CISO Lens

Benchmark 2019

Produced by CISO Lens
www.cisolens.com
Published: December 2019

In partnership with

AustCyber
Australian Cyber Security Growth Network

Table of contents

Introduction

In June 2019, CISO Lens conducted a benchmark exercise among 58 of the leading cyber security executives across Australia and New Zealand. This benchmark survey asked questions in seven core areas: demographics, security budget, the role of the Chief Information Security Officer (CISO), team size, security strategy, security operations, and attitudes and opinions on strategic vendors.

This is the second year that CISO Lens has conducted this benchmark exercise. The first benchmark in 2018 was a pilot study and the questions asked of the participants were subsequently revised for the 2019 benchmark.

This report is published to support two core objectives of CISO Lens, to improve:

1. Cyber security governance within organisations, and
2. Cyber resilience across the Australian and New Zealand economies.

Cyber security governance within organisations

An ongoing challenge for all organisations is to understand whether they are doing and spending enough, not enough, or too much on cyber security.

This benchmark enables the participating cyber security executives to assess how their organisation compares to their peers. **This information enables evidence-based decision making around strategy and resource allocation.** The goal is a commensurate response to the cyber risks these organisations face, and part of the challenge of presenting a commensurate response is the need for continual evolution.

Cyber resilience across the Australian and New Zealand economies

Given the interdependencies between organisations, the whole ecosystem must be addressed. It is not enough for one organisation to be world-class, while their peers and suppliers hang back and, inevitably, fall behind.

Consequently, organisations that are committed to delivering shareholder/ taxpayer value must, as a matter of necessity, look out from behind their own defences and contribute to the resilience and security of the entire ecosystem through proactive participation.

At an organisational level, our ecosystem is interconnected and interdependent, so no competitive advantage is gained through isolationism. At an individual level, the staff of one organisation are also customers and users of many other organisations.

> Cyber security is a clear area where collaborating external and investing internally – better training for people, informed processes, and more effective application of technology – can deliver more benefits than the sum of the parts.

How to use this report

Our intention in publishing this report is to support cyber risk management decision making in Australian and New Zealand organisations with independent information.

Most organisations do not have a CISO – a dedicated executive accountable for cyber security, a person who is highly connected to their industry peers and is their organisation's internal subject matter expert on cyber risks.

However, the information in this benchmark report is drawn from organisations that **have** allocated the resources to appoint an executive to be accountable for cyber security. That executive supports their organisation by advising on pragmatic response to cyber risks.

Consequently, the information provided in this report should be used as a reference point against which to challenge or validate the management and resource allocation of cyber security in your organisation.

When comparing your organisation to the information in this report, the value is in understanding **why** there is a variation, because the goal in cyber risk management is an informed decision. Use the information presented in this report to drive deeper conversations, both internally and externally.

The most important step toward a better cyber risk management capability is the knowledge that the more value you create, the more value you have at stake and the more risk you will be expected to manage.

Demographics

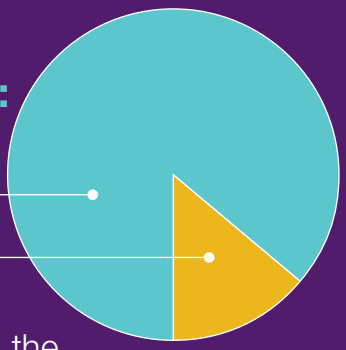
The 58 participating organisations collectively:

Employed over 980,000 people (average of 17,000 each).

Spent in excess of $18 billion in the last year on ICT.

Of the 58 organisations:

50 were from Australia and 8 from New Zealand.



30 companies were listed on the ASX and/or the NZX.

As at 2nd July 2019, the collective market capitalisation value equated to 42 per cent of the total ASX200.

19 organisations were unlisted.

9 were government organisations from both Australia and New Zealand.

Industries represented in the benchmark included:

- Critical infrastructure (including power generation and distribution, as well as telecommunications);
- Financial services (including banks, superannuation and insurance);
- Government;
- Industrials;[2]
- Technologists (including software and online service providers); and
- Other (incorporating large organisations that did not have enough participating industry peers to create their own industry group, but were of sufficient scale to have a CISO function).

1. Data points in this report are rounded unless otherwise stated. All dollar amounts are in Australian dollars (AUD).
2. A category of companies defined by the Australian Stock Exchange.

Cyber security budget for the coming 12 months

56 organisations were able to share their security budget as a dollar amount for the coming 12 months, and these budgets totalled AU$1.063 billion.

Figure 1 is created by ranking all 56 budgets from largest to smallest, then segmenting this list into Tiers, each Tier with eight organisations. This figure provides a sense of the comparative scale of the largest budgets.

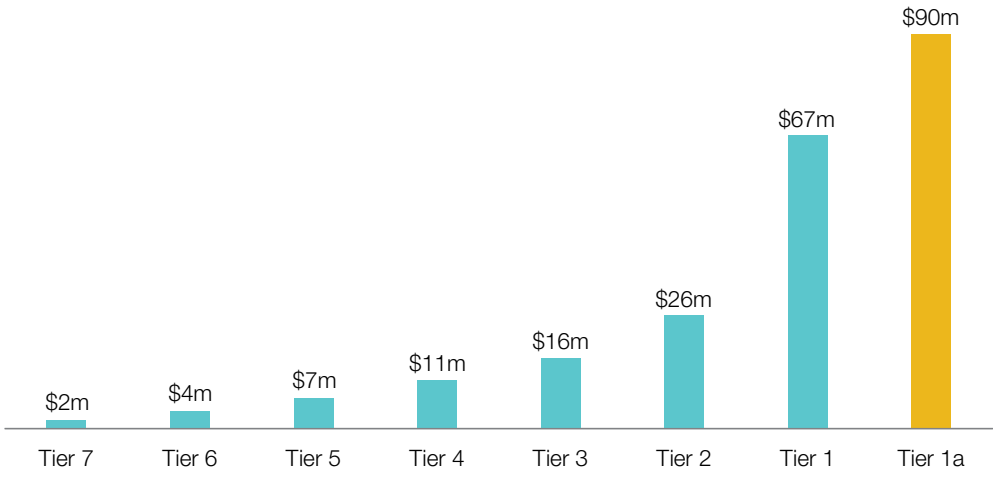


FIGURE 1: Visual comparison of average budgets between Tiers. Each Tier represents the average of eight organsiations. Tier 1a is a subset of Tier 1 and indicates the average of only the top four budgets.

The total average budget is $19 million. As is seen in Figure 1, organisations with budgets close to this average are in Tier 3. However, as the median average is $11 million – corresponding with Tier 4 – we can see that the average is drawn up substantially by the size of the budgets at the top of the list in Tier 1. Tier 1a, with an average budget of $90 million, is the average of only the top four budgets of Tier 1.

Another useful point of comparison is that the total of the eight budgets in Tier 1 made up 51 per cent of the total budget amount for all 56 organisations. In other words, the eight budgets in Tier 1 exceeded all the budgets of Tiers 2–7.

While the sheer size of the Tier 1 budgets is spectacular by local standards, there are two points worth noting.

1. Globally, these numbers are not large. At the upper end of the global scale, JP Morgan Chase is spending nearly US$600 million a year[3] on their cyber security, which is more than all of the Tier 1 budgets combined.
2. There are organisations in Tier 6 and Tier 7 that have large employee numbers (over 10,000), as well as sensitive information and services.

Various ways security budgets are split out

The broad trend was for budgets to be split:

- 32 per cent capital expenditure (CAPEX) and 68 per cent operating expenditure (OPEX).[4] This split is shown in Figure 2.
  - It is worth noting that the industry groups that, typically, had a more mature view of cyber risks (that is, Technologists and Financials) tended toward much higher OPEX figures, for example in the 80+ per cent range.
  - 100 per cent OPEX was the mode average reported.

FIGURE 2: Budget splits: CAPEX vs OPEX (n=42).

- 60 per cent 'business as usual' (BAU) and 40 per cent Projects.[5] This split is shown in Figure 3.
  - Naturally, organisations that need to perform significant ramp up will have a higher allocation to Projects.
  - This broad 60/40 split across organisations shows the importance of maintaining tempo after significant capability shifts are delivered. The cost is not just in the project itself, but in maintenance and capability sustainment thereafter.

FIGURE 3: Budget splits: BAU vs Projects (n=29).

3 "Letter to fellow shareholders". JP Morgan Chase. Accessed December 2019. https://www.jpmorganchase.com/corporate/investor-relations/document/ceo-letter-to-shareholders-2018.pdf

4 42 organisations were able to provide a split between CAPEX and OPEX.

5 29 organisations were able to provide a split between BAU and projects.

Budget increases

Of those surveyed:

- 65 per cent of the participants expected an increase in total budget for the coming year.
  - The expected budget increase average is 18 per cent (median 13 per cent).
- 20 per cent of the participants expected their total budget to remain the same.

However, it is important to note that **none of the respondents reported that they are cutting back on capability.**

Even the 15 per cent that reported that their budget would be decreasing also shared important qualifiers. For example:

- One organisation was coming to the end of a very large step change in overall capability. It's CISO stated that next year would largely be about embedding its new capability. This was a typical qualitative response among those with decreasing budgets – their budget had been higher than normal for a period, and was returning to a more sustainable level until the next step change.
- One organisation noted that while they expected to have a ten per cent decrease in CAPEX, they would also have a five per cent increase in OPEX.

Security budget through different lenses

Security is only a response to risk, and risk only matters if it ultimately affects a human. Consequently, two of the more interesting ways to compare security budget are by people; both internal and external.

It is important to note that no organisation spends its security budget purely on protecting either its staff or customers. These numbers are high level indicators of how the participating organisations compared when viewed through the complex lens of people.

Finally, security budget as a percentage of IT budget is presented.

It is not recommended that any of these three metrics should be used in isolation.

Security budget divided by total organisation FTE

Dividing the security budget by the number of staff in an organisation produces a dollar amount per full time equivalent (FTE).[6]

- The Technologists led the field, with an industry group average of $4,252 per FTE.
- The Financials group was second with an average of $3,248 per FTE.
- The total average was $2,412 per FTE.

6 This section used data from 53 organisations.

Security budget divided by number of customers

This is a particularly interesting data point for organisations with individuals as customers, whether they are retail banks or government agencies. Complexity invariably grows with the number of people. So, while organisations with larger customer numbers also achieve some relative economies of scale, they must also deal with the complexity that comes with success. In other words, more customers does not necessarily equate to a lower spend per customer.[7]

Dividing the security budget by the number of customers:

- The total average was $4.66/customer.
- The Financials group led the field with an average of $7.66/customer.
  - It is important to note that this average was drawn down by a few outliers. Most Financials were spending over $10/customer.
- The Government group had the lowest average of $1.93/customer.

Security budget as a percentage of IT

Security budget as a percentage of IT budget is inherently problematic – if for no other reason than it sets the false assumption that security is only an issue for IT and that only IT should be paying for it. It remains a legacy metric that many organisations still use.[8]

- The total average was 6.31 per cent.
- The industry group with the highest average was Technologists with 7.88 per cent, but it is important to note that the highest median average was the Financials with 8.0 per cent.
  - More than half the Financials reported 8.0 per cent or higher, and ranged up to 10.5 per cent.

... the highest average was Technologists with

7.88 per cent

7 This section uses data from 38 organisations, as it only includes organisations that count customers who are individuals and not businesses or households.

8 This section includes data from 46 organisations.

Role of the CISO

Most organisations want to be able to say, whether to the public, media, shareholders or regulators, that they take security seriously. How the role of their CISO is empowered will provide compelling metrics for assessing the veracity of that claim.

There are three key points of interest around the structural empowerment of the CISO role:

1. What role does the CISO report to?
2. How far is the CISO from the CEO?
3. How often, and for how long, does the CISO brief the full board?

Reporting lines

38 per cent of the benchmark participants reported to a Chief Information Officer (CIO), and 22 per cent reported to a Chief Technology Officer (CTO) or Chief Digital Officer (CDO). A further 21 per cent of the participants reported to partial technical roles which included functions like strategy, and shared services.

However, 19 per cent reported to a **non-technology** oriented executive (including: CEO, Chief Risk Officer, Chief Operating Officer, etc). Having, essentially, one in five CISOs reporting to other business executives shows a maturing in approach from these progressive organisations on how to deliver a better response to cyber risk. Figure 4 shows the proportions of the various reporting strategies.

For some organisations, having a CISO report to a technology oriented executive (e.g. CIO) works because of a solid working relationship between the CIO and the CISO.

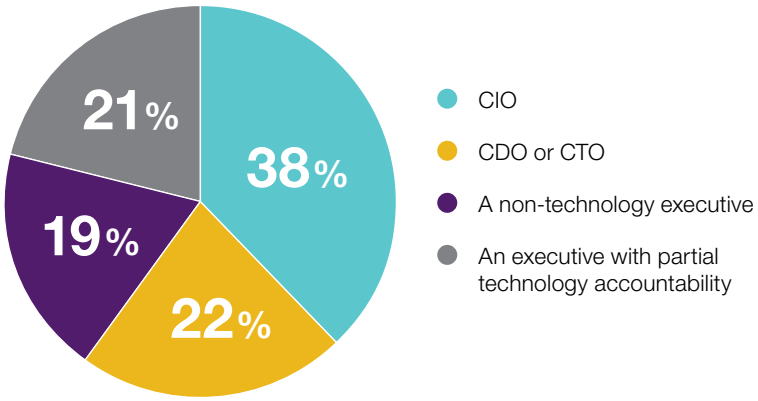


FIGURE 4: Who do you report to? (n=58).

This reporting structure is aided considerably when the CIO appreciates the role of security in managing business risk.

However, this reporting structure can be a legacy of the past, reflecting an organisation that views cyber security as merely an IT problem instead of as a business risk.

Reporting through a technology executive is not inherently wrong – there is 'no one size fits all' structure that all organisations should follow. But, CISOs are increasingly gaining accountability for diverse non-technical domains that have (or could potentially have) a cyber aspect. These domains include privacy, business continuity, crisis management, disaster recovery, and internal/external fraud.

There are also highly technical domains that the CISO role is often assumed (sometimes erroneously) to be accountable for. These domains can include physical security and building management systems, as well as the security of operational technology.

These areas outside of typical cyber security were all reported by the benchmark participants as being areas that were either already in their function, or were often under active consideration to be included.

Proximity to the CEO

The proximity of a CISO to their CEO in reporting lines is as an indicator of the amount of information dilution that occurs before it reaches the head of the organisation. The goal is a more informed risk decision, and CEOs who have multiple layers between them and their CISO are getting a fraction of the information.

58 per cent of respondents were one step or less removed from the CEO. This is a clear statement from these organisations on the importance of making expert advice easily – and continually – available to the executive.

Figure 5 sets out the distance that the benchmark participants were from their CEO. Note that the Financials had twice as many represented at the C-2 than they did at C-3, whereas most industry groups had a rough balance between C-2 and C-3. This is a strong indicator of the maturity that the financial sector has developed in response to evolving cyber risks, and is a model that other organisations should give strong consideration to.

It is also worth noting that more than three quarters of the benchmark participants that were at C-2 (see: Figure 5) were reporting to a CIO/CTO/CDO, who was then reporting to the CEO.

This means that 43 per cent of the benchmark participants were reporting to a CIO/CTO/CDO that was reporting directly to the CEO. This is important because it is an indicator that in these organisations **both** technology and security are likely viewed as strategic capabilities.

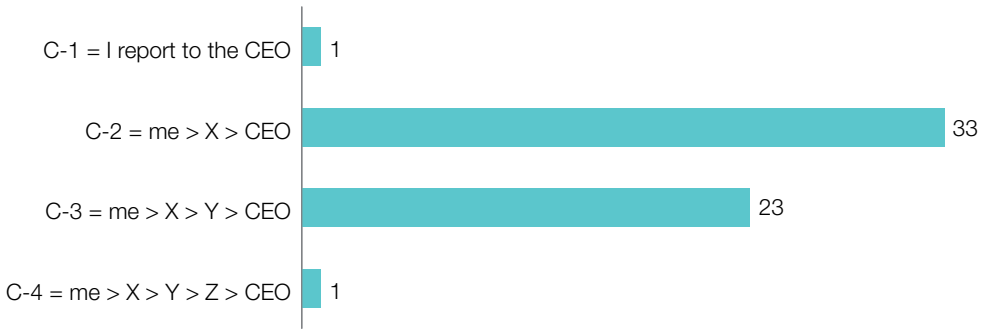


FIGURE 5: Proximity to the CEO (n=58).

Regardless of what role the CISO is reporting to (and each organisation must determine the best structure for itself) having this number of technology executives reporting directly to their CEO is a strong sign that technology has strategic focus at these organisations.

Predictably, this strategic focus will increase the likelihood that technology is being used progressively to empower the business, just as security is there to manage the risks that come hand in hand with the speed and scale that technology introduces.

Presently, having a CISO at C-2 (reporting to an executive that reports directly to the CEO) appears to be a pragmatic fit for most organisations.

Reporting to the full board

39 of the benchmark participants reported presenting to their full board in the last 12 months.

- The total average was for two briefings per year.
- The average duration was 27 minutes per briefing.

Interestingly, it was the mid-tier financial security executives that were reporting the most frequently to their full boards.

- Tier 2 organisations (see: Figure 1) had the highest average (4.3 times in the last 12 months).
- The Financials industry group had the highest median (3.5 times in the last 12 months).

Tier 2 organisations had the highest average:

4.3 times in the last 12 months

However, it is worth noting that this metric – reporting to the full board – did not count some of the qualitative answers:

- Most organisations had their CISO reporting frequently to the Audit and Risk Committee equivalent (typically averaging four briefings, or more, in the last 12 months), or
- That many of the CISOs were engaging with individual board members to provide regular deep dives and 'ask me anything' sessions that could last hours, or
- That 30 minutes was the most often cited duration (mode average), but
- Many of the CISOs reported that their board presentations (either to full board, or the Audit and Risk Committee equivalent) would extend well beyond the allocated time.

Qualitative interviews with both CISOs and CIOs indicate that board members are becoming more informed and interested in cyber risk, and the qualitative information provided in the benchmark answers reflects this.

Third parties speaking to boards

While there are innumerable third parties seeking to present their opinions to boards, the best approach is usually to hear from the internal CISO, who has direct accountabilities and understands the operating environment of their organisation.

In Australia and New Zealand, the enterprise CISO community is incredibly well connected. These security executives are informed on what their cross-organisation and cross-industry peers are doing. This means that the insights from a CISO are current, and the result of both formal and informal collaboration with a wide network of peers.

Cyber security teams

Collectively, all 58 organisations accounted for 3,102 security FTE.

That produces an average of 53 FTE per team, but this average was skewed by organisations in Tier 1 and 2 (as per Figure 1).

The average number of direct reports was 5.8. However, this number was necessarily larger for those with very large teams (i.e. teams over 200).

Security team divided by organisational FTE

One way of analysing whether an organisation is putting forward a reasonable response to cyber risk is by considering the ratio of security staff to organisational FTE.

More mature organisations – those that are aware of the risks they face, the risk to the assets they hold, the value of these assets to the organisation as well as to criminals, and the capability of adversaries – will proportionately require more security staff.

To provide an analogy for the interpretation of Figure 6, imagine one security guard trying to protect a crowd of 537 people, versus one security guard trying to protect 67 people. Fewer people per security guard predictably enables better security overall.

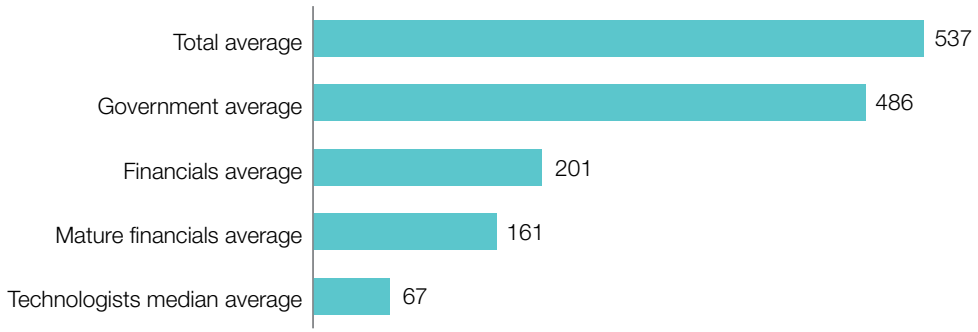


FIGURE 6: Ratio of one security staff to x organisational FTE. Lower numbers mean proportionally more security staff.

The total average was one security person for every 537 staff. However, that number was skewed substantially by some outlying organisations that had ratios larger than one security person per 2,000 staff.

The two leading industry groups were, unsurprisingly, Financials and Technologists. For Financials the ratio was 1:201, but for the larger Financials that have mature security practices, the ratio was even lower (1:161).

The most favourable ratios came from the Technologists – organisations that produce software and have strong Internet presence and capability. These organisations recognise that their businesses do not exist without securing digital assets and staff. This industry group had a ratio of one security person for every 67 staff.

People remain the most important pillar to an organisation's security. **Over time, the value of people appreciates while technology depreciates.** This is true for both security professionals and general staff, and underscores the importance of ongoing security awareness and behaviour training.

Technologists... had a ratio of one security person for every

67 staff

Security strategies

The participants were asked about a range of areas in their strategy. This section includes information about their responses to three core areas:

- Strategy in a sentence
- Metrics
- Priorities

Strategy in a sentence

The purpose of a strategy in a sentence is to help communicate with people who might not otherwise understand the need for security. The strategy in a sentence aims to create context and relationship in a soundbite.

Strategies in a sentence range from principles that are easy to repeat and drop into conversations, through to more detailed statements which include 'the how'.

It is hard to capture a 'Why' in a strategy sentence, however being able to answer 'Why?' is crucial because it may be the next question from an executive.

For example:

- 'Get the basics right' was one of the provided strategies. If asked 'Why?' we can imagine the CISO/CSO coming straight back with 'because that's where we'll come unglued' or 'because the basics are the hardest'. A statement like 'Get the basics right' speaks to an attitude of quality, consistency, discipline and reliability.
- 'Visibility – if we can't detect we cannot defend', was another of the provided strategies. You know this team is on a quest to know exactly what's going on because they have an organisation to protect. Again, if you asked this CISO 'Why?', you know there are facts and experience to back this position. It also paints a picture of an organisation potentially under siege. This positioning may or may not communicate with executives depending on their level of awareness and concern.

Metrics to align with business requirements

The benchmark participants provided a varied list of metrics which showed:

- Varying levels of engagement with the business;
- Biases toward either technical measures or business impact; and
- Different levels of operational capability.

The comment one CISO provided about this section is worth noting: 'I have different *most important* metrics depending on who I'm talking to. We've got one for my team which is straight capability and another for the (executive committee) which is aligned with what they care about.'

This quote highlights two facets on the role of a CISO:

- The importance of a CISO being able to curate the message to the audience, and
- A clear understanding of business objectives to ensure that all security effort is aligned to what the business actually cares about.

Strategic priorities

The benchmark participants were asked to list their top three priorities for the coming year. 171 responses were provided (three lists from 57 participants). These 171 responses were coded into 25 categories. The top 12 are shown in Figure 7. These 12 categories had five or more benchmark participants nominating them.

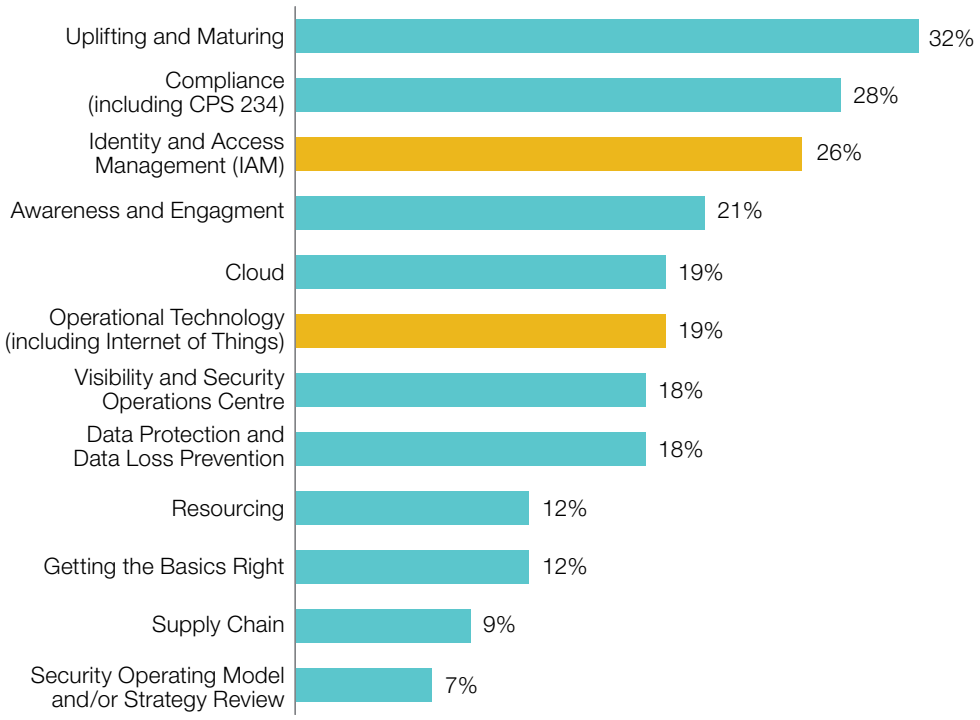


FIGURE 7: Aggregation of the top three priorities nominated by benchmark participants. Multiple responses provided means that the total will exceed 100 per cent. (n=57).

The top priority by number of respondents is Uplifting and Maturing of capability. This category covers a range of activities. As the label indicates, it's around retooling, efficiency, delivery and uplifting existing capabilities.

Identity and Access Management (IAM) and Operational Technology (including Internet of Things) are both highlighted in Figure 7, due to the high priority the participants gave these categories. While Uplifting and Maturing had 32 per cent of the benchmark participants nominate it as part of their top three:

- OT had the highest level of participants nominating it as their number one priority.
- IAM was the second highest for being nominated as the first priority, and also had the highest rate of second priority nominations.

Compliance was ranked strongly by respondents in Financials and Critical Infrastructure. APRA's prudential standard CPS 234 has made significant waves among its regulated entities. The security of critical infrastructure is also an area undergoing fundamental transformation.

From an industry perspective, a number of similar projects will place higher than usual demand on specific skill sets across the region. This will include demand on the market from service providers trying to support their customers.

Operations and sourcing

Perhaps the most surprising finding from the benchmark was the broad dissatisfaction with outsourcing. Figure 8 shows the responses to this question on broad sourcing approaches. The qualitative responses provided are reviewed in the bullet points below.

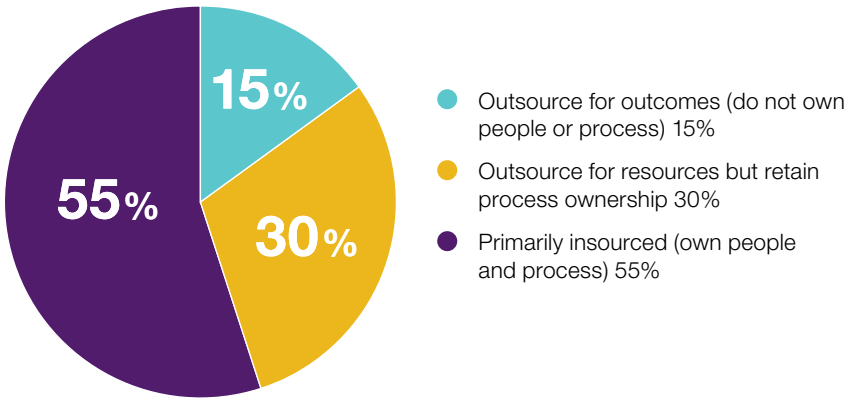


FIGURE 8: General approach to sourcing security capability (n=54).

- 55 per cent stated that they primarily insourced (owned the people and the process).
  - Four of these 30 respondents also stated that they had minor plans to change this approach. These changes were to make very slight adjustments to refine resource allocation.
- 30 per cent stated that they primarily outsourced, but for resources (owned process).
  - Eight of these 16 respondents also stated that they had plans to change this approach, typically to bring some resources back internally and use service providers more selectively for commoditised work.
- 15 per cent stated that they primarily outsourced for outcomes (did not own people or process.
  - Four of these eight respondents were planning on changing their approach to include more insourcing.

In summary:

1. The organisations that reported insourcing as their primary approach were broadly satisfied.
2. Of the 24 that were outsourcing (either for outcomes or resources) half of these planned to increase their insourced capability in some way.

To quote an experienced financial services CISO, 'My people will work as long as they have to, with whatever they have at hand, to resolve an issue. I cannot count on any service provider doing that.'

The implication for the industry is that a substantial number of organisations are looking to improve their internal capabilities with more people, and they are all fishing from the same pond.

There is a clear requirement for ongoing talent pipeline development – both young people coming into the workforce, as well as searching across professional domains for people with aptitude and transferable skills.

Vendors

The benchmark participants were asked to:

1. List their top five vendors that helped support the security and resilience of their organisation, and
2. Score these vendors on a scale of 0–5 to indicate the level of security industry leadership each vendor demonstrated (see Figure 9)

86 vendors were nominated, and the **four that received the most nominations** were:

1. Symantec (21 nominations)
2. Microsoft (20 nominations)
3. Cisco (11 nominations)
4. AWS (9 nominations)

It is worth noting that only one of the above four vendors is considered a security vendor – Symantec. The remaining three – Microsoft, Cisco and AWS – are infrastructure vendors.

Security leadership

The three vendors that received the highest averages for security leadership (see Figure 9) were AWS, Crowdstrike and Zscaler.

The five vendors that were given two or more scores of five were: Symantec, Microsoft, AWS, Crowdstrike and Zscaler.

It is worth drawing out the performance of Microsoft. AWS is a cloud vendor by DNA and has come to exemplify the difference between cloud and non-cloud architecture. Microsoft, however, is an industry veteran and born in another era of the computing industry. The fact that so many services from Microsoft (from Azure to O365 to ATP) feature so frequently in conversations among CISOs is a testament to this vendor rebuilding itself to meet the needs of its enterprise customers. This marks quite a difference from the pre-Satya Nadella era of Microsoft.

Security leadership was graded on a six point scale:

5 = Excellent industry leadership

4 = An industry leader

3 = Useful industry participant

2 = Broadly keeping pace with industry

1 = Losing ground in the industry

0 = Holding the industry back

Figure 7: Security leadership was graded on a six point scale.

Note:

- This benchmark was conducted prior to official disclosure of Symantec's acquisition. Now that the acquisition by Broadcom is in motion, it will be interesting to see how this impacts Symantec's rating next year.[9]
- The performance of Crowdstrike and ZScaler are also worth noting. These two vendors are considered by their customers to consistently deliver solid capability, as communicated in numerous CISO conversations.
- Kasada, an Australian startup, performed very well in the ratings. Kasada was one of only 12 vendors that received both multiple nominations, and at least one security leadership rating of five.

9 For a deeper assessment, see: 'What Symantec's acquisition by Broadcom means for enterprise customers', by James Turner, published on LinkedIn, August 2019.

What now?

This benchmark is published for the benefit of business and technology leaders. Our intention is that you use this information to help ensure that your organisation is putting forward a cyber security posture commensurate to the value you deliver.

As discussed in the section, *How to use this report*, the information provided should be used as a point against which to challenge or validate the management and resource allocation of cyber security in your organisation.

Questions to ask of your organisation

Whether your organisation is an ASX50 organisation or not, consider asking the questions set out below. These questions are a starting point. Better questions lead to better answers.

The role of a CISO

1. Do we have a CISO? If not, why not? Are we confident that we have a complete understanding of the cyber risks to our organisation, our management of these risks, and our ability to manage and recover from a security incident?
2. If we have a CISO:
    a. Are they sufficiently resourced to support our organisation?
    b. Who does the CISO report to in our organisation? Is this the best reporting line?
    c. Is our organisation's dependence on technology reflected by the proximity of our CISO to our CEO?
    d. How often is our CISO reporting to the full board?
    e. How often is our CISO reporting to the audit and risk committee?
3. Is there a designated person on the board who is our nominated lead on cyber security? Is that person passionate about the topic? Is their knowledge current?
    a. How often is that person spending time with our CISO for deep dives on our current status?

Security budgets

4. What is our CAPEX/OPEX split? Is this split different from the benchmark? If so, why?
5. What is our BAU/projects split? Is this split different from the benchmark? If so, why?
6. How much are our peers spending on security?
7. Are we comfortable with our security spend per FTE?
8. Are we comfortable with our security spend per customer?
9. If we gauge our security budget by using a percentage of IT, are we confident our IT budget is right?
10. Is there a better metric that we could link our security spend to – such as percentage of total operating expenses, or
11. If our marketing budget is an indicator of the value of our brand, how much should we be spending on security to protect the value of the brand?

Security strategy

12. Do we have our security strategy summed up in a sentence?
13. Do I know what our security strategy in a sentence is? If there is a strategy in a sentence but staff don't know it, then it has not permeated. This may be either because it is not being repeated enough, or it does not align with the organisation's culture.
    a. Does our IT team have security key performance indicators (KPIs) to ensure that we're getting the behaviours we want?
    b. Do general staff have security KPIs to ensure that we're getting the behaviours we want?
    c. Are we providing enough security awareness training to support the behaviour we are expecting of our staff?
14. What are the security metrics we are reporting internally? Do these metrics make sense in light of the risks our organisation has, or are they metrics we picked some time in the past? Are these metrics measuring the security capability and risk management that our business needs?

Priorities and sourcing

15. Do we have enough people to deliver and maintain the security capability we require internally?
16. Are we moving quickly enough to fill vacancies in the security team?
17. Have we looked across our business for people who may have an aptitude for security, and who would bring additional skills and business perspectives to the security team?
18. Does our approach to outsourcing assume that our suppliers will always have the full set of skills they require to support us, as well as their other customers?

Final thoughts

Through this benchmark report, the importance of people, as well as the right structures to ensure those people are appropriately supported and resourced, are both clear.

Obviously, your organisation needs to hire professional security people to help advise and execute, because you cannot manage what no one understands or knows about.

The art of cyber security comes from the people – the security professionals – who proactively engage with the business and have a deep understanding of what the business needs are, and then explores options with business leaders as a collaborative engagement.

The science comes through the implementation of processes and technology that can deliver consistency of outcome. The identification, implementation and maintenance of these processes and technologies are a journey of collaboration, experimentation, and continual refinement.

Security leadership is about blending the art and the science; it is about finding the people who can accept the need for dynamic tension between risk, cost and reward, and thrive in the exploration of that balancing act.

Our hope is that this benchmark helps you make more informed decisions around the cyber risk management requirements for your organisation.

James Turner
Founder and Managing Director
CISO Lens

Methodology

- 72 organisations were invited to participate in the benchmark between 31 May and 30 June 2019.
  - CISO Lens approached the lead individual accountable for cyber security in each of the 72 organisations.
- Within this window, 58 organisations responded (80 per cent response rate).
- Not all the benchmark participants are members of CISO Lens, and not all CISO Lens members participated in the benchmark.
- Participants were asked 43 broad questions covering seven core areas:
  - Demographics
  - Budget
  - Your role
  - Your team
  - Your strategy
  - Operations
  - Vendors
- All questions were optional.
  - Most questions were free-text for qualitative responses.
- All information exclusively collated, normalised, analysed, presented and reported by James Turner of CISO Lens.

If you would like your organisation to participate in the 2020 benchmark, please contact: benchmark@cisolens.com.au

Caveat

While CISO Lens has taken care to diligently analyse the information provided by the respondents, and we assert that this report has fidelity to the information provided, CISO Lens cannot make any assurance on the accuracy of the information provided to us. We assume the information was provided in good faith and have analysed it accordingly. Decisions based on this information and our commentary are taken at your discretion.

About CISO Lens

CISO Lens is a forum for Chief Information Security Officers of large Australian and New Zealand organisations. Our mission is to support the cyber resilience of the economies – and thereby, the people – of Australia and New Zealand. CISO Lens works toward this mission by empowering and enabling CISOs through: peer networking, structured collaboration, and benchmarking.

A key driver for the creation of CISO Lens was the recognition that cyber risk is a business issue that can be most effectively addressed through collaboration across organisations and industries.

CISO Lens was founded by James Turner, who has worked as an industry analyst since 2005.

www.cisolens.com

About AustCyber

AustCyber – the Australian Cyber Security Growth Network – supports the development of a vibrant and globally competitive Australian cyber security sector and in doing so, enhances Australia's future economic growth in a digitally enabled global economy.

AustCyber works to align and scale Australian cyber security research and innovation related activities in the private sector, research community, academia and across Australian governments. Charged with building infrastructure to support the growth of a sector, AustCyber collaborates across the Australian economy to support a range of other government initiatives related to Australia's cyber security readiness and resilience.

AustCyber also works internationally with a range of partners to develop sustained export pathways for Australian solutions and capability. This further enables the rapidly growing Australian cyber security sector to tap into global hubs located within cyber security 'hot spots' around the world.

www.austcyber.com