products and solutions as the primary barrier to secure cyber environments.

What were the two most widely adopted cybersecurity solutions in APAC, and their adoption rates, per the survey?

The post says antivirus had the highest take-up rate at 69 per cent, followed by firewalls at 67 per cent.

What adoption rates did the survey find for more advanced security solutions like two-factor authentication and biometrics?

The post says far fewer companies had adopted more advanced solutions: two-factor authentication at 27 per cent, anti-ransomware at 25 per cent, and biometrics at 22 per cent.

What proportion of APAC organisations increased their cybersecurity budgets, and how large were those budgets?

The post says two-thirds of APAC organisations had increased cybersecurity budgets from the previous financial year, with up to 74 per cent dedicating a sizeable 5 to 15 per cent of total IT spend to

cybersecurity.

What percentage of organisations reported a cybersecurity breach in financial year 2016-17, and what percentage reported large financial losses?

The post says 52 per cent of organisations reported a cybersecurity breach in financial year 2016-17, and 30 per cent reported financial losses of over US\$100,000 from those breaches.

What proportion of APAC organisations believe a 'detect and respond' approach is more important than prevention?

The post says a majority of organisations in APAC, 58 per cent, believe a 'detect and respond' approach is more important than prevention, a mindset the post argues needs re-evaluation given the continued prevalence of breaches.

What were the top three challenges organisations identified in ensuring cybersecurity, per the survey?

The post lists lack of employee awareness as the top internal threat at 47 per cent, risk from third-party vendors second at 36 per cent, and migration to cloud third at 31 per cent.

What particular cybersecurity challenge did government organisations report, according to the survey?

The post says governments displayed a need to be more agile in adapting to technology trends, with updating legacy IT systems identified as their largest hurdle.

Source

origin post (2017)

Knowledge Base

What is the main barrier hindering Asia-Pacific organisations from ensuring secure cyber environments, according to the survey discussed in this blueAPACHE article?

According to 46 per cent of respondents in the Palo Alto Networks survey, the struggle to keep up with rapidly evolving cybersecurity technologies, products and solutions is the primary barrier hindering Asia-Pacific organisations from ensuring secure cyber environments.

Which cybersecurity solutions have the highest and lowest adoption rates among APAC organisations, based on the survey?

Antivirus (69 per cent) and firewalls (67 per cent) have the highest take-up rates in the region, while more advanced solutions such as two-factor authentication (27 per cent), anti-ransomware (25 per cent) and biometrics (22 per cent) have far lower adoption rates.

Did increased cybersecurity budgets correspond with adoption of more advanced security solutions in APAC?

Not necessarily. Despite two-thirds of APAC organisations increasing their cybersecurity budgets from the previous financial year, and up to 74 per cent dedicating 5 to 15 per cent of total IT spend to cybersecurity, adoption of advanced solutions like two-factor authentication, anti-ransomware, and biometrics remained low.

What approach to cybersecurity do most APAC organisations favor, and what breach statistics call this approach into question?

A majority of organisations in APAC (58 per cent) believe a 'detect and respond' approach is more important than prevention. However, in financial year 2016-17, 52 per cent of organisations reported a cybersecurity breach, and 30 per cent reported financial losses of over US\$100,000 from those breaches, suggesting this mindset may need re-evaluation.

What were the top internal cybersecurity challenges reported by organisations across different APAC markets?

Lack of employee awareness was the major internal threat for 47 per cent of those surveyed, risk from third-party vendors was the second most prominent concern (36 per cent), and migration to cloud was the third-biggest pain point (31 per cent). Governments in particular struggled with updating legacy IT systems as their largest hurdle.

Where can readers access the full Palo Alto Networks report mentioned in the blueAPACHE article?

The full report can be accessed via a link provided in the article, pointing to a PDF hosted on Palo Alto Networks' website titled 'the-state-of-cybersecurity-in-asia-pacific.pdf'.