Benchmark 2020

Produced by CISO Lens

Published: November 2020

www.cisolens.com/benchmark

In partnership with AustCyber

AustCyber
Australian Cyber Security Growth Network

Table of Contents

Foreword from Michelle Price, the CEO of AustCyber

Globally, we are consistently hearing that one of the most common barriers to the success of cyber security leadership in organisations is maintaining the trust of executives and Boards (or equivalent in public sectors) in the judgements CISOs and equivalent make in responding to the complexities, pace and scale of cyber risk. Not in the management of risk, but the response to risk.

This points to an economy not yet having normalised cyber security for the set of business and societal risks that it is. This is certainly true in Australia. In a year when 'normal' has been truly challenged, perhaps we need to start challenging ourselves on whether at least some elements of the cyber endeavour ever will be normalised, relative to anything else. I say this to indeed be provocative; we do need to give ourselves permission to talk about cyber resilience being a game of responsive versus reactive. Because cyber risk is so contextual.

Benchmark 2020 enables clarity as you consider your last 12 months going into 2021. It supports us to face tomorrow's intensifying conversations about leveraging the lessons that have surfaced during one of the most comprehensive crises we have faced in almost a century. More than this, the utility of the Benchmark is in how it helps get cut-through, with context.

As the broader economy starts to grasp the horizontal nature of cyber security and its intimate relationship with privacy and safety, cut-through circles back again from around five or so years ago to being critical.

It is now less about policy change, business sluggishness and societal unawareness. It is far more about helping senior decision makers appreciate the cyber dimensions in the convergence of strategic risks; convergence of technologies - existing, emerging/ edge or brand new; misaligned legislation and regulation; changing conceptions of trust, value for money, supply and value chains; and geopolitical tensions with increasingly localised impacts.

Sense check - will cyber security as an endeavour ever normalise, relative to others?

AustCyber's partnership with CISO Lens continues to be a key aspect of how both organisations deliver on our complementary missions and deepen our respective positions in value chains. We continue to see the benefits this combined effort delivers to the buyer community, the development of globally competitive, innovative Australian cyber security products and sectoral infrastructure including skills and workforce development.

This document reflects a part of our sector who are among the hardest working - it is in no small part due to the high calibre of CISOs around the nation whose focus, judgement and commitment defend us 24/7, that Australia is a respected and valued nation in cyberspace. My congratulations to CISO Lens for their ongoing significant contribution to the sector and beyond, especially this year in making sense of a highly unusual period. In anyone's context.

I commend the Benchmark 2020 to you - read with the 2020 Update to Australia's Cyber Security Sector Competitiveness Plan, you are armed with globally unique data and insights to look forward.

Michelle Price
CEO, AustCyber

Introduction

The **CISO Lens Benchmark 2020** is published to support two core objectives of CISO Lens. Firstly, to support cyber security governance within organisations. Secondly, to support cyber resilience across the Australian and New Zealand economies. 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.

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 an informed decision, resulting in a commensurate response to the cyber risks these organisations face. Part of the challenge of presenting a commensurate response is the need for continual evolution, and 2020 has been a graphic example of this need.

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

Most organisations in the broader economy 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.

This report captures data from organisations that have invested in a CISO capability and is relevant to both the cyber security executive and the non-specialist whose multiple remits include cyber security. It is the intent of this report to share insights with the wider community and specifically those organisations that lack the benefit of a CISO.

Consequently, treat the information in this report is 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.

Each organisation has a unique context and preferences; copying someone else's strategy is no guarantee of success. We encourage you to not treat this benchmark as an exercise is numeric comparisons, but to 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.

Author's Note

It's important to state at the start of this report that comparisons to last year are an exercise in wistfulness. In establishing the Benchmark in 2018, our intention was not just to create snapshots, but also to create a data set which can be used to track trends longitudinally. And for a number of years, the Benchmark has been able to achieve that.

However, there's no sense in which 2020 could be considered a normal year. Many variables were thrown up in the air, and it's not yet clear which of the resulting changes are temporary and which will be an enduring feature of work and/or life. In short, be careful when comparing the two years' data to make inferences, beyond those we've drawn.

Through this year's document, we will occasionally touch on differences to 2019. But the value from this 2020 benchmark is as an - almost - clean slate that 2021 and 2022 should check back against. In doing so, we hope that we will realise how far we have come.

Further notes on comparative data

- All dollar amounts are in Australian dollars. All numbers and percentages are rounded.
- Not all organisations who contributed in the Benchmark 2019 were able to this year.
- Organisational structural changes over the last 18 months have impacted the responses of some participants.

Demographics of responding organisations

The 62 participating organisations are some of the largest across Australia and New Zealand. While many of these organisations are multinationals, 56 of the participating executives were based in Australia, and six were based in New Zealand.

The FY20 combined annual revenue (where provided) for the companies was $424 billion (n = 41).

Twenty-nine of the participants were ASX-listed. These companies had a combined market capitalisation of ~$640 billion dollars, representing 35 per cent of the total market capitalisation of the ASX200.

The participating organisations employed 1.6 million people, typically concentrated in Australia and New Zealand. There were an average number of 27,000 (median = 5,100) employees per organisation.

Participating organisations were classified into four industry groups to protect their identities while providing industry vertical insights:

- **Critical infrastructure** (n=14). While the common usage of this term may change in the coming months and years, for this report it refers to electricity generation and distribution, as well as telecommunications.
- **Financial Services** (n=22). This group includes banking, insurance, and superannuation.
- **Government** (n=10). This group includes both Australian Commonwealth and State government agencies.
- **Industrials** (n=16). This broad group includes aviation, healthcare, logistics, property, resources, retail, and technology firms. The ASX listed companies in this group have an average market capitalisation of $24 billion, and a median ~$16 billion. The difference between the average and median is explained by the inclusion of some extremely large companies in this group.

Overall impact of the COVID-19 pandemic on whole organisations

The respondents were asked an open-ended question in each of the sections of the benchmark about the impact of the pandemic.

Some issues were common to all industry groups. The primary issue being that most large knowledge-worker-centric organisations were designed around the assumption that most of their people work in an office most of the time. The flip to enable a majority of knowledge workers to work consistently from home introduced many technical problems and risks – all at once, with little warning.

Critical Infrastructure

The majority of the security executives from this industry group reported three core areas of impact.

- A need to quickly enable between 80 per cent and 95 per cent of their workforce to be able to work from home at the start of the national lockdown.
- The speed of the transition, which for most of these organisations was two weeks or less. Both the scale and the speed of the transition compelled many organisations to take immediate action, without spending the time and resources to identify and deliberately accept the incremental risks. This resulted in substantial work post-transition as these risks were identified and reviewed.
- A sharp impact to revenue for energy companies, due in part to plummeting wholesale prices.

Financial Services

The majority of Financial Services participants reported significant changes to their operations, and notable decreases in profitability.

The changes in operations were driven by the sudden and dramatic shift in focus for technology and security teams as they worked to enable remote work at scale, while discovering that some underlying assumptions about business processes were inaccurate. For example, many processes assumed that physical access to buildings was always possible, or that there would not be a surge in demand for specific technologies and skills causing a local market shortage.

Market conditions hit the hip pocket of many components of the Financial Services sector. Insurers received elevated claims against income protection policies, superannuation funds saw many members withdraw super under Australian government's COVID-19 early release initiative, and consumers more broadly changed their spending and borrowing habits.

Some in the Financial Services sector also saw a noticeable increase in criminal activity, ranging from phishing scams, through to exploitation of the COVID-19 early release of super initiative. Many witnessed the exploitation of public fear around COVID-19 in phishing lures.

Government

The impact of the COVID-19 pandemic was likely felt the sharpest by government security staff. Government departments, by definition, exist to serve the public. During March through to at least July (and even longer in Victoria) the challenges and complications across many facets of public interest and wellbeing kept many government staff – especially security staff across all portfolios – exceptionally busy.

As with the other sectors, security teams were working intensively to enable their agencies' staff to work from home where possible, while also defending their organisation. But in some instances, these security teams were also facing heightened attacks and even more hours were required to help defend their jurisdiction.

The Australian Prime Minister's announcement in June about the malicious cyber activity against Australian networks was a powerful emphasis to the experience that many had gone through for months.

The challenges that public servants had to manage through this time also included having to respond, sometimes within hours, to policy and program announcements from politicians.

Industrials

Through the main peak of the pandemic, many of the challenges of the companies in the Industrials group played out in the daily news:

- the extreme and immediate demand for personal protective equipment (PPE) and sanitation materials for frontline staff,
- historically unprecedented oil price movements due to jockeying between Saudi Arabia and Russia,
- toilet paper panic buying and other supply chain stressors,
- the impact of closed borders on the travel and tourism industries,
- the impact of domestic lockdown on retailers and eating establishments, and
- deferrals of elective surgery to free up hospitals for any influx of COVID-19 cases.

The list of societal impacts goes on, as first, second and third order effects played out during this time.

Security budgets

We deferred conducting this benchmark in part to September and October due to organisations' uncertainty around security budgets. Note that participants were asked for their security budget for FY21, as opposed to "this year" as in prior benchmarks.

Within the data collection window, 57 participants were able to share their FY21 security budgets. The total for all these security budgets was $1.14 billion.

The respondents unable to provide budget data within our data collection window gives some indicator of the level of uncertainty that many were working under this year. Many executives were still trying to establish what their security budget was, even in October; it was a very unusual year.

Budget changes from Benchmark 2019

As covered in the Author's Note, not all organisations in Benchmark 2019 appear this year.

In Benchmark 2019, a total of 56 organisations reported combined security budgets of $1.06 billion, with an average security budget of $19 million.

While there was little change at a high level between the budget numbers in Benchmark 2019 and Benchmark 2020, when we compare what the Benchmark 2020 participants themselves said about their budgets for FY21 compared to FY20, as shown in Figure 1, we get more nuanced information.

	Benchmark 2020			
	FY20	FY21	Difference	Change
Total	$1.04 billion	$1.14 billion	$100m	+10%
Average	$19m	$20m	$1m	+5%
Median	$10m	$11m	$1m	+10%

Figure 1: Comparison among Benchmark 2020 participants of their FY20 and FY21 budgets. Rounded. (n=56)

Figure 1 shows that while there was a 10 per cent increase in total budget, the average security budget per organisation is lower than the median by the stability of the Financial Services participants, who made very little budget changes overall (see: Figure 2). In short, the big spenders were mostly consistent in their spending, but many other organisations increased the security budgets noticeably. This is expanded in Figure 2 and Figure 3.

The budgets of Critical Infrastructure and the Industrials both increased from FY20 to FY21. This aligns to the growing awareness and interest around cyber risk among the directors of listed companies.

Figure 2 shows the difference between FY20 and FY21 – both median and average – across the four industry groups. The noticeable difference between the average and the median is particularly stark in Financial Services, where we see the gap in security budget between large banks and the much smaller security budgets of other Financial Service organisations.

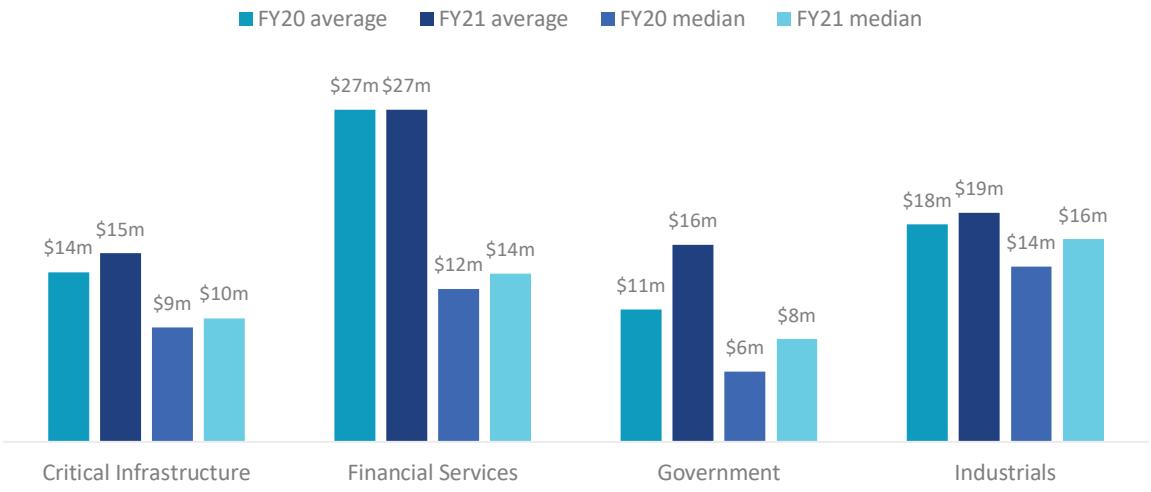

Figure 2: Average and median security budget, split by industry group, in millions. Rounded. (n=56)

It is also gratifying to see the increased investment from Government organisations, which Benchmark 2019 revealed were spending much less per staff member or per customer than the private sector.

Especially with the news cycles of 2020 — for example, the Australian Prime Minister's announcement in June that Australian organisations were under sustained attack from a sophisticated adversary — it is gratifying to see that the Australian government appears to be recognising that each Department and Agency also urgently needs incremental resources to improve their own capabilities.

Tiers

We have ranked the organisations from largest to smallest security budgets for FY21 and segmented this list into Tiers of eight organisations per Tier. We have only included organisations that were able to provide both FY20 and FY21 security budget data. Figure 3 shows the total security budgets for all eight organisations in each Tier, and compares FY21 to FY20.

On the whole, organisations are increasing their security spending regardless of their size. The organisations in Tier 1 have a marginal increase of 4 per cent. The non-Financial Services organisations in Tier 1 experienced an average increase of 14 per cent, where the Financial Services organisations in this Tier saw only minor increases.

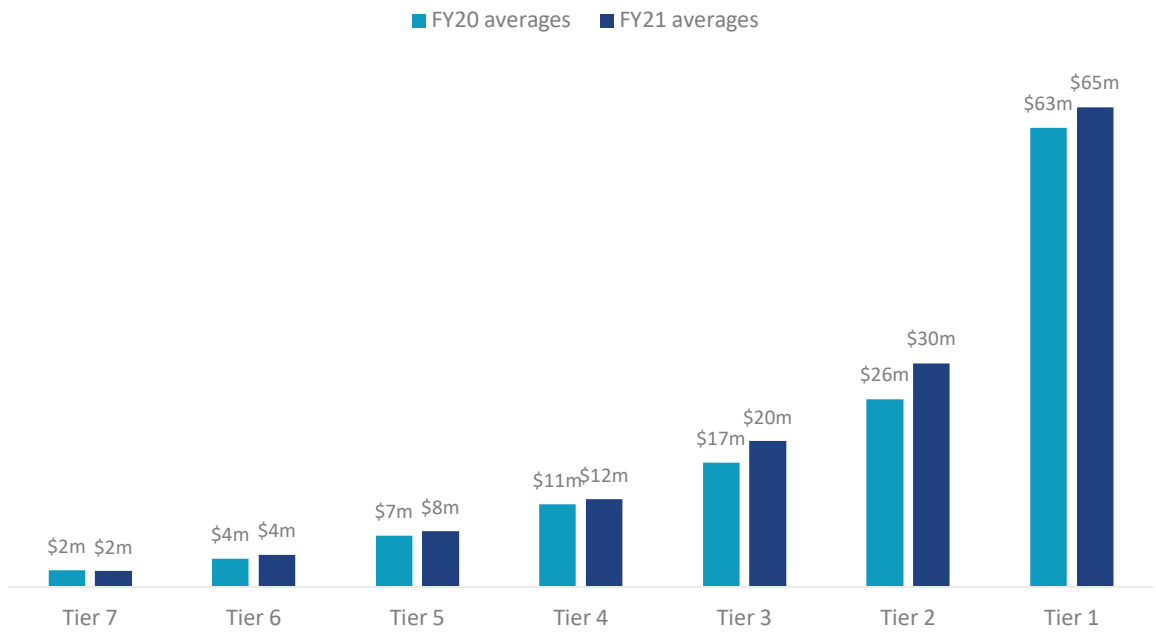

Figure 3: Average security budgets per Tier, comparing FY20 and FY21. Note, 8 orgs per Tier, in millions, numbers are rounded. (n=56)

Tier 2 and Tier 3 organisations typically saw significant expected increases in funding, of approximately 20 per cent. This is a compelling indicator of the growing awareness of cyber risk in larger organisations, and the need to rapidly invest in ongoing capability.

OPEX

OPEX as a percentage of security budget dropped from 68 per cent in Benchmark 2019, to 65 per cent in Benchmark 2020. However, given the comparatively small sample size of these data sets, that percentage difference is negligible. Further, an enduring issue for CISOs is the myriad ways that companies count their expenditure. Capital expenditure is a well-known staple for organisations that are used to buying *things*, like plant equipment.

However, the shift to cloud computing and subscription models for software and software/service fusion offerings means that many CISOs have a strong preference for as much of their budget in OPEX as possible, with the discretion to allocate from this.

Security operating models

Of the respondents, nearly two thirds (63 per cent) were fully funded. This preference for central funding was dominant across all four industry groups. Incidentally, eight of the top 10 organisations by security budget size all had a fully funded approach.

However, Figure 4 shows how the total security budget for FY21 ($1.14 billion) would be allocated across the industry groups depending on their operating models.

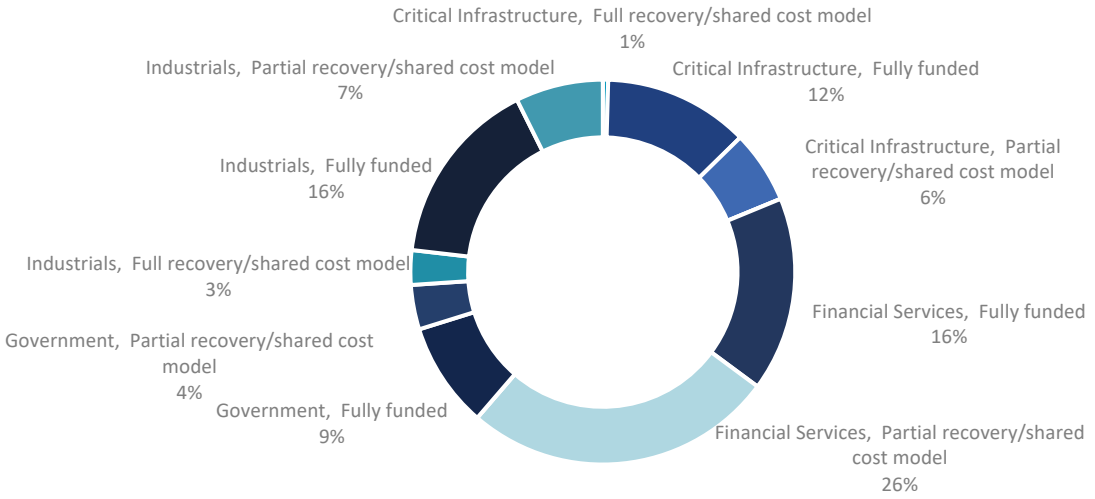

Figure 4: The percentage of the total security budget for FY21 ($1.14 billion) divided by industry groups, and how their budget is allocated: Fully funded, Partial recovery, or Full recovery. Numbers are rounded. (n=57)

If we compare the Financial Services group that had a Partial recovery model, these organisations represent 11 per cent of the organisations in this benchmark, but they represent 26 per cent of the total budget. The key takeaway is that while more organisations in this Benchmark are using the fully funded model, there is more security budget flowing through partial recovery models.

Note: This section builds on Benchmark 2019 which grouped 'partial recovery' together with 'full recovery'. This 2020 benchmark splits these out into two categories. Remarkably, the data Is essentially unchanged when compared to Benchmark 2019.

In Benchmark 2019, 64 per cent of the respondents said they were centrally funded (fully funded using the terminology of the 2020 Benchmark), while 36 per cent said they had partial or full recovery. So, the 'fully funded' cohort has decreased by 1 per cent. Given the size of this data set that difference is too small to count as meaningful.

Security budget as a percentage of IT budget

Setting a security budget through a percentage of IT budget is inherently complex – 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. We include it as it remains a legacy metric that many organisations still use.

More sophisticated organisations are actively moving away from this metric. The total IT intensity of an organisation is typically now much larger than what is captured in a traditional "IT budget", given the increased use of Software as a Service providers and business-managed IT, all of which requires security regardless of which part of the organisation sources it. Further, how does an organisation know whether it is spending the 'right' amount on IT? Consequently, determining a security budget as a proportion of IT budget runs the risk of dramatically under-estimating the realistic needs of an organisation. Treat these percentages therefore as an absolute floor on a reasonable budget.

Figure 5 shows the averages for the four industry groups, and the horizontal line represents the total average across organisations answering this question.

Critical Infrastructure, and some Industrials, can be problematic as the nature of these organisations means that the IT budget can be vast and is increasingly bleeding into the Operational Technology (OT) budget, so this lower percentage is unsurprising.

The Government industry average is concerning, however. Government agencies can infamously struggle with the delivery of large-scale IT projects at the best of times. This comparatively low percentage appear to be a further indicator that the wrong costs are getting cut. Of the eight Government respondents, three reported that their security budget represented 3 per cent or less of the IT budget.

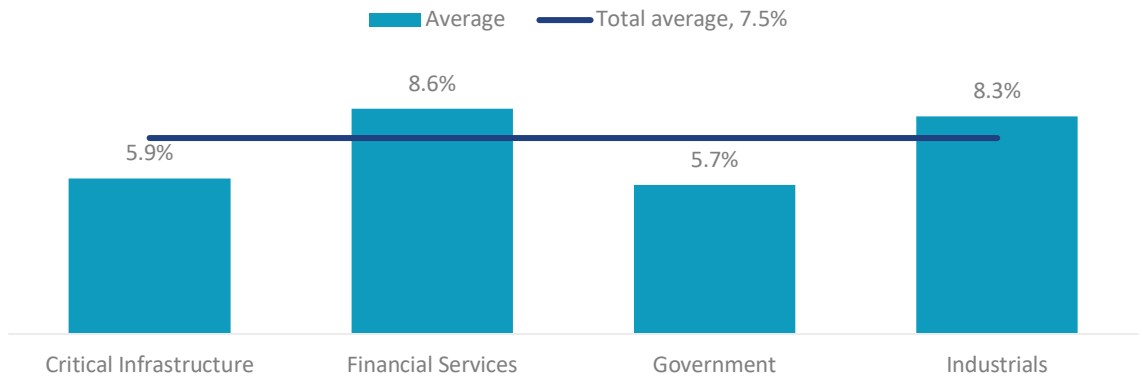

Figure 5: Security budget expressed as a percentage of IT budget (FY21). (n=49)

Of the fifteen Financial Services respondents, seven reported percentages of 10 per cent or higher, including one at 15 per cent. Only one of the Financial Services organisations had less than 5 per cent, and if this outlier were removed, the Financial Services group average would increase from 8.6 to 9 per cent.

Further, the Tier 1 security budgets reported an average of 9 per cent. The Tier 2 organisations reported an average of 8 per cent.

Security budget divided by organisation headcount

An average security budget per full time employee (FTE) of $2,799 (median = $2,000) can be found by dividing each respondent's security budget by their total FTEs.

The lower median reflects the impact of some organisations with the combination of comparatively smaller FTE and larger-than-average security budgets which resulted in some astronomical security budget per FTE figures, that skewed the total average up.

These skewing organisations are highly risk averse and recognise cyber security as a core competency to their services and customers.

Picking the top 10 organisations, ranked by their security budget per FTE, the average of this top 10 is $7,500. Five of these top 10 are Critical Infrastructure organisations. These organisations absolutely skew the average substantially above the median.

However, a concerning counterpoint is that four of the five organisations at the bottom of the list for security spend per FTE are Government, and this is reflected in Figure 6.

The Government respondents were spending on average $1,388 per FTE (median = $1,067) and both average and median are glaringly below their private sector peers.

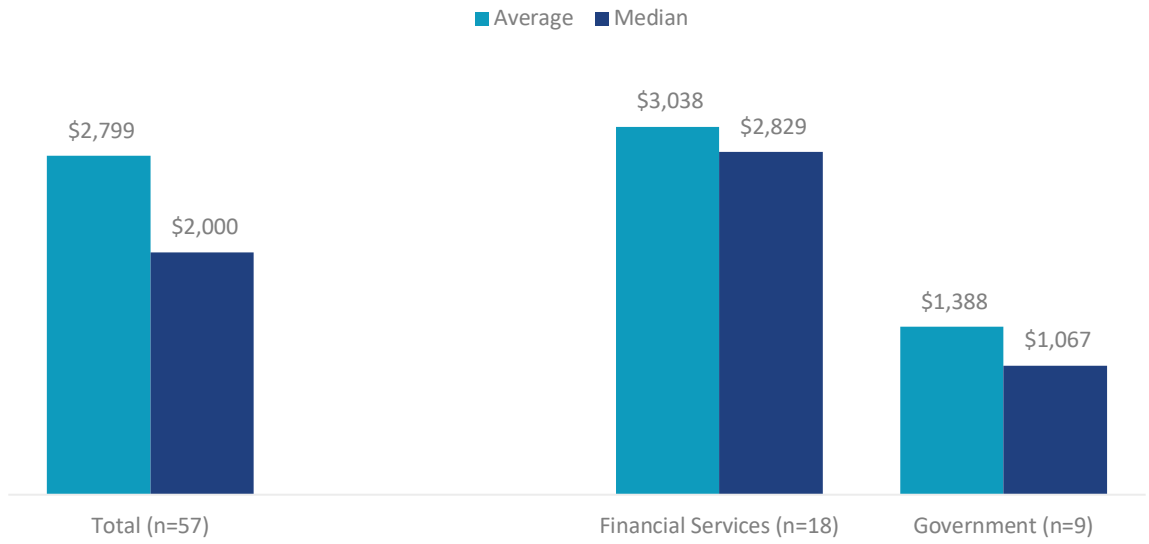

Figure 6: Security budget divided by organisation FTE. Average and median shown for Total averages, which encompasses the two split out industry groups: Financial Services, and Government.

Probably the best cohort to present this metric in a realistic and sustainable perspective is the Financial Services cohort, which had the tightest coupling between its average and median. The simplest interpretation should be that $2,000 is a solid starting point for most organisations to argue up from.

Budget expectations for FY22

Given the turbulence of 2020, asking the participants to predict what would happen to their security budget in FY22 had the potential to be an interesting balance between how their organisation had faired this year and what they thought was needed going forward. Figure 7 shows the aggregated results across the responding organisations.

Overall, there is optimism: 31 per cent expect their budget to remain the same, 47 per cent expect an increase of some amount, and 22 per cent expect a decrease of some amount.

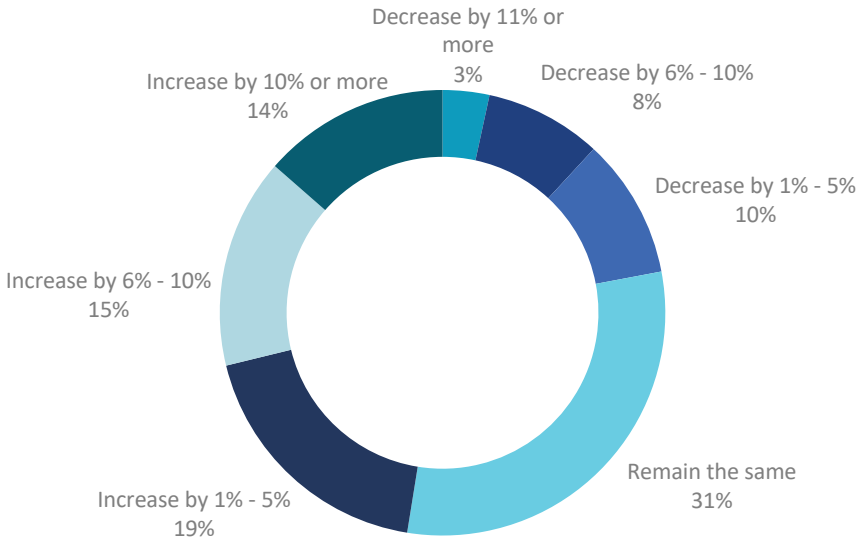

Figure 7: Predictions of budget increase or decrease for FY22, as a percentage of total. Rounded. (n=59)

Interestingly, the most confidence for the future was from the Critical Infrastructure group (n=14), with 64 per cent expecting an increase and the overall average response across this industry group was to expect a budget increase of 1 to 5 per cent. The respondents in this group may think this was foreseeable, due to legislative changes across Five Eyes countries that have a focus on driving up the security capability of Critical Infrastructure organisations.

However, the Government industry group had the greatest number of respondents expecting an increase of 10 per cent or more. That optimism may be driven by the experience of this year, and the belief that things cannot be left as they are amid the sustained attacks from capable adversaries described by the Federal Government.

Impact of COVID-19 on security budgets

The global impact of the pandemic will continue to play out for years, but many security budgets seem to have been reasonably insulated. Figure 8 shows the aggregated answers, broken down into three categories: No impact, Increase, or Decrease.

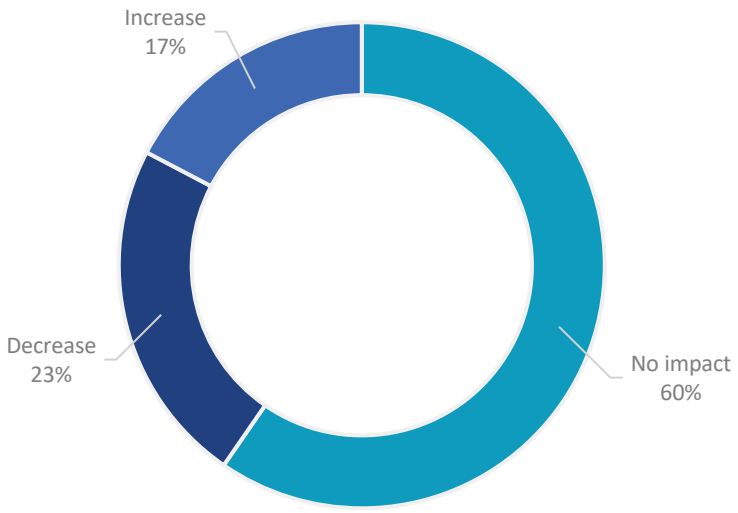

Figure 8: Aggregated answers to whether respondents experienced an impact on their security budget. Numbers rounded. (n=52)

Among the 17 per cent reporting an increase in budget, were two respondents who had technically had their budget cut, but their FY21 budget was still an increase overall from FY20. Most of these budget increases were directly to address threats these organisations were experiencing, while some were a recognition that the pandemic was an extraordinary event that required an extraordinary response to protect the organisation's people, customers, assets and reputation. Many lingering little problems that had previously been tolerated and/or ignored, were swiftly dealt with as a matter of new priorities.

60 per cent of respondents said that there had been no impact on their budgets, including one respondent who noted that they had their budget cut, only to have it restored in order to respond to the new threats their company faced. Four respondents said there was no immediate impact, but they expected changes in the future; and they had not seen the change at the time data was collected.

The respondents reporting a decrease (23 per cent) predominantly indicated that the impact was playing out as deferred initiatives (re-prioritisation), slowed pace of initiatives (recognition that the capability was still important but no longer urgent), some headcount freezes, some headcount reductions, and specific costs targeted. Some of these cost areas of reduction included travel, software, and external consultants.

The role of the CISO

Naturally, the dominance of CISOs and CSOs participating in this benchmark, who collectively represented 76 per cent of the titles of respondents (64 per cent were CISOs and 12 per cent were CSOs) is unsurprising as this demographic group was the target.

The same number (38 per cent) of respondents reported to a CIO in Benchmark 2019 as they did this year.

Interestingly, last year's report noted that 22 per cent of the respondents reported to a CDO or a CTO, but in Benchmark 2020 that reporting structure has increased to 40 per cent.

Reporting levels from the CEO

Regarding proximity to the CEO, remarkably, despite a considerable amount of movement in the Australian and New Zealand CISO community over the past 18 months, the percentages are essentially unchanged from Benchmark 2019 (see: Figure 9). The sole difference is one additional respondent, who reports directly to the CEO.

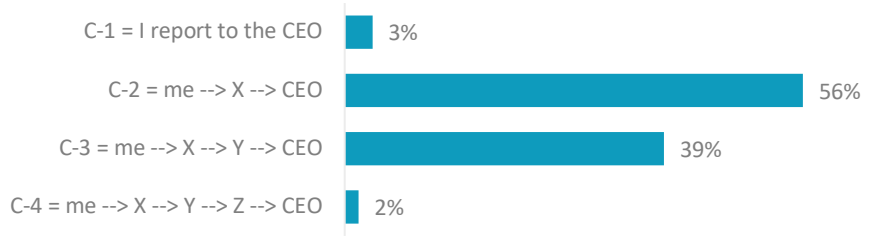

Figure 9: How many reporting levels are you from the CEO? Rounded. (n=59)

For Tier 1 organisations, the majority of the respondents were C-2. But, starting in Tier 2, and all the way through to Tier 7, there is no correlation between budget size and reporting distance from the CEO.

Financial Services are most likely to be C-2 (72 per cent), followed by C-3 (22 per cent).

Government respondents were most likely to be C-3 (67 per cent), with the remainder at C-2 (33 per cent).

Industrials had both the C-1 respondents that reported to the CEO.

Board exposure and influence

Australia is adopting legislation designed to adjust the cyber risk tolerance of executives.

These are a product of the failure of the industry to use the free market to make risk decisions that align with societal expectations.

The Australian Securities and Investments Commission (ASIC) drove a collaborative project - the ASX 100 Cyber Health Check Report - with large audit firms, Deloitte, EY, KPMG, and PWC on the back of Australia's 2016 Cyber Security Strategy.

A notable data point from the ASX 100 Cyber Health Check Report effectively set the baseline for the level of engagement for Board engagement from listed companies.

> "Cyber risk is often the domain of either the board's audit or risk committees (64% of respondents), allowing a subset of directors with the relevant skills to focus on cyber risk issues and discuss them with management and external advisers. However, in a significant minority of cases (28%), the main board considers cyber risk, reflecting its significance as a strategic business risk."
>
> - ASX 100 Cyber Health Check Report, April 2017.

Then in 2018, the Australian Prudential Regulation Authority introduced CPS 234. This prudential standard became enforceable from the 1st July 2019.

> "The Board of an APRA-regulated entity (Board) is ultimately responsible for the information security of the entity. The Board must ensure that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity."
>
> - Prudential Standard CPS 234 Information Security, APRA

Executives in the Financial Services sector commented at the time when CPS 234 came out, that it was a bellwether for how the government was thinking, and that other industry sectors should expect their own versions soon. Then, in November 2020, the department of Home Affairs released an exposure draft of Security Legislation Amendment (Critical Infrastructure) Bill 2020.

> "A responsible entity must give an annual report relating to its critical infrastructure risk management program. If the entity has a board, council or other governing body, the annual report must be signed by each member of the board, council or other governing body."
>
> - exposure draft of Security Legislation Amendment (Critical Infrastructure) Bill 2020

The Security Legislation Amendment (Critical Infrastructure) Bill 2020, and CPS 234, both put directors on notice that they are expected to be informed on cyber risk management.

Benchmark 2020 respondents were asked how frequently over the last 12 months, and for what duration, they presented to:

- the full Board,
- a partial Board,
- the audit and risk committee,
- the Board Chair in a one-to-one meeting, and/or
- a single Board member with an interest in cyber.

Presenting to the Audit and Risk Committee

Eight-six per cent of the respondents stated they had presented to their audit and risk committee. Of these, the typical duration was 15 to 20 minutes, but nearly 20 per cent were presenting for an average of 45 minutes or longer. Also, the majority of respondents were said they presented four times or more over the last 12 months.

It is not surprising to have such a strong representation of participants presenting to the audit and risk committee as, typically, the audit and risk committee has a strong representation of the full Board, and often meets with a more regular cadence than the full Board. Financial Services respondents are strongly represented in this group, with 65 per cent of this industry group reporting to the Audit and Risk Committee four times or more in the last 12 months. Industrials show strongly to this section, with just over half their group reporting three times or more in the last 12 months.

Presenting to the Full Board

Three quarters of the respondents stated they had presented to their full Board. This group was split almost evenly between those that had reported three times or more to the full Board, and those that had reported twice or less in the last 12 months. It's worth noting that the respondent at C-4 (see: Figure 9) had also presented to their full Board six times in the last 12 months.

By industry group, the Financial Services respondents had the most access to the full board, and represented the half of the respondents reporting four or more times in the last 12 months. There was a loose correlation between time spent briefing the full Board and size of security budget.

Finally, it is important to note that on the whole, the longest presentations were to individuals – either to the Board Chair or to a single Board member who was interested in cyber. These meetings invariably lasted half an hour or longer. These sessions are deep dives that enable CISOs and CSOs to present business context and nuance, which then enable that board member to be the resident cyber specialist for all the matters that come before the Board.

It is interesting to note that while Financial Services respondents tended to get more presentation time with the Full Board, Critical Infrastructure respondents got more presentation time with the Audit and Risk Committee.

Security teams

The data from 57 respondents is used to compare security teams by security budget size, and size of total organisation by FTE. These 57 organisations collectively employed 4,105 security professionals. The average security team size was 71 (median = 25, showing the impact of a small number of very large teams).

The average number of direct reports was five, but this increased with team size. Respondents with security teams larger than 100 typically had eight direct reports.

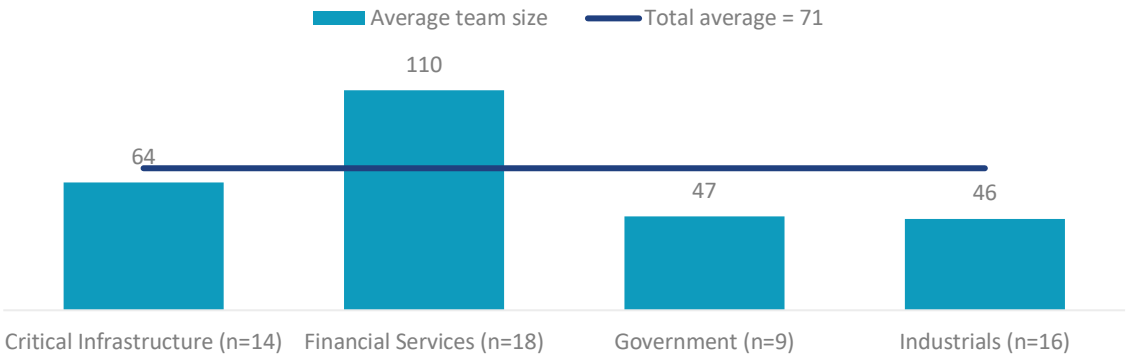

Figure 10: Average team size of security professionals, split by industry group. Rounded. (n=57)

Figure 10 shows the average team size by industry group, compared to the total average (blue line).

All 57 respondents provided information on whether their team size had increased, remained the same, or decreased over the past six months.

- 49 per cent reported an increase.
- 30 per cent reported no change.
- 21 per cent reported a decrease.

Interestingly, 20 of the 57 respondents that reported that they had increased their team size in the last six months also reported that it to increase again in the coming six months. Most of these organisations were Critical Infrastructure.

Open headcount

Most (45 respondents) stated that they currently had open headcount. The range of open headcount per organisation ranged from one person through to 60 FTE within one organisation. Interestingly the likelihood of open headcount was more correlated to budget size than to existing team size.

The average across all 45 organisations was for eight open FTE, with a total of 367 current vacant roles. Eleven organisations had vacancies for 10 or more people

Number of organisation staff per security professional

The importance of this section is that the more staff a security professional supports, the more that professional needs to rely on technology as a force multiplier or, through minimising other variables such as uniformity of roles, permissions and access. Consequently, there are two categories of organisation that can still provide a stronger security posture with higher organisation FTE to security professional ratios.

- Large environments with high uniformity of roles, such as large retail.
- Large financial institutions that have both large numbers of staff, but also large and highly specialised security teams that also are able to leverage both general technology and specialised security technologies to provide faster response.

Both of these categories have higher security budgets and are also able to leverage considerable ongoing general technology investments made by the company.

Ranking the respondents by total organisation size (number of FTEs) the top 10 organisations, employing a total of 1.3 million people, had an average of 618 FTE per security professional.

Note that these extremely large employee numbers do skew the average number of FTE per security professional, but they are typically from the two categories of organisation identified above, plus some government agencies.

To produce more normalised data, two government respondents were removed, as their exceptionally large organisation FTE number skewed the data considerably. So, across 55 organisations, the average was 414 FTE per security professional. Despite the exclusion of two government agencies from this total, respondents from the Government industry group consistently had more FTE per security professional. This is set out in Figure 11.

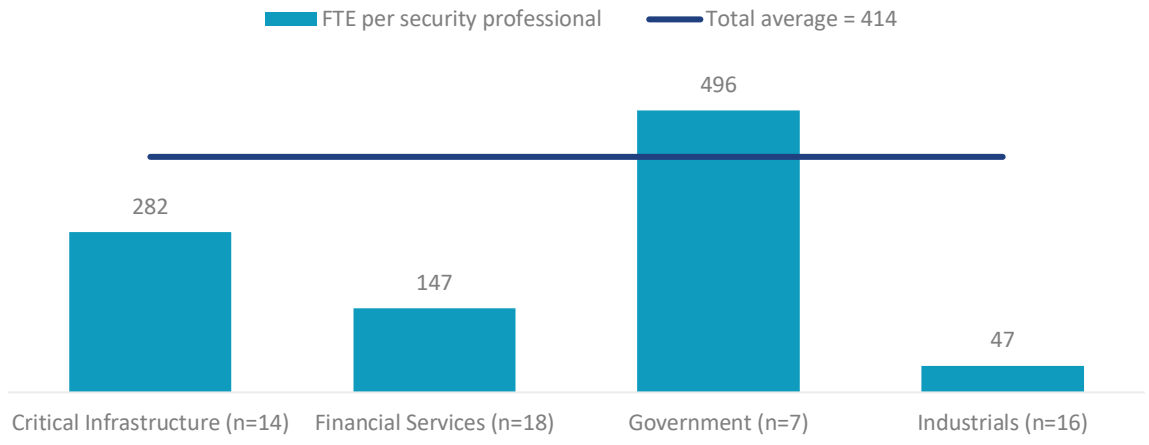

Figure 11: Organisation FTE per security professional, split by industry group. Rounded. (n=55)

Note that if these two government agencies had not been removed, the number of organisation FTE per security professional score for the Government industry group would be in the thousands.

What is the percentage of women in your security team?

In a CISO Lens gathering in late 2019, after hearing from a representative from Male Champions of Change, the community agreed that we would include a question about gender split in the 2020 benchmark.

57 organisations were able to provide data on this question. The average across all organisations was 25 percent with a median of 22 per cent, showing that while some organisations reported higher and lower percentages, the 25 per cent figure is representative. This percentage is probably higher than many would expect, but it's still a long way from equality.

These 57 organisations collectively employed 1,136 women in their security teams. As Figure 12 shows, there is a substantial gap between where each industry group is now, and gender equality at 50 per cent.

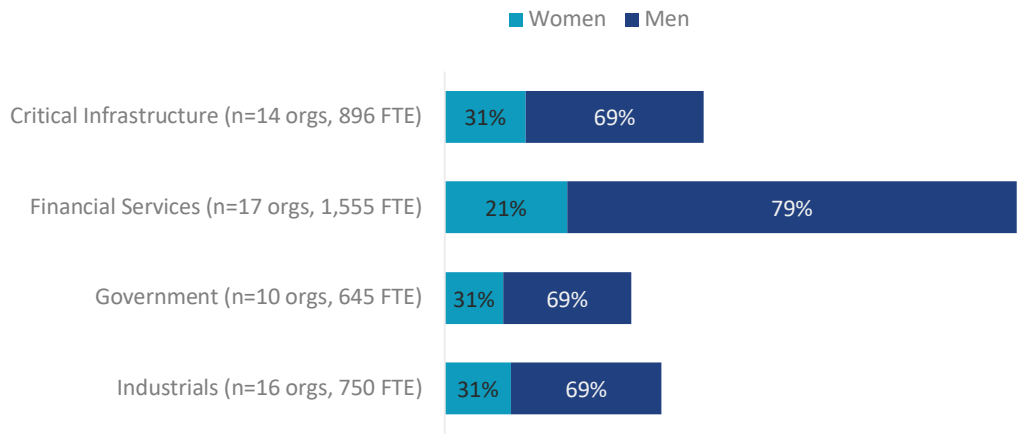

Figure 12: Total number of security professionals per industry group, with gender split shown. Rounded. (n=57)

There, there was a strong harmonic between size of security budget, size of security team, and the percentage of women in the security team.

In other words, ranking the 57 organisations by the number of women in the security team revealed that the top 10 organisations for employing women accounted for 71 per cent (810) of the women in security teams that participated in this benchmark.

Impressively, the top four organisations employing the greatest number of women in their security teams reported that women made up, on average, 40 per cent of their security teams. These four teams collectively employed over 460 women.

Impact of the COVID-19 pandemic on your security team.

Thirty-nine respondents noted if they thought there had been an impact of the COVID-19 pandemic on their security teams.

- 28 per cent reported either no impact, or negligible impact.
- 26 per cent noted significant increases in stressors for their teams. These comments included observations about mental health, clashes with other teams, and dealing with the operational challenges that came with having technology, policies and assumptions that all relied on an environment that had fundamentally changed. Respondents from Government organisations noted a pronounced impact on their teams, as did respondents when talking specifically about their staff that were in cities that went through additional lockdowns, specifically Melbourne and Auckland.
- 46 per cent spoke mainly of operational issues; the shift to work from home for both the security team as well as their employer's staff, the challenge of onboarding new starters, challenges in managing remote staff, and of the reluctance of prospective candidates to leave a secure role due to the uncertainties around the pandemic.

Priorities

The aggregated results of the 60 respondents able to share their top three priorities for the coming 12 months are shown in Figure 13.

These are the priorities of enterprises that have a dedicated security executive, and team. It would be a gross misinterpretation to look at Figure 13 and assume that the enterprise market was not concerned with, for example, backup capability.

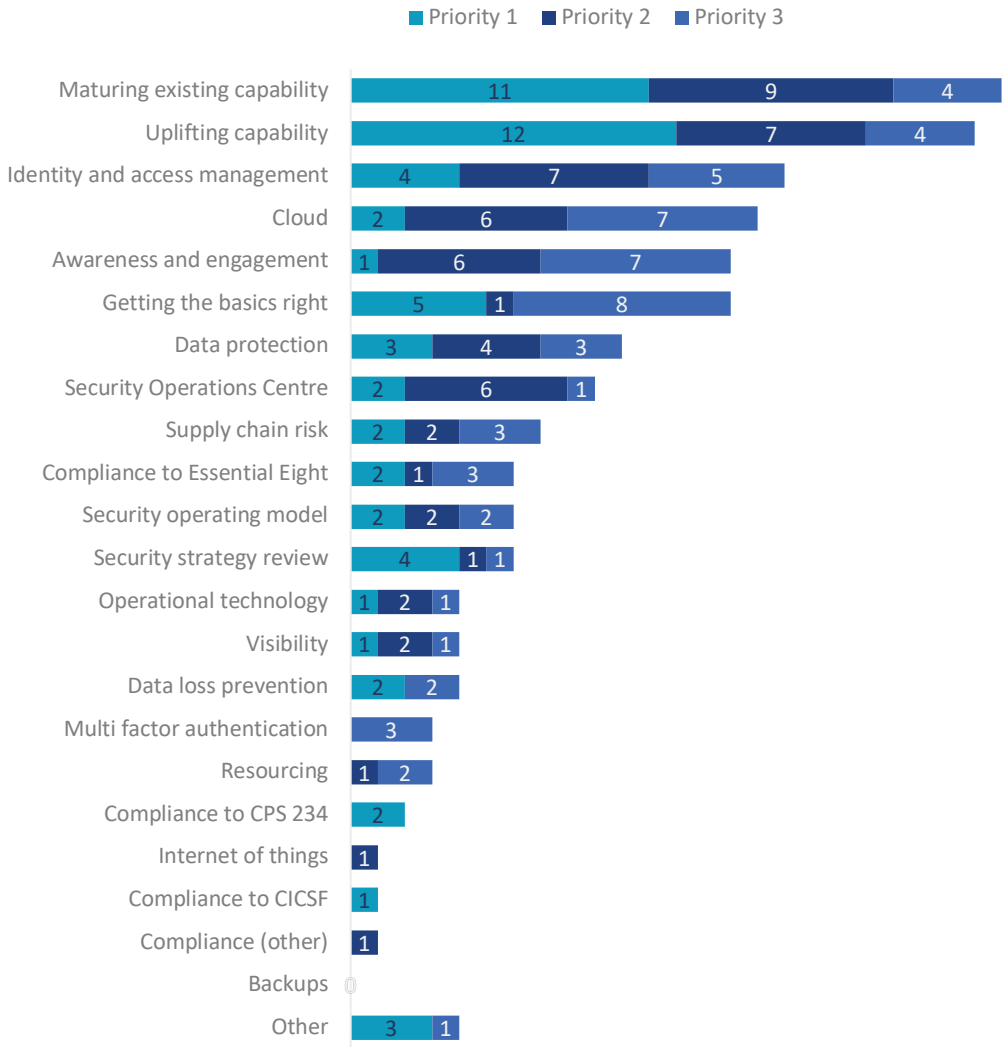

Figure 13: Top three priorities for the coming 12 months. (n=60)

Backup is incredibly important, and a recurring issue in CISO Lens discussions and correspondence through 2020. It is an integral part of resilience, especially in the face of ransomware attacks. However, backup is not usually in the remit of a CISO. Security executives will be seeking assurance around their enterprise's backup capability, but it will be an area they seek to influence and oversee, rather than execute.

Note that the highest ranked priority in Figure 13, 'Maturing existing capability', was a top three selection for most of the respondents in the Tier 1 budget category, followed by 'Uplifting capability', followed by 'Data protection'.

However, for the respondents in Tier 2 'Uplifting capability' was the most common top three selection, followed by 'Getting the basics right', and 'Awareness and engagement'.

Tier 3 respondents chose 'Uplifting capability', followed by 'Maturing existing capability', followed by 'Cloud'.

Despite ranking third on the list of priorities overall, 'Identity and access management' was typically chosen as a top three priority by respondents in Tiers 4, 5, 6, and 7.

Most important security metric for your organisation

The answers from 58 respondents who provided information for this section are aggregated into these categories.

- Vulnerabilities (n=12). The most common 'single most important metric' offered was around vulnerabilities; number of external services that do not support MFA, number of vulnerable assets, external facing vulnerabilities, percentage of critical vulnerabilities, and average age of vulnerabilities.

- Incidents (n=11). These metrics centred on preventing attacks, limiting their duration, impact, or dwell time. This section included metrics such as 'mean time to contain', and zero news articles based on material security incidents.

- Risk (n=11). These metrics revolved around variations of risk; residual cyber risk, number of out of appetite risks, and risks not under active management.

- People (n=6). These metrics were either about managing stakeholder relations (for example, assessing access to, and confidence of, the Board) through to metrics around phishing.

- Patching (n=5). Patching metrics included compliance to patch policy, cadence, ASD Top 4 compliance, and overall endpoint policy compliance including EDR.

- Maturity (n=4). These metrics included assessments against frameworks and noted the upside of being externally validated.

- Hygiene (n=2). These responses merely stated hygiene with no further qualifications.

- Others (n=7). This category included responses such as: critical asset protection, identity and access management, and regulatory compliance.

Impact of the COVID-19 pandemic on security strategy

Eight organisations (19 per cent) reported that the pandemic and consequent shift to work from home and all the other second order effects had no impact on their security strategy, but these organisations were in the minority.

Of the remaining 34 respondents (81 per cent) the impacts varied from:

- Needing to overhaul the strategy to reflect that most users were not working within the confines of the corporate network. This required adjustments to endpoint security strategies, but also the architecture required to support a distributed/remote workforce. Issues included how remote patching and vulnerability management were to be addressed.
- Three respondents noted that the impact of the pandemic increased executive visibility of the security strategy.
- Many respondents noted that the shift in budget resulted in reprioritisation, deferring projects that had lessened in priority, accelerating some initiatives (often patching) that was overdue.
- Five respondents noted an increased push/appetite toward a zero-trust approach.
- Permission of some activities that would previously have been outside risk appetite according to a few respondents. Security leaders will remember, through the pandemic there was an initial rush to make things happen, and this was followed in quick succession by a considerable amount of work identifying what risks had just been accepted through this period, and whether these risks were still acceptable.

It is worth noting that the respondents from organisations with the largest security budgets (Tier 1) typically reported that specific initiatives had been accelerated. Naturally, there was reprioritisation, but the executives at these organisations (all ranked as '4: Improving' or higher for both general and cyber risk management) clearly recognised that the shifting risk environment demanded response.

General approach to sourcing security capability

Sixty respondents provided their answers to this section, and their answers are set out by industry groups in Figure 14. Unsurprisingly, there is a clear bias toward insourcing as the general approach – unsurprising as these respondents are from organisations that have made the commitment to appoint an internal security leader and, for the most part, multi-million dollar security budgets.

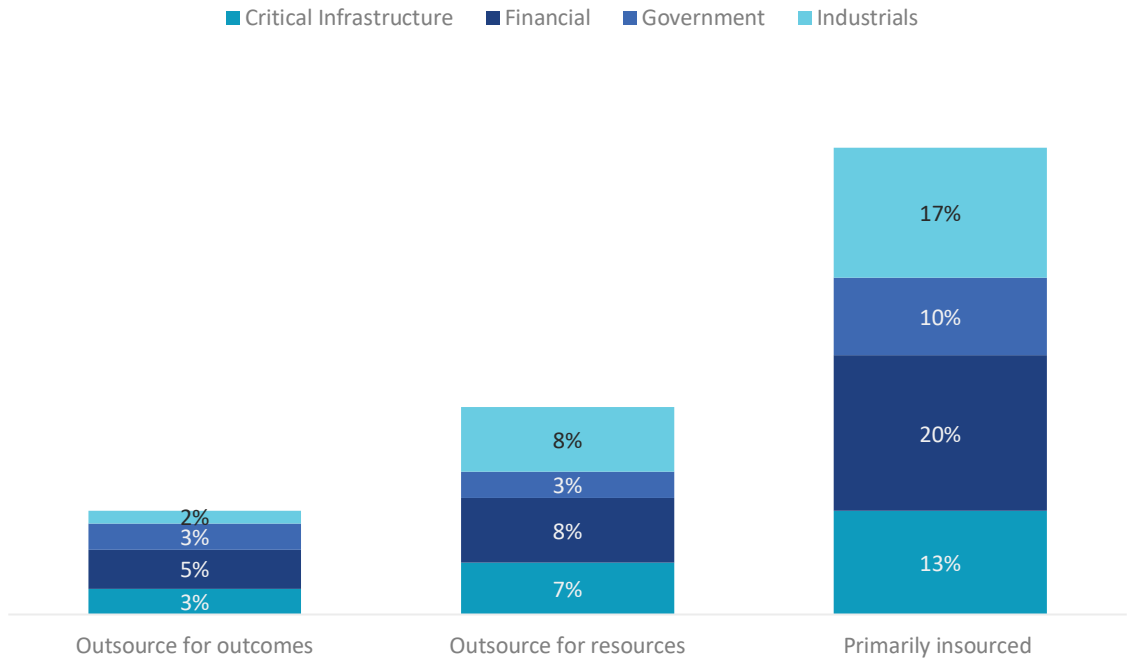

Figure 14: What is your general approach to sourcing security capability? Rounded. (n=60)

Interestingly, of the 60 respondents, only 13 (22 per cent) said they were planning on changing their approach in the coming financial year. All, bar one, of these respondents said that they intended on moving to variations of 'outsourcing for outcomes', and they noted this was specifically for services they viewed as commodity services.

The exception was a Tier 1 that was going to insource further. Two of these 13 respondents that said they intended to change, noted that they were already in the midst of changing their approach due to the COVID-19 pandemic and its impact on their organisation.

Insourcing was the strong preference for all bar one of the Tier 1 organisations. Outsourcing for resources started to gain popularity through the Tier 2 organisations but did not exceed insourcing for popularity. Typically, outsourcing for outcomes was more popular in organisations with security budgets lower than $10 million

Vendors

CISO Lens has a standing agreement that members are free to share their experience and opinions on vendors but may not discourage any other member from engaging with a vendor.

CISO Lens and its members are committed to adhering to all relevant competition laws. When CISO Lens aggregates information regarding the experience of security leaders with vendors, such as in this report, we do so with the intention of helping share good news.

We recognise that Australia and New Zealand are small portions in the global cyber security marketplace, and the experience of a small, targeted, group of security leaders in this region may not reflect the experiences of this region or, other markets around the world.

In short, your decision to engage, or not, with any of the vendors listed here remains your decision and you must consider the nuances of your requirements.

The respondents were asked to select from a list their top five vendors that they relied on most to support the security and resilience of their organisation. Respondents were then asked to rate their satisfaction with the vendors they had chosen. A number of respondents rated more than five vendors.

The purpose of this section was to help identify vendors that the respondents deemed were helping them secure their organisation. Everyone wants to know about the vendor that can be counted on. Consequently, the performance of some vendors is worth highlighting.

It is impossible to ignore the market dominance of Microsoft, which could itself be viewed as global critical infrastructure. Much like electricity or water, when Windows, Office 365, or Azure stop working there is a material impact. Some 61 per cent of the respondents selected Microsoft as one of their top five vendors (see: Figure 15).

No one could reasonably argue that Microsoft has not evolved in leaps and bounds in the last four years. However, the market will soon become Microsoft's to lose. One need only look at Figure 15 to see some names of vendors that now appear to be floundering, and their struggles would have been unthinkable even two years ago.

To that point, it is concerning to see the satisfaction rankings given to Broadcom. In the CISO Lens Benchmark 2019, Symantec was the top nominated vendor by the respondents for the leadership it had shown in the industry. The data for Benchmark 2019 was collected in June 2019, and the announcement of the acquisition by Broadcom of Symantec came out later in the year. It is concerning to see a vendor that had been so important to the community manage to lose so much goodwill within 18 months.

Vendors that are both strategically important but also provide an unsatisfactory experience will, logically, be targets for removal. The dramatic reversal in goodwill for Broadcom/Symantec should serve as an important warning to any vendor.

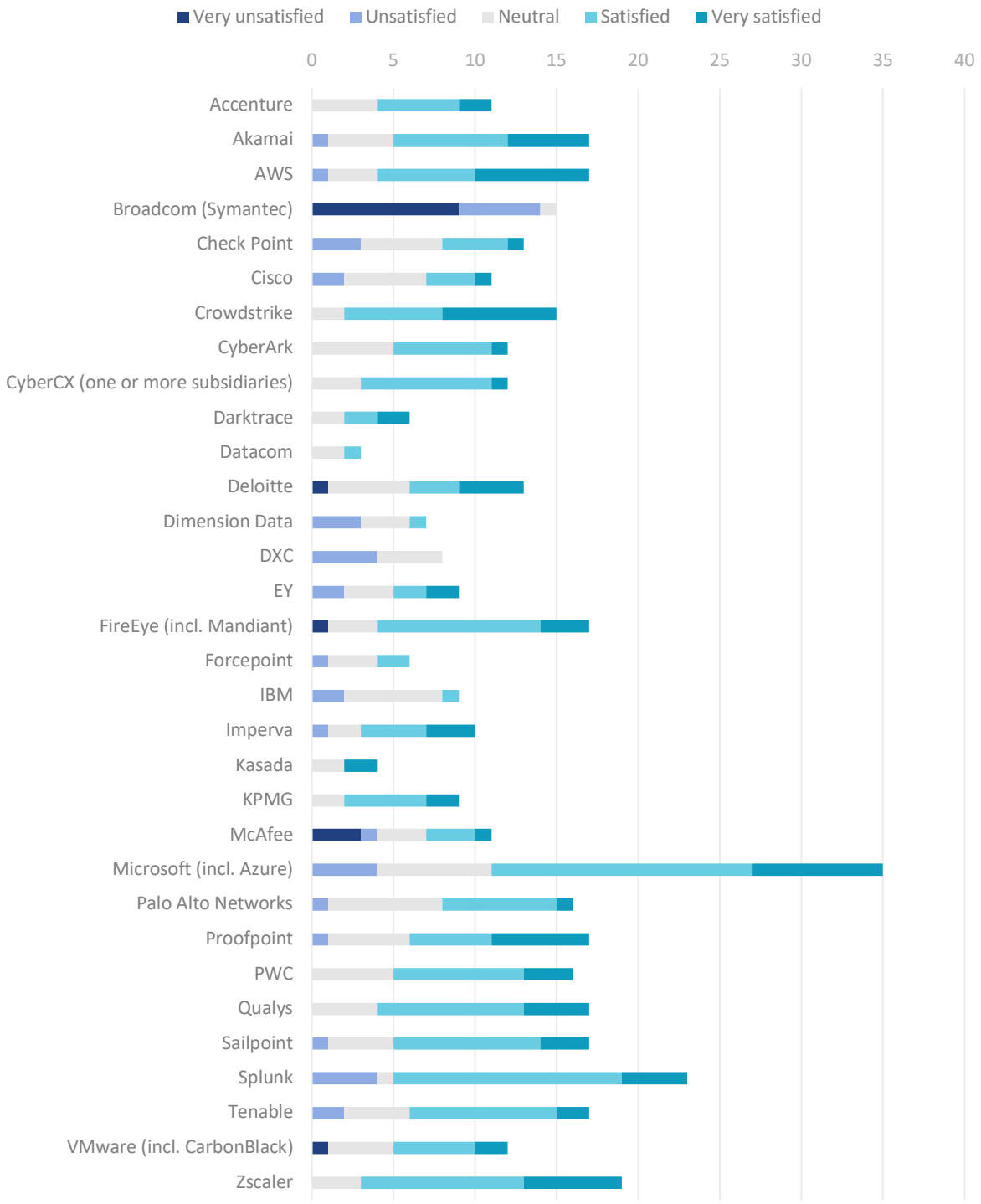

Figure 15: Satisfaction ratings by respondents of strategically important vendors. Listed alphabetically.

The performance of Crowdstrike, Zscaler and AWS, are worth highlighting. As shown in Figure 15,

- Crowdstrike performed remarkably. Not only did 26 per cent of the respondents select it in their top five, of those respondents 47 per cent rated their satisfaction with Crowdstrike as Very satisfied. This was the highest percentage among the 37 vendors. Further, 87 per cent of Crowdstrike respondents rated their experience as Satisfied or higher and this was the highest aggregated score for both Satisfied and Very Satisfied.

- Zscaler, too, delivered good satisfaction to its customers. 33 per cent of the respondents selected Zscaler as one of their top five vendors, and the 84 per cent of these respondents rated their experience as Satisfied or higher.
- AWS also performed exceptionally well. 30 per cent of the respondents select it in their top five, and of those respondents 41 per cent rated their satisfaction with AWS as Very satisfied. Further, 76 per cent of the respondents that selected AWS rated their satisfaction as Satisfied or higher.

Honourable mentions are also due to Qualys, Akamai and Proofpoint. Each of these vendors had a comfortable majority of the respondents that rated them in their top five vendors, also rating their satisfaction as Satisfied or higher. It is also pleasing to see CyberCX, a new Australian security service provider, performing well.

Overrated security controls

After the release of the 2018 Benchmark, one of the participants asked for a question 'if you could rip out one control, what would it be?' A number of other benchmark participants made the point that they would actively already be targeting these as they were likely to represent a waste of time and money.

So, we are delighted to include this question which elicited both insightful and controversial responses.

The normalised responses with three or more response are ranked below:

- Artificial Intelligence and Machine Learning (some respondents named one or the other, mostly they were used interchangeably), (n=5)
- Compliance, (n=4)
- Data Loss Prevention, (n=4)
- Firewalls, (n=4)
- Zero Trust, ("No vendor seems to mature enough yet to meet our needs"), (n=3)
- Awareness and end user training. ("necessary, but not hugely effective"), (n=3)
- Anti-virus, anti-malware, (n=3)

Sovereignty

With many of the geopolitical issues emerging as the world discovers interdependencies in every aspect of life; from supply chains, to cloud suppliers, knowledge workers, toilet paper supplies, and vaccines, we are also learning what it means to understand our common and connected wealth, as communities, nations, and regions.

While some countries appear to be driving toward Balkanisation of the Internet, others are seeking opportunity. With the creation of AustCyber in 2016 by the Australian Commonwealth government, Australia took an important step toward being able to commercialise the expertise it develops as it works to protect its people and organisations.

Australia has a phenomenal track record of inventions that changed the world: Wi-Fi, the Cochlear implant, the Black Box flight recorder, and the electronic pacemaker to name but a few.

As Australia grows its national capability in cyber security, which carries a considerable opportunity cost, it makes economic sense to also become proficient at exporting that expertise to the world.

But first, in order to be able to compete in the global marketplace, we need the local capabilities. Once we have the local capabilities, not only do our people and organisations benefit economically from the export, but we also help make the world a safer place online. And a safer world online is the definitional rising tide that raises all boats.

The CISO Lens partnership with AustCyber has resulted in AustCyber sponsoring this Benchmark and nominating it a companion document to AustCyber's Sector Competitiveness Plan. The goal for both organisations from the production of these documents is the facilitation of decision support with local, independent, evidence.

On behalf of AustCyber, we asked a series of questions in this Benchmark. These answers are intended to help suppliers in the local market understand what the priorities are for the security leaders of Australia and New Zealand's largest organisations.

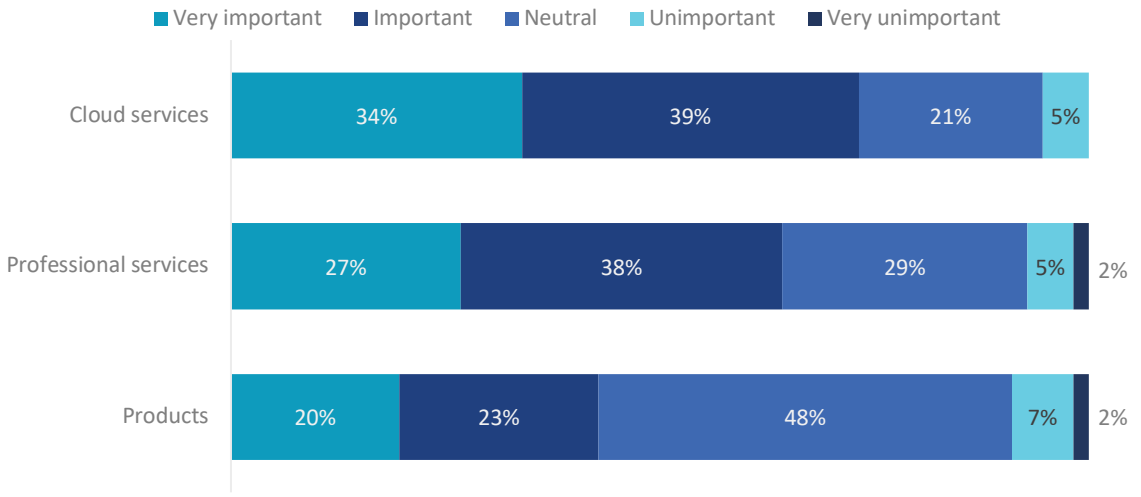

Figure 16: "How important is sovereignty to your selection criteria when procuring new cyber security and privacy related: Cloud Services, Professional services, Products". Rounded so may not total 100. (n=56)

Across the board – even when analysed by industry groups or size of security budget – the trend was for cloud services to be ranked the most important of the three categories for sovereignty, followed by professional services, and then products.

This is visible in Figure 16 where the Very important percentage starts at 34 per cent for Cloud services, drops to 27 per cent for Professional Services, and falls again to 20 per cent for Products. The same trend holds true for how the respondents ranked what they thought was Important.

The trend is most visible with the 21 per cent of the respondents reporting that sovereignty was of neutral importance for Cloud services, 29 per cent reporting it was of neutral importance for Professional Services, and then a sizable 48 per cent reporting that it was of neutral importance for Products.

Again, it is worth noting that this broad trend held true across industry groups, as well as size of security budget. In fact, the respondents with the top 8 budgets in this section (totalling $455 million) followed the same trend but considered sovereignty to be slightly less important than the average for the whole group.

This makes sense, as these organisations have larger budgets because they come from established risk averse organisations and have had years to design compensating controls to any perception of risk from extra-judicial product or services.

Selection criteria

The respondents were asked to select their top two selection criteria when considering a prospective supplier. 'Ability to demonstrate capability and capacity to solve/manage the problem at hand' was rated as one of the top two selection criteria by 77 per cent of the respondents (see: Figure 17).

Respondents show a strong preference for knowing that the proffered product and/or service will actually do what it claims. This strong preference to have assurance that the solution will work speaks to a deeper need that organisations do not have people, time or money to waste.

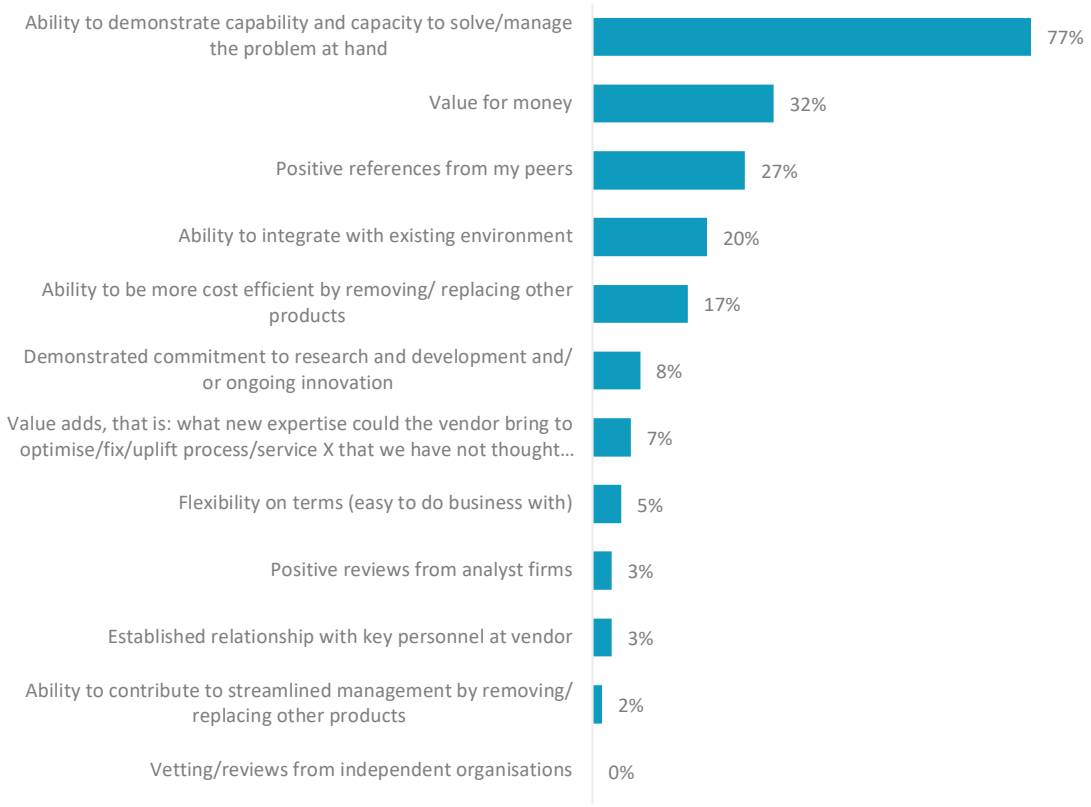

Figure 17: What are your top two selection criteria? Rounded. Multiple responses allowed. (n=60)

Any sale has, at its core, the need to minimise the risk of the transaction. Regardless of whether this is a CISO asking for additional budget for a project, or a startup trying to get a foot in the door; the person being asked to hand over money needs their concerns addressed. And, the greater the ask, the greater the risk that potentially comes with the transaction.

Consequently, startups aspiring to break into a market should review the rest of the priorities in Figure 17 and see where else they can address concerns. Especially on the back of 2020, demonstrating value for money will be critical. Positive references are vital, and the CISO Lens community is always keen to share what works. Naturally, ability to integrate with the existing environment is important.

Note that the respondents were asked to limit themselves to their top two selection criteria, and even 'Ability to be more cost efficient by removing/replacing other products' was still nominated by 10 respondents as one of their top two selection criteria.

Impact of COVID-19 pandemic on vendor relationships

Forty respondents provided information in response to this question, and 83 per cent noted that there was no, or minimal, change.

Many of the respondents' comments reflected this quote, "COVID-19 highlighted our reliance on vendors and the need to know more about their operations and business continuity."

One respondent noted, "We have discovered that many vendors are stretched to provide quality resources given the volume of demand. We have identified which vendors we can rely on for their commitments."

During the peak of the pandemic, many CISO Lens member discussions touched on the challenge that overseas managed services providers were experiencing. This could range from staff t used to working in call centres with company provided equipment being sent home and expected to continue working on their own equipment in whatever home environment they were in – from shared accommodation, to dealing with home schooling, to poor internet connectivity.

On one group call, one member stated, "Our BCP (Business Continuity Plans) assumed we could go to another building and keep working normally there, but that's off the table. The same is happening for the MSPs."

Fortunately, one Government respondent noted that as part of the response to the economic impact of the pandemic, they were choosing to increase their business with local suppliers.

Methodology

In September, CISO Lens invited 74 cyber security executives to participate in our 2020 Benchmark. Within the time window available for data collection, 62 of these executives were able to participate.

The respondents are both CISO Lens members, and non-members.

The Benchmark was based on many of the questions from our 2019 report. All questions were optional.

All information was exclusively collated, normalised, analysed, presented and reported by James Turner, of CISO Lens.

We are deeply grateful to the participants for sharing their time and insights, and to those participants who also provided feedback on our draft reports.

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 and Chief 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