ExtraHop 2022

CYBER CONFIDENCE INDEX: ASIA PACIFIC

It’s been a busy five years in cybersecurity in Asia Pacific. This is what IT security leaders intend to do next.

IT security professionals and teams have spent the past five years firmly in the spotlight. They are an area of the organisation that has attracted—and continues to attract—an increasing share of the IT budget. Regardless, security teams are still far short of the budget and talent they need to face the growing challenges of modern cybersecurity.

The increase in resourcing is a testament to the understanding that boards, executives, and decision makers generally have of the role that cybersecurity plays in organisations today.

Much of the understanding comes from real experiences of attacks.

Our study shows 83% of organisations in the region have been breached by ransomware at least once in the past five years. It’s likely that the percentage is even higher, as organisations may be reluctant to discuss attacks—the study also shows that 20% of organisations won’t tell anyone if they get breached.

The breach numbers are a problem when you consider that boards and executives expect their investments in cybersecurity to afford them greater confidence to conduct business in a secure, undisrupted manner.

- How can IT security decision makers move the needle on security posture when the threat landscape is changing faster than ever?
- How can IT security decision makers in the region become more confident in their organisation’s ability to detect and block threats so they can pass this confidence to executive committees, boards, and staff?

In this report, we start by analysing declarations of confidence by IT security decision makers. We then look at some of the factors that may undermine these declarations of confidence and finally discuss how to address any imbalance in order to create a more confident cybersecurity posture that reflects reality and justifies ongoing investments.

Contextualising Confidence

Confidence and cybersecurity aren't mutually exclusive concepts, but inherent risks in the sector mean that expressions of confidence are often purposely muted.

Public displays of confidence in one's cybersecurity posture can backfire, making firms a target for unwanted attention. Such expressions may also be tempered by the historical imbalance between attackers and defenders: As much as defenders can try to de-risk and identify blind spots, new threats will always emerge that we can't foresee—flaws in common protocols, or new exploit or vulnerability chains, for example—that undermine security and confidence.

Despite this, we've seen in similar, previous research overconfidence on the part of some IT security leaders as to their organisational readiness and ability to identify and repel threats. There's an apparent gap between expressions of security confidence and the implications of security data—such as the surprising prevalence of insecure protocols and the frequency of successful attacks.

It was with this in mind that we set out on a search for answers in the Asia Pacific region. What you have in your hands are the results of research spanning Australia, Singapore, and Japan. All three are significant regional markets but with very different business cultural characteristics that are reflected in the outcomes of this study. We present both a whole-of-region perspective, as well as a breakdown by country which will better highlight differences in approaches being taken.

Only 39% have high confidence in their organisation's ability to prevent or mitigate cybersecurity threats.

On a whole-of-region basis, we find IT security leaders are largely pragmatic about the threats they face, and express confidence in their organisation's ability to handle these threats accordingly. Only 39% have high confidence in their organisation's ability to prevent or mitigate cybersecurity threats. An equal percentage have a low level of confidence.

There are key regional differences, though: 52% of Singaporean IT security leaders have high confidence in their postures, compared to 43% in Australia and 23% in Japan. How each justifies its confidence level is a hot topic for further discussion.

As we've alluded to, confidence in cybersecurity is a fraught concept. Purely from a historical and risk perspective, it makes sense to keep confidence in check or understated.

Yet we also need to keep in mind the context of cybersecurity operations in the past five years and of cybersecurity's increased internal profile and stature. Organisations have backed cybersecurity with increased investment, and for that, boards and executives expect a return on investment that—to a large extent—is expressed in confidence terms.

Just under two-thirds (61%) of organisations expect cybersecurity budgets to increase in 2022. This is higher in Singapore (70%) and Australia (66%) but lower in Japan where 48% anticipate budget increases and 49% expect to see stable budgets year-on-year. Across the board, very few expect cybersecurity budgets to decrease.

While external messaging on security is often couched in terms of the inevitability of being targeted or attacked, boards and the C-Suite are increasingly accountable to these risks and need to be confident enough to sign off on them. To do so, they rely here on the confidence and assurances of their IT security leaders and teams. But having that accountability may increasingly drive boards and executive committees to undertake their own, separate, independent assurance and due diligence on whether internal confidence around cybersecurity is justified or overstated.

The extent to which it is overstated may be difficult to determine given the technical nature of the security discipline. However, this paper offers some guidance on incongruities: Instances where leaders express confidence even though the patterns and practices of their actions undermine that stance.

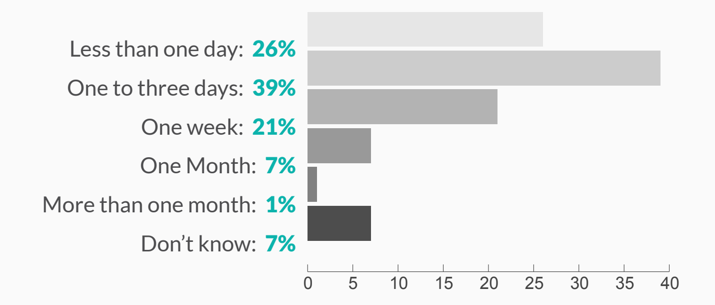
Knowledge and awareness of these incongruities is useful because it helps to understand where to ask additional questions and really test the robustness of the expressions of confidence that boards and executives are receiving.

Where to Ask Questions

A major part of this study identifies shortfalls in best-practice approaches to IT security that may not be adequately reflected in organisational confidence scores or in the very least undermine some of those scores.

To preface this, there are areas where security teams already perform well or where additional scrutiny may be unwarranted.

How long does it take your team to respond to a critical vulnerability, either apply the patch or implement the solution?



A positive in 2022 for most countries is that access controls and the potential for supply chain attacks appear to be well understood. Just over half (51%) of organisations allow third-party access to their networks and most of this cohort (86%) have considered the security aspects. This is highest in Singapore (96%) and Australia (87%) but lower in Japan (74%) where one in five haven't assessed the security implications of such arrangements.

In addition, most security teams are responsive to the discovery of vulnerabilities with 64% of teams able to enact mitigations or apply a patch (where available) within three days. However, that means 28% of instances take a week or more to mitigate against or patch. Breaking this down even further, 26% of teams respond in under a day, 39% take one-to-three days, 21% need a week, and 8% need a month or more. Benchmarking your own organisation's response times is important. However, just as important is understanding that addressing vulnerabilities does require some time. Dependencies and interdependencies between systems require considerable testing of patches and mitigations to ensure that they do not break more than they fix. Allowing security teams appropriate time to do their work is essential if unanticipated repercussions to production systems are to be avoided.

In other aspects of cybersecurity posture, some well-placed questions may be required to test expressions of confidence.

First, there isn't necessarily a consensus on where most resources should be trained: 24% of respondents focus most resources on detecting threats at the perimeter, 32% at detecting post-compromise activity on the network, and 42% give equal weight—and resources—to both. It's worth checking where your organisation sits and why. In saying that, reduced focus on perimeter security may be because most organisations, 81%, are confident they already have it covered.

Second, despite resourcing and investment levels, exactly half of cybersecurity incidents are caused by having an outdated security posture. On the surface, this looks high given the resource backing of security functions. The word *posture* is doing a lot of heavy lifting though, and it may be necessary to deconstruct overall security investment between people, process, and technology-based activities and outcomes.

Exactly half of cybersecurity incidents are caused by having an outdated security posture.

On the 'people' side, 79% of respondents have dedicated internal security personnel, and 71% of this group also have an external managed services partner to assist them. More likely than not, organisations have access to adequate personnel. Though the recruitment market remains challenging, not least due to salary costs, fully remote work models have expanded the available market for talent with 66% of respondents reporting the work-from-home trend as a positive. Forty percent plan to increase or recruit dedicated internal security staff in 2022, and the same number of respondents also intend to engage external resources.

On the flipside, 6% of organisations do not have a dedicated internal team or external team. This may seem a low figure, but if applied to all organisations it is a very large number that lack basic cybersecurity protection. Being a part of this cohort may be a cause for concern.

Most organisations have also achieved process maturity in cybersecurity. That is important where teams are a mix of internal and external people. The study also shows that 82% of respondents know their role in a response to a cyberattack or cyber emergency. Again, while it may be of concern to be outside of the main cohort, the likelihood is that process maturity is not contributing to an outdated security posture.

That largely leaves technology as a key cause for concern, and this is supported by the study. Unpatched devices and the use of outdated protocols are sapping the confidence of defenders. More than half (54%) of respondents last updated their cybersecurity infrastructure in 2020 or before and one-fifth of organisations have technology that has gone at least three years without being updated. Additionally, 76% state they are concerned about legacy systems being attacked.

Perhaps unsurprisingly, the three top priority areas for investment to improve posture in 2022 are technology related: 51% intend to invest in threat detection and response tools, 48% in improving security for hybrid and remote workforces, and 39% in improving hybrid and/or multi-cloud security.

Cyber Stats by Region

Australia
at a glance

43% are very or completely confident in their ability to handle cyber threats

19% say they can always identify and block ransomware

77% are confident they can prevent attackers from breaking into internal networks

69% are concerned about legacy systems being attacked

66% expect IT security budgets to increase in 2022

76% have a dedicated internal security team or staff

63% say it is difficult to find staff for the cybersecurity team

71% say remote work makes it easier to recruit cybersecurity staff

56% are confident staff can recognise social engineering attacks

64% say threat of legal action and fines promotes action by senior management in security decisions

49% have a network detection and response (NDR) solution

Singapore
at a glance

52% are very or completely confident in their ability to handle cyber threats

31% say they can always identify and block ransomware

88% are confident they can prevent attackers from breaking into internal networks

87% are concerned about legacy systems being attacked

70% expect IT security budgets to increase in 2022

87% have a dedicated internal security team or staff

66% say it is difficult to find staff for the cybersecurity team

77% say remote work makes it easier to recruit cybersecurity staff

63% are confident staff can recognise social engineering attacks

86% say threat of legal action and fines promotes action by senior management in security decisions

74% have a network detection and response (NDR) solution

Japan
at a glance

23% are very or completely confident in their ability to handle cyber threats

17% say they can always identify and block ransomware

76% are confident they can prevent attackers from breaking into internal networks

73% are concerned about legacy systems being attacked

48% expect IT security budgets to increase in 2022

75% have a dedicated internal security team or staff

24% say it is difficult to find staff for the cybersecurity team

56% say remote work makes it easier to recruit cybersecurity staff

35% are confident staff can recognise social engineering attacks

68% say threat of legal action and fines promotes action by senior management in security decisions

55% have a network detection and response (NDR) solution

A side note on the state of ransomware

The study tested the confidence, responsiveness, and fallout of ransomware incidents in Asia Pacific.

Ransomware attacks spiked in 2021 in both frequency and severity, and while there's some upheaval among operators, the attacks keep coming at a rate of thousands per day on a global basis.

Only 17% of respondents to this study said they experienced no ransomware incidents in the past five years.

- 48% had experienced 1-5 attacks
- 35% had experienced 6 or more

But 20% say that even if they were breached, they would limit who they told as much as possible. As discussed elsewhere in this report, the self-identified number of organisations that experienced an infection is conservative and likely to be much higher. That's particularly likely when you consider 58% of organisations experienced up to five ransomware incidents in the past five years and 42% have experienced six or more. On average, one ransomware attack gets through every year.

Only one in three organisations make a full and frank public disclosure of an incident. This often runs counter to the desire of security teams, where two-thirds are in favour of transparency. This indicates the potential for reputation or financial damage trumps more ethical considerations or social license to operate considerations.

This study also found:

- 45% of organisations have paid a ransom, despite a majority believing that paying increases the number of attacks
- 44% are covered by either specific or general insurance policies

Action Items for 2022

Network detection and response

42% intend to invest in network detection and response (NDR) systems this year, adding to the **34%** of organisations that already have such systems in place.

Social engineering strategy

47% of respondents plan to implement a social engineering strategy in 2022, building on the **21%** that already have one in place today and the **58%** that train staff to recognise social engineering cues.

Improved threat training and identification

46% plan to implement staff threat training, and the same proportion plan to improve the speed of threat identification.

Bring in more resources

40% of organisations plan to increase or recruit dedicated internal security staff. The same proportion intend to engage external managed security services in 2022.

Conclusion: The price of assurance

IT security leaders in the Asia Pacific aren't overconfident in their own, or their organisation's, ability to defend against the volume and sophistication of threats. But at the same time, too many express low confidence in their defensive capabilities. It's only a matter of time before boards and CEOs challenge these leaders' low confidence assessments and ask them to 'show cause' on why existing investment levels into cybersecurity should be maintained.

The answer to that question might be to look to the experiences of teams that lack appropriate backing. For the 20% of IT security leaders that have gone three years or more without system updates, there's a real urgency now for investment and action. For others, high levels of fear around the security implications of legacy environments and the very real threat of multiple breaches a year is a reminder of just how quickly cybersecurity postures can become outdated and vulnerable.

Put simply, there are things all businesses could do to boost confidence in their security postures and setups. While there are many possible solutions, one stands out to most IT security leaders: renewed investment in threat detection and response tools. A fresh round of investment and upgrades may be enough to raise the confidence of all parts of cyber defense to a more comfortable level of assurance.

About this study

The study was commissioned by ExtraHop and conducted by StollzNow Research in January 2022. It involved 100 IT decision makers in each of Australia, Singapore and Japan, at organisations of at least 50 people and operating in a broad range of vertical markets.

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud scale AI to help enterprises detect and respond to advanced threats—before they compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

ExtraHop

info@extrahop.com
www.extrahop.com