Securing Australia's education institutions

How universities, TAFEs and school systems are responding to the escalating cyber security threat

Author: Brad Davies, Managing Director, Vector Consulting **Date:** July 2019

Independent research undertaken by Vector Consulting

Commissioned by Cisco

VECTOR consulting

Context and approach

The education sector is more exposed than most when it comes to opportunities and risks presented by cyber security.

On one level cyber security represents a growth market for universities and TAFEs, particularly given the projection that 3.5 million cyber security jobs are likely to go unfilled globally by 2021[1]. The education sector is responding with course offerings, from Graduate Certificate through to Post-Doctoral levels, albeit not at a pace that meets the market. It's also creating opportunities for research collaboration with industry, with the Cyber Security Cooperative Research Centre (CSCRC) one example.

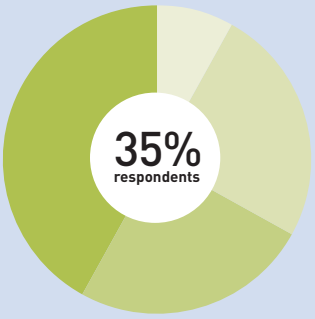
On another level cyber security also presents major risks. Educational institutions are particularly challenging to protect due to the high volume of unmanaged and personal devices that connect to their networks. This makes it complex to protect personal student data, employee records, commercial in confidence data and research IP. Increasingly, institutions also ingest data from industry partners and governments which must also be protected. The fact universities and training institutions offer cyber security courses and research IP – thereby positioning them as experts – makes them even more of a target for potential attackers.

At the same time the education sector is being forced to embrace technology change in administration, teaching and learning, student engagement and research. Education institutions are having to deliver more services to more stakeholders, and to deal with larger and more unstructured datasets. Digital is no longer a tool for institutions, it is driving strategy.

Vector Consulting was commissioned by Cisco Australia and New Zealand to better understand how universities, training colleges and K12 systems were perceiving the cyber security threat and mitigating risks through changing practices and organisation culture. The study involved desktop research, targeted interviews and a comprehensive survey that captured responses from half of all Australian universities and TAFEs, as well as K12 perspectives.

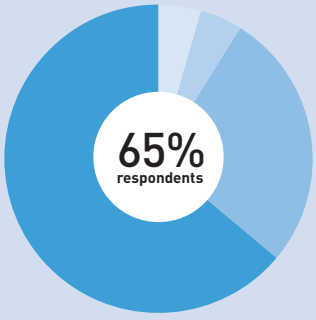
The study included perspectives from technology and non-technology roles

Role in organisation



Non-technology focused role

- COO or equivalent 41.67%
- Line of business 25%
- CISO or equivalent 25%
- Policy role 8.33%



Technology focused role

- CIO 63.64%
- Infrastructure director/manager 27.27%
- Specialist cyber security role 4.55%
- Other technical role 4.55%

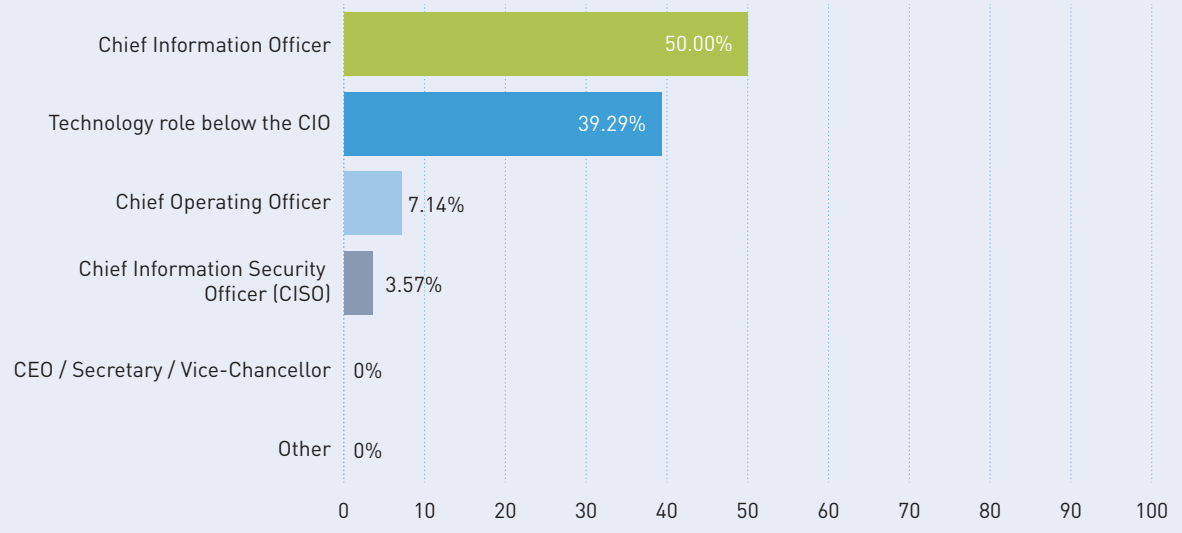
The responses included approximately one-third from non-technology personnel, with the majority of those being Chief Operating Officers or Line of Business roles. The technology responses were dominated by Chief Information Officers (64 %). The study had broad geographic representation.

How institutions are preparing themselves to combat security threats

One important decision for organisations is how to structure internally.

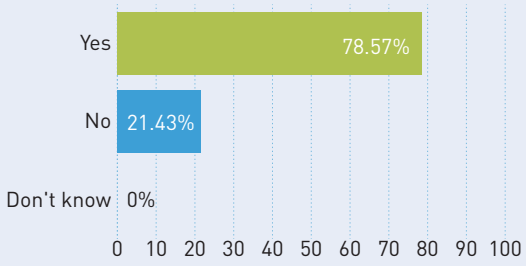
The education sector has adopted a different approach to the most progressive industry sectors from a cyber security perspective, such as banking and finance and insurance. In those sectors it is typical for the most senior cyber security expert to report to a Chief Information Security Officer who tends to be more focused on data than technology. This is in sharp contrast to universities, TAFEs and K12, where the CIO dominates from a reporting line perspective (50%). Almost 40% of institutions indicated that the most senior cyber security expert reported to a technology-focused role below the CIO.

Who does the most senior cyber security expert directly report to?

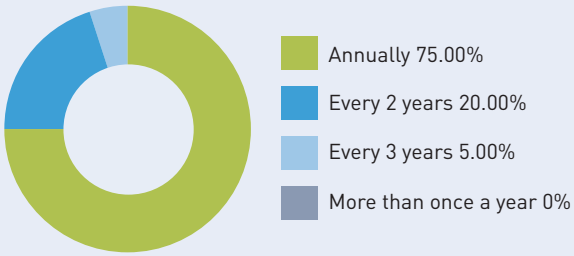


The existence and currency of an organisation's cyber security strategy is also revealing. While the vast majority do have a strategy – and most of them update it regularly – an alarming 21% do not.

Does your organisation have a documented cyber security strategy?

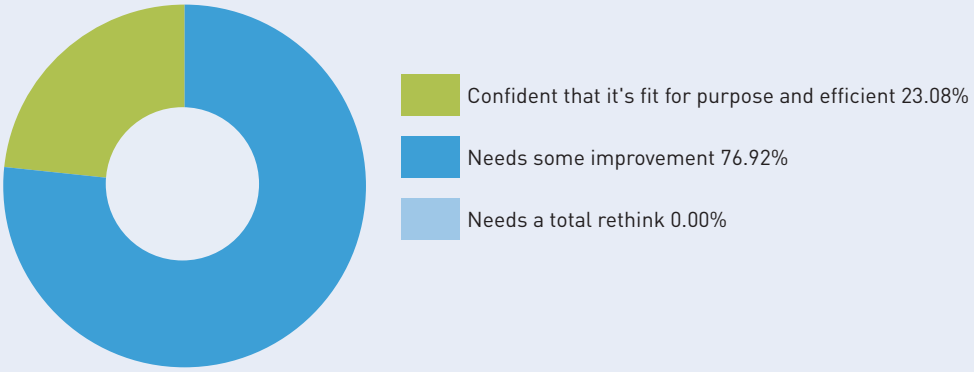


How often is your cyber security strategy refreshed?



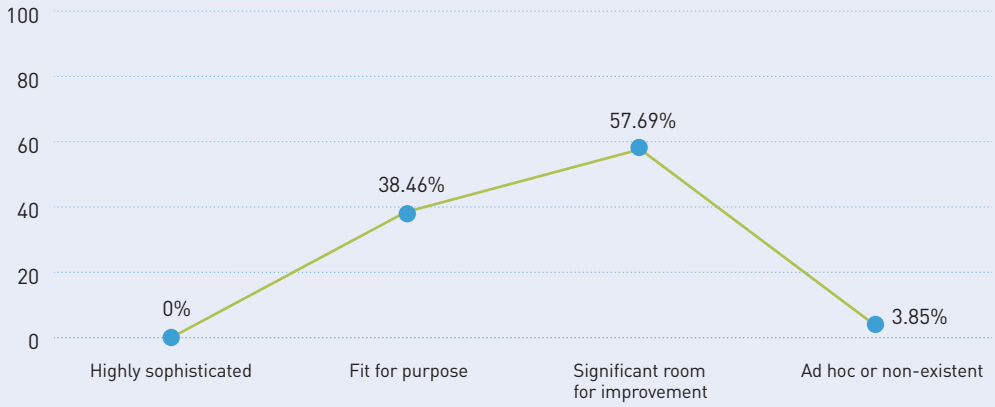
Perhaps even more revealing is the level of confidence in those strategies. The vast majority of organisations suggested their approach to cyber needed improvement and only 23% thought their approach was both effective and efficient.

What is the level of confidence in your institution's current approach to cyber security?



This was reinforced by sentiment about the data protection policy approach where no organisation self-described as highly sophisticated and 58% thought there was room for significant improvement.

Which statement best describes your data protection policy and approach?



A changing landscape: where risks and threats are coming from.

The threat landscape is changing.

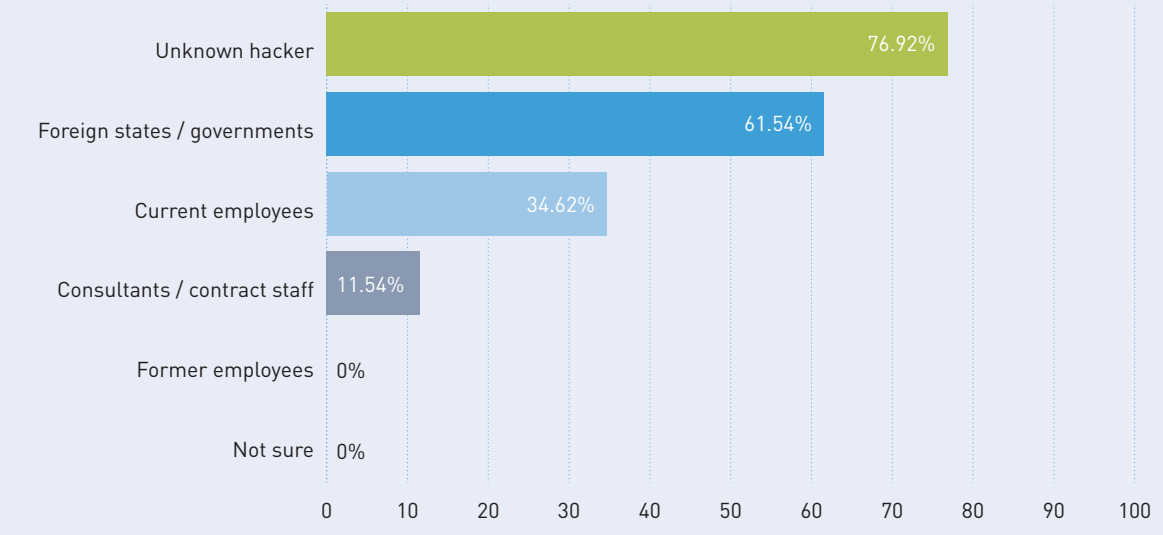
The proliferation of the Internet of Things (IoT) will connect 50 billion devices, sensors, vehicles and appliances to the network and drastically increase the attack surface. IoT devices often contain computers that could be used to download files, compile code and execute arbitrary commands. As a result, an attacker who gains control of the device could use it for other malicious purposes, such as downloading and compiling malicious code to run on the device. Another aspect of IoT that is under-estimated is how often the average user connects their smart device to the network, but forgets to update those devices. Few people think, "Hey! It's the first Monday of the month I should check and see if my TV needs to be patched!" As a result, IoT devices that do not have an easy-to-use notification and updating mechanism are prone to being left alone, out of date, and vulnerable to compromise.

The rise of 'dev ops' and focus on speedy solutions can also have negative consequences. In some cases, the need to do things quickly reduces scrutiny on projects, compromises what's ultimately delivered and creates a way in for attackers.

There are more attackers, they are more sophisticated and have access to more dangerous tools – many of which can be bought from online marketplaces. Machine learning is also allowing attackers to scale and accelerate the deployment of threats, and helping them stay ahead of target institutions. While attackers are generally seeking access to personal and commercial information, they're also targeting infrastructure assets, which can be on-sold on the black market.

When it comes to threats most organisations agree that the threat generally sits outside of their environment via unknown hackers and foreign states. However, just over a third of institutions see their primary threat coming from current employees (35%) or consultants / contract staff (12%).

Who is your primary threat from a cyber security perspective?



High profile cyber security attacks in the education sector

The education sector was ranked the worst out of 17 industries from a cyber security threat perspective. IT consultancy SecurityScorecard[2] undertook a 2018 Cyber Security Report, concluding that the education industry is not taking many of the necessary steps to protect students from cyber vulnerability. According to the study, the main areas of cyber security weaknesses in education are application security, endpoint security, patching cadence and network security.

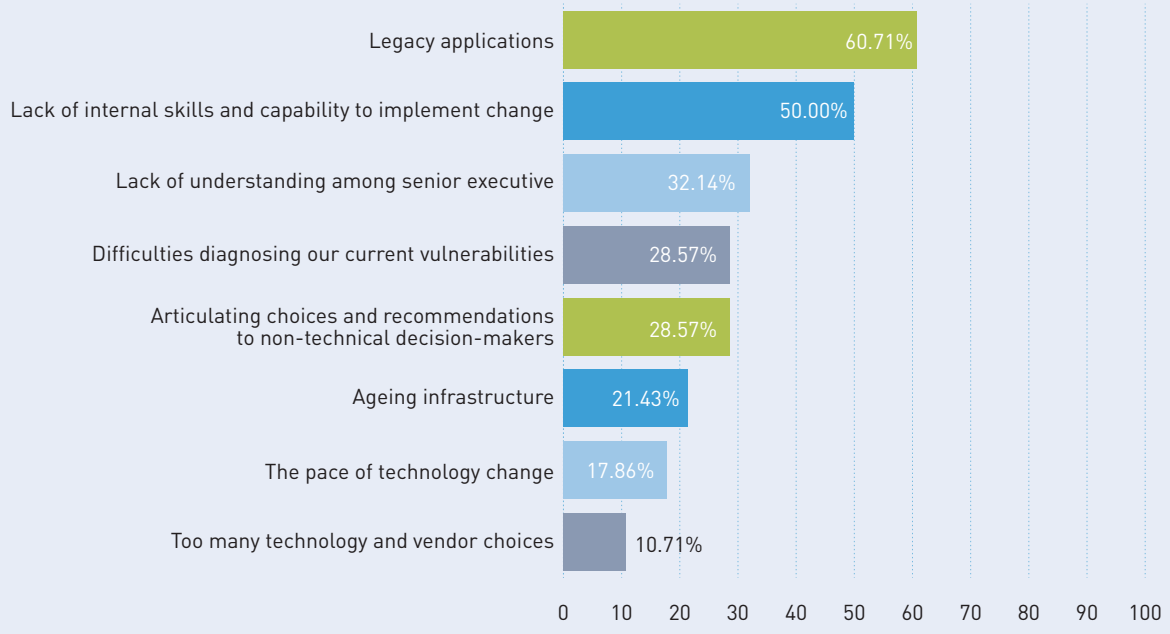
	Nature of attack	Damage and Impact
2019 ACU Australian Catholic University	An email pretending to be from the ACU tricked users into clicking on a link or opening an attachment and then entering credentials into a fake ACU login page.	Staff login credentials were obtained successfully via the phishing email and were used to access the email accounts, calendars and bank account details of affected staff members.
2019 Australian National University	Information accessed in the data breach included: names, addresses, dates of birth, phone numbers, personal email addresses, emergency contact details, tax file numbers, payroll information, bank account details, passport details and student academic records.	Attackers accessed up to 19 years' worth of sensitive data. The university has confirmed an estimated 200,000 people have been affected by the hack, based on student numbers each year and staff turnover.
2016 University of Calgary	A ransom was demanded, and paid, when attackers compromised university IP. Investigators allege the malware encrypted data and files, and the suspects demanded payment to restore access to affected systems in what the FBI called "21st-century blackmail".	The university paid a ransom of $20,000 after the 2016 attack to preserve an option to restore critical research data.
2018 300 global universities	Over 300 universities worldwide suffered from a giant cyber-attack organised by nine Iranian hackers. The suspects infiltrated 144 US universities, 176 universities in 21 other countries, 47 private companies, and other targets such as the United Nations and the US Federal Energy Regulatory Commission. The attacks used spear-phishing emails to trick professors and other university affiliates into clicking on malicious links and entering their network login credentials.	According to the official information, 31 terabytes of "valuable intellectual property and data" was exposed. This case became one of the biggest hacker campaigns. The DOJ says the hackers stole 31 terabytes of data, estimated to be worth $3 billion in intellectual property.
2018 UCL	UCL is a centre of excellence in cyber-security research, a status awarded by the GCHQ intelligence and monitoring service. The central London university says a "widespread ransomware attack" activated by a staff member clicking on a "compromised" website which created a pop-up page might have spread a malware infection.	Potential exposure of commercially sensitive research.
2015 University of Nebraska	A student at the University of Nebraska compromised the university's PeopleSoft system and accessed the database so that Chadron State, Peru State and Wayne State colleges were also impacted because two years earlier Nebraska college system started using a shared student information system.	Critical information of 654,000 students and employees was exposed. Moreover, it led to leakage of the bank account details of 21,000 people.

In the wake of a breach, CISOs[3] are most concerned about operations (36 per cent), customer retention (33 per cent) and brand reputation (32 per cent), according to Cisco's 2019 CISO Benchmark study.

"Breaches cost more than money. A breach impacts trust, and when a brand is impacted this can result in challenges in customer retention." – Steve Moros, Cisco

In terms of the attack surface, organisations view their legacy applications as the primary vulnerability, while legacy infrastructure also presented major risks. Challenges accessing and retaining internal cyber capability was the second-biggest risk, along with low levels of cyber-literacy among executives and getting an accurate picture of the organisation's vulnerability to a successful attack.

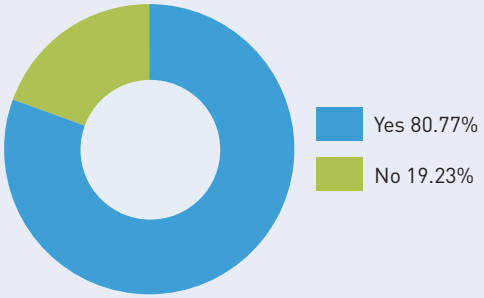
What creates the biggest risk to your organisation from a cyber security perspective?



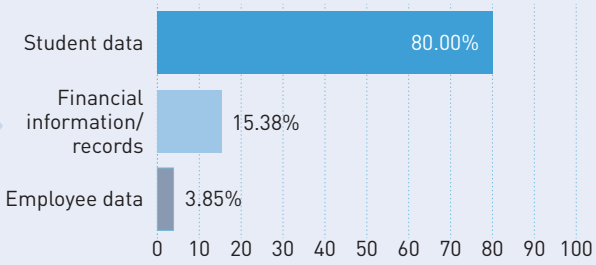
One of the first questions an organisation needs to ask in relation to data protection is 'where are the crown jewels'?

Because the cyber attack surface is large, and growing, it's critical that organisations prioritise the importance of different types of dataset. In the education sector the response was mixed; while 80% knew where the crown jewels were, one in five did not. Overwhelmingly those crown jewels tend to be related to student data and research IP more than financial records or staff data.

Do you have a clear understanding of what your 'crown jewels' are from a data perspective?



What type of data gets the highest priority when it comes to cyber security?

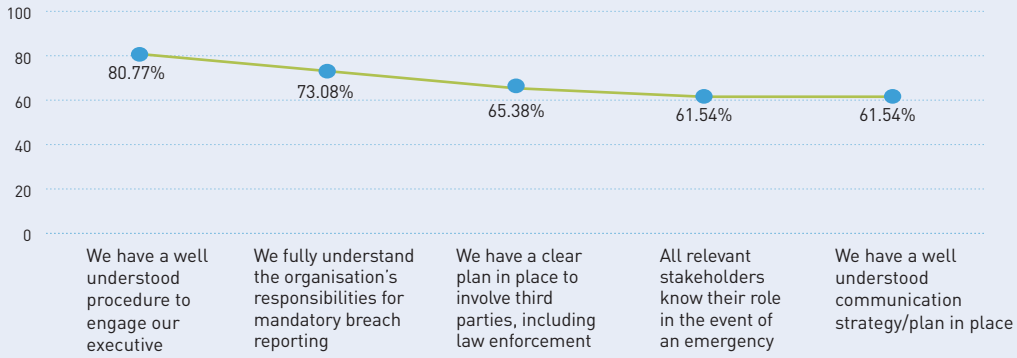


Preparedness for an incident

On the surface, most organisations suggest that they are broadly prepared for a cyber security incident. However, some results are concerning at the more granular level. This is revealed when you consider the inverse commentary to the findings below:

- 27% don't understand their responsibilities in relation to mandatory breach reporting
- 35% don't have a clear plan in place to involve third parties in an incident
- ~ 40% of organisations say relevant stakeholders don't understand their roles in an emergency or have a well understood procedure in place

Which of these statements are true of your organisation in the event of a cyber security incident?



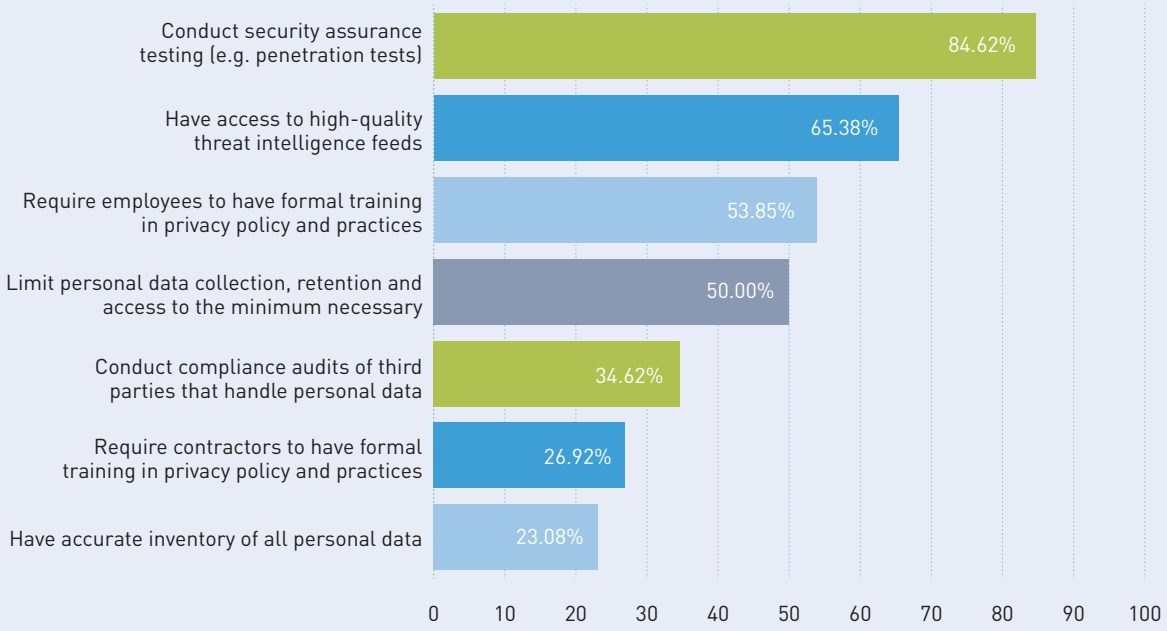
The preparation phase was also identified as offering greatest room for improvement compared with during an incident or in the clean-up phase.

Where do you think your organisation can make the greatest improvements?

The reason for the low confidence is revealed by the some of the specific responses in terms of what organisations are actually doing to prepare themselves. While security assurance testing and access to high-quality intelligence feeds are commonplace (as you would expect for organisations that hold so much sensitive data), at the other end of the spectrum many organisations are thoroughly under-prepared. To demonstrate:

- 77% of organisations do not have an accurate inventory of personal data
- 73% do not require contractors to have any training in privacy policy / practices
- 65% do not audit third parties who hold sensitive personal data on their behalf

Which of the following statements is true of your organisation / agency?

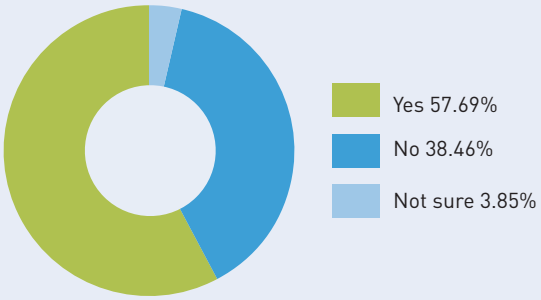


How organisations are responding

The logical priority from an organisational perspective is to resource and upskill its workforce.

Almost two-thirds of organisations increased their spending on cyber security in the most recent budget, and the average increase in expenditure was 30%. In some cases it was considerably more – up to 200%.

Did cyber security funding increase in your most recent budget?

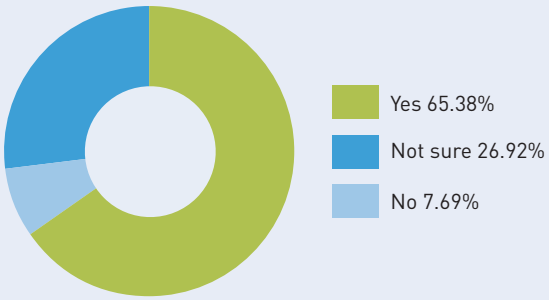


Average increase in spending was 30% and for individual institutions as high as 200%

Those increases will be dwarfed by the forecast expenditure in coming years. Only 8% of organisations believed that their organisation wouldn't increase spending, and the average quantum of that increase was approximately 40%. One university forecast an increase of 300% in spending on cyber security in its next budget, and several said it would be in the range of 200-300%.

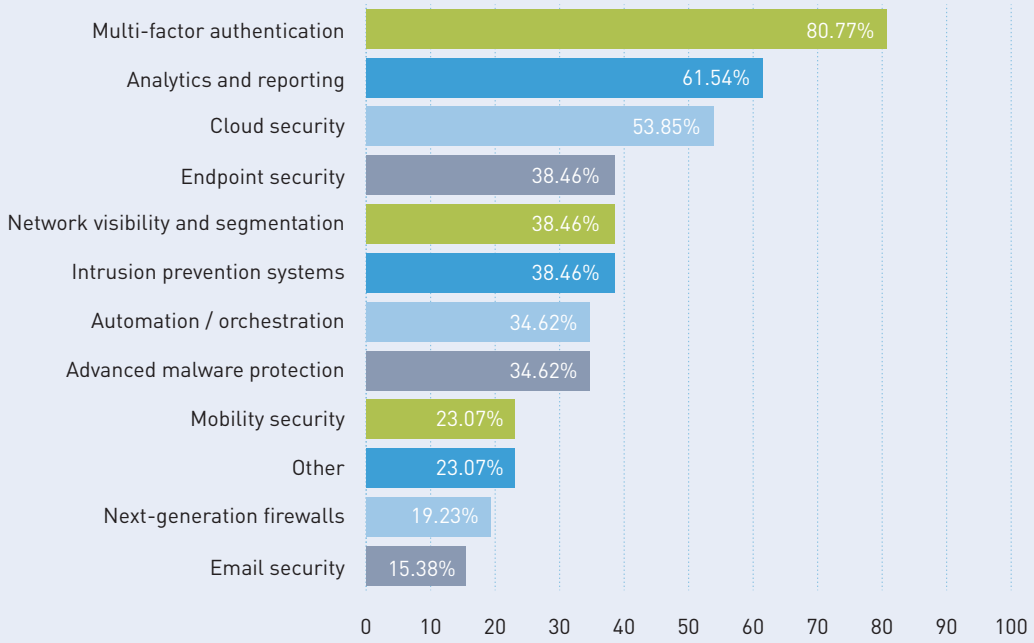
More interesting than the aggregate numbers are the planned focal points for expenditure. Multi-factor authentication dominated as the specific issue that will get greater funding support (80%), followed by analytics and reporting (62%), cloud security (53%) and network visibility and segmentation (38%). One surprising finding was that email security would get very little additional resourcing despite it being one of the critical gateways for cyber attackers.

Will you increase spending on cyber security next year?



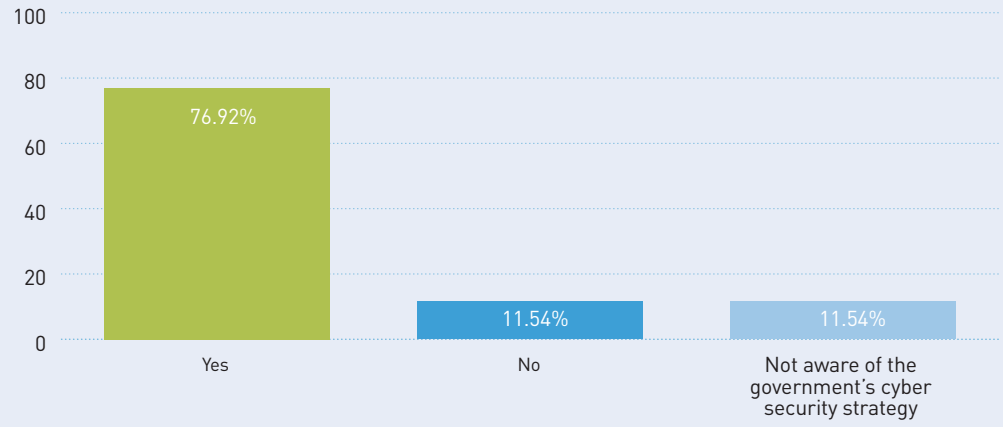
Average increase in spending is forecast to be 30-40% and for individual institutions as high as 300%

Which of the following security services will get more funding in the coming year?



One useful reference point to test the sophistication of a cyber approach is alignment to government strategy. All States and Territories, as well as the Commonwealth Government, have developed policies and frameworks for public sector organisations to guide their security response. Almost four in five educational organisations believe they are aligned, and 11% weren't aware of the existence of a government cyber strategy.

Are you aligned with the cyber security strategy of your State / Territory government?

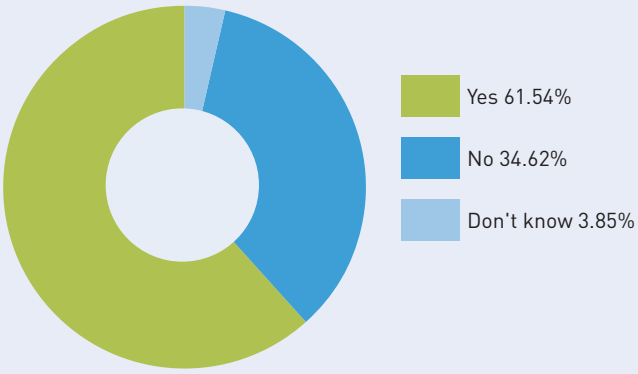


Scrutiny on cyber security function, and worst-case scenarios

While it's clear that senior executives are recognising the cyber security threat, the next logical question is whether the same is true for their board level representatives.

In separate studies conducted by Cisco we know that this is certainly the case in sectors such as healthcare and banking. Considering the range and seriousness of risks facing Boards, it's interesting to note that more than 60% of institutions consider cyber security one of the three top priorities at Board level.

Would you consider cyber security to be one of the top 3 priorities of your Board / Council / stakeholders?

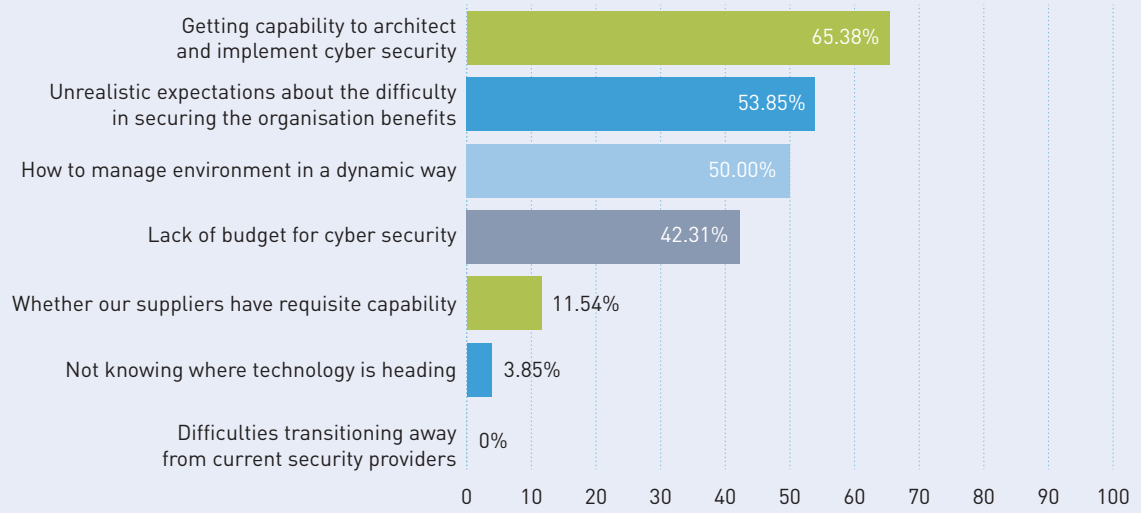


No doubt this scrutiny at Board level is creating sleepless nights for senior executives, as is the case in the private sector, where mandatory breach reporting is now adopted as a formal accountability at board level. The intensity of this scrutiny is manifesting in a range of ways, led by challenges assembling the capability required to architect and implement cyber security measures. This is compounded by a perceived lack of empathy for the sheer complexity involved in securing an organisation when attackers are highly sophisticated, heavily resourced and almost impossible to apprehend. For many organisations the response is to avoid 'big bang' projects and try to manage their environment in a dynamic way, which is clearly challenging in itself according to 50% of organisations.

References

[1] https://www.cnbc.com/2018/08/09/cybersecurity-jobs-non-technical-workers.html
[2] https://edscoop.com/education-ranked-worst-at-cybersecurity-out-of-17-major-industries/
[3] https://which-50.com/what-price-do-companies-really-pay-when-they-breach-consumer-trust/
[4] https://www.ibm.com/downloads/cas/861MNWN2
[5] https://www.cisco.com/c/dam/global/en_au/assets/pdf/cisco-cybersecurity-response.pdf

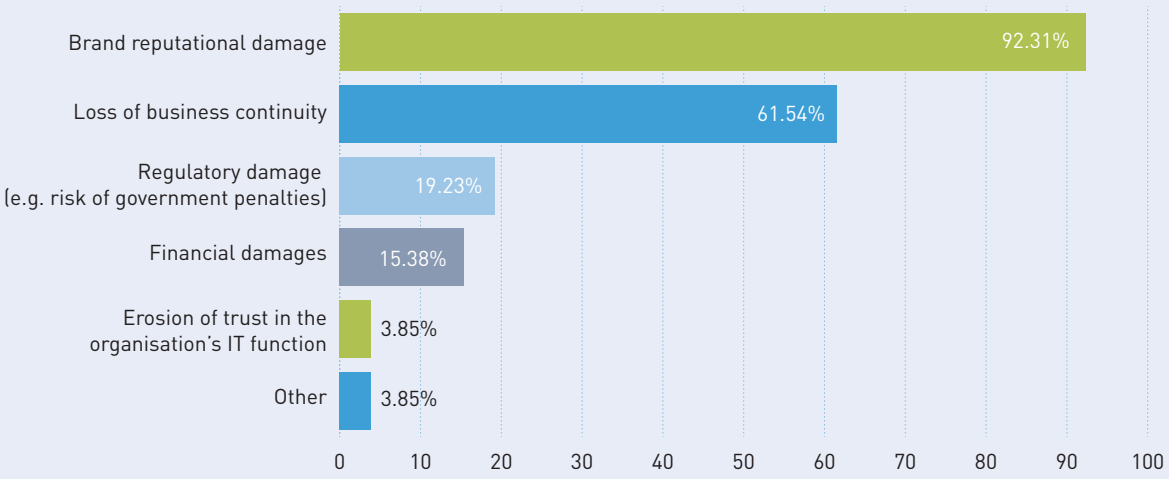
Which of the following cyber security-related issues keep you awake at night?



Should the worst happen it's interesting to ponder what a worst-case scenario looks like. For educational institutions the overwhelming fear was that a successful attack created lasting and deep brand reputation damage. This is not surprising given the competitiveness of education – particularly for higher and vocational education – most notably for international students. The current international education market in Australia is valued at >$30B, dominated by the brand-sensitive Chinese student market. Brand reputation damage would permeate far beyond students and would potentially impact on industry partnerships, student employability outcomes (particularly for cyber graduates), employee engagement / trust and government funding. Loss of business continuity was the next greatest fear.

Financial damage was a long way down the list in terms of concerns. This is despite the fact that cyber attacks reportedly cost the US economy between $59B and $109B annually, according to a White House report in terms of lost productivity, theft and extortion, and the average cost of a data breach[4] is $3.86 million (up 6% from the previous year). The potential cost to Australia could be as high as $17B[5].

What are your greatest concerns in the event of a major security breach?



Conclusions and recommendations

Security has to be embedded in the technology and organisational culture

One employee will always click on `the link', and attackers will generally find a way through the perimeter defence. The challenge is to ensure that the underlying infrastructure is in place when the inevitable happens.

Embedding security in infrastructure is increasingly common so threats can be detected early and responded to quickly. Approximately 24% of issues can be resolved by products alone, with the remaining 76% resolved by addressing people and process issues. Security is a complex capability to get right and cyber resilience hard to achieve. The starting point needs to be sourcing technology that reduces time to detect, and the time to remediate.

The fragmented nature of cyber platform investments, and the sprawl of isolated technologies that serve a single function, take organisations further away from their resilience goal. An integrated security architecture with threat intelligence and automation capabilities built into the network is critical.

Cyber security needs to be treated as active combat, not a checkbox exercise

One of the major challenges with cyber security is the fact that resilience is a moving target. Cyber security is an arms race with protagonists that are sophisticated and well resourced. Checkbox approaches to security aren't likely to be successful because the threats keep changing. Digital extortion is not only on the rise, the extortionists are also becoming more convincing.

One of the more insidious phishing campaigns has preyed upon recipients' fears in order to extort Bitcoin payments. Some campaigns claim that they caught the recipient on camera looking at pornographic web sites. Others include fake bomb threats. Ultimately, the threats are completely fabricated, all in the hope of tricking enough recipients into filling the attackers' Bitcoin wallets.

Office 365 phishing is also becoming more commonplace. An ongoing phishing campaign centred on stealing credentials from Microsoft Office 365 accounts after duping users into providing logins.

Visibility of the end-to-end information technology environment is critical

Information Technology and workloads are distributed. While it's not always possible or desirable to centralise all technology, organisations do need to maintain consistent security controls, and achieve visibility across the network, cloud and endpoints by adopting an integrated architectural approach to cyber security. The 'see once, block everyone' objective is only possible when an organisation has full visibility and control of its environment.

Be prepared...

There are a number of tactics that organisations can employ to prepare themselves and reduce risk. This starts with understanding where the crown jewels are from a data perspective, and ensuring that responsibility for protecting them is everyone's responsibility. Organisations can address basic vulnerabilities – such as overly generous database administration rights – and implement internal phishing awareness campaigns to raise awareness and change behaviours.

Six ways to reduce risk

There's a lot of cyber security challenges to overcome, but following the best practices below can reduce exposure to emerging risks, slow attackers' progress and provide more visibility into threat landscape.

- Implement first-line-of-defence tools that can scale, like cloud security platforms
- Emply network segmentation to help reduce outbreak exposures
- Perform deeper and more advanced analytics
- Review and practice security response procedures
- Back up data often and test restoration procedures
- Access timely, accurate threat intelligence data and processes

Choose the right partners

Given the combative nature of cyber security you need partners and a high level of trust, particularly at an infrastructure level. According to Cisco's 2019 CISO Benchmark Study approximately 17% of organisations were dealing with 20 vendors or more. While it's unrealistic to expect one vendor to handle an organisation's requirements, a robust, scalable and proven infrastructure partner is critical.

High-quality security threat feeds are an important part of the cyber armoury

The key to detecting and remediating is having platforms that leverage threat intelligence to increase visibility and ability to detect known and emerging threats immediately to minimise impact. The most valuable threat data is aggregated and identifies patterns at micro as well as macro scale. Cisco's Talos organisation demonstrates the sheer volume of data that needs to be monitored. Its Intelligence Group is one of the largest commercial threat intelligence teams globally and analyses 16 billion Web queries daily. The group comprises over 300 researchers, in addition to a team of analysts and engineers using telemetry and systems to create accurate, rapid and actionable threat intelligence for organisations.

Vector Consulting is a specialist strategy and technology consulting firm based in Melbourne. Founded by Brad Davies, Vector has advised governments, universities, TAFEs and peak bodies on the impact of technology in education. Vector Consulting has a long-standing relationship with Cisco.

Contact details:

Vector Consulting
Brad Davies
Managing Director
brad@vector-consulting.com.au

VECTOR
consulting