FOUNDRY MARKETPULSE:

CYBERSECURITY TOPS 2023 IT CHALLENGES

WHAT'S INSIDE:

- The surprise #1 spending priority for 2023
- Why email is still a key attack vector
- The top challenges faced by IT in 2023
- IT workforce challenges
- Top delivery priorities for 2023

EXECUTIVE SUMMARY

Investment in cybersecurity is the top priority for Australian companies in 2023, new Foundry Marketpulse research for Kaseya has shown.

The survey, conducted in December 2022, showed that half of all respondents ranked cybersecurity and data protection in their top 3 company challenges.

This result follows numerous major breaches of Australian companies in 2022, which led to significant reputational damage for the target companies, pressure from state and federal government intervention and even legislative change.

Australian companies were already facing a significantly heightened security compliance environment under the Positive Security Obligations, but following the high-profile breaches at Optus and Medibank the Albanese Government has introduced significantly tougher penalties for serious data breaches.

The new legislation increases penalties from their previous maximum level of $2.2M to the greater of $50M, three times the value of any benefit obtained through the misuse of the breached information, or 30 percent of a company's adjusted turnover in the relevant period.

The reputational shock factor of the major data breaches, coupled with this impending new regulatory landscape is clearly heavily influencing the priorities of organisations surveyed by Foundry Marketpulse.

Capacity and speed of network infrastructure is the second highest ranked priority for IT departments in 2023 at 34%.

Half of all organisations say they will increase their IT security budget for 2023, and 62% of larger companies with 500+ employees said their IT security budget was increasing this year.

THE SURPRISE #1 SPENDING PRIORITY: EMAIL PROTECTION

Given cybersecurity is the top challenge faced by Australian companies, it makes sense that IT teams are planning to spend up to bolster their security.

However, the top priority for CIOs isn't to truck in container loads of additional firewall devices, or investing in bleeding edge threat detection technologies. Instead, they're looking to secure something much more fundamental: email.

Email security, including phishing protection, tops the list of intended spending for Australian and New Zealand companies, with more than a third (36%) ranking it as their highest priority area for investment in 2023.

WHY EMAIL IS STILL A KEY ATTACK VECTOR

Although email is not a 'zero day' vulnerability space where hackers are exploiting just-discovered vulnerabilities in software that haven't yet been patched, it remains a wide-open door in company defences.

The trouble with email is that it allows criminals to communicate easily with employees and manipulate them using non-technology-based social engineering techniques. This allows criminals to essentially be 'invited in', allowing them to jump over network boundary defences.

Their objective is to trick users into sharing a legitimate username and password or changing payment details for an existing supplier to the criminal's bank account.

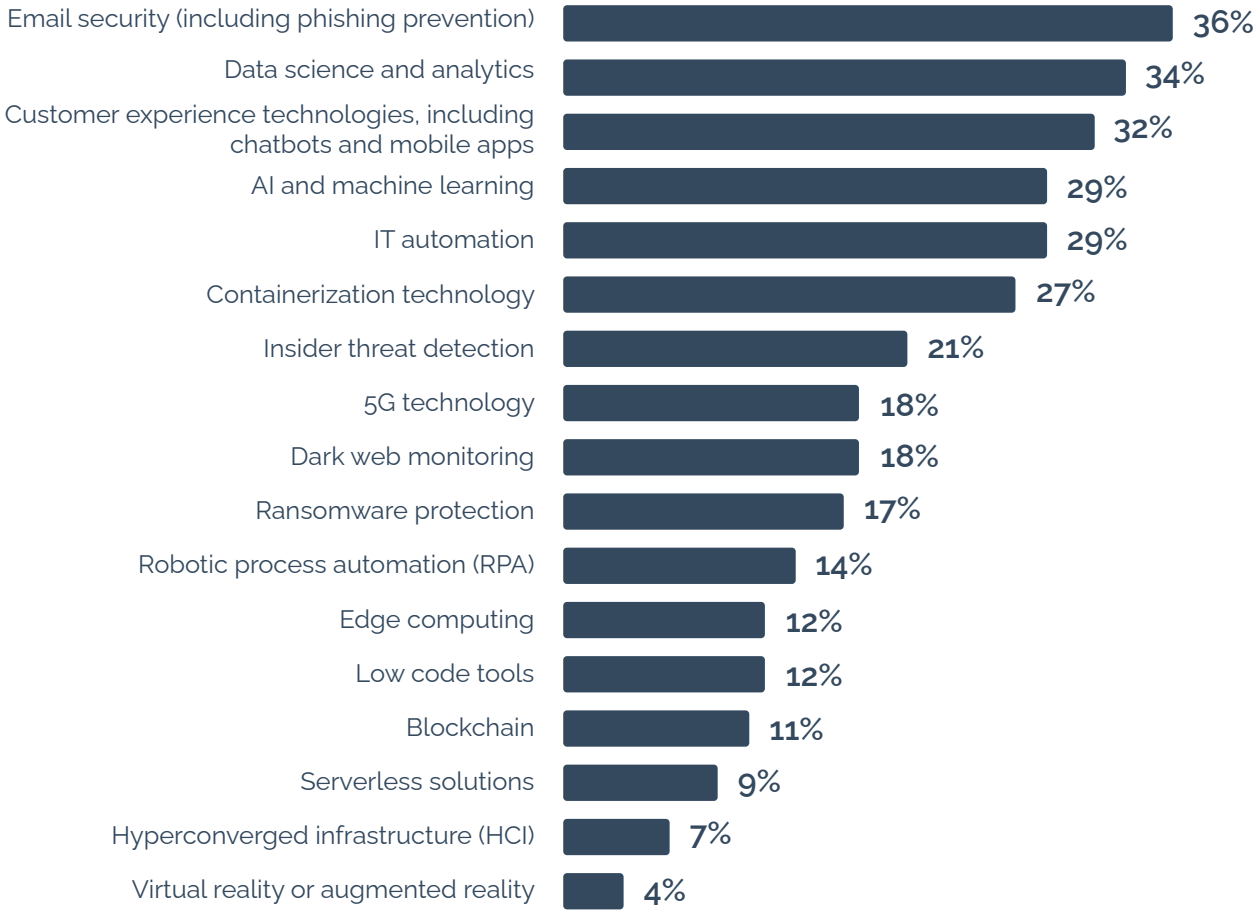
Phishing and spear phishing, business email compromise (BEC), account takeover (ATO), identity spoofing, malware and ransomware can all be delivered by email.

The recent breakthroughs and productisation of generative AI mean that email scams are likely to become much harder for staff to detect in the next 12 months.

Fluent text generation engines like GPT3 (the underlying tech of OpenAI ChatGPT) are publicly available, which may allow scammers whose first language is not English to target Australian and New Zealand companies with fluently written scam emails, linking to perfectly written scam web pages.

Email security now requires a broad, multi-layered approach combining training, awareness, content analysis of both inbound email and employee responses, and analysis of the target content from URLs that are provided in an email. An email security solution, such as Graphus or Bullphish ID, can also play a pivotal role in bolstering an SMB's security position by improving end-user awareness training.

TECHNOLOGY INVESTMENT IN 2023



THE TOP CHALLENGES FACED BY IT IN 2023

Across the board, cybersecurity and data protection tops the charts of greatest challenges faced by IT organisations, with 50% of respondents saying this was their biggest current issue.

However, concern over capacity and speed of network infrastructure was significant in smaller companies, with 43% ranking it in their top 3, compared to only 26% of larger companies.

The evergreen issue of trying to constrain spending on infinitely elastic cloud resources comes in an equal third, with 25% of respondents naming that as a major challenge, along with the complexity of managing multiple cloud environments.

ISSUES IT NOW HAS A GOOD GRIP ON

Earlier in the pandemic, issues such as supporting workforces remotely were of significant concern to IT teams, which found themselves having to rush out planned deployments of video conferencing software and collaboration tools.

Perhaps not surprisingly, IT teams now feel like they have thoroughly got their arms around the issue of supporting users working remotely long term, with only 4% of respondents naming this as a top challenge.

Process documentation and planning is of similarly low concern, with only 5% of respondents listing that as being in their top three issues.

IT WORKFORCE CHALLENGES

The federal government's National Skills Commission recently added 10 IT roles to the Skills Priority List, including roles such as ICT Business Analyst, Web Developer and Network Administrator.

This list is used to inform the government's vocational training plan with 450,000 fee-free TAFE places, and its skilled migration program which provides permanent residency for workers from other countries who fit the criteria of the skilled worker role.

However, Skills Minister Brendan O'Connor, has acknowledged that skilled migration "is a part of the solution but it's not the only part, it's not a binary choice".[1]

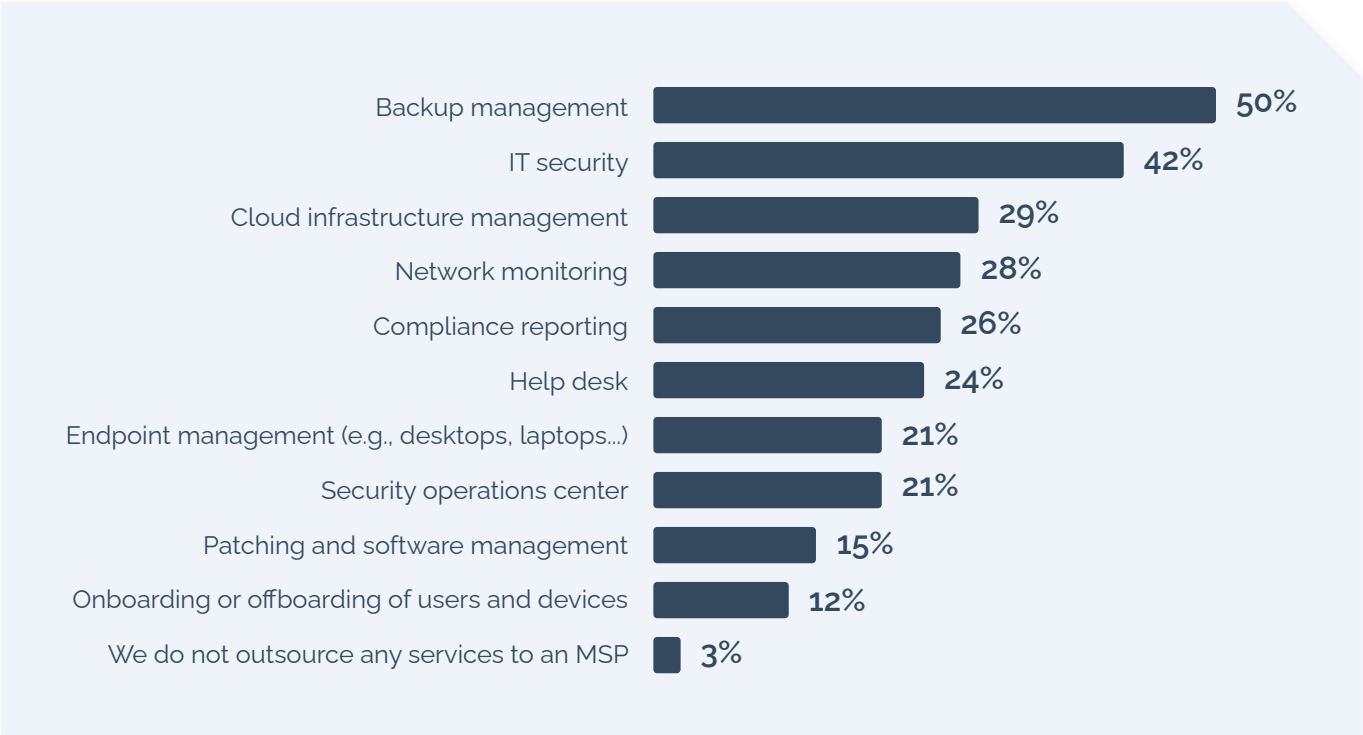
The Foundry Marketpulse survey found these workforce capacity limitations evident – with the vast majority of survey respondents (80%), regardless of company size, having fewer than 50 internal IT staff.

As a result, nearly every respondent (97%) stated that their organisation outsourced at least one function or task to an IT managed service provider (MSP).

The largest proportion (50%) were using MSPs for backup management, which was even more evident in larger organisations, with 64% outsourcing this critical but laborious function.

42% of respondents also outsource IT security – a highly specialised field where competition for talent can be intense.

[1] Govt adds 10 more IT occupations to shortage list, Australian Computer Society, 6 October 2022, https://ia.acs.org.au/article/2022/govt-adds-10-more-it-occupations-to-shortage-list.html



The largest difference between big and small companies in their outsourcing approach was around cloud infrastructure – just 14% of smaller companies were outsourcing this compared to 41% of larger organisations.

Smaller companies were also more likely to outsource their helpdesk function – 33% compared to just 17% of larger organisations.

REACTIVE vs PROACTIVE vs STRATEGIC

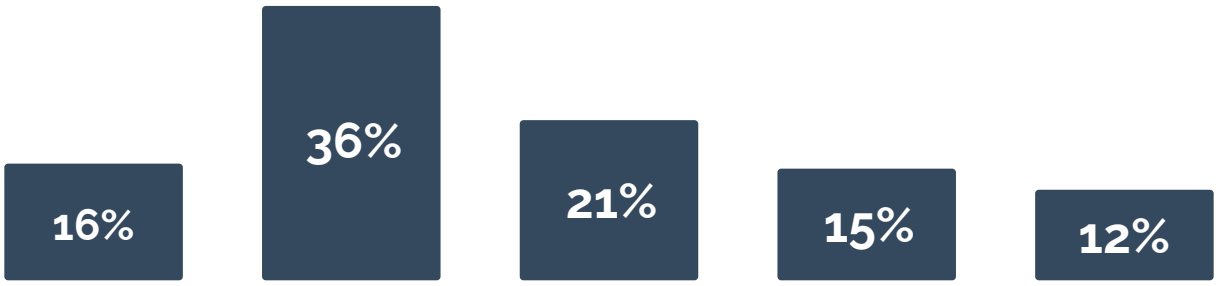
Respondents' IT organisations had widely varying perceptions of the level of service they were managing to provide to the business.

Only 21% said they believed they were operating proactively, with 52% saying they considered themselves to be just 'efficient' or 'reactive'.

Even fewer said they were aligned with requirements of their service-level agreements (15%) or strategic – achieving operational IT excellence and taking a strategic role in driving business innovation (12%).

The data shows that IT teams continue to have a heavy workload and are often only afforded very limited time for strategic development and fine-tuning delivery against key performance indicators.

APPROACH TO IT MANAGEMENT CAPABILITIES



Reactive
Responsive to individual challenges and requests

Efficient
Systematic in our approach to solving known issues and dealing with daily tasks

Proactive
Proactive in our approach to IT management, automating repetitive tasks and many remedial actions

Aligned
Actively track and manage against service-level agreements (SLAs) or availability/ performance expectations

Strategic
Achieve IT operational excellence and take a strategic role in driving business innovation

TOP DELIVERY PRIORITIES FOR 2023

What companies are prepared to spend money on is sometimes misaligned with what IT organisations are expected to deliver.

While Foundry Marketpulse found that email security was the area of greatest interest for investment, the largest proportion of survey participants (41%) named cloud migration as the top priority for IT to deliver in 2023.

This was closely followed by a focus on improving IT security overall (39%) and increasing productivity through automation at 35%.

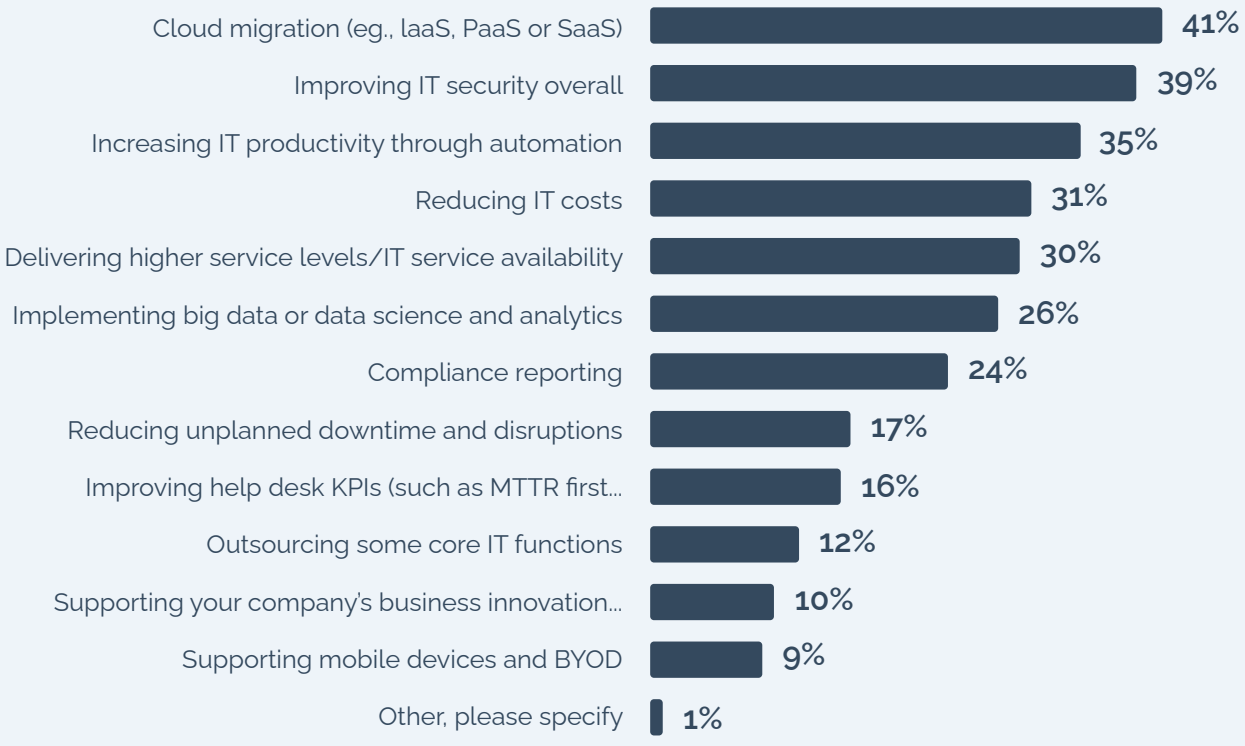
These focuses are clearly reflected in respondents' budget priorities for the coming year – 52% of companies said they were increasing spend on cloud services, and 50% on security services. These results were even more marked in larger companies of 500+ employees, with 62% of respondents saying their companies were increasing spending in these areas.

In all other areas of spending, the majority of respondents said they were keeping spending the same.

However, there is a clear disparity in IT budgets between small and large companies. Small to medium-sized businesses reported a median annual budget of only $644K, while larger companies reported a median of $5.1M. This creates a much stronger focus on price for smaller companies (47% at smaller companies rather than 38% of larger companies).

CHALLENGES IN INFRASTRUCTURE AND SECURITY ARE BEING PRIORITISED FOR 2023

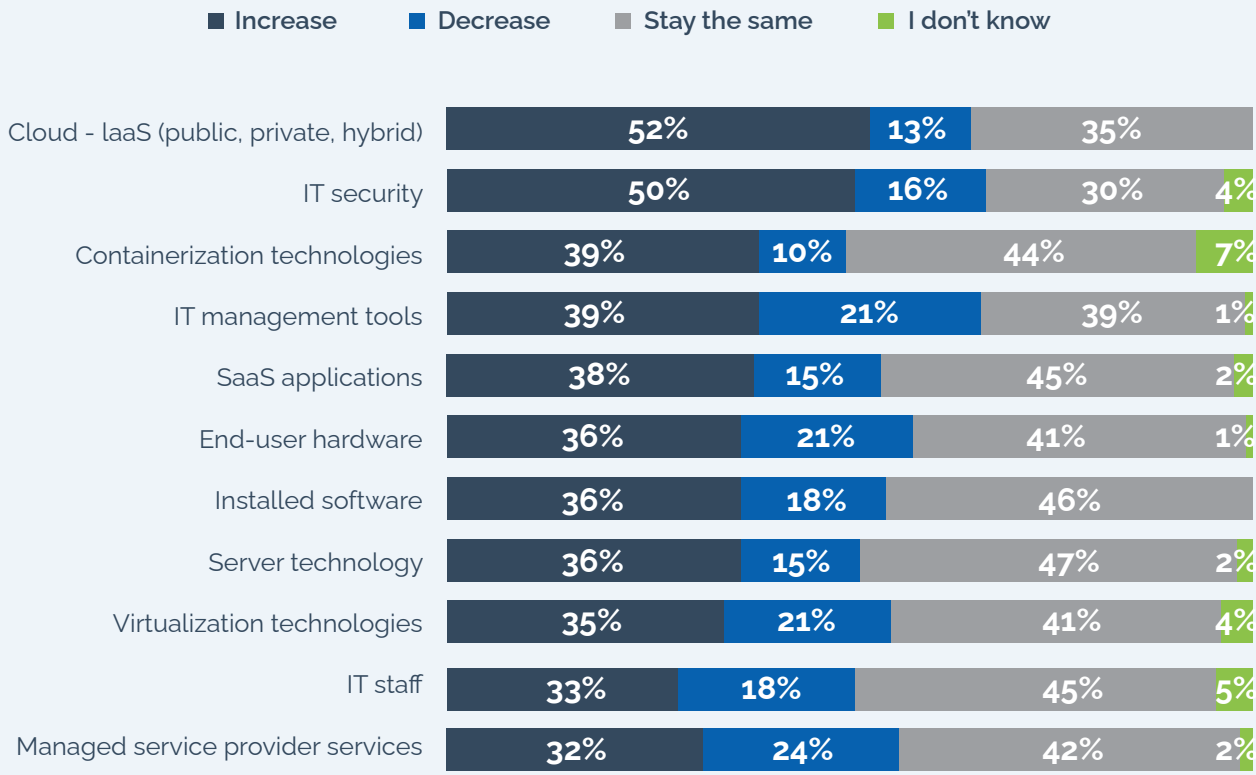
TOP 3 PRIORITIES FOR ORGANISATIONS IT IN 2023



COMPANY SIZE COMPARISONS

	1 - 499	500+
Cloud migration eg., laaS, PaaS or SaaS)	24%	55%
Implementing big data or data science and analytics	35%	22%
Reducing IT costs	27%	34%

CHANGE IN IT BUDGET



ABOUT THE SURVEY

The survey was commissioned by Kaseya and conducted by Foundry. Its objective was to take the pulse of the ANZ IT industry and provide this data back to the same group to help inform where the peer group was heading in 2023.

All of the 107 survey participants were employed in a role within the IT organisation of their company. The survey received responses from across both Australia (83%) and New Zealand (17%).

- A little over half of the respondents (54%) worked in companies with 500 to more than 3000 employees, and the remaining 46% worked in smaller companies with less than 50 and up to 500 employees.
- The largest number of respondents (18%) worked in healthcare, followed by financial services (17%), retail (14%), manufacturing (13%), managed IT services (11%), technology – software/hardware (10%), education & government/public sector (8%) and professional services (8%).
- The largest group (36%) were Directors of IT, followed by IT manager/supervisor (17%), project manager (15%), vice president (13%), system administrator or technician (7%), network engineer (7%), head of technology or C-Level IT executive (6%).
- The largest functions that responded to the survey were IT security (13%), network management (11%) and IT operations (10%), with the remaining responses distributed across 10 other functions.

KASEYA.COM/GET-STARTED