Left and Right of Boom in Cybersecurity 2022

Gauging Australian and New Zealand Cybersecurity Leaders' Positions on Preventative Security, Security Engineering and More

elastic

Corinium

Contents

Click below to navigate

Executive Summary

While many cybersecurity practices exist to respond quickly to intrusions, contain and eliminate threats and keep businesses up and running, the increasingly hostile threat landscape demands that organisations balance detection and response methods with preventative measures. That is, mitigating a potential threat before a system can be compromised.

This proactive security mindset can be described as a 'Left of Boom' approach to cybersecurity. The 'Left of Boom' concept, to borrow a term previously used in military circles, stipulates that CISOs must increasingly consider what measures they can move to the 'before incident' side of their security posture. 'Right of Boom', in this analogy, therefore, represents the set of strategies predominantly concerned with responding to and mitigating damage after a breach or attack has occurred.

In this report, we sought to explore the extent to which cybersecurity leaders in Australia and New Zealand are responding to threats and attacks with preventative, Left of Boom measures.

With a survey from 100 cybersecurity executives in the region, as well as commentary from cyber leaders, we will gain an understanding of the extent that such strategies are being put in place, what the components of those strategies are, and the challenges inherent in redirecting resources to make this shift.

We found that while many organisational cybersecurity practices do have a mix of preventative and responsive measures in place, there are cybersecurity leaders who skew their strategies, either in favour of incident detection and response, or in favour of preventative controls, rather than designing their strategies as a genuine mix.

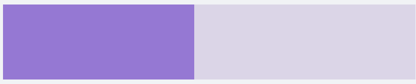
Our findings also suggest that ransomware remains one of the key threats cybersecurity leaders focus on when developing their strategies, along with phishing and customer data theft.

While many cybersecurity leaders have security engineering capabilities in place, there is also a large percentage that do not. However, building out more preventative security measures in the next 12 months is a priority for almost half of those surveyed.

Key Findings

46%

of respondents say investing in more preventative controls is a top priority for the next 12 months



14%

of respondents report having the minimal essential cybersecurity systems and practices in place

44%

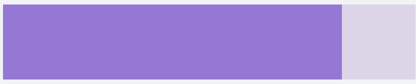
of surveyed cybersecurity leaders do not have an engineering capability within their department

33%

of respondents describe their security strategy as having a genuine mix of prevention and incident detection and response controls

82%

of surveyed cybersecurity leaders say they either plan to implement, are implementing or have implemented DevSecOps initiatives



Source: Corinium Intelligence, 2021

Methodology

This representative survey of 100 cybersecurity-focused leaders was conducted in February of 2022. Of these, 76% were from Australia and 24% were from New Zealand.

Respondents were selected from enterprises with at least 1000 employees and are responsible for their organisations' data strategy functions. They have job titles ranging from C-level to SVPs, VPs, directors, general managers, leads and heads of department.

Their enterprises operate in financial services or banking (24%), government (22%), insurance (5%), retail (5%), energy and utilities (5%) IT and/or telecommunications (5%) and healthcare (5%). The remaining 29% were selected from other industry verticals.

We asked respondents questions about their organisations' cybersecurity strategies and priorities, their technology use and constraints, challenges in procuring best-of-breed solutions, expected revenues and how they see their growth and performance over the next 12 months.

We then combined our findings with commentary from four industry experts to put these insights into context to capture a snapshot of the balance of preventative and responsive cybersecurity controls. ■

Contributors

Christoph Strizik
Chief Information
Security Officer
Origin Energy

Elrich Engel
Director Cyber Security
(CISO)
AMP

Bradley Busch
Chief Information
Security Officer
Tyro Payments

Jonathan Owen
Acting Chief Technology
Officer
ACT Government

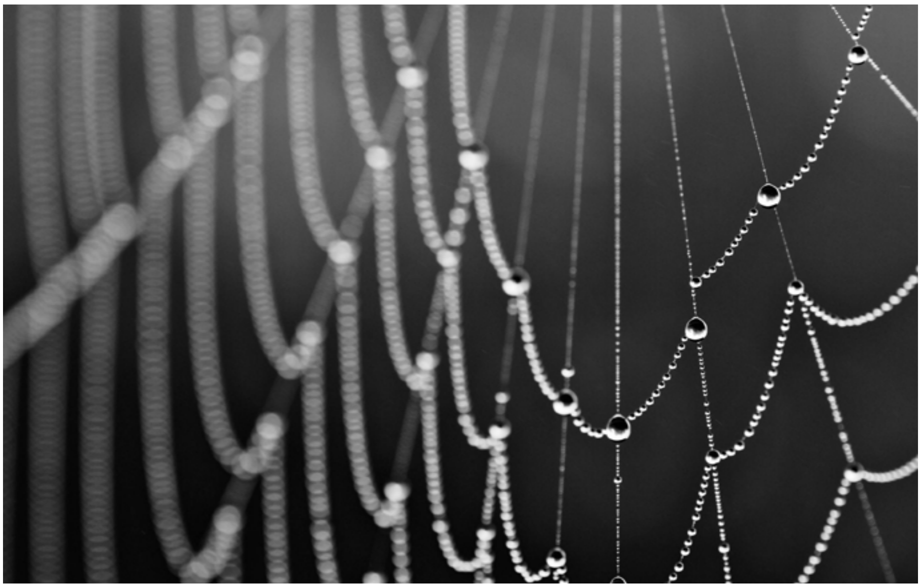
Asjad Athick
Senior Security
Specialist, Australia
and New Zealand
Elastic

Kathryn Green
Chief Information
Security Officer
Australian Radiation Protection
And Nuclear Safety Agency

Cyber Threats and Strategies in 2022

KEY FINDING:

Dealing with ransomware is a top strategy priority, strategies are mostly revised every two-to-three years



A fact of life that has been accepted among cybersecurity leaders and indeed the boardrooms of organisations globally is that while cyber-risk can be mitigated, it cannot entirely be eliminated.

For years now this understanding has meant that cybersecurity strategies have to be comprehensively devised to observe, protect and respond to threats as and when they occur. Whatever risk tolerance an organisation seeks to maintain, cybersecurity programs and solutions have sought to detect attacks and respond to protect business and infrastructure in as timely a fashion as possible.

With more digitisation occurring across business in Australia, New Zealand and the world, there is a recognised opportunity among security leaders to more deeply integrate security into solutions, services, applications and offerings.

A holistic defence posture can also include measures spanning people, processes and technology to prevent the occurrence of attacks from ever taking place. This preventative side of the cybersecurity approach comes in many forms that have existed and ventured in and out of fashion for decades, and for some time it has been characterised as "Left of Boom" cybersecurity.

The "Boom" in "Left of Boom" security refers of course to a cybersecurity incident. The Left or Right side of that event represents the actions taken to either prevent or manage said event.

To gain some insight on the goals of modern cybersecurity strategies in Australia and New Zealand, as well as how preventative and responsive elements factor into these strategies, we surveyed 100 cybersecurity leaders across the region. We asked about the threats they prioritise in their strategy, the preventative vs responsive aspects of their cyber programs, investment levels and more.

Our research is also supported by select commentary from expert cybersecurity leaders, like Origin Energy Chief Information Security Officer Christoph Strizik, who says when it comes to left or right of boom thinking, the cybersecurity industry's focus has fluctuated throughout the years.

"I've been around long enough to know that initially cybersecurity was all about preventative controls, that's where everyone invested. But then people started realising that regardless of how much money was spent on left of boom, incidents were still happening in their environments," he says.

"There was almost a resignation to the fact that breaches would occur, so there was a drive to get better at finding breaches and dealing with them, to the point where preventative controls started to get neglected.

"Now, I think we are back to the stage where organisations are taking up more preventative controls again. The impact of attacks is getting bigger, so cybersecurity leaders can't take a philosophy of only dealing with the incident when it comes.

"Strategies ebb and flow based on the thinking and threats in the cybersecurity landscape. Now, particularly with ransomware becoming really big, there is definitely more emphasis on preventative controls again."

Ransomware Remains a Focus for Cyber Resources

The cybersecurity threat landscape is vast. Because of this, cybersecurity leaders need to be prepared for myriad threat scenarios and remain vigilant against any potential attack vector.

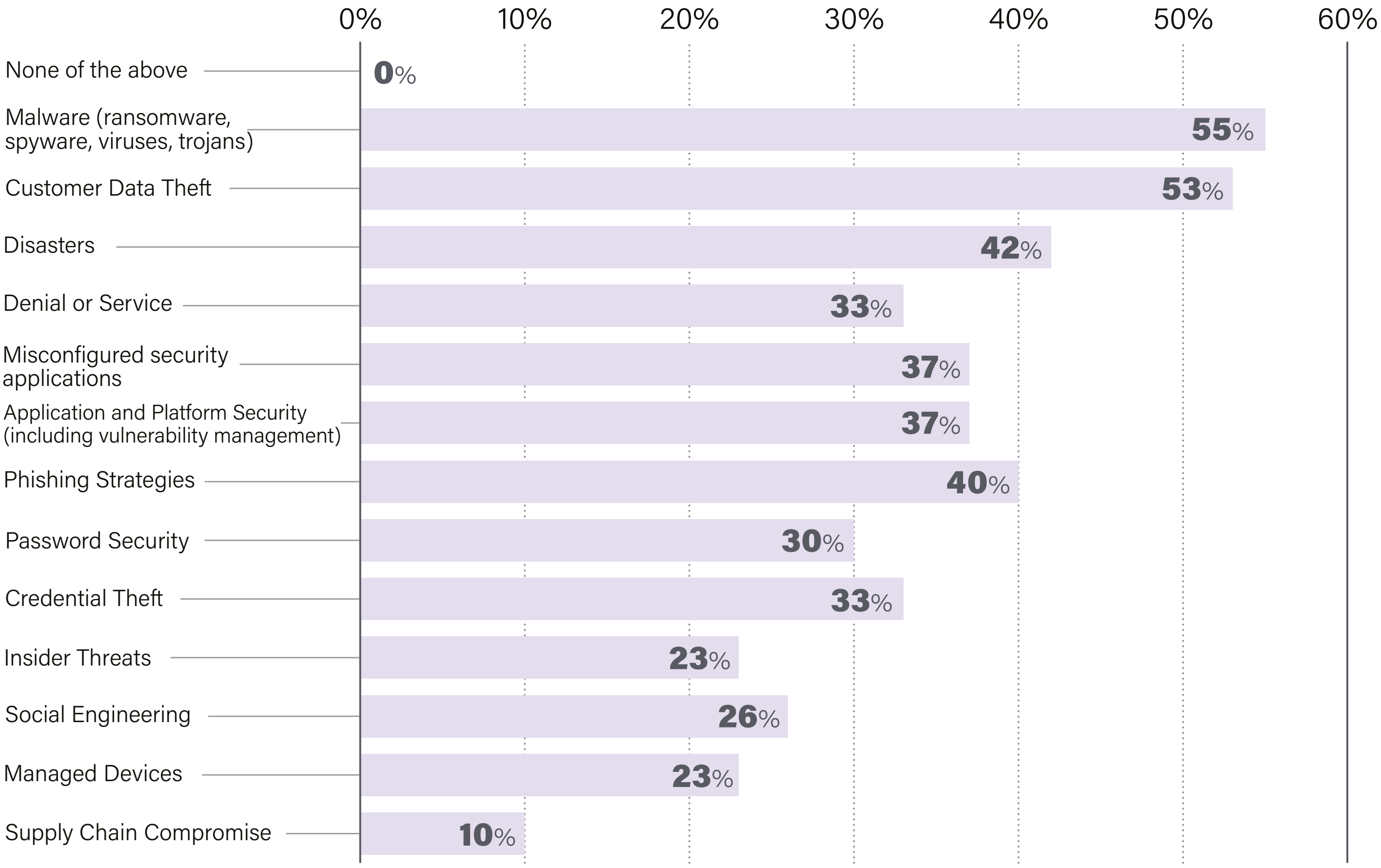
To contextualise some of the kinds of strategies our surveyed cybersecurity leaders indicated they were investing, we also sought to determine what threats they were most focused on.

Of the 100 cybersecurity leaders we surveyed, 55% listed Malware (ransomware, spyware, viruses and trojans) as the cybersecurity threat they were mainly focused on strategizing their cybersecurity posture around.

Following Malware, Customer Data Theft was seen as the second biggest threat in focus, with 53% of respondents highlighting it. Respondents were able to select more than one threat from our list.

The third most focused on threat by our 100 cyber leaders was Disasters, with 42% of respondents selecting it, followed by Phishing Strategies, which attracted votes from 40% of respondents.

What cybersecurity threats and practices are you mainly focused on strategizing your security posture around? *(Can select more than one)*



Ransomware and fraud were also represented as serious cybercrimes by the Australian Cyber Security Centre last year.

In its 2021 Annual Cyber Threat Report, the Australian Cyber Security Centre highlighted it had observed 67,500 cybercrime reports, an increase of 13 percent from the prior year. Fraud, online shopping scams and online banking scams were the top reported cybercrime types, while some 500 ransomware reports were also filed.

"While the number of ransomware-related cybercrime reports is a relatively small proportion of the total number of cybercrime reports, ransomware remains the most serious cybercrime threat due to its high financial impact and disruptive impacts to victims and the wider community," the ACSC reported.

Meeting Compliance and Roadmapping

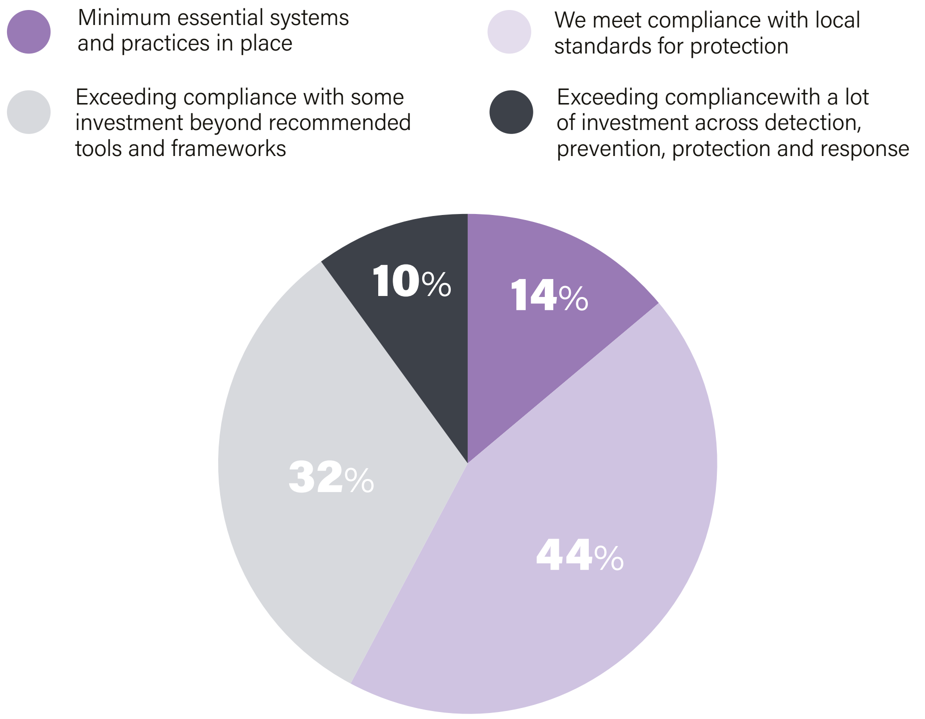
In working to protect their organisations from ransomware, data theft, phishing and disaster events, surveyed cybersecurity leaders in Australia and New Zealand by and large reported meeting or exceeding cybersecurity compliance.

When asked how they would describe the sophistication of their cybersecurity strategy, 44% of respondents answered that they meet compliance with local standards for protection.

Furthermore, 32% of respondents said they exceeded compliance with some investment beyond recommended tools and frameworks, while 10% said they exceeded compliance with a lot of investment across detection, prevention, protection and response.

A small but still concerning percent of respondents, 14%, described their strategies as having the minimum essential systems and practices in place.

How would you describe the sophistication of your security strategy?



> *"It used to be common to do strategies every three-to-five years, now it's more like 18-24 months... That's just because things change so quickly now."*
>
> **– Christoph Strizik**
> Chief Information Security Officer
> Origin Energy

We also asked cybersecurity leaders how often they revised their roadmaps and cybersecurity strategy, to understand how often they considered updating toolsets and practices to combat the threats they view as being most pertinent.

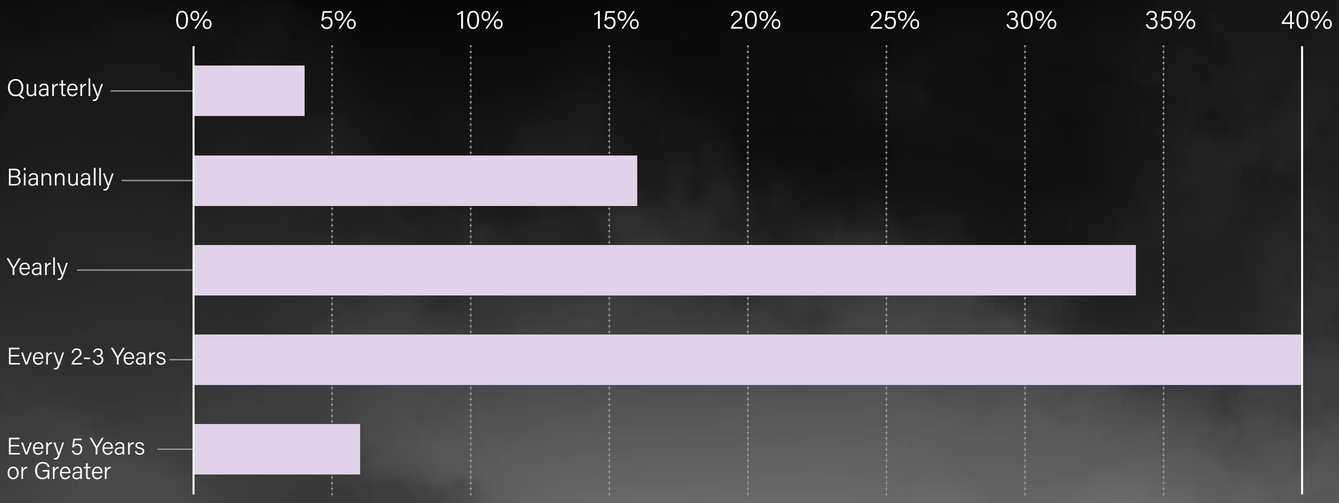
For 40% of respondents, their cybersecurity roadmap is revised every two-to-three years. However, 34% of surveyed Australian and New Zealand cybersecurity leaders report reviewing their strategy yearly. A 16% portion of the group reported reviewing their strategy biannually, while 4% reported they were revising the strategy every quarter.

A small portion of 6% of respondents reported revising and roadmapping their cybersecurity strategy every five years or more. Given the way events like COVID can disrupt ways of working in such a short timeframe, such a long cadence of strategy review should be quite rare in most industries.

"It used to be common to do strategies every three-to-five years, now it's more like 18-24 months," says Origin Energy's Christoph Strizik. "That's just because things change so quickly now."

With an established sense of how surveyed cybersecurity leaders rank the threats they are concerned with, the level to which they meet compliance and their strategy revision intervals, we are ready to take a closer look at how much of their reported strategies are preventative versus responsive." ■

How often do you revise and roadmap your cybersecurity strategy?



Left and Right of Boom

KEY FINDING:

Most cybersecurity leaders surveyed reported focused more on incident detection and response controls in their cybersecurity strategies

Cybersecurity strategies are varied in their approaches to dealing with the most prominent threats that security leaders observe in the market. Many focus on incident detection and response, or 'Right of Boom', while some put emphasis on outright prevention, or 'Left of Boom'.

Of course, there is not likely any organisation focusing solely on 'Left of Boom' or 'Right of Boom' approaches. As a requirement of the ASD's Essential Eight, cybersecurity teams are mixing these preventative and responsive cybersecurity controls to certain extents. For example, to achieve Essential Eight maturity level one, organisations must be scanning for vulnerabilities and patching regularly and also maintain backups of important data.

Asjad Athick, Senior Security Specialist for Elastic Australia and New Zealand, says it's important to get cybersecurity leaders thinking holistically to shore up preventative elements in cybersecurity strategies.

"Depending on what kind of organisation you are, your mix between preventative and responsive will be different," he says. "But I think everyone should have the ambition to shift more resources to 'left of boom', the question is how much are they able to do it?

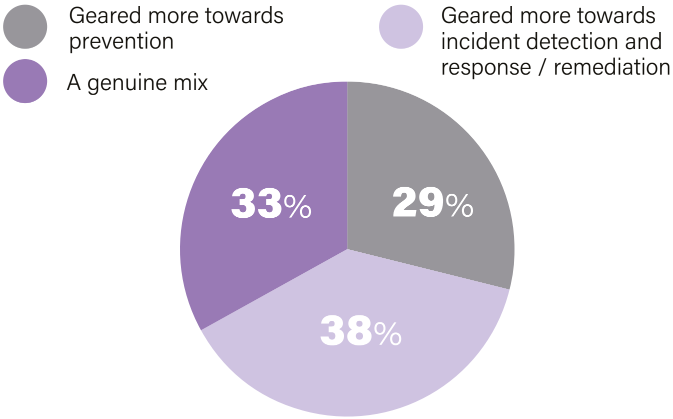
"It's one thing for the CISO to say, 'We want to improve preventative controls, and do more early', but being able to influence the business and become part of the business, which is really how the best preventative security comes about, that can be a challenge."

Our research suggests the extent to which organisations lean into preventative or responsive controls differs considerably. In our survey of 100 Australian and New Zealand cybersecurity leaders, we asked if they would describe their strategy as geared more toward prevention, more toward incident detection and response or a genuine mix.

The results suggest most organisations feel they either lean more toward incident detection and response or have a genuine mix, with 38% of respondents saying their security strategy is geared toward incident detection and response / remediation and 33% of respondents reporting a genuine mix between the two.

Just 29% of respondent reported that their security strategy was geared more toward prevention.

Would you describe your security strategy as...



> *"...It's one of our goals to limit our exposure to the need to respond, but obviously we still invest in response because we know breaches can occur and it can't be ignored."*
>
> **– Jonathan Owen**
> Acting Chief Technology Officer
> ACT Government

ACT Government Acting Chief Technology Officer Jonathan Owen says while he sees the mix of approaches as very important, the ACT Government's cyber strategy is focused on ensuring preventative measures are in place.

"There are several pillars in our cybersecurity strategy, and many of them hinge around building our people and capabilities in terms of both building skills along with our broader security culture. We significantly focus on becoming the least attractive target," he says.

"Of course, we continue to build out our operational capabilities, and having incident response measures in place, but we've spent a lot of time focusing on pre-breach preventative measures and we continue to do so. It's one of our goals to limit our exposure to the need to respond, but obviously we still invest in response because we know breaches can occur and it can't be ignored.

"But similar to the system development lifecycle, the earlier you can remediate security issues, the cheaper the fix will be, so the more that we can bring controls to the prevention side, the better."

At the Australian Radiation Protection and Nuclear Safety Agency, Chief Information Security Officer Kathryn Green says preventative controls are also a focus, and she too observes across industry the need for work to progress on both approaches.

"Preventative cybersecurity is a major part of our strategy and it takes up the lion's share of my team's time and our operational budget," she says.

"However, the responsive side of security also remains highly relevant. I do think a continuing focus remains on how a significant cybersecurity event is managed and that's where scenario planning is very useful. However, it can be quite theoretical because we really don't know what the incident will be, nor the impact it could have and therefore need to be nimble and prepared to respond to any eventuality.

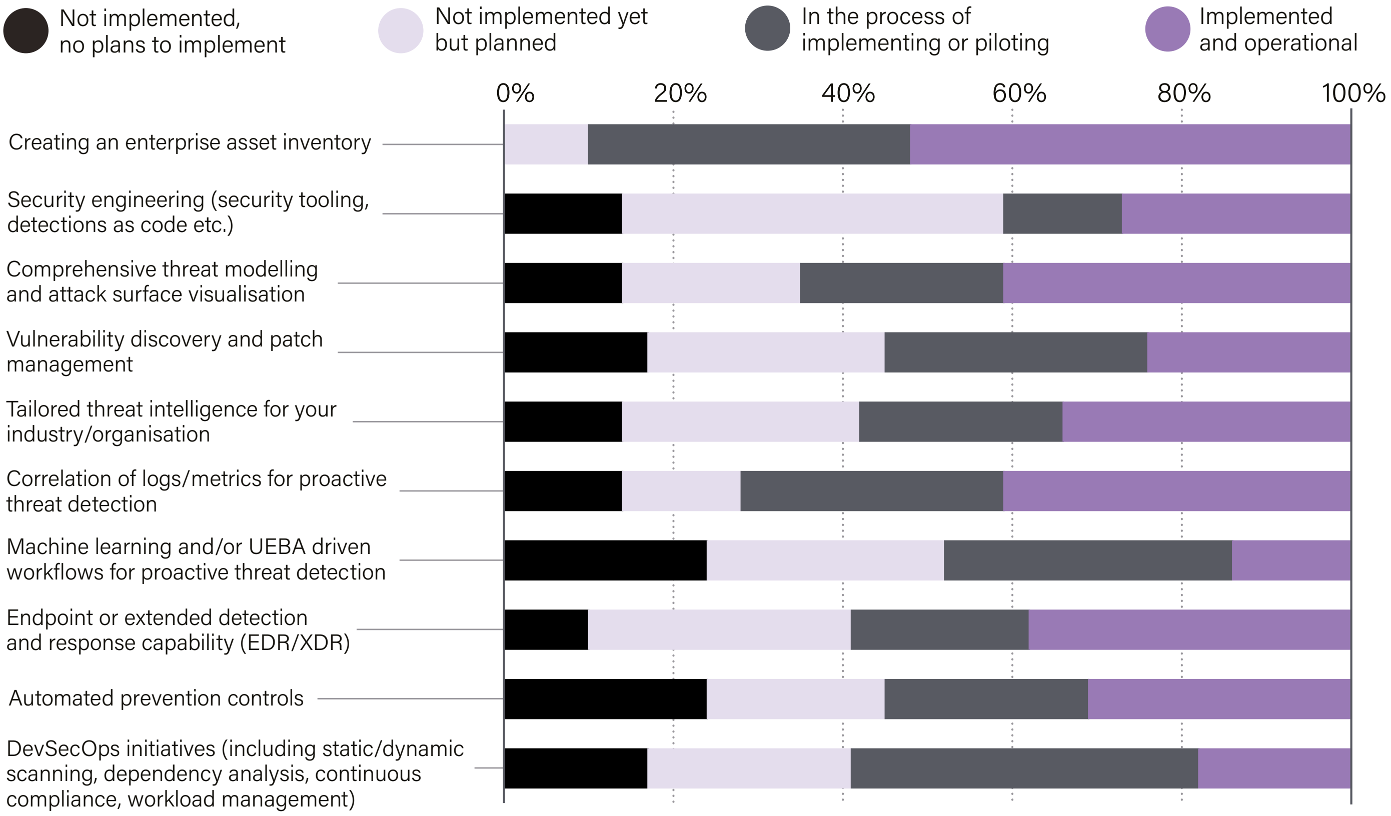
"In cybersecurity today, there is a focus on training your executive and the board on how to manage threats and incidents, and on our enabling both engineering staff and operational staff to manage events as they arise and unfold."

Preventative Measures in Focus

We also asked our survey respondents to break down the degree to which they have implemented a range of measures typically considered left and right of boom, or preventative vs responsive. We accept that there are many practices that could be filed into either of these categories and that they are not necessarily definitive.

To highlight the measures that are implemented most, we split up the respondents based on whether they described their strategies as being geared more toward prevention or more toward incident response and compared some of their responses.

To what degree have you implemented these preventative measures into your cybersecurity strategy?
(Prevention-focused cybersecurity leaders)



Looking first at the preventative measures listed, as shown in the chart above, surveyed cybersecurity leaders that indicated their strategies were geared more toward prevention reported, 'Creating an Enterprise Asset Inventory' was the most implemented and operational, at 51%. However, this measure was also reportedly implemented by 55% of response-focused cyber leaders.

Interestingly, just 25% of prevention-focused cyber leaders reported having implemented 'Vulnerability Discovery and Patch Management' measures.

Meanwhile, 'Comprehensive Threat Modelling and Attack Surface Visualisation' has been implemented by 41% of surveyed prevention-focused cybersecurity leaders, and by about 31% of response-focused leaders.

'Correlation of Logs/Metrics for Proactive Threat Detection' has reportedly been implemented by 41% of prevention-focused survey respondents. Conversely, this measure had been implemented by just 21% of incident response-leaning survey participants.

About 59% of preventative cybersecurity leaders surveyed reported that DevSecOps initiatives had either been implemented or were in the process of implementation. This is compared to 50% from the incident response-focused group.

Responsive Measures in Focus

For cybersecurity leaders that indicated their strategies were geared more toward incident detection and response / remediation, 'Intrusion Detection and Alerting' was the measure most had indicated having implemented and operational, at 55%.

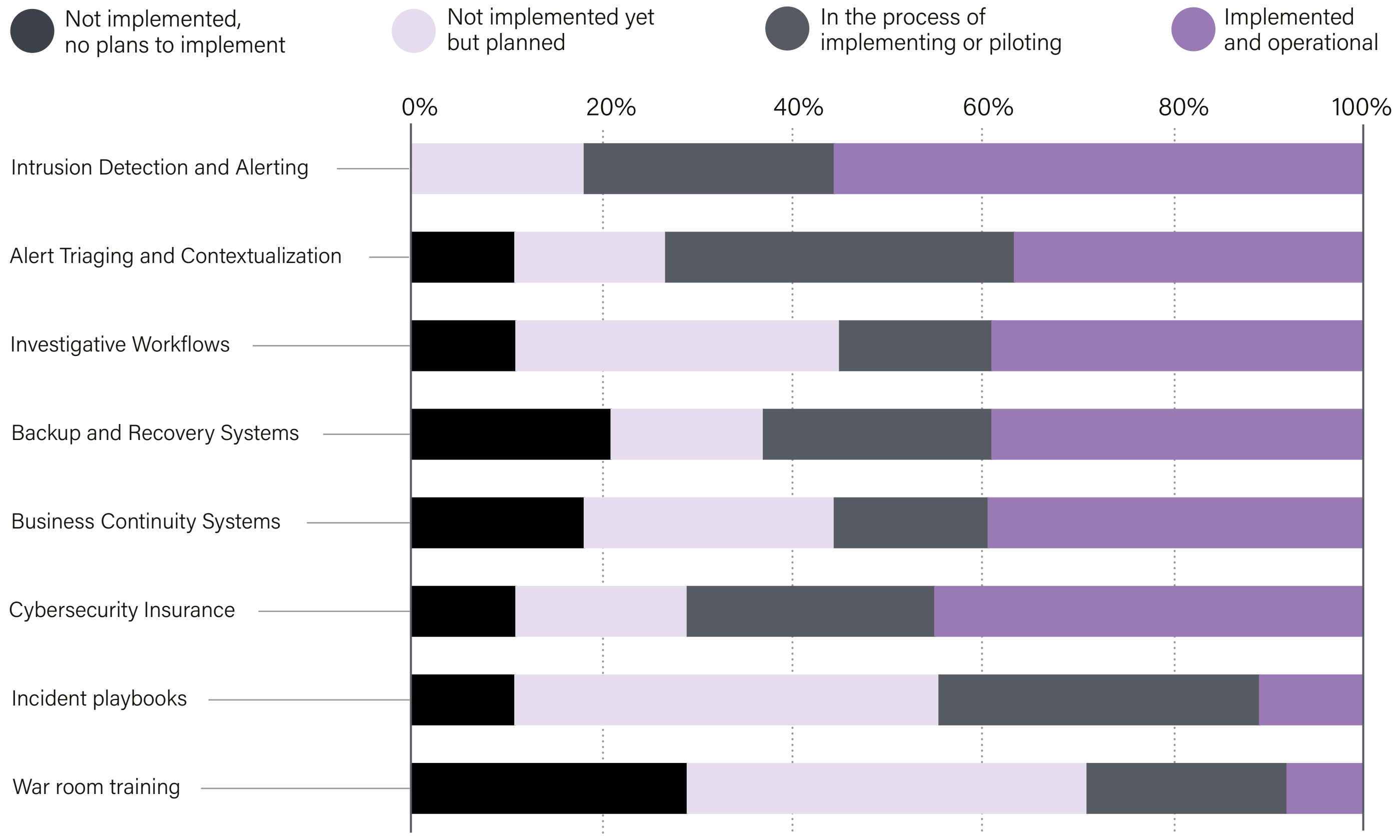
'Cybersecurity Insurance' was another responsive measure that was highly implemented by this group, with 44% of surveyed response-focused cybersecurity leaders having it implemented. However, 52% of the preventative-focused cyber leaders had also reported implementing this measure.

Interestingly, while 'Backup and Recovery Systems' were reported by 39% of response-focused cyber leaders as being implemented and operational, 21% of response-focused cyber leaders also said these systems were not implemented and they had no plans to implement them.

'Alert Triaging and Contextualization' was either in the process of implementation or already implemented by about 74% of response-focused cybersecurity leaders, compared to 62% in prevention-focused survey participants.

To what degree have you implemented these responsive measures into your cybersecurity strategy?

(Response-focused cybersecurity leaders)



Security Engineering Complements Preventative Movement

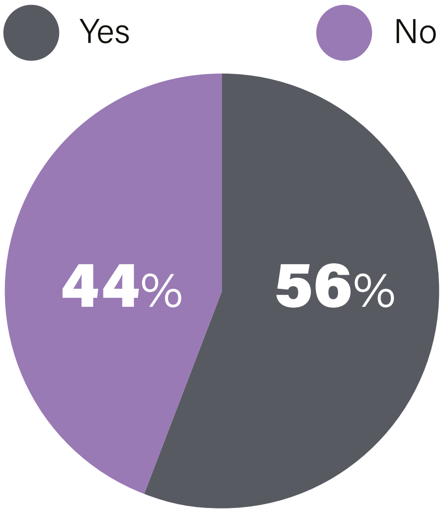
One of the major ways organisations across Australia and New Zealand are improving the amount of security control they have on their internally developed systems and processes is through security engineering.

Security engineering refers to the process of implementing security controls as an integral or coded part of an organisation's systems. It concerns designing and building systems and applications from the ground up with as much emphasis on security as there is on capability and useability.

In being closely connected with the design and build process, security engineers can facilitate the use of secure code and control what aspects of programs are exposed online. By reducing the vulnerability of systems, rather than patching them when discovered, security engineering offers strong preventive security benefits.

In our survey of 100 Australian and New Zealand cybersecurity leaders, when asked if their department included a security engineering capacity, 56% responded 'Yes' and 44% responded 'No'.

Does your department include a security engineering capacity?



Elastic Senior Security Specialist for ANZ Asjad Athick says as more businesses become digital businesses, security teams need to have a key role in enabling embedded foundational security, which will serve to be preventative.

"As they become increasingly digital, companies are in part becoming engineering-based businesses, so security must work to enable these businesses to deliver. Historically, you would have had centralised security, and the business would come to the security team with a request or question. In a modern security team in 2022, security needs to be distributed as part of the actual business," he says.

"That's a construct in which preventative security works. Because you are embedding security people across the business and security decisions are made sooner, much earlier in the process of deployment."

At Origin Energy, CISO Christoph Strizik says security professionals join various digital business teams for DevSecOps workflows for creating new products and services.

"We inject the 'Sec' into the teams that are developing and operating digital products, they have a dotted line back to us and this is a good model. It's moving away from a model where different silos of teams try to achieve an outcome," he says.

"Bringing development, security and operations into a team to own a project end-to-end for a business product or service is a very powerful way to ensure the quality of the product in its own right but also its security posture."

ACT Government's Jonathan Owen says the Territory government is continuing to increase the capability position of security engineering team.

"We traditionally had engineering and operations together as one team, with business-as-usual (BAU) in addition to engineering. We've just commenced the process to split those functions out more separately," he says.

"We find that all the time spent on BAU doesn't facilitate the engineering and continual improvement aspects as much as we would like, especially when we aim to embed security prevention controls into services. We build from the ground up and really concentrate on that 'Left of Boom' side.

"So, we've made the conscious decision to really enhance more of our engineering capability and dedicate engineering people to make those improvements up front."

At ARPANSA, CISO Kathryn Green says the agency's smaller size enables her team to closely understand the structure and purpose of the agency, and how security and technology can help it achieve its goals.

"Even though working in a small agency has its challenges, there's also immense benefit because we can do fit-for-purpose design and delivery and integrate security from the ground up. Our security engineering and operations teams work closely with the design and delivery team and with the business," she says.

With security engineering capabilities absent from 44% of our surveyed cybersecurity leaders' departments, it suggests there is still work to be done for organisations to add more embedded, preventative security controls to their defensive position.

> *"...Historically, you would have had centralised security, and the business would come to the security team with a request or question. In a modern security team in 2022, security needs to be distributed as part of the actual business."*
>
> – **Asjad Athick**, Senior Security Specialist, ANZ, **Elastic**

Cautioning Sprawl and Aiming for Balance

As noted earlier in this chapter, only a third of all surveyed cybersecurity leaders described their strategies as being 'A genuine mix' of preventative and responsive controls. Such a skew may suggest that cybersecurity practices are limiting their potential resilience.

To further understand the degree to which cybersecurity leaders are embracing preventative, Left of Boom, controls, we asked our survey respondents how confident they were that deploying known measures for preventing cyber incidents would stop attacks.

While 74% said they were 'Somewhat Confident', 21% said they were somewhat sceptical. Just 5% reported being highly confident.

Part of the reason for this may be to do with assumptions around what amounts to preventative security in 2022, which has traditionally been endpoint protection, firewalls and very narrow controls targeted at specific threats that do not suit complex manageable cybersecurity strategies, according to Tyro Payments CISO Bradley Busch.

"In the case of the emergence of ransomware, the market tends to respond with many very deeply focused, narrow controls from brand new vendors; for example: tools to detect bulk file encryption and kill the process responsible. This leads to many CTOs and CISOs consolidating their portfolios, wanting to rely on existing vendor solutions to plug the gap rather than chasing after the latest idea and having yet another tool to rollout." he says.

"Cybersecurity is a complex and dynamic system and cybersecurity leaders have to be concerned with the tension of defence in-depth. We need to be able to enable the business and prevent threat access across multiple layers. You'll hear the Swiss cheese model discussed, to successfully prevent a threat the holes in the cheese slices should never line up top to bottom.

"Defence-in-depth doesn't mean having multiple vendors in the line of duty, it means a variety of defensive controls that are deployed from the outside to the inside.

"Many of us have grown up defending the castle by building high walls, using email security and firewalls. But as infrastructure goes to the cloud, there has been the shift to capturing and corralling attackers once they are detected and kicking them out, and doing that in a safe and repeatable way."

With a stern caution on applying narrow controls for prevention, Busch does advocate a balanced approach of preventative and responsive security if well integrated.

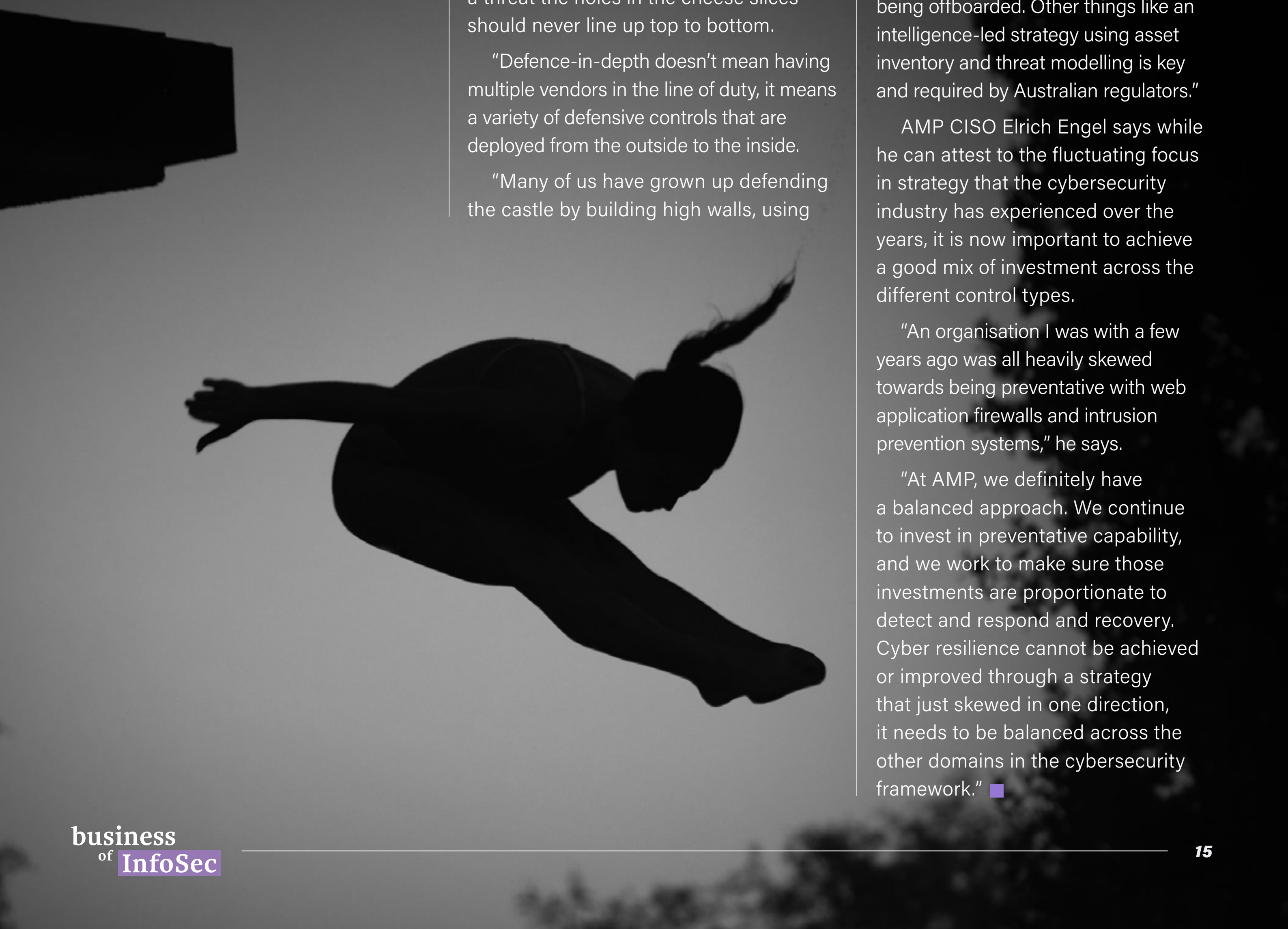
"We don't so much have our own castle walls to defend now. Modern systems are hosted in data centres and the cloud. The physical perimeter has shifted to a logical perimeter. Identity and access control has become the new perimeter," he says.

"So our 'Left of Boom' capability here is to uplift the way we govern someone being onboarded, managed during their operational lifecycle and being offboarded. Other things like an intelligence-led strategy using asset inventory and threat modelling is key and required by Australian regulators."

AMP CISO Elrich Engel says while he can attest to the fluctuating focus in strategy that the cybersecurity industry has experienced over the years, it is now important to achieve a good mix of investment across the different control types.

"An organisation I was with a few years ago was all heavily skewed towards being preventative with web application firewalls and intrusion prevention systems," he says.

"At AMP, we definitely have a balanced approach. We continue to invest in preventative capability, and we work to make sure those investments are proportionate to detect and respond and recovery. Cyber resilience cannot be achieved or improved through a strategy that just skewed in one direction, it needs to be balanced across the other domains in the cybersecurity framework."

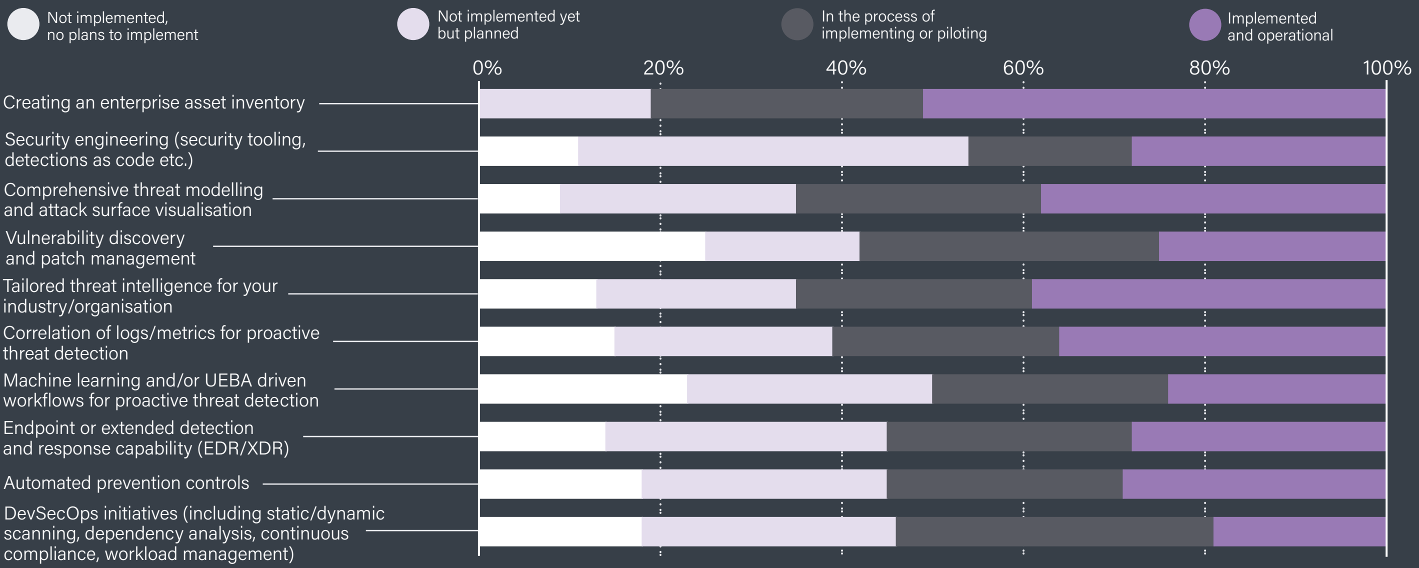


Prevention and Response Control Uptake

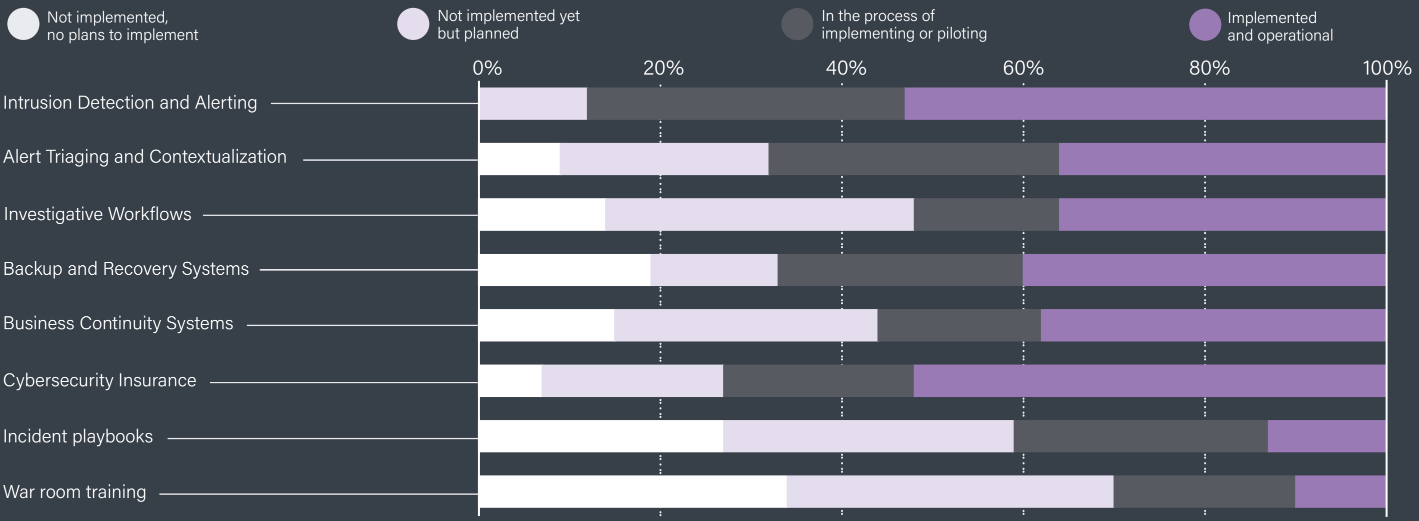
KEY FINDING:

Asset inventories, threat modelling and intelligence among top preventative controls

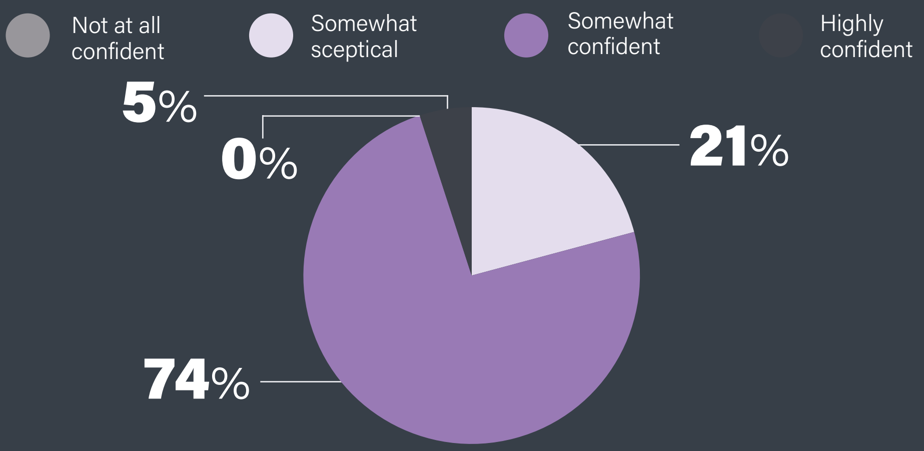
To what degree have you implemented these preventative measures into your cyber strategy? *(All respondents)*



To what extent have you implemented these responsive measures into your cybersecurity strategy? *(All respondents)*



How confident are you that deploying currently known measures and solutions focused on preventing incidents will actually thwart cyber attacks?

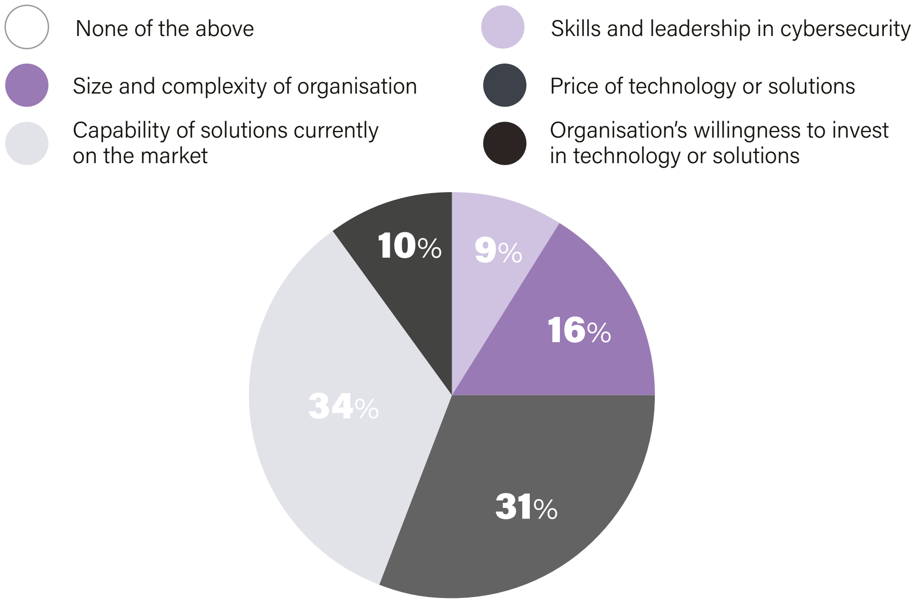


Barriers to Preventive Capabilities and Security

KEY FINDING:

Market offerings and price dissuade some cyber security leaders from preventative approach

Which of the following do you see as the biggest barrier to realising cyber incident prevention capabilities?



We asked our 100 Australian and New Zealand cybersecurity leaders what they saw as the biggest barrier in realising cyber incident prevention capabilities.

Available responses included, essentially: skills, size of organisation, price of solutions, capability of solutions and organisational willingness to invest.

Interestingly, 34% of respondents identified 'capability of solutions currently on the market' as the biggest barrier to realising incident prevention, while 31% cited 'price of technology or solutions' as the biggest barrier.

A 16% portion of the group responded that 'size and complexity of organisation was the biggest prevention capability barrier, and 10% said it was the 'organisation's willingness to invest in technology or solutions'. Just 9% noted 'skills and leadership in cybersecurity'.

The response breakdown on this question suggests about 65% of cybersecurity leaders surveyed feel that current market offerings cannot solve preventative security gaps or are too expensive.

While skills may not be thought of as a large barrier to the preventative security effort per se, this remains an area that security departments find to be an ongoing challenge.

"I think for many cybersecurity leaders our biggest concern at the moment is firstly staff retention," says AMP's Elrich Engel. "The market is super buoyant at the moment. Staff retention and flight risk are some of the big challenges.

"I also think ensuring the team remains suitably skilled and equipped to deal with threats as and when they evolve. We also need to be able to set ourselves up to allow the business to take advantage of innovative business models and growth."

ACT Government's Jonathan Owen adds that alongside skills, influencing change and the improvement in security programs requires the support and understanding of both decision makers and staff across the wider organisation, which can be a challenge many organisations find themselves up against.

"Uplifting the security culture is not easy," he says. "But it requires embedding security into BAU thinking and processes. Security by design is something we focus on, but it isn't easy and does cost money and time. Particularly during COVID, the demand to roll things out in very short time frames makes these goals challenging."

Thinking Preventatively

We've looked at the position cybersecurity professionals in Australia and New Zealand take on certain preventative and responsive controls, as well as the uptake of security engineering and its value as a preventative control measure.

"For organisations that do not yet have security engineering capabilities or a balanced set of preventative and responsive cybersecurity controls, or who feel the market may not currently cater to preventative security goals, there are still some relevant and accessible 'Left of Boom' processes that cybersecurity leaders can turn on for their business.

I think organisations that have adopted modern workplace technologies and a somewhat modern security stack, probably have the things they need to start strengthening their preventative controls," says Origin Energy's Christoph Strizik.

"It's just a matter of applying tools consistently on the assets that matter. A good example is switching on multi-factor authentication. The moment you do that you can stop about 99% of account takeover attacks.

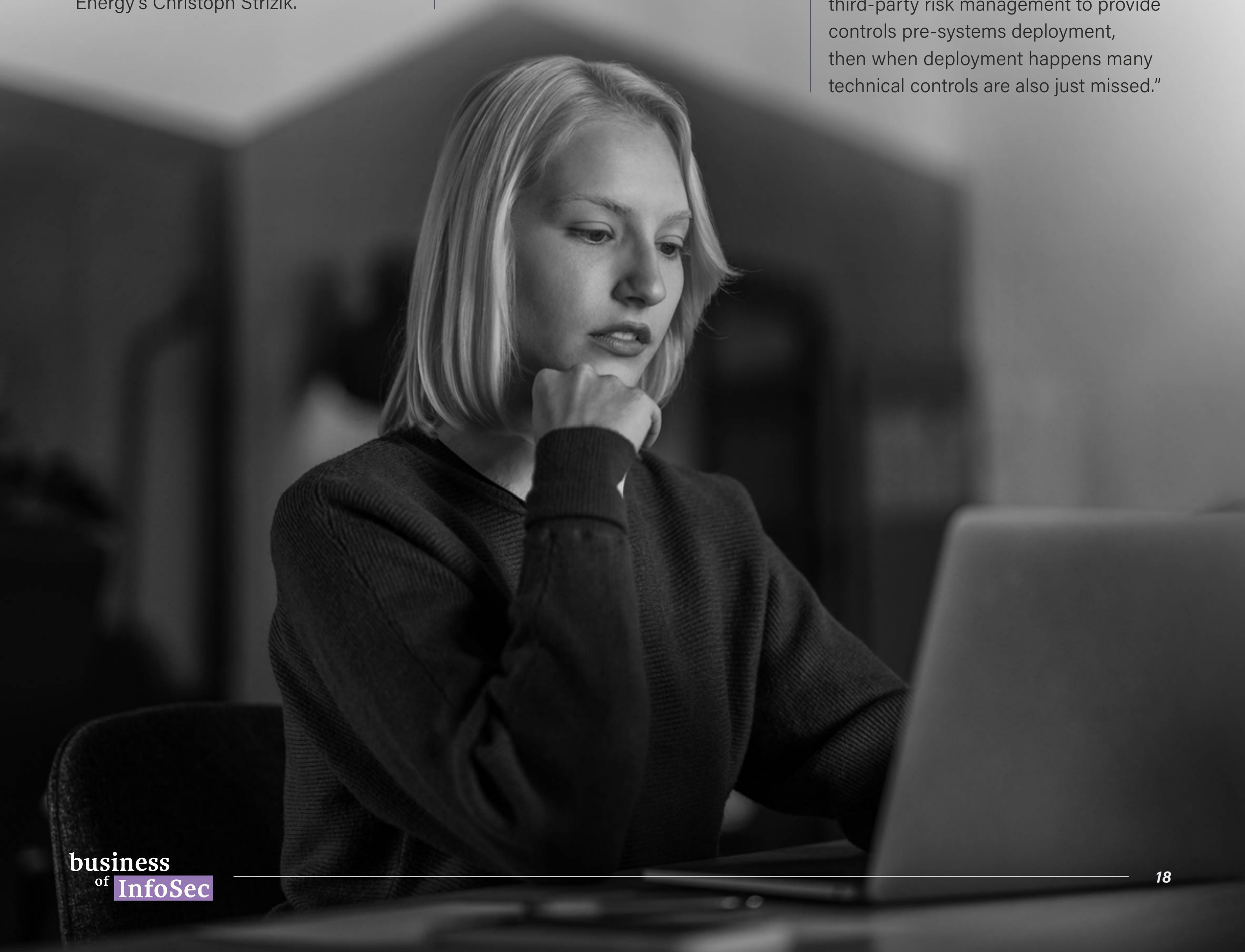
"You can also put security guardrails in place. One of the big benefits of the cloud and digital space, but which also creates some risk, is that you can automate and do so much at scale. Humans make mistakes though, so if, for example, someone automates something at scale and exposes customer data to the internet, you've got a huge problem.

"What we can also do using automation in the cloud is detect a change happening, if somebody runs code or an operation that creates risk, we can revert the code and that risk, and it's fully automated. That to me is still 'Left of Boom' because you intervene so quickly that nothing actually happens."

Aside from technology, ACT Government's Jonathan Owen says educating, training and communicating with staff across an organisation to normalise security thinking also counts toward preventative security.

"Building that culture enables people to want security as part of their technology and processes" he says.

"If you don't have a board-level member understanding that they need to do security by design, including engaging security on contracts and third-party risk management to provide controls pre-systems deployment, then when deployment happens many technical controls are also just missed."



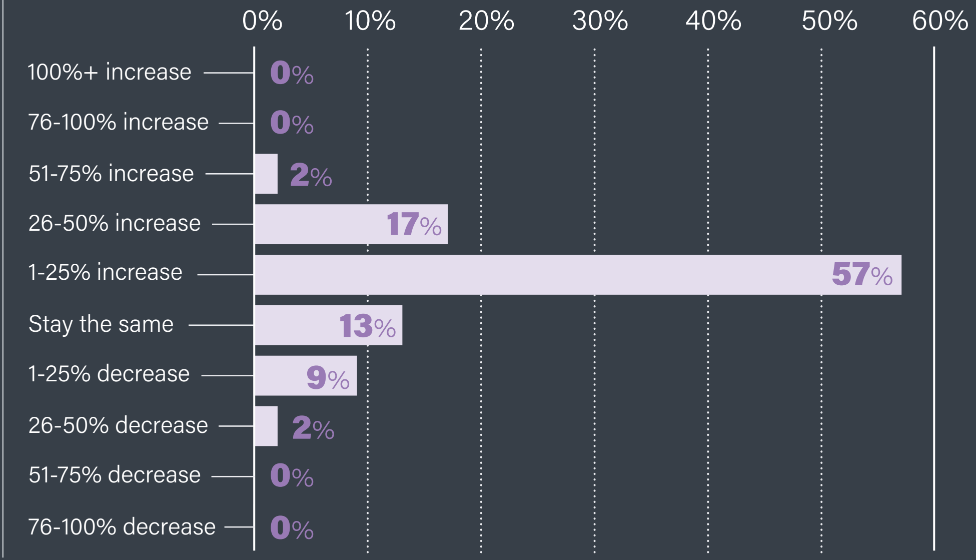
Looking Forward

To round out our survey of 100 cybersecurity leaders across Australia and New Zealand we asked some questions about budget and staffing expectations over the next year.

When asked how they expected their department's staff numbers to change over the next 12 months, 57% of those surveyed said they expected a 1-25% increase in headcount. Some 17% expect a 26-50% increase and 2% expect an increase between 51-75%.

The total number of cybersecurity leaders expecting their staff numbers to reduce was just 11%, with 9% expecting a 1-25% decrease and 2% expecting a 26-50% decrease. 13% expect no change.

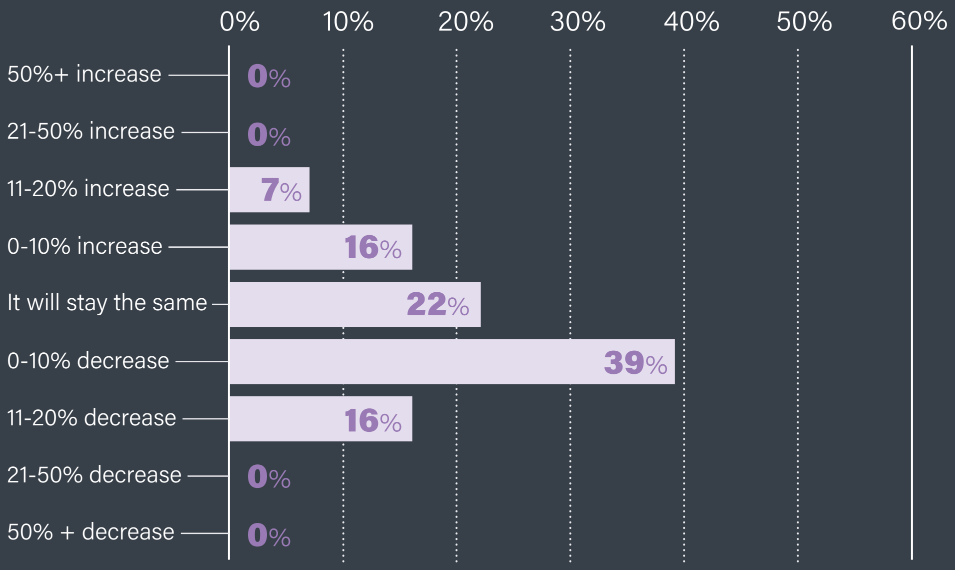
How do you expect your department's staff numbers to change over the next 12 months?



Concerning financials, we also asked survey respondents how they expected their department's budget to change over the next 12 months.

The results suggest a little less confidence among security leaders compared to the staffing question, with 55% expecting budget cuts of up to 20%. Just 16% expect up to a 10% increase in budget, with 7% expecting a budget increase of between 11-20%. The portion of respondents not expecting any change was 22%.

How do you expect your department's budget to change over the next 12 months?



Lastly, we asked cybersecurity leaders what they consider to be their top priorities within their organisations over the next 12 months. Respondents were able to select more than one answer.

Perhaps not surprisingly given some of the discussion in this chapter regarding staff skills and retention challenges, 56% of those surveyed selected 'Building a high-performance team' as a top priority.

Just under half of all respondents, at 47%, indicated that working on a 'major cybersecurity modernisation project' was also a top priority.

'Investing in more preventative controls' was another top answer, with 46% of respondents indicating it as a top priority, as was 'Increasing investment in technology for controls', which was cited by 44% of respondents as a priority.

At ARPANSA, CISO Kathryn Green says one of her priorities is to call for more IT providers and vendors to integrate security with their solutions.

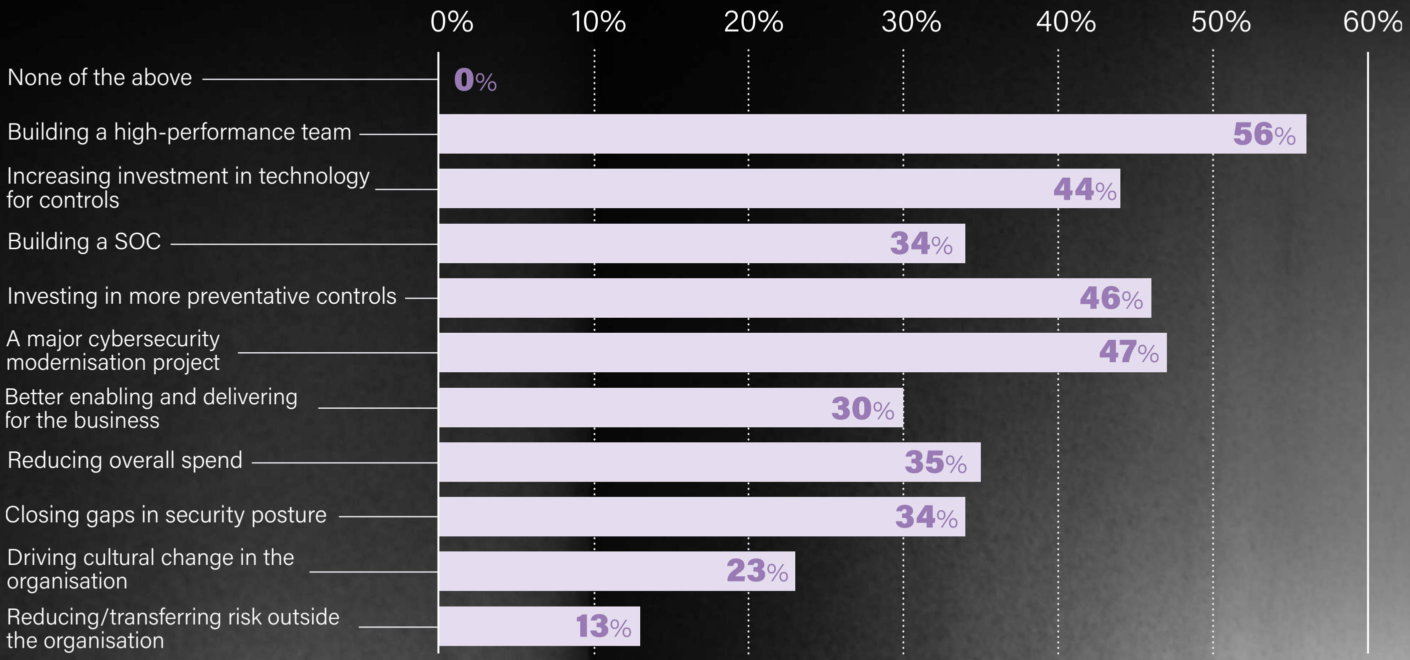
"It's calling for software quality and security by default," she says. "We are looking at securing our systems by insisting that new systems include the highest cybersecurity elements, that is not always part of the package because it's not always part of the financial imperative when procuring, it's often seen as an additional element.

"When a system has been pitched to business owners, they talk about the suitability for its delivery, for its function and requirements. We then say, 'Well, you must realise we have cybersecurity requirements as well'.

"That's been a conversation we've had over the years, and vendors are happy to talk about it, but we have certainly been more insistent in the past 2-3 years that this can't just be an add-on, it's incredibly important and should be put front and centre.

"An example of this being that we insist on MFA for any external portals or systems that will go to external customers, and often when we talk to vendors about MFA, they'll say, 'You're welcome to add an MFA solution on top of this'. I believe they need to be building that into their systems by default." ■

What do you consider your top priorities as a cybersecurity leader within your organisation in the next 12 months? *(Can select more than one)*



Conclusion

Cybersecurity leaders are working hard in high-risk times. The digital evolution of businesses and increasing threat of cyber attacks like ransomware provides plenty of programs of work and strategising for professionals in this space to tackle and manage.

In this report we've looked at the role preventative security controls play in modern cybersecurity strategies, and how they might be thought of as beneficial areas of investment along side responsive controls and digitally transforming business and security departments.

Strategic positioning and focus when it comes to preventative security is mixed, perhaps unsurprisingly given the reality of security breaches and the way preventative security used to be achieved. However, with security engineering, DevSecOps and security thinking around people, process and technology moving forward, we see new opportunities for preventative securities to round out holistic modern strategies. ■

About Elastic

Elastic is the company behind the Elastic Stack — that's Elasticsearch, Kibana, Beats, and Logstash. The Elastic Security solution equips teams to prevent, detect, and respond to security threats with speed and at scale.

Elastic brings SIEM, Endpoint, and Cloud Security controls to a single unified platform to help you prevent security breaches by shifting left. Modernise your security operations by eliminating blind spots, searching across petabytes of data, and arming your analysts to hunt for and remediate threats to your organisation.

elastic

Find out more: www.elastic.co/security

Get in touch: www.elastic.co/contact

About the Editor

Michael Jenkin is an editor and journalist with more than a decade of experience producing content across broadcast, print and digital media. He specialises in enterprise IT and technology writing.

At Corinium, Michael develops content to inform and support data and analytics and information security executives.

To share your data story or enquire about appearing in a Corinium report, blog post or digital event, contact him directly at michael.jenkin@coriniumgroup.com

Discover More Essential Information Security Insights

As anyone who has attended our global conferences or events will know, our 300,000-strong network of information security leaders boasts many of the most forward-thinking minds in the industry.

Our new content hub, **Business of InfoSec**, brings those same essential insights direct to you and is packed with exclusive research, video podcasts, in-depth articles, interviews, and reports. Discover how other information security leaders are tackling the challenges they face today while maintaining the confidentiality, integrity, and availability of their organization's data.

For a limited time, subscribing to the **Business of InfoSec** is free. So, make sure to subscribe today for complimentary access to exclusive insights you just can't find anywhere else.

SUBSCRIBE NOW

Corinium

Partner with Business of InfoSec by Corinium

We'll develop industry benchmarking research, special reports, editorial content, online events and virtual summits to establish your brand as an industry thought leader.

FIND OUT MORE HERE

Supply Chain Security Trends, Australia 2022

Australian cybersecurity leaders discuss challenges in supply chain cybersecurity management and consider best practices for security teams

RAPID7

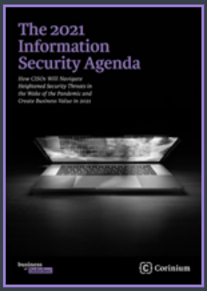
Corinium

Vulnerability Management Trends in Australian Government

The shifts Australian government cybersecurity leaders are seeing and responding to as the need for effective patching increases

Qualys.

Corinium



The 2021 Information Security Agenda

How CISOs Will Navigate Heightened Security Threats in the Wake of the Pandemic and Create Business Value in 2021

business of InfoSec

Corinium

Discover Corinium Intelligence

Corinium is the world's largest business community of more than 700,000 data, analytics, customer experience and digital transformation leaders.

We're excited by the incredible pace of innovation and disruption in today's digital landscape. That's why we produce quality content, webinars and events to connect our audience with what's next and help them lead their organisations into this new paradigm.

Find out more: **www.coriniumintelligence.com**

Connect with Corinium

- Join us at our **events**
- Visit our **blog**
- Read our **reports**
- Follow us on **LinkedIn**
- Like us on **Facebook**
- Find us on **Spotify**
- Find us on **YouTube**
- Find us on **iTunes**