FORTINET

delivered to you by CORE DATA

Networking and Cybersecurity Adoption Index

Australia 2021

ABOUT FORTINET

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organisations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networked, application, multi-cloud or edge environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 465,000 customers trust Fortinet to protect their businesses. Both a technology company and a learning organisation, the Fortinet Network Security Expert (NSE) Training Institute has one of the largest and broadest cybersecurity training programs in the industry. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

ABOUT COREDATA RESEARCH

CoreData Research is a global specialist financial services research and strategy consultancy, founded in 2002 and headquartered in Australia, with operations in Sydney, Perth, London, Boston and Manila.

It provides clients with bespoke and syndicated research services through a variety of data collection strategies and methodologies, along with consulting and research, database hosting and outsourcing services.

CoreData provides both business-to-business and business to-consumer research, while the group's offering includes market intelligence, guidance on strategic positioning, methods for developing new business, advice on operational marketing and other consulting services.

CONTENTS

FOREWORD

Jon McGettigan,
regional director
Australia, New Zealand,
and the Pacific Islands,
Fortinet

The rapid digitisation of business processes and the move to remote work in the wake of COVID-19 have put cybersecurity top of mind for government agencies and businesses of all sizes.

As organisations increasingly rely on connected networks, cloud services, and hybrid working arrangements, the opportunity for cybercriminals to significantly disrupt operations continues to grow. New threats emerge all the time and organisations can inadvertently introduce new security vulnerabilities as their IT environments evolve. This, combined with pre-existing security gaps, has created a threat landscape that's putting significant pressure on IT teams to maintain network performance and accessibility alongside a strong security posture.

In this inaugural *Networking and Cybersecurity Adoption Index*, Fortinet shares insights based on a comprehensive survey of 300 Australian IT decision-makers. Participants were asked more than 50 questions across the three key areas that affect cybersecurity: people; processes; and platforms.

People

Untrained, under-resourced or unsupported employees are a major cybersecurity risk facing organisations. The index examines the training, resourcing and employee cybersecurity skills of Australian organisations.

Process

Having the proper processes to address IT vulnerabilities and protect online assets is a key challenge for Australian organisations. Small and large businesses alike need to consider their current cybersecurity processes to assess their preparedness, and potential exposure, when it comes to a cybersecurity incident.

Platforms

New cybersecurity platforms are constantly emerging, so it can be challenging for organisations to know how these platforms integrate with, or impact, their existing IT ecosystems. Considering the need for organisations to build greater levels of resilience through IT agility and scalability that keep pace with market changes, the chosen platform must deliver a comprehensive cybersecurity solution.

In addition to providing information about the current networking and cybersecurity adoption status of Australian organisations, this index provides valuable guidance about how organisations can address their cybersecurity concerns. We hope you find this index insightful and informative when shaping your organisation's cybersecurity strategy.

Research methodology

This research was conducted by CoreData Research, in collaboration with Recognition PR and Fortinet, to explore Australian businesses' approach and attitudes towards their cybersecurity ecosystem.

This report has been prepared based on a comprehensive survey of 300 IT decision-makers in various-sized Australian businesses:

- Organisations with 20 to 99 employees: 96 responses.
- Organisations with 100 to 199 employees: 85 responses.
- Organisations with 200 or more employees: 119 responses.

The survey was in field from 14 December 2020 to 25 January 2021.

As a part of this research, the Fortinet Cybersecurity Index has been developed, aligning results from three main focus areas to assess the strength of an organisation's cybersecurity readiness. This score can be used as a diagnostic tool for businesses, as well as to paint an overall picture of the cybersecurity strength of Australian businesses. Ultimately, as time progresses, the cybersecurity index score can be used to benchmark and track the progression of Australian cybersecurity landscape. It also provides a peer comparison tool for businesses to assess their relative strengths and weaknesses.

EXECUTIVE SUMMARY – THE FIVE KEY TAKEAWAYS

Smaller organisations struggle more to manage different aspects of their cybersecurity preparedness

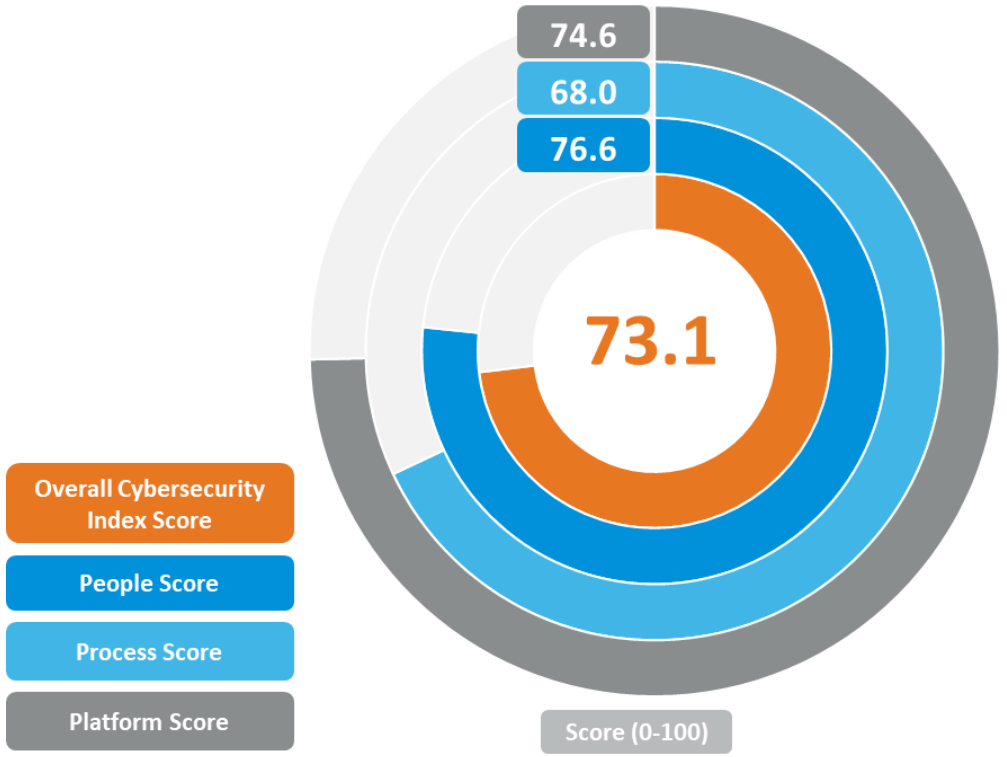
Cybersecurity is an all-or-nothing commitment; any vulnerabilities can put the entire system at risk

Cost, lack of expertise, and time and effort required are the greatest perceived barriers to cybersecurity success

Remote working opens a new cybersecurity vulnerability for many businesses in the long term, warranting further investment in the coming year

Considerable IT security investments have been made recently and are planned soon. Lack of decision-making efficiency around IT investment and planning can impede implementation of meaningful and timely improvements

EXECUTIVE SUMMARY – THE FORTINET CYBERSECURITY INDEX



n = 300, senior IT decision-makers in organisation

- The Fortinet Cybersecurity index produces a score between 0 and 100. The scores are meaningfully calibrated according to responses, with 100 being extremely well prepared and 0 being completely unprepared in terms of cybersecurity preparedness.
- Scores north of 75 indicate a robust, organisation-wide cybersecurity strategy.
- The index rolls up three critical pillars of success. This is about more than just getting the tech right.
- Process is the component that appears to need the most improvement, with an average score of just 68. Platforms and people are both relatively stronger components overall, with average scores of 74.6 and 76.6 respectively.

EXECUTIVE SUMMARY – SMALLER ORGANISATIONS STRUGGLE MORE

Smaller organisations tend to struggle a bit more with managing the *people* and *platform* components of their cybersecurity environment, whereas medium and larger organisations fare much better. For instance, when asked how prepared their incident management team was to deal with a cybersecurity threat, only 27.1% of small companies said they were highly prepared. This was far less than the 38.8% of medium businesses or the almost half (47.9%) of large businesses. Similarly, only 61.4% of small businesses conducted cybersecurity testing at least quarterly, much below the proportion seen from medium (80.0%) and large (79.8%) companies.

Organisations of all sizes struggled with implementing the necessary *processes* of a successful cybersecurity ecosystem and found it difficult to maintain discipline and staff buy-in to the cybersecurity cause. Only just over half (56.7%) of companies said they were successful in aligning their security and business objectives, and even fewer (54.7%) said that there were clear responsibilities and security accountability throughout their organisation. Aligning the *processes* with the *people* and the *platforms* is an important consideration, and the poor reflection of cybersecurity processes in this report should serve as a call to action for many organisations.

EXECUTIVE SUMMARY – CYBERSECURITY REQUIRES GETTING IT ALL RIGHT

The major through-line of cybersecurity is that it needs to be wholly embraced by a company, with buy-in from all stakeholders. Any small vulnerability poses a risk, so it's important that there isn't any chink in the armour. Over two thirds (67.3%) of companies said an IT security breach would cause their business to cease operating and/or incur a significant cost. This was even more prevalent in firms with more than 200 employees (76%). Despite this, just over half (57.7%) of all companies said they had a disciplined adherence to all the established best practices for cybersecurity. Overall, only 29% felt highly prepared for an IT security threat. 11% were unsure, which also suggest further vulnerabilities.

Even more worryingly, only 36% of businesses said they had complete transparency around risk vulnerability in cybersecurity. This kind of exposure is not ideal in any security environment, let alone one with such grave consequences from even a minor breach. Companies were mostly concerned about advanced malware, phishing and social engineering, ransomware login attacks and malicious insider threats coming from organised cybercriminal gangs and employee action (both malicious and unwitting). Competitor espionage is a particular concern for smaller organisations.

EXECUTIVE SUMMARY – CYBERSECURITY REQUIRES GETTING IT ALL RIGHT

Close to 1 in 2 respondents had undertaken culture/behavioural change management or digital transformation programs that addressed IT security in the last year.

Only just over 1 in 5 had never done this. More than 1 in 2 planned to undertake this in the next year and a further 3 in 10 expected to but didn't have immediate plans in place.

Overall, only 2 in 5 felt there were plenty of IT security specialists to support industry requirements. More than 2 in 5 said it could be hard to find the good ones.

While close to 1 in 4 had already implemented zero trust security, just more than 1 in 3 planned to in the next 12-18 months. 15% were not aware of zero trust security and a further 8% were aware but weren't sure how to implement it. In other words, close to 1 in 4 felt bit in the dark about zero trust.

EXECUTIVE SUMMARY – COST AND COMPLEXITY ARE KEY BARRIERS

1 in 2 respondents had made considerable IT infrastructure investment in the last year and 1 in 2 were planning to do so in the next 12 months.

IT security (70%) and IT architecture and networking (61%) were by far the most common areas for their next IT infrastructure investments. Only 3% reported failed expectations from the benefits seen from their IT security investment. 66% of businesses supported both an IT and OT environment.

When it came to implementing and choosing new cybersecurity solutions, cost remained the biggest challenge for small companies, with most (71.9%) citing it as a main barrier. As such, smaller companies were far less willing to invest in cybersecurity upgrades to keep up with the times. Only a minority (14.6%) of small businesses were planning to considerably invest in IT over the next three months, much fewer than medium (32.9%) and large (42.9%) businesses.

EXECUTIVE SUMMARY – COST AND COMPLEXITY ARE KEY BARRIERS

Alternatively, complexity seems to be one of the more troubling aspects of upgrading IT for the larger organisations surveyed. Large (47.9%) and medium (54.1%) companies were far more likely to see complexity as a major infrastructure barrier than smaller companies (36.5%).

1 in 3 felt multiple vendors and technologies added cost and complexity to their IT environment and tried to avoid it. Just over 1 in 2 agreed but believed it was worth it sometimes. This may, in some part, explain Cisco's current dominance over the current firewall (59.3%) and SD-WAN (49.0%) infrastructure of the companies interviewed. However, Fortinet figures highly in the consideration set.

EXECUTIVE SUMMARY – REMOTE WORKING POSES NEW CHALLENGES

Many companies had a significant proportion of their workforce working remotely. Almost two thirds (62.7%) of all companies had at least half of their workforce still working remotely to some degree, with the vast majority expecting this proportion to increase (41.3%) or stay the same (35.7%). These companies understood that this exposed their company to greater cybersecurity risk, with a majority saying this had placed at least a reasonable (35.3%) or considerable (22.4%) amount of pressure on their existing IT infrastructure.

Most companies acknowledged that more investment was likely necessary to minimise this vulnerability. To specifically protect their remote workforces, more than half (55.2%) had plans to invest, and a further 31% anticipated investing but didn't have a plan yet. These numbers were even greater for large companies at 59.2% and 30.3% respectively. Constrained by cost, smaller companies found it more difficult to justify investment, with just under half (47.4%) having plans to invest in the next 12 months.

EXECUTIVE SUMMARY – EFFICIENT DECISION-MAKING IS KEY

In an area as dynamic and rapidly changing as cybersecurity, businesses can rarely afford to move slowly. In fact, a large majority of businesses (84.7%) said that introducing efficiency into network operations was at least reasonably important, with a similar proportion (79.0%) saying the same about simplifying complexity.

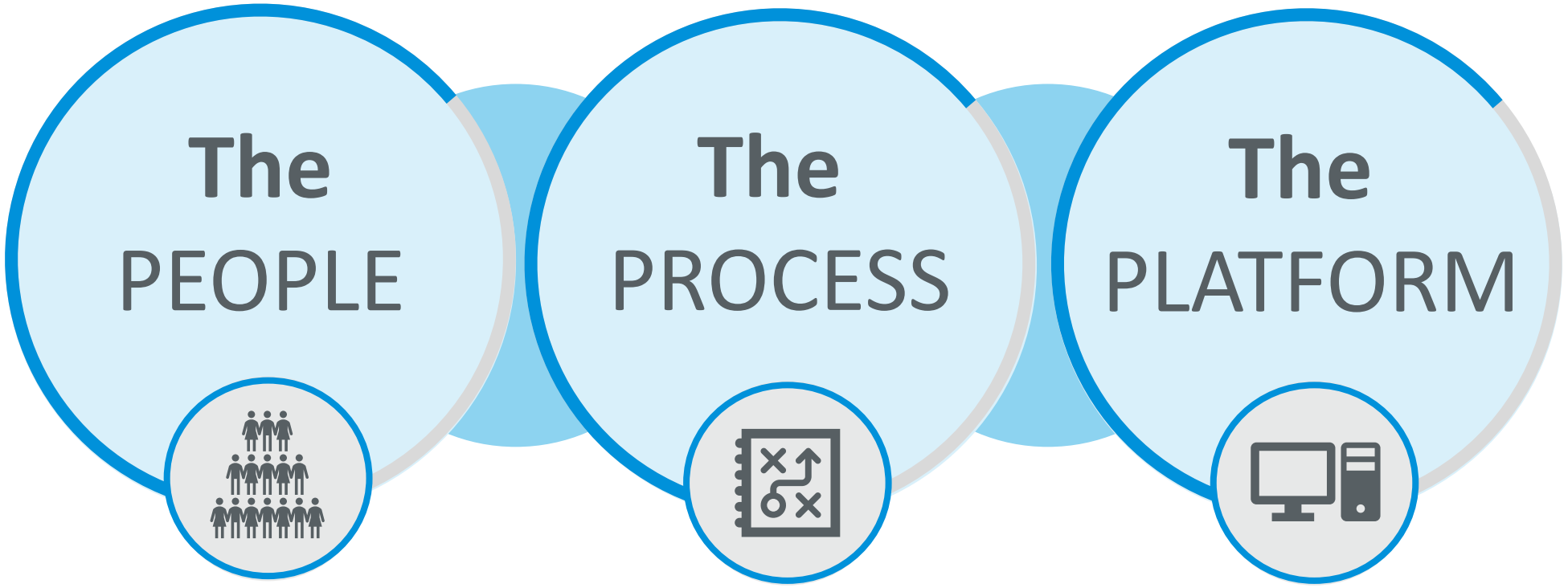
Overall, 84% of businesses rated the effectiveness of their organisation's IT security decision-making as reasonably or highly effective. 73% felt IT security decisions were made more effectively than other key operational areas in the business.

At an overall level, most cybersecurity decisions were either made by an executive leadership team (41.3%), or at least approved by one (49.0%). In fact, most companies said that their IT decisions were highly (29.3%) or reasonably (43.3%) visible by executive leaders, and most (72.7%) agreed that IT decisions were at least somewhat more visible to leaders than other decisions in the business. However, this still left 3 in 10 reporting that IT security lacked reasonable executive leadership visibility and only 3 in 10 feeling it was highly visible.

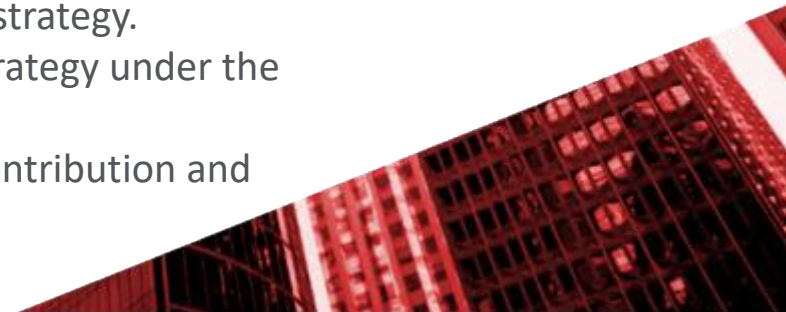
Many employed specialist consultancies to help formulate their IT security strategy (53% ongoing basis and 27% in the past). Decisions about investment in security, including which areas it will invest in (e.g. adoption, planning and preparedness, training) tended to be most often led by an internal IT security management team.
These investment decisions were less frequently outsourced.

The Fortinet Cybersecurity Index

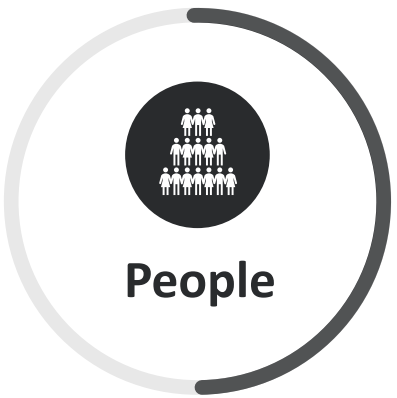
The Fortinet Cybersecurity Index



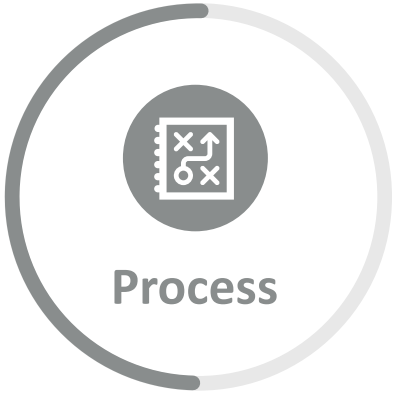
- To standardise the measurement of cybersecurity strength and preparedness, we have identified the three key measurable components of a business's cybersecurity strategy.
- Key IT decision-makers were asked to assess their company's IT systems and strategy under the three main components of: **people; processes;** and **platforms.**
- This allowed for the creation of a holistic index score which understands the contribution and alignment of key components for a successful and safe IT environment.



Breaking things down – the index components



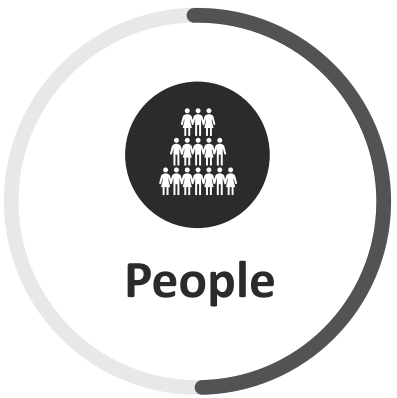
- One of the main cybersecurity risks facing any large business is the vulnerability of untrained, under-resourced or unsupported staff.
- The *people* component of the cybersecurity index assesses the exposure of businesses to these risks, through targeted questions that seek to understand a company's IT training, resourcing, and staff expertise.
- Staff buy-in and executive support are also crucial areas included in this component, as most cybersecurity initiatives are destined for failure if either are lacking.



- To achieve cybersecurity success within an organisation, having the proper processes to deal with vulnerabilities and protect assets is imperative.
- The *process* component of the cybersecurity index delves into the coverage and depth of a business' cybersecurity processes to assess their preparedness for a cybersecurity incident, and how well they protect their data and other IT assets from any potential vulnerabilities with their established processes.
- Discipline, decision-making and cultural buy-in are all important aspects of the success of any cybersecurity processes and are also factored into the index calculation for this component.

- With the plethora of cybersecurity providers, it can be difficult for an organisation to stay on top of the platforms that they need.
- The *platform* component of the cybersecurity index is an assessment of a company's current cybersecurity IT ecosystem, and how scalable and adaptable that ecosystem can be over time. It is important for a company to have a comprehensive cybersecurity solution and to also be ready for change when necessary.
- Regular testing and reviews of the platforms are also a relevant consideration and have been included in the calculation of this index component.

Breaking things down – the index components

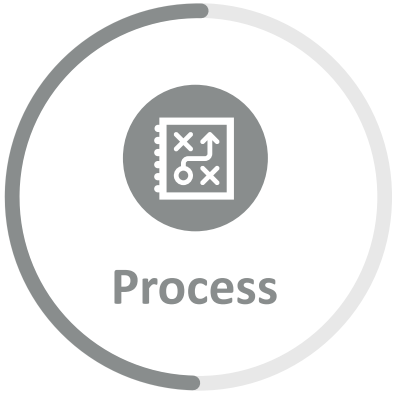


Key strengths

- Physical security to protect data assets and IT infrastructure.
- Executive management endorsement of IT security efforts.
- Incident management team preparation to deal with the latest breaches and cyber exploit threats.

Key weaknesses

- Staff resources to protect the data assets and IT infrastructure (i.e. budget and time provided for training and ongoing support).
- Providing cyber hygiene practices and onboarding orientation programs.



Key strengths

- Effectiveness of IT security decision-making (i.e. the speed and quality).
- Cultural commitment to IT security.

Key weaknesses

- Overall budget resourcing to protect data assets and IT infrastructure.
- Regular schedule of auditing and drill regimes (including simulations and tabletop exercises).
- Enterprise risk management and implementation plan in place.
- Transparency around risk vulnerability.

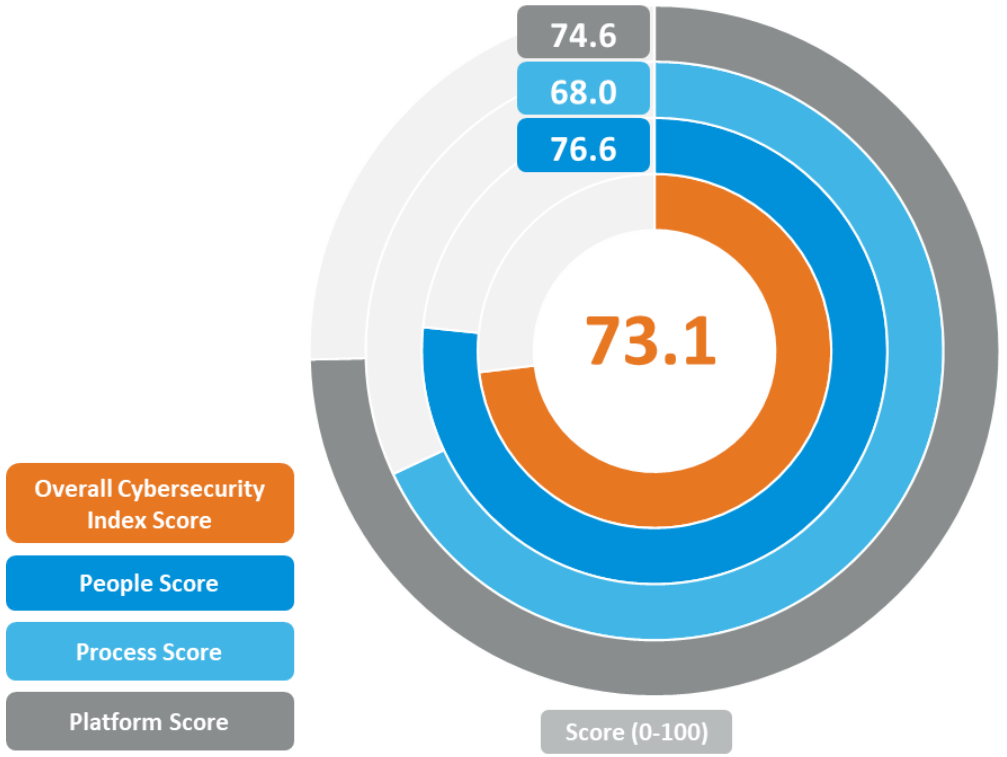
Key strengths

- IT security architecture has high interoperability, scalability and agility
- Confident in networking and cloud security technologies

Key weaknesses

- Suitable antivirus and firewall solutions for the organisation's needs up to date.
- Annual review of SD-WAN, antivirus and firewall provider suitability.
- Monthly network security testing.
- Up-to-date maturity, compliance and certification assessments as well as intrusion detection and threat intelligence operating models.

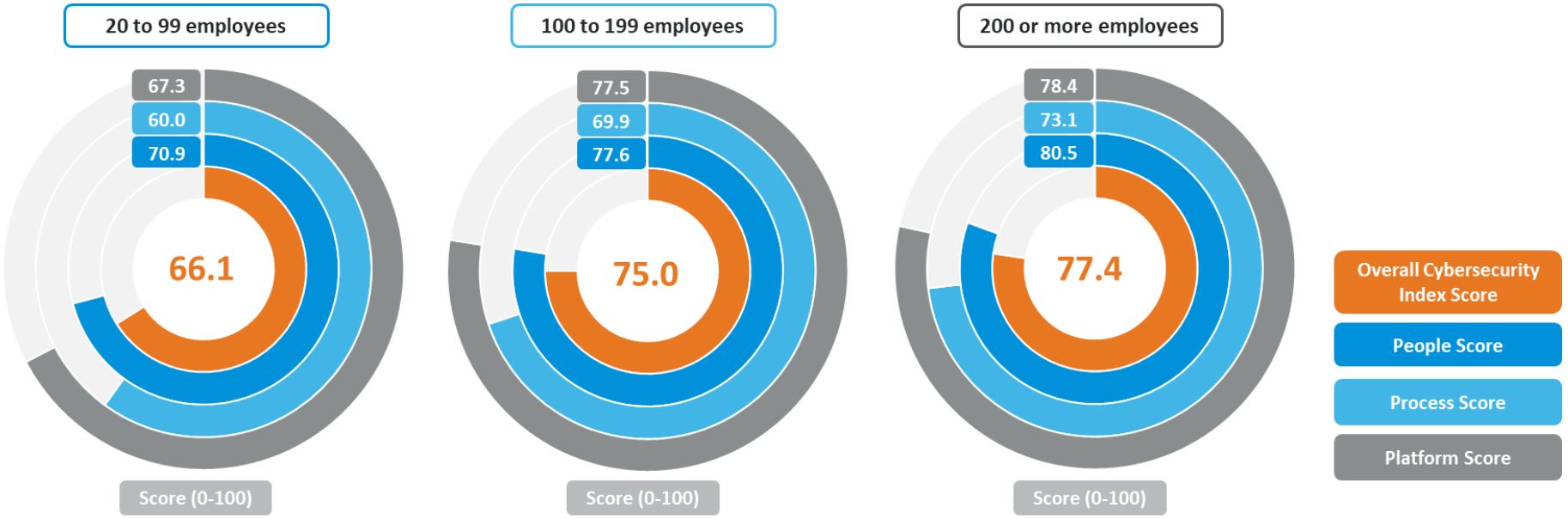
The Fortinet Cybersecurity Index Results (overall)



n = 300, senior IT decision-makers in organisation

- The Fortinet Cybersecurity index produce a score between 0 and 100. The scores are meaningfully calibrated according to responses, with 100 being extremely well prepared and 0 being completely unprepared in terms of cybersecurity preparedness.
- Scores north of 75 indicate a robust organisation-wide cybersecurity strategy.
- The index rolls up three critical pillars of success. This is about more than just getting the tech right.
- Process was the component that appeared to need the most improvement, with an average score of just 68. Platforms and people were both relatively stronger components overall, with average scores of 74.6 and 76.6 respectively.

The Fortinet Cybersecurity Index Score (by business size)



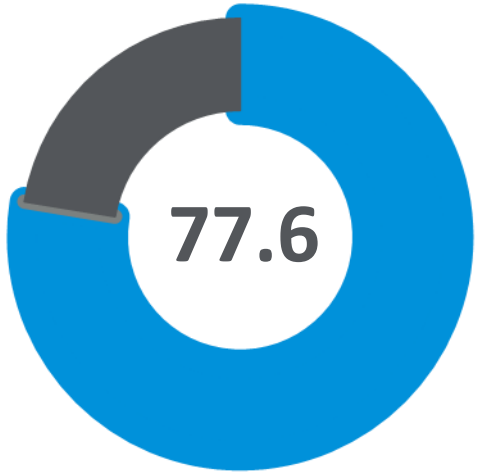
n = 96 organisations with 20 to 99 employees; 85 organisations with 100 to 199 employees; 119 organisations with 200 or more employees

- Organisations with the scale and resources to implement strong cybersecurity protocols are afforded the safety and strength that these protocols bring across the board. However, inertia in upgrading legacy systems and decision-making became more of a challenge as organisations lost some nimbleness as they grew.
- Companies with 200 or more employees performed significantly better than companies with 20 to 99 employees across all three components and were also slightly ahead for all components when compared to companies with 100 to 199 employees.

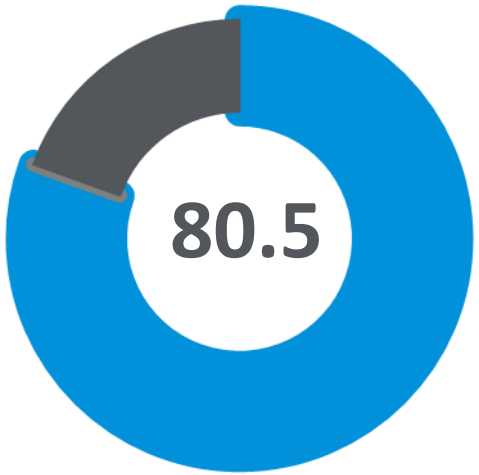
The people component

The *people* component index results

20-99
employees



100-199
employees



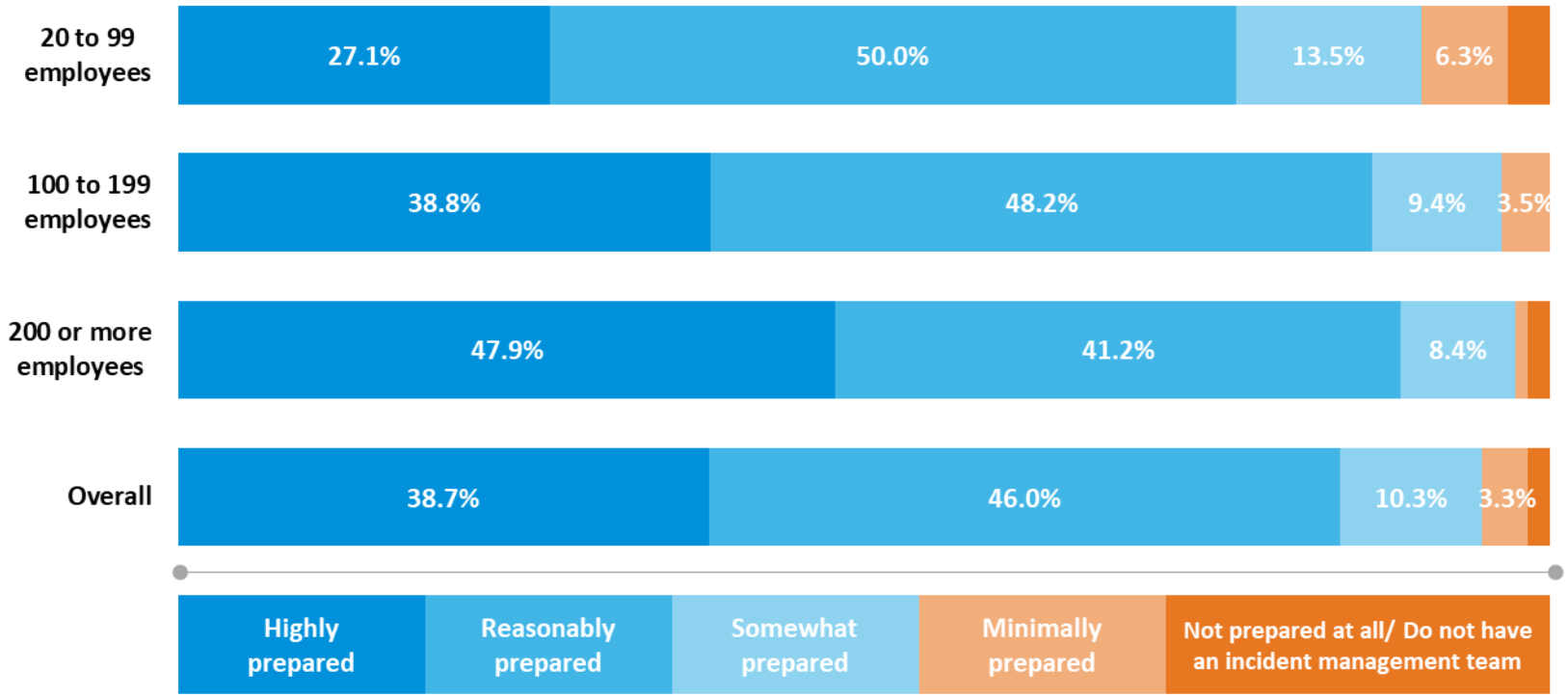
200+
employees

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

While the *people* component was stronger than the others across the board, smaller organisations still tended to struggle a bit more with managing this aspect of their cybersecurity environment

Organisations of all sizes were reasonably prepared to deal with threats…

How well prepared is your incident management team to deal with the latest breaches and cyber exploit threats to your organisation?

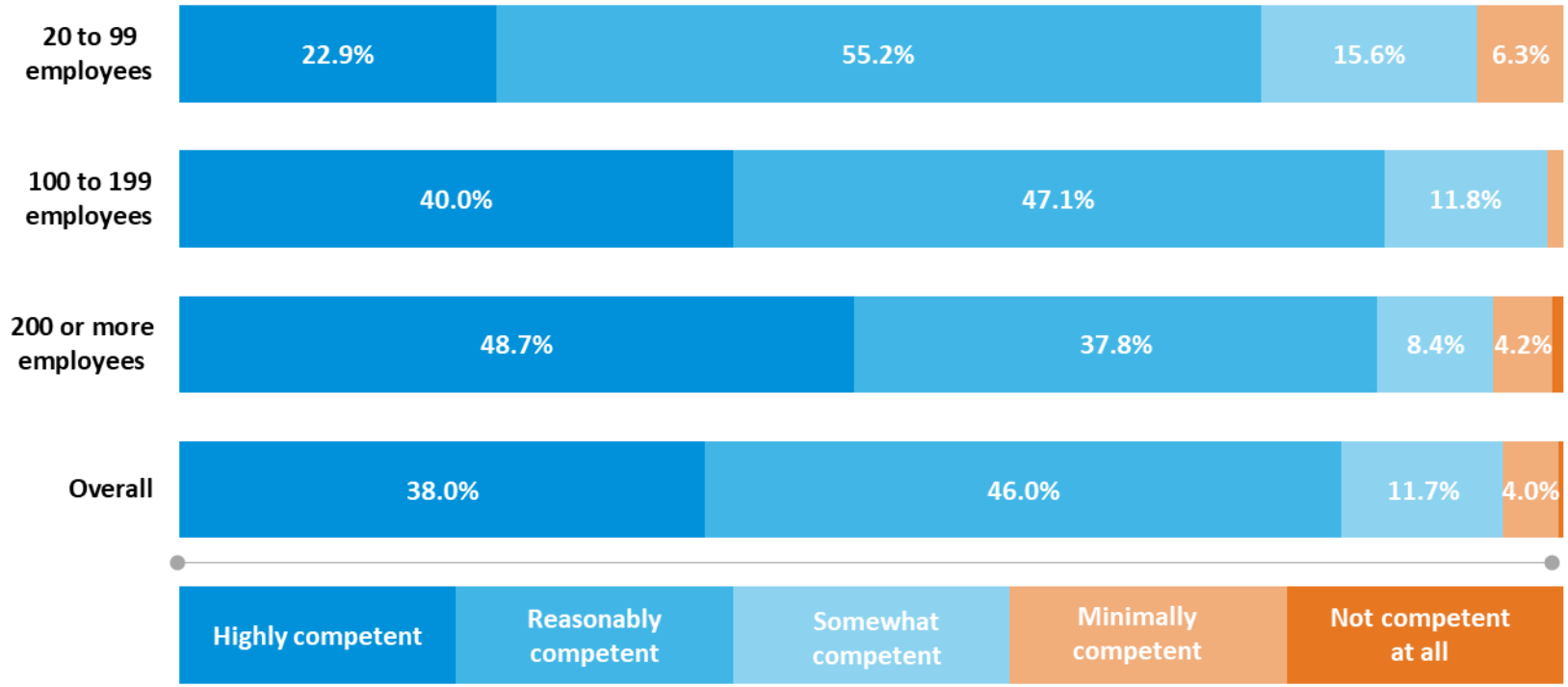


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

… but the competency of IT protection staff was lower in small businesses

How would you rate the competency (i.e. relevant skills and expertise) of your staff to protect the data assets and IT infrastructure of your organisation?

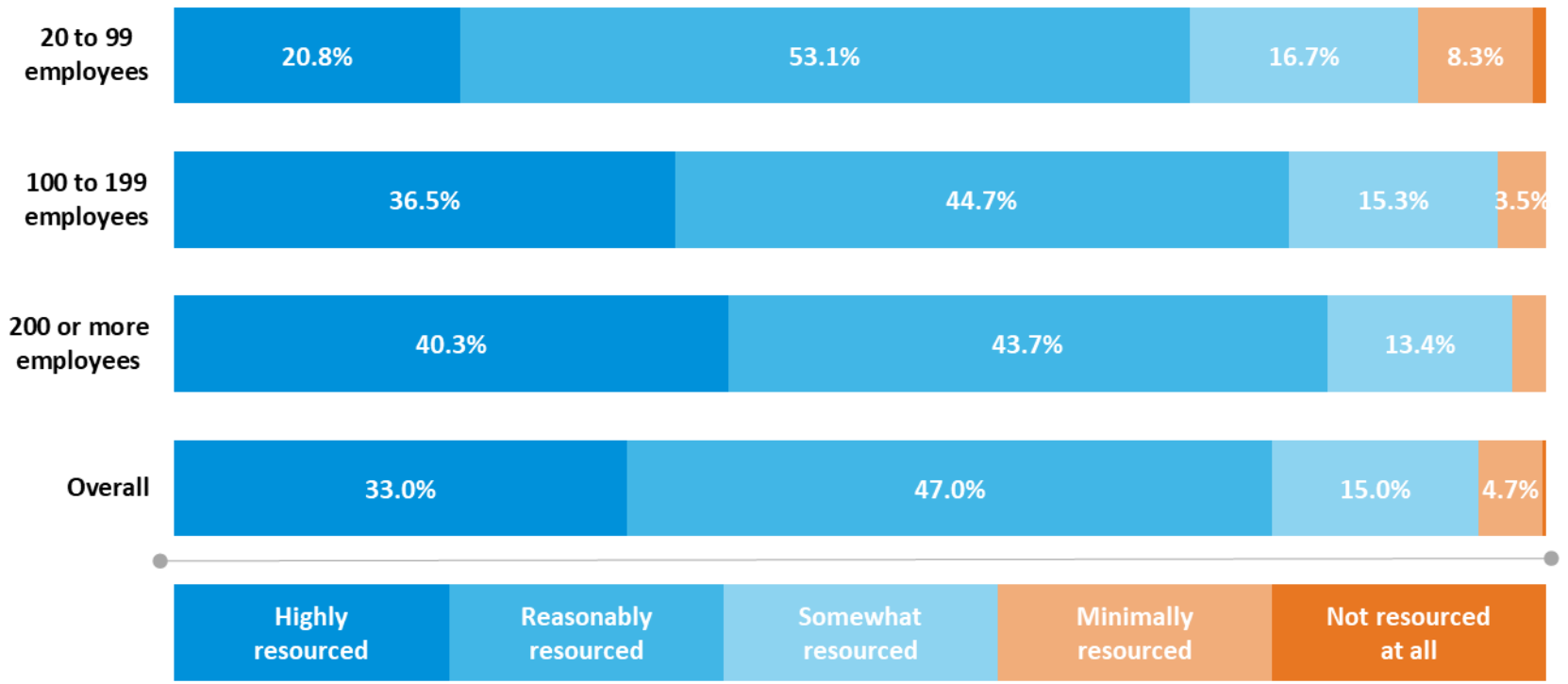


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Resourcing for IT and data protection had room for improvement

How well resourced are your staff to protect the data assets and IT infrastructure of your organisation (i.e. budget and time provided for training and ongoing support)?

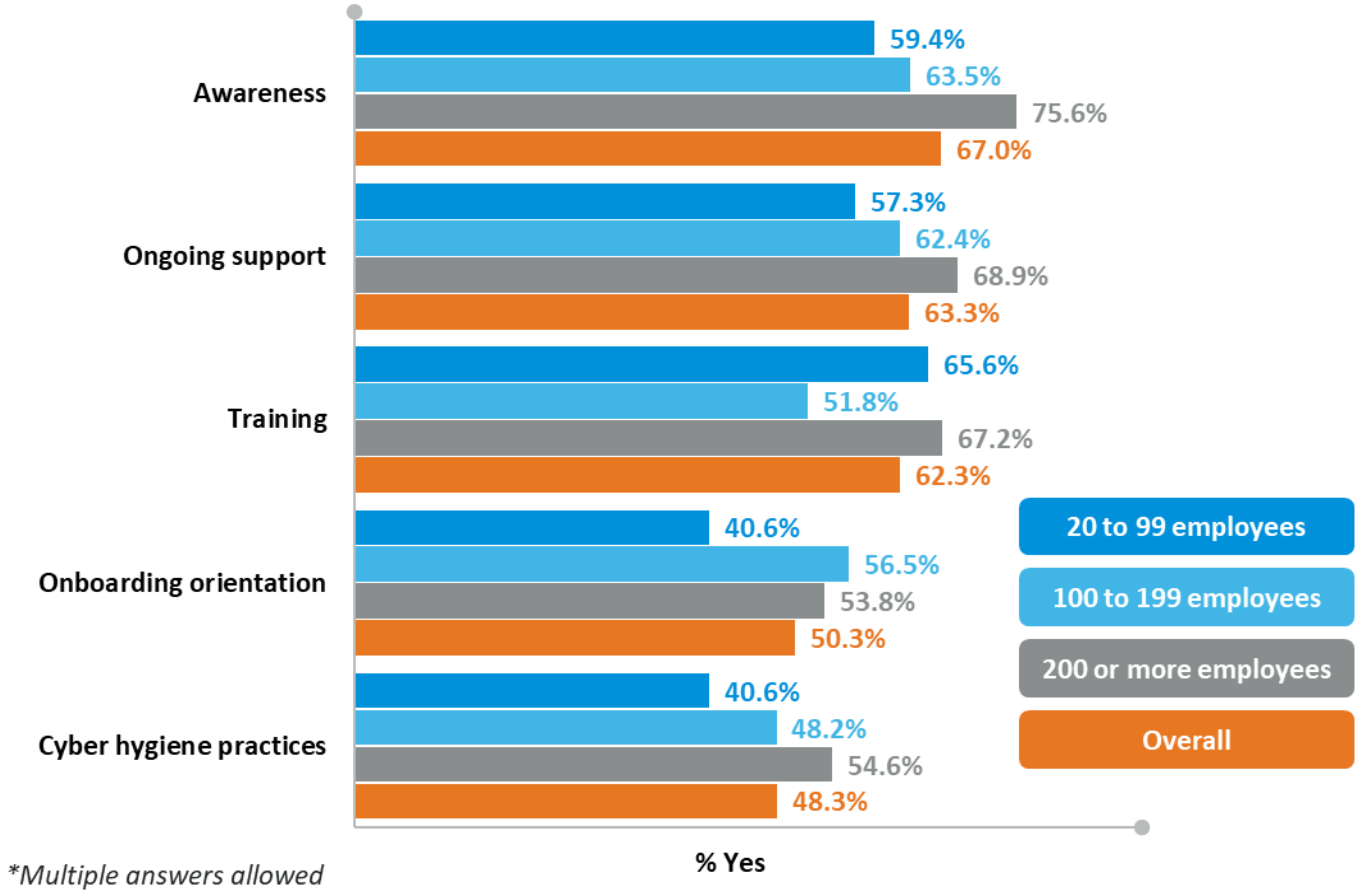


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Organisations of all sizes could improve employee programs for security

Do you provide any of the following IT security programs for employees?



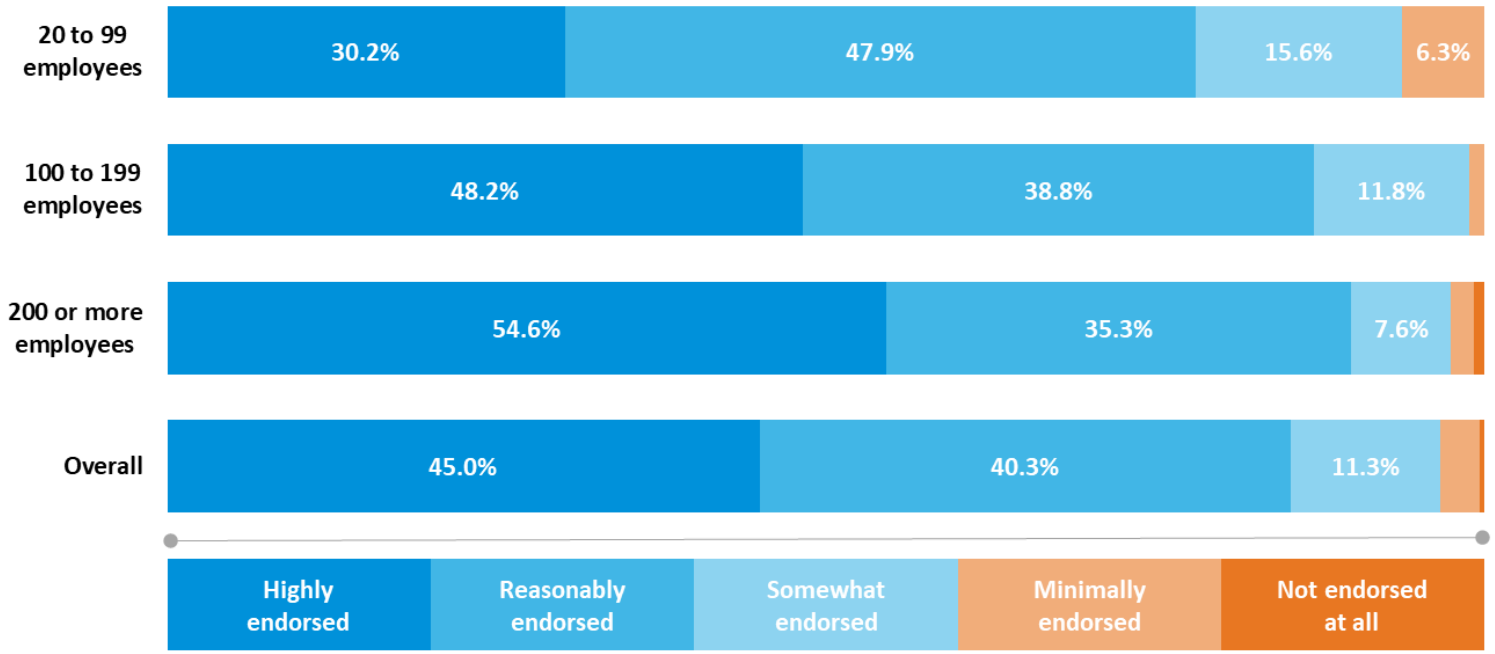
*Multiple answers allowed

n = 300, overall (senior IT decision-makers in organisation)

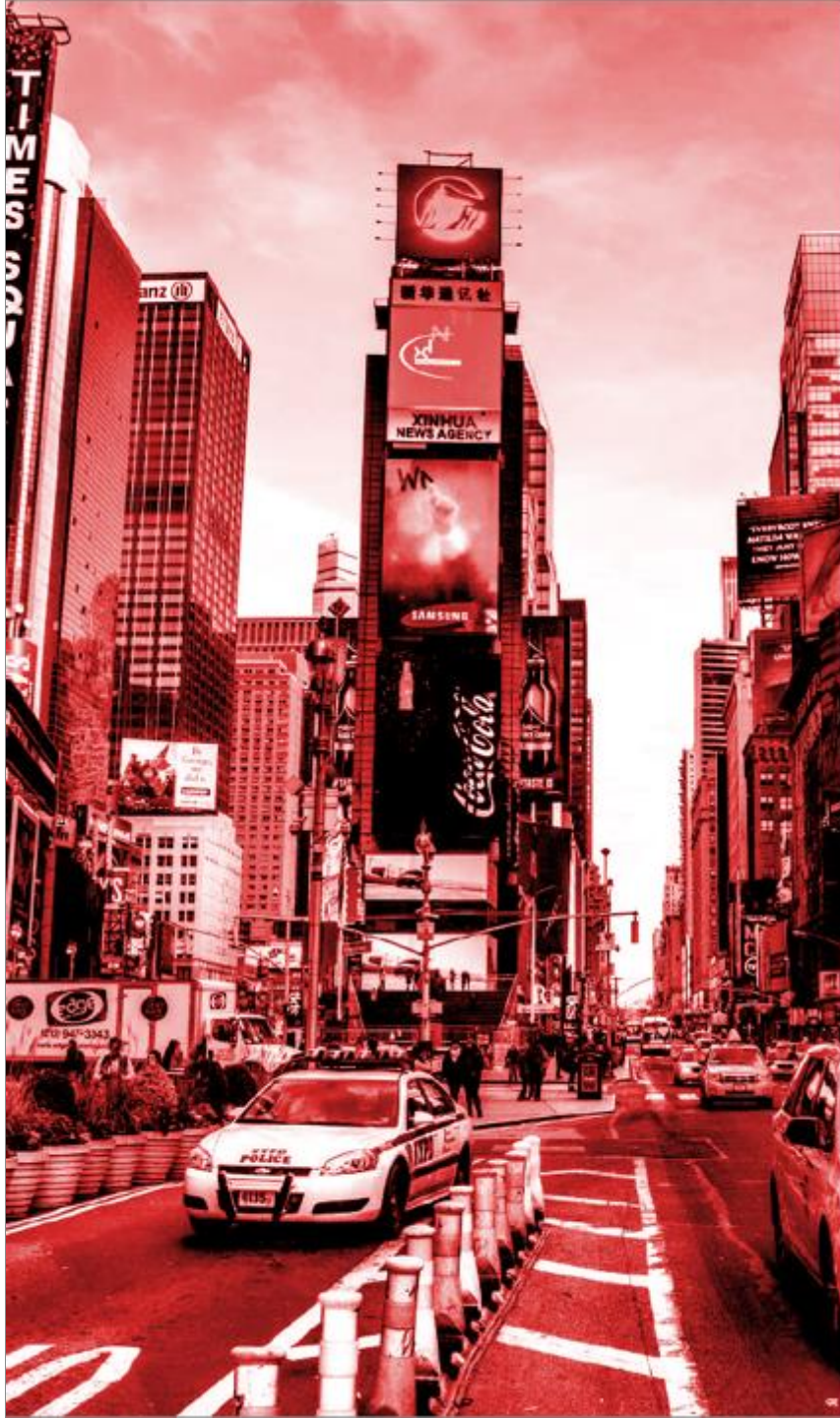
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Executive management generally understood the importance of IT security efforts

How strongly does executive management endorse your organisation's IT security efforts?

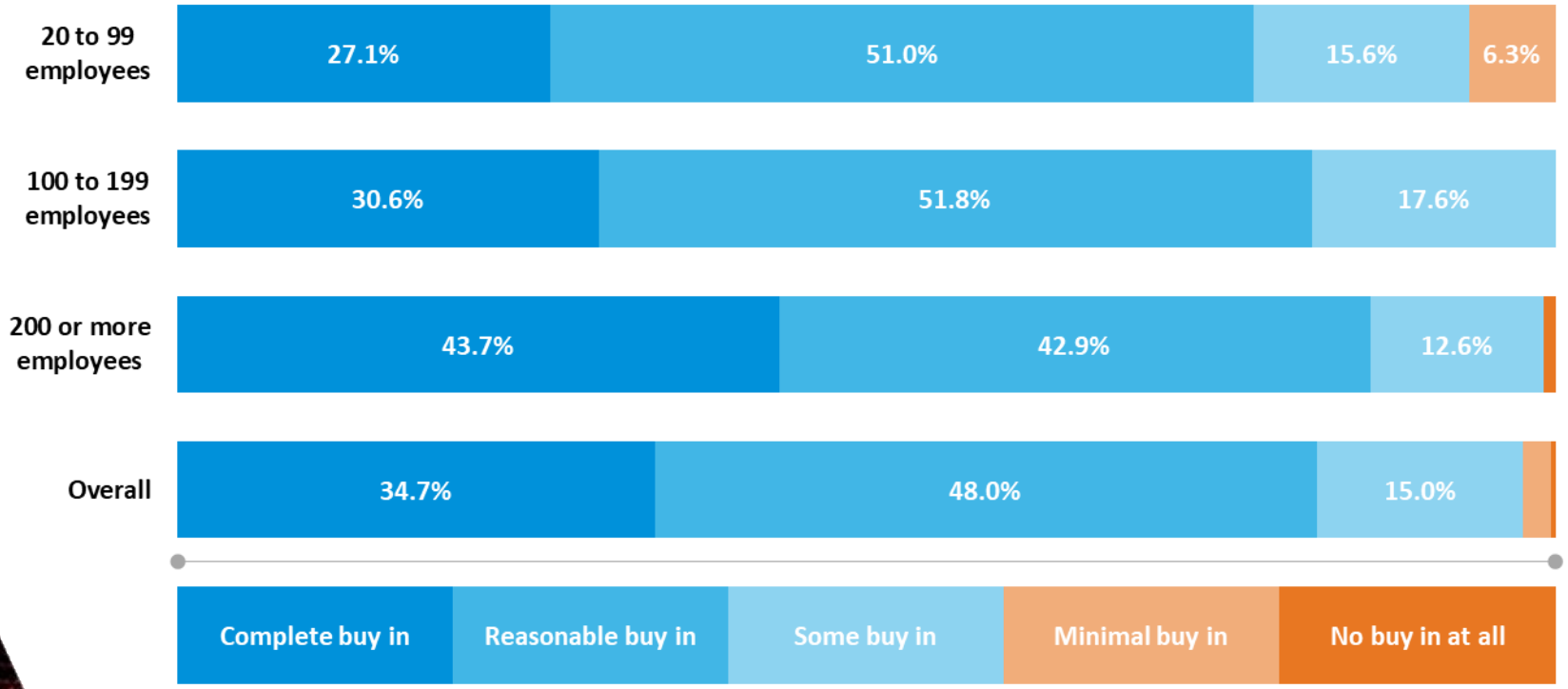


n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees



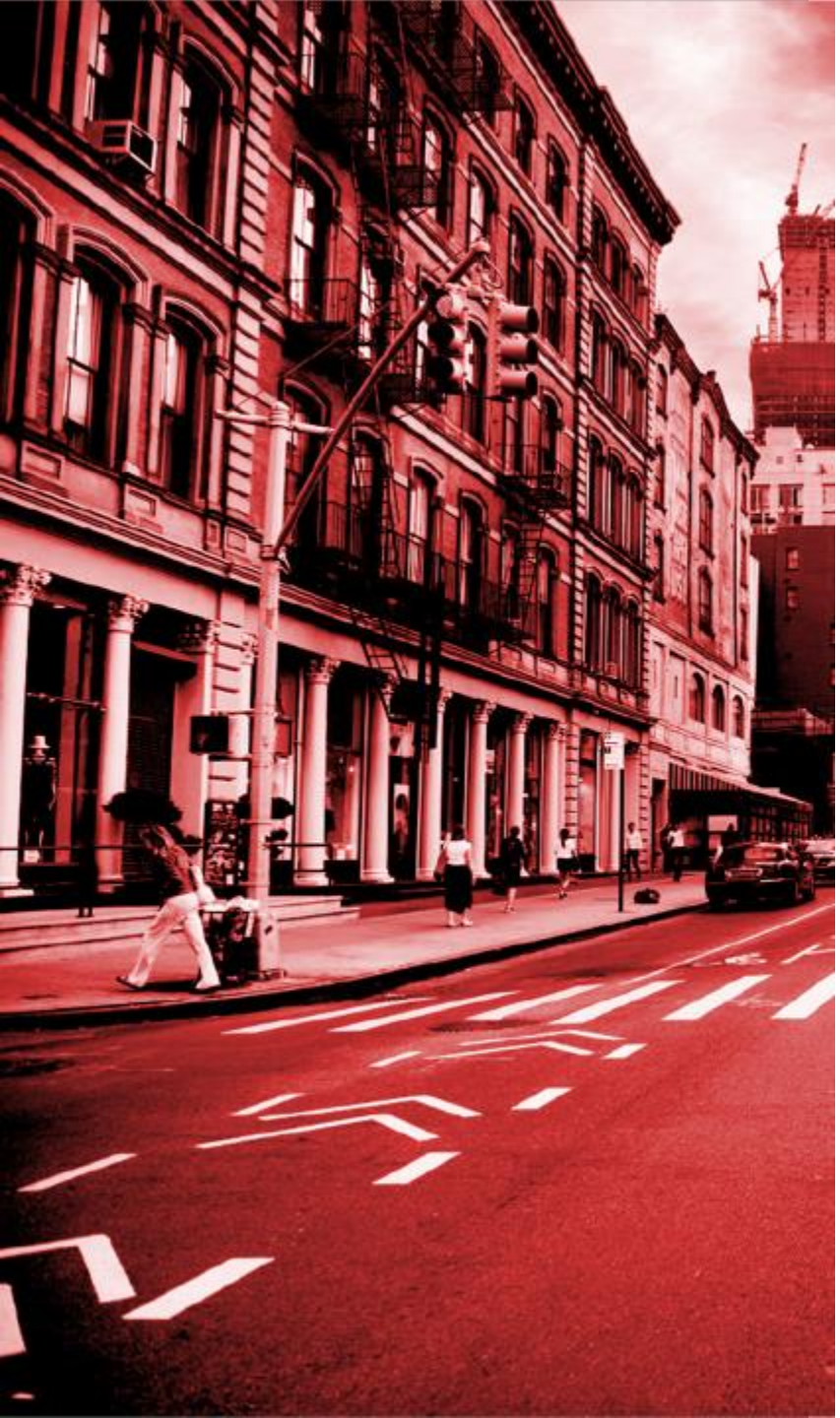
Staff buy-in for organisational security had room to be much stronger

How strongly do your staff ‘buy in’ to the importance of your organisation's IT security efforts? (i.e. believe IT security is a critical organisational risk and a responsibility for all staff to manage)



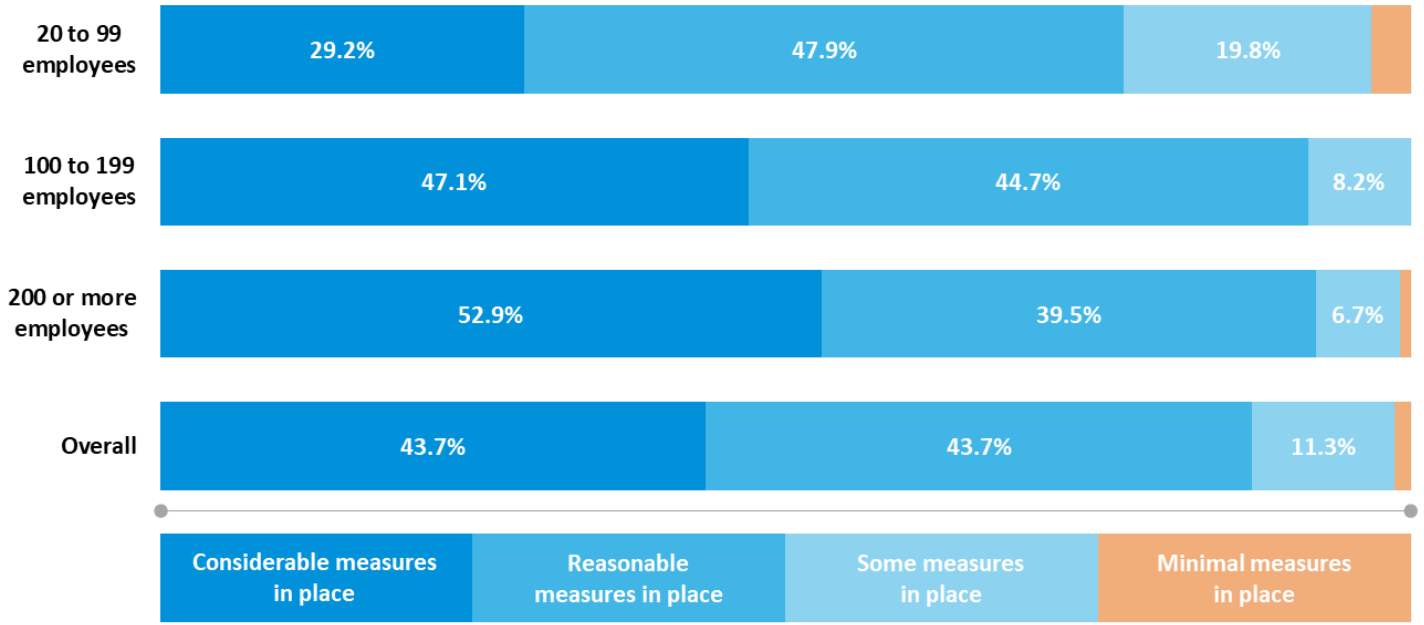
n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees



Large companies were reasonably strong performers with their physical IT security

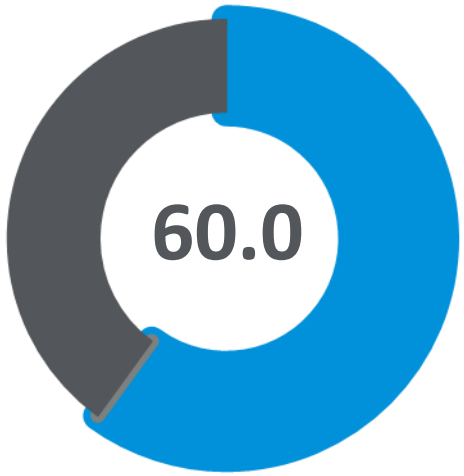
How would you rate the standard of your organisation's physical security to protect data assets and IT infrastructure? (i.e. access to workstations and hardware)



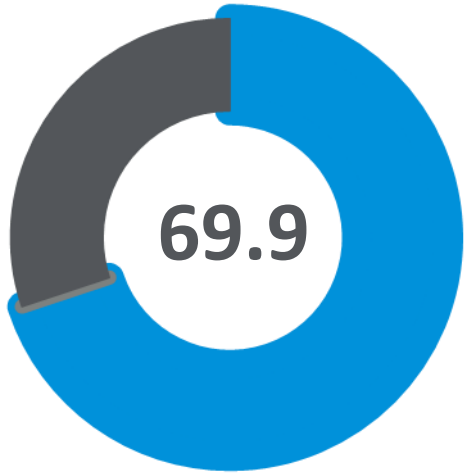
n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

The process component

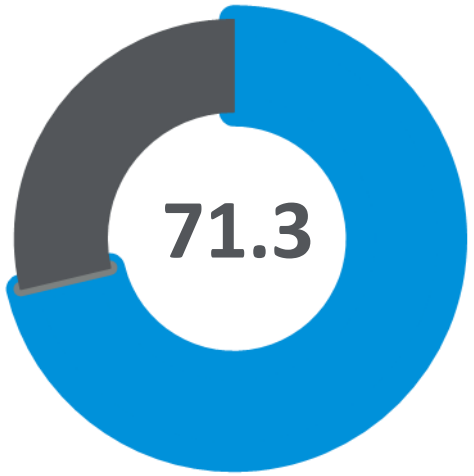
The *Process* Component Index Results



20-99
employees



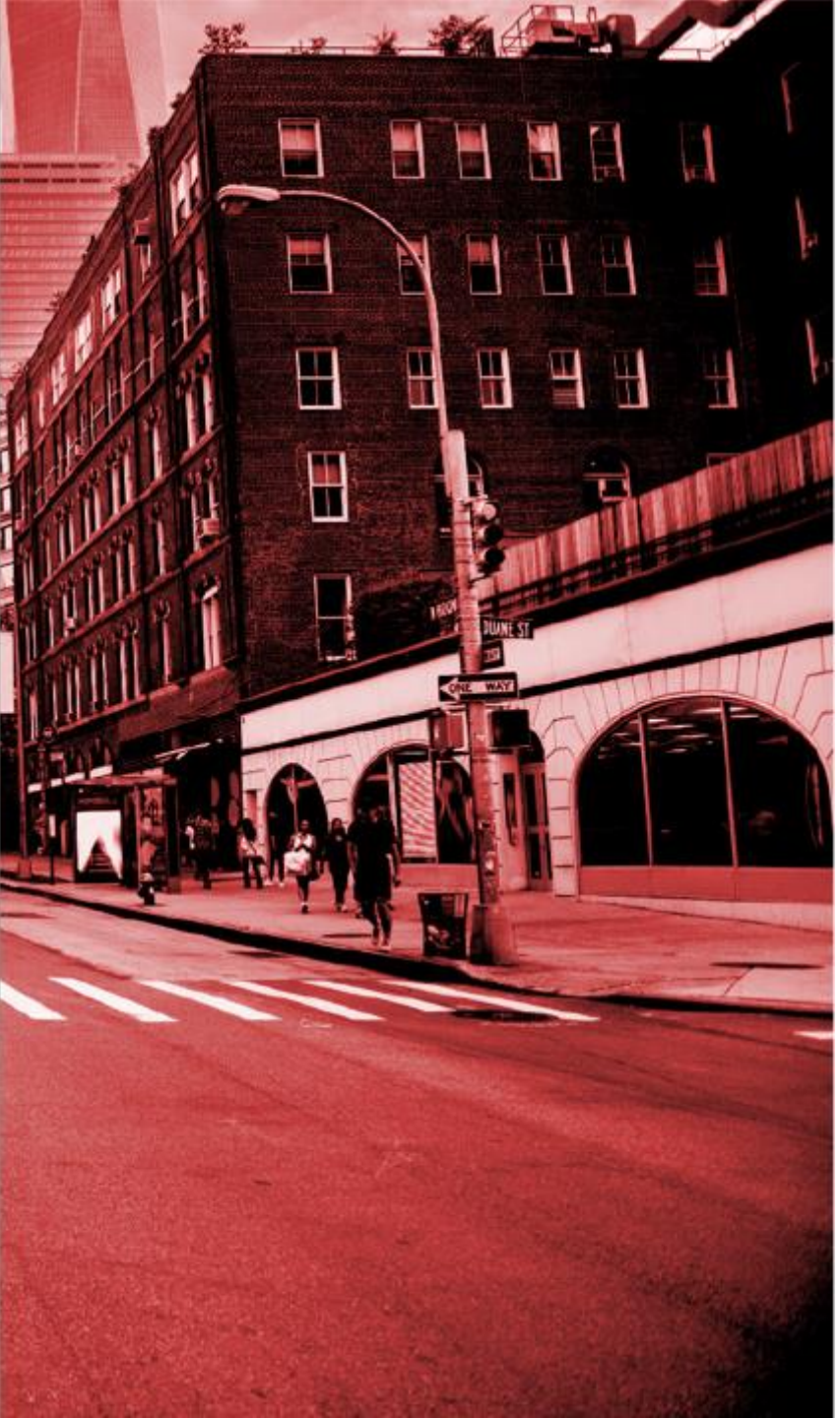
100-199
employees



200+
employees

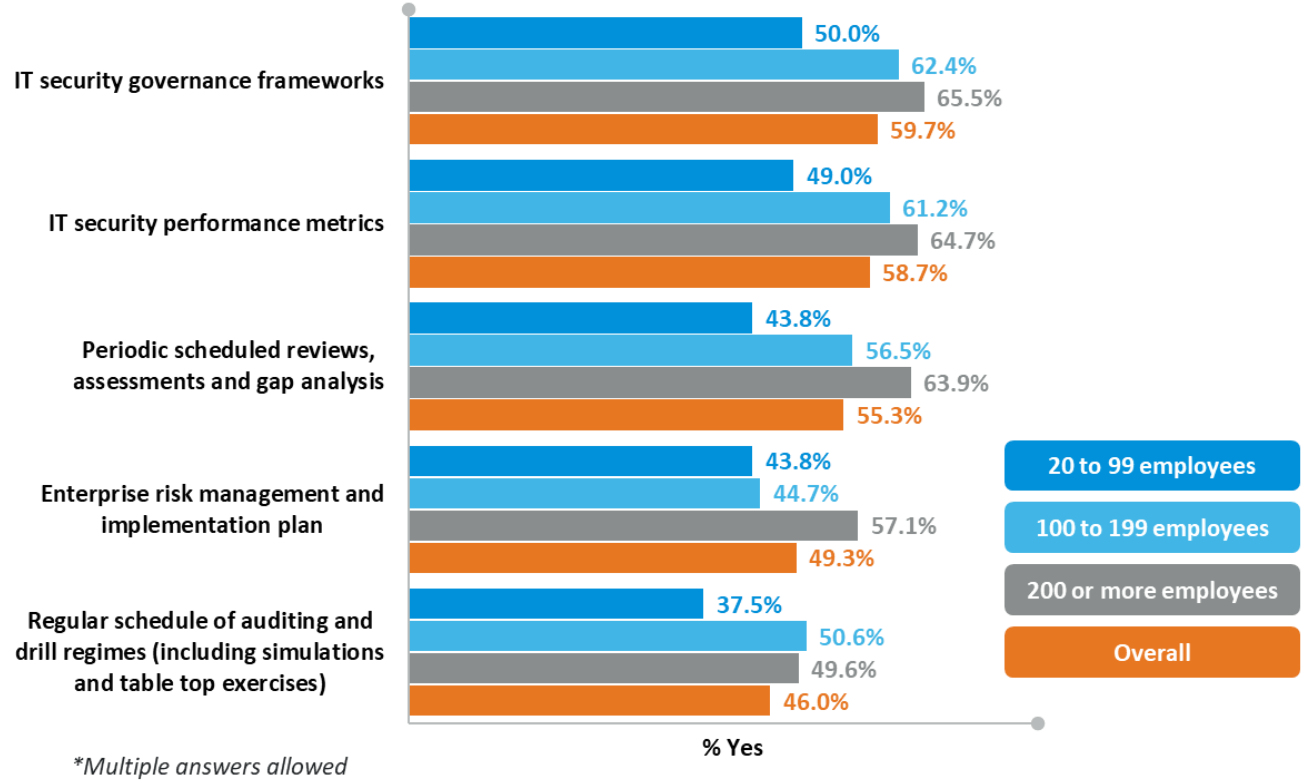
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Process is, by far, the lowest-scoring index component across the board, with most organisations struggling to implement the proper practices, be dynamic in their adaptability, and facilitate staff buy-in, to reap the cybersecurity benefits of strong process management.



Companies rarely had a complete suite of the necessary IT procedures and processes

Does your organisation have any of the following procedures and processes currently in place?

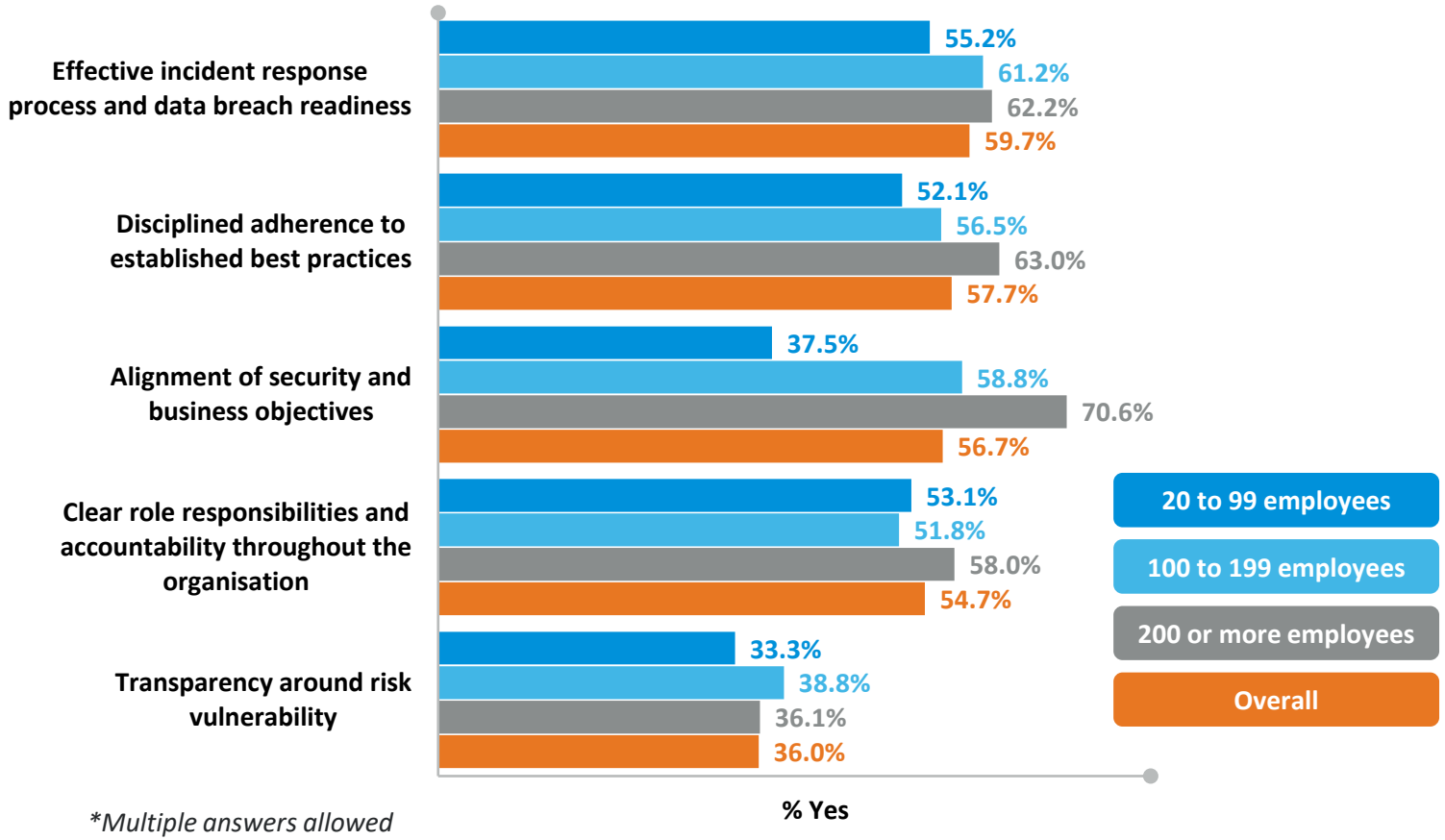


**Multiple answers allowed*

n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees;
85, 100 to 199 employees; 119, 200 or more employees

Business IT security discipline and incident response were also low

Has your organisation adequately achieved the following in implementing IT security procedures and processes?



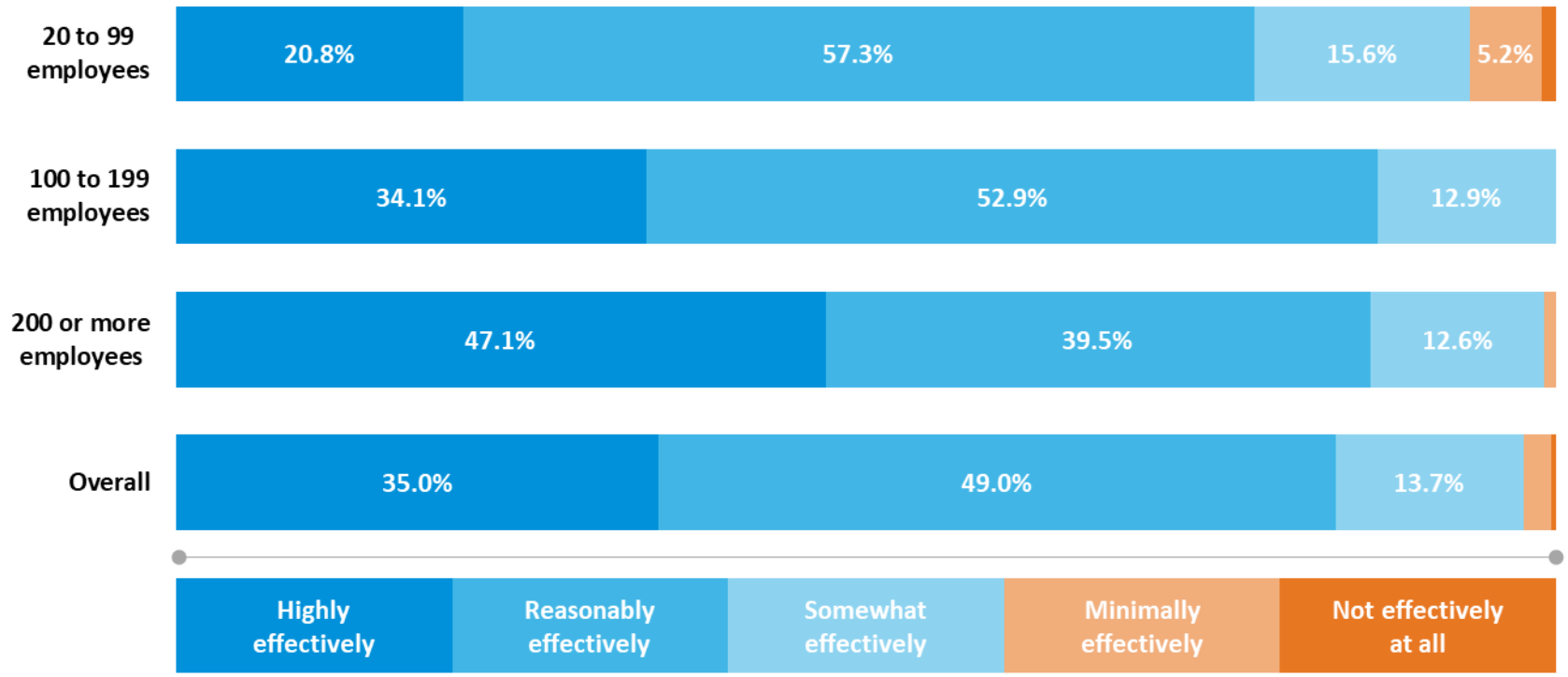
**Multiple answers allowed*

n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

IT decisions moved through organisations relatively effectively

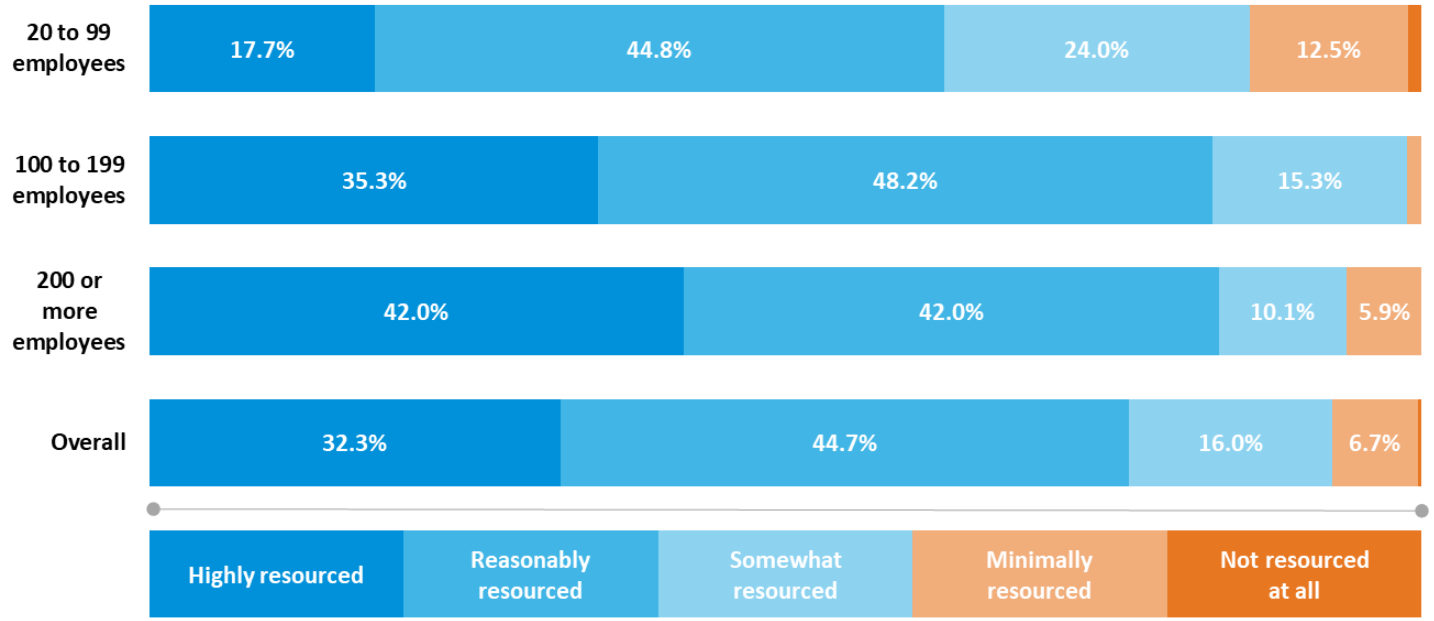
How effectively are IT security decisions made in your organisation? (i.e. the speed and quality of the decision-making process)



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Data and IT protection could use better resourcing and budgets

How well-resourced is your organisation's overall budget to protect its data assets and IT infrastructure?

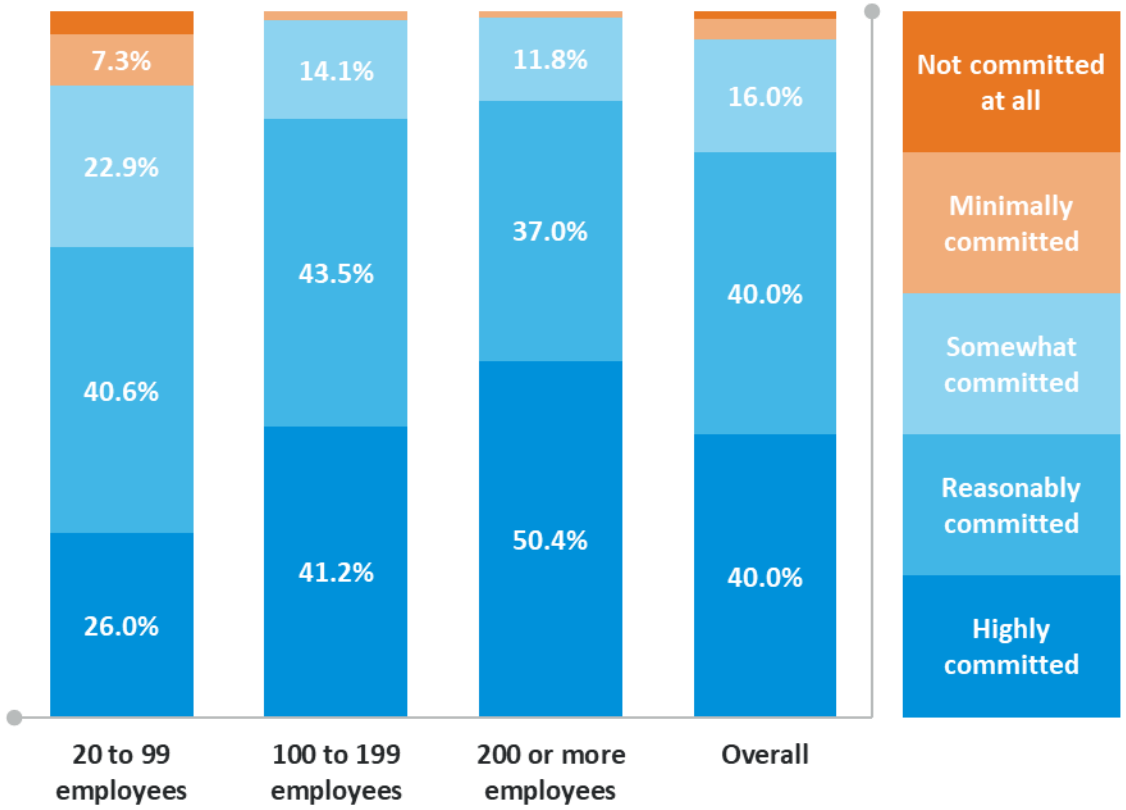


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

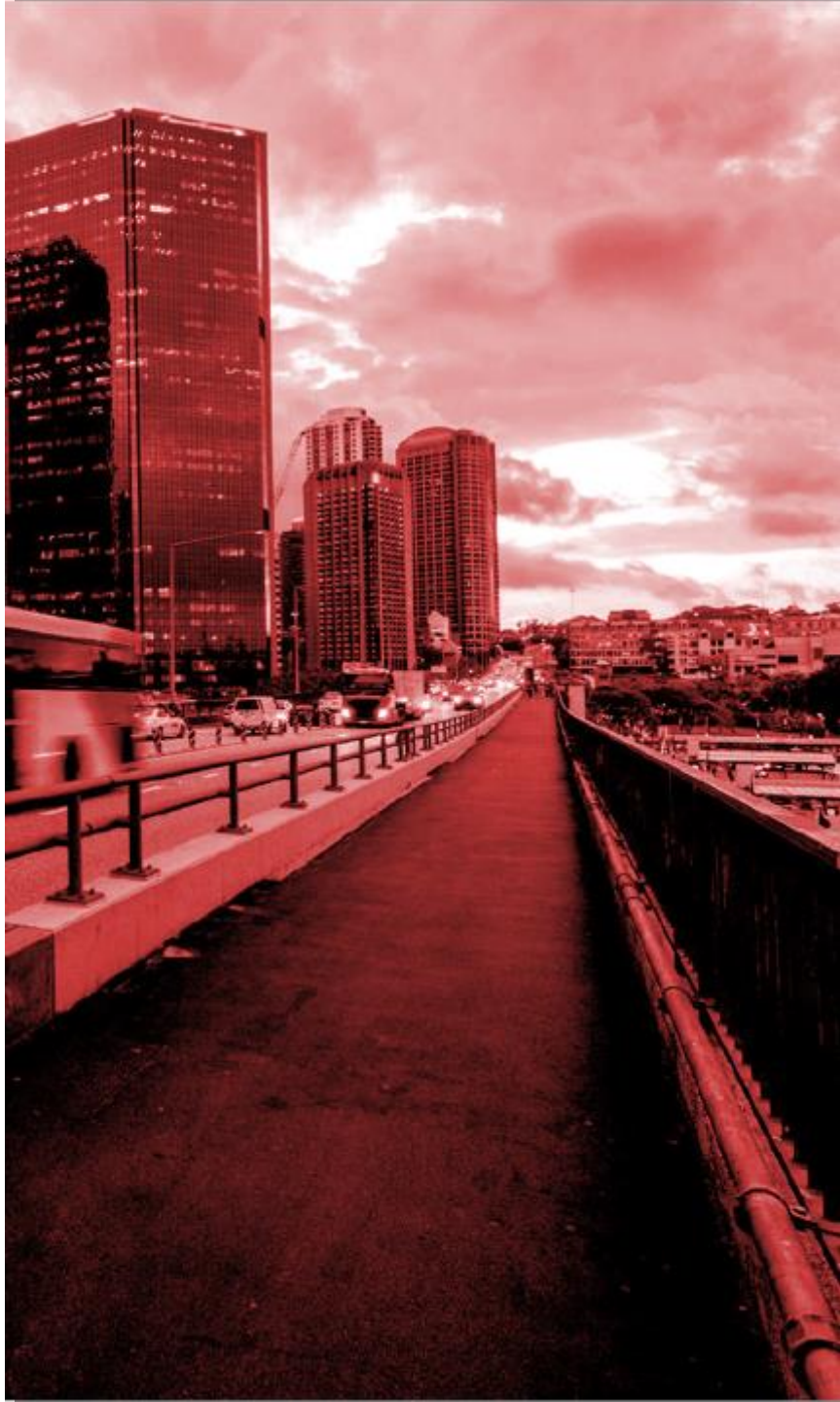
Cultural buy-in to taking security more seriously was needed in smaller organisations

Overall, how strong is your organisation's cultural commitment to IT security? (i.e. something the entire organisation top to bottom lives and breathes vs they just pay lip service to)



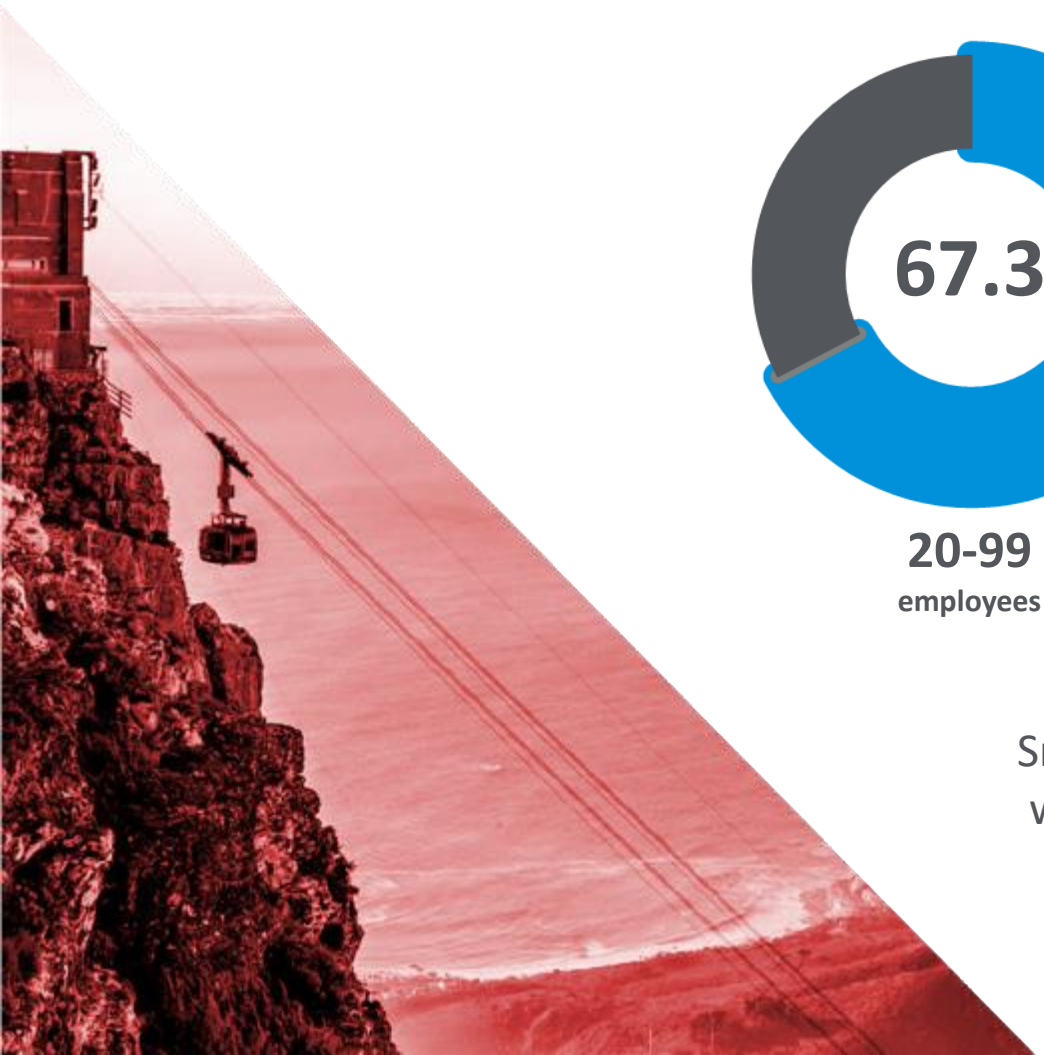
n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

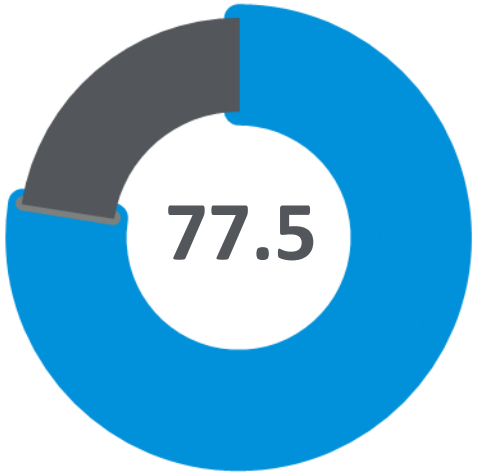


The platform component

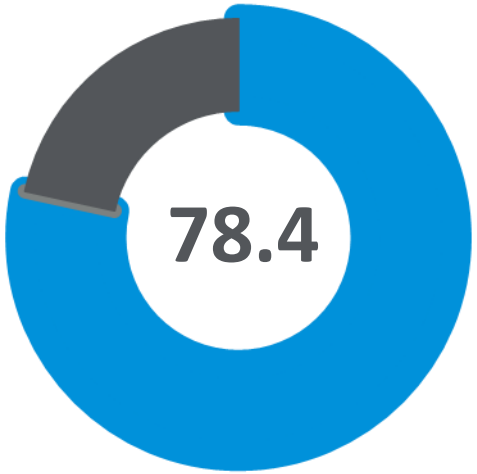
The *Platform* Component Index Results



20-99
employees



100-199
employees



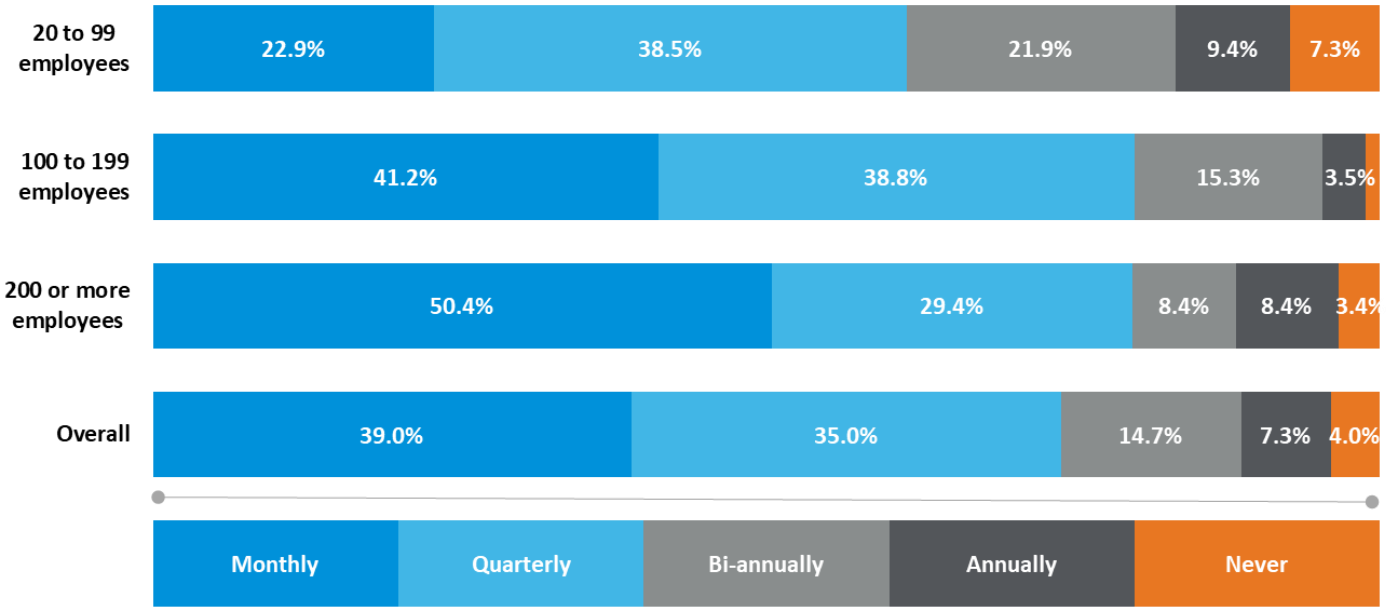
200+
employees

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Smaller companies were struggling to keep up with the rest of the pack when their *platforms* were assessed in the index. They struggled much more with scalability, and found it difficult to justify allocating many resources to IT.

Regular security testing was common, but 3.4% of large companies still never tested

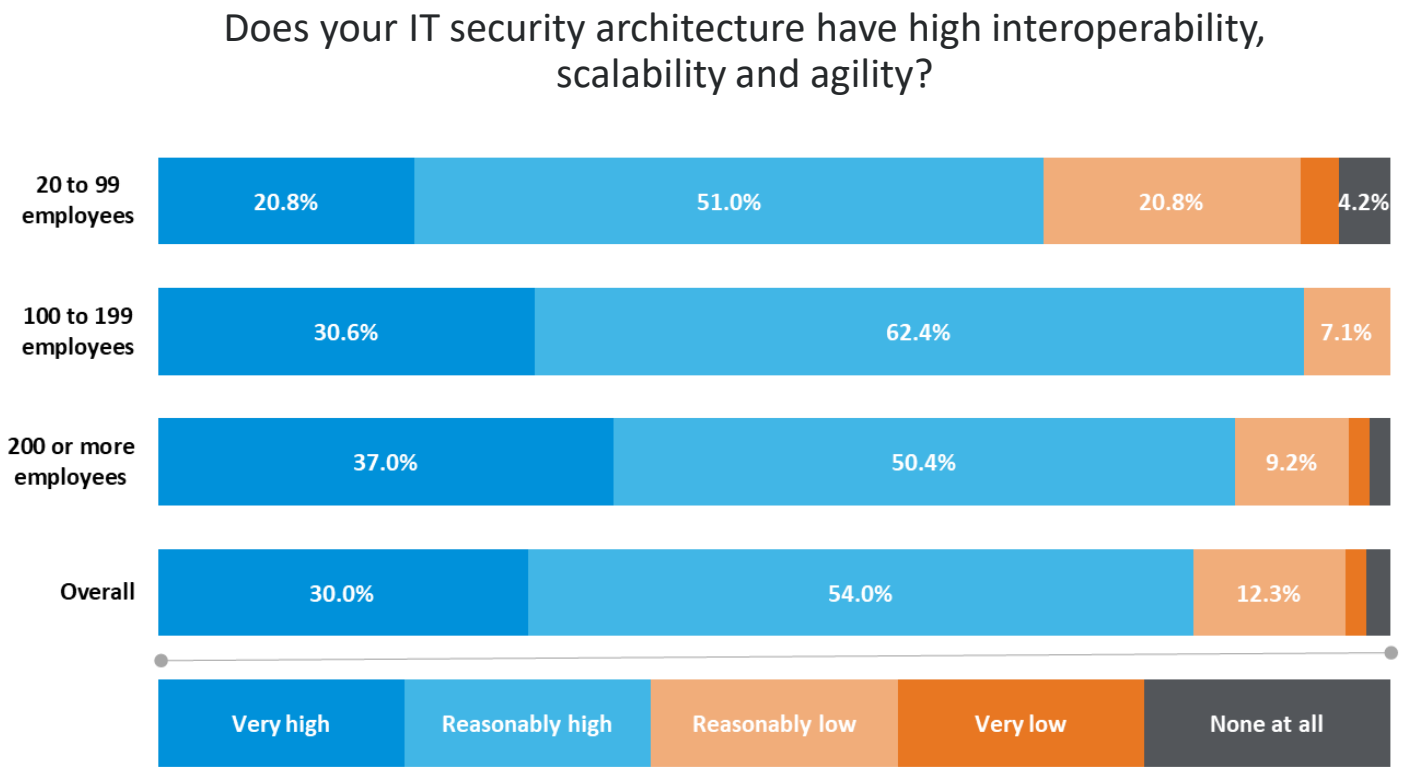
How often is network security testing conducted (including functional testing, vulnerability scanning and penetration scanning)?



n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Smaller companies were unprepared for IT infrastructure to grow with them

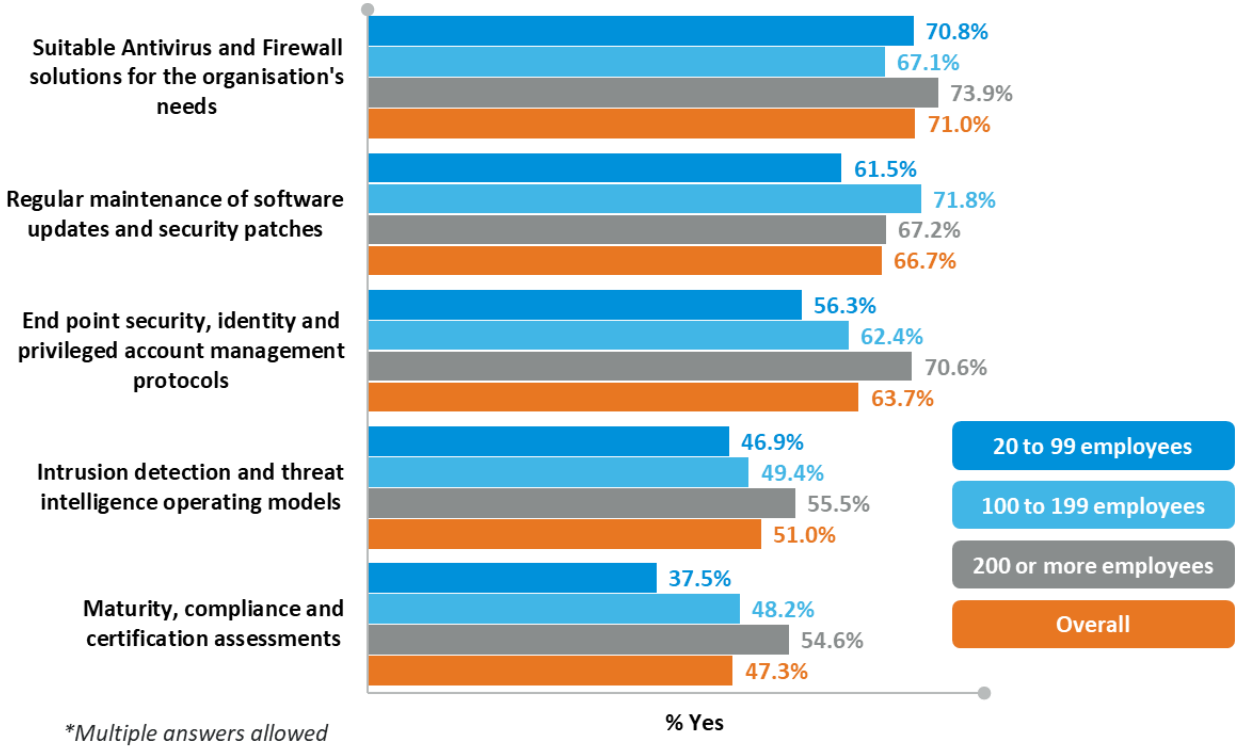


n = 300, overall (senior IT decision- makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Intrusion detection and compliance certification was lacking across the board

Do you currently have the following up to date?



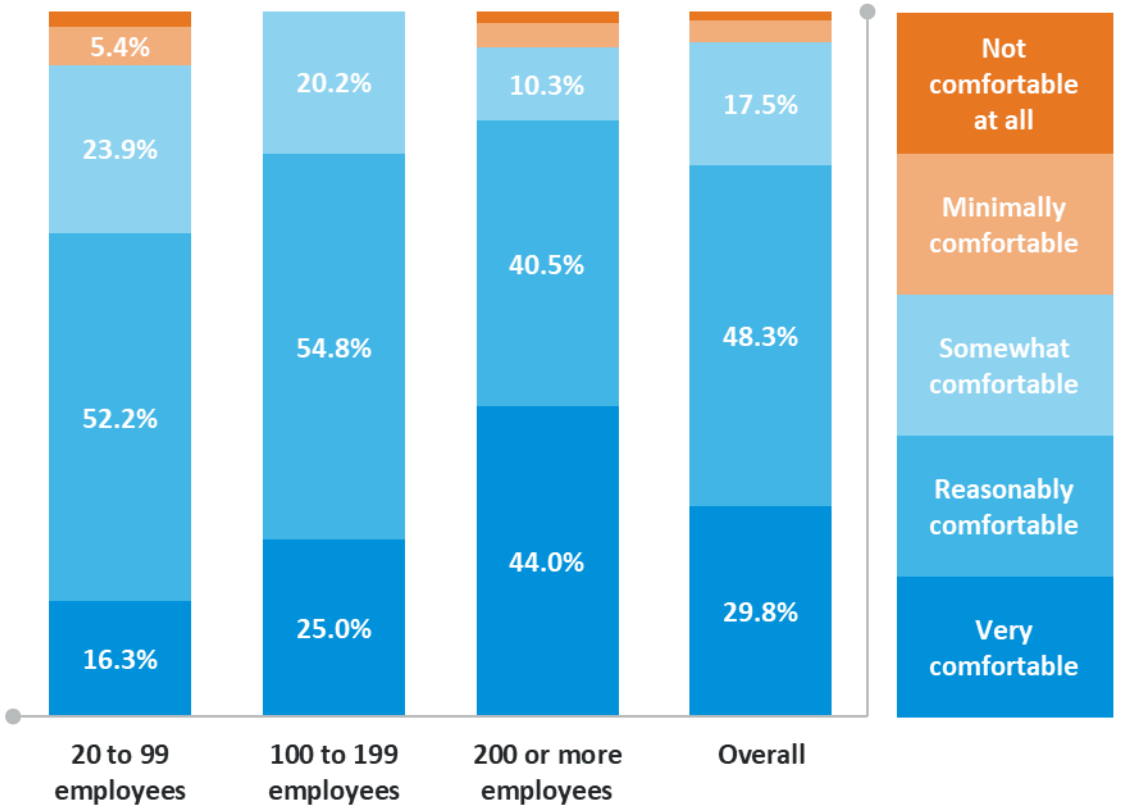
**Multiple answers allowed*

n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Comfort levels for companies in protection against attacks weren't particularly strong

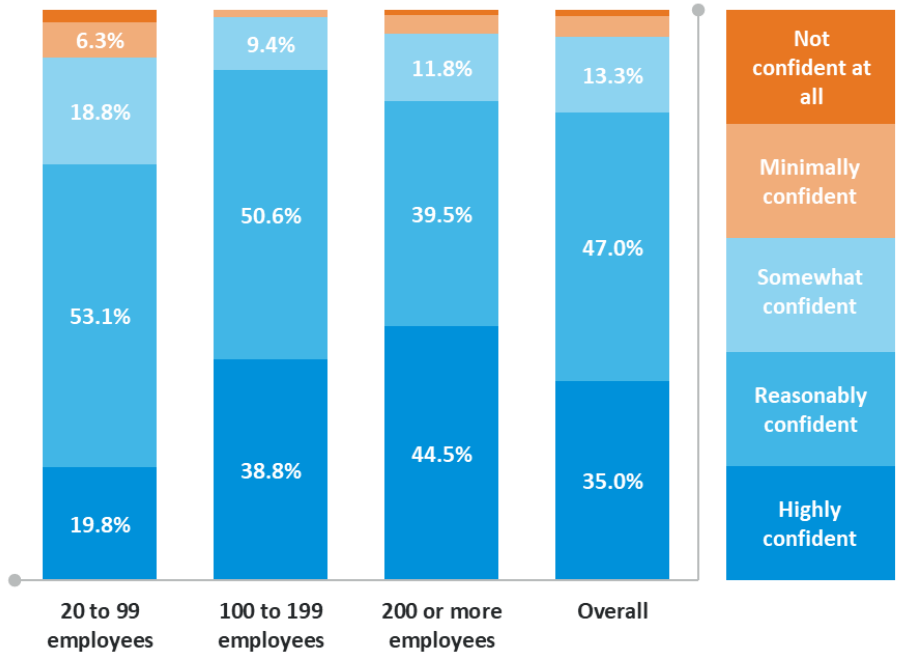
How comfortable are you that your distributed environment (if applicable) is protected across the entire attack surface?



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees;
85, 100 to 199 employees; 119, 200 or more employees

Cloud and networking security also lacked confidence

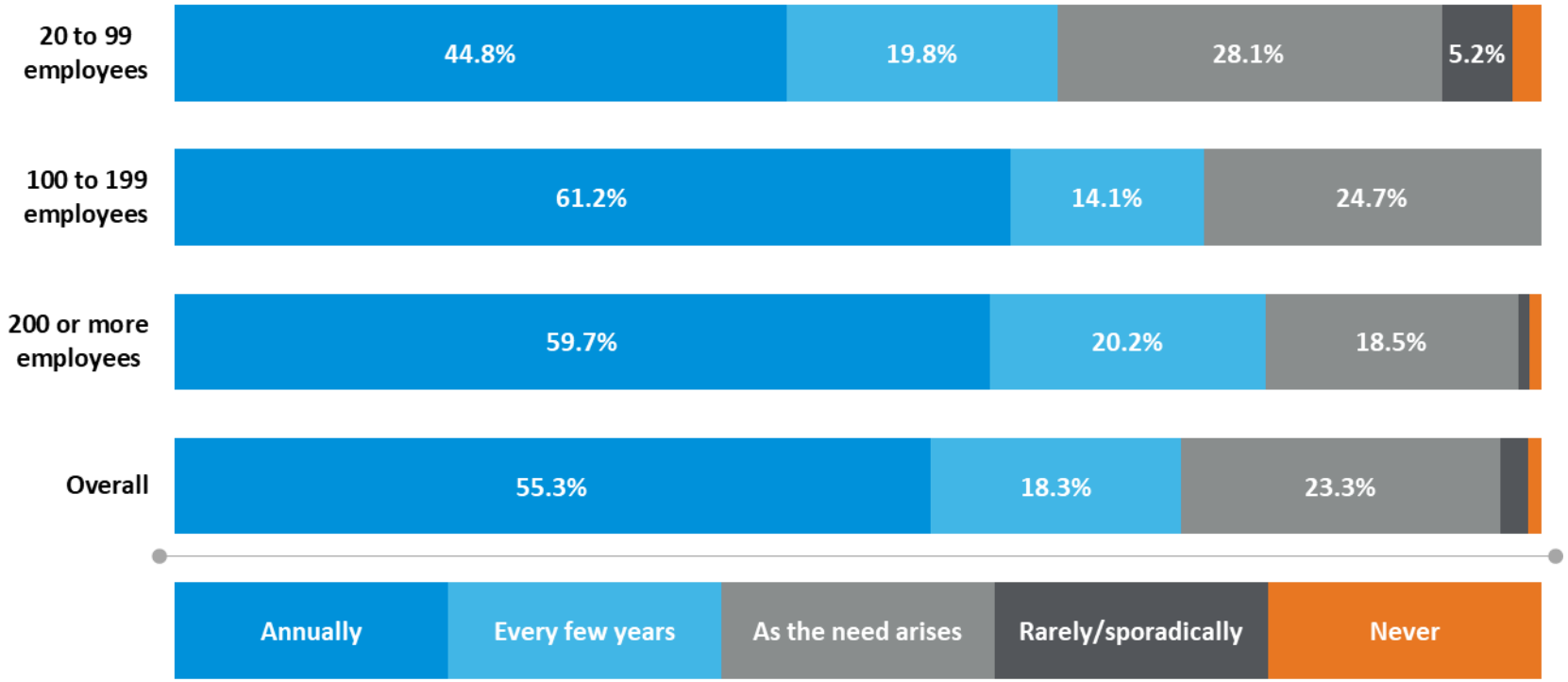
How confident are you that your networking and cloud security technologies are sufficient to protect current data assets and IT infrastructure?



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Periodic antivirus and firewall reviews weren't common

How often do you review the suitability of your antivirus and firewall solution providers for your organisation’s needs?

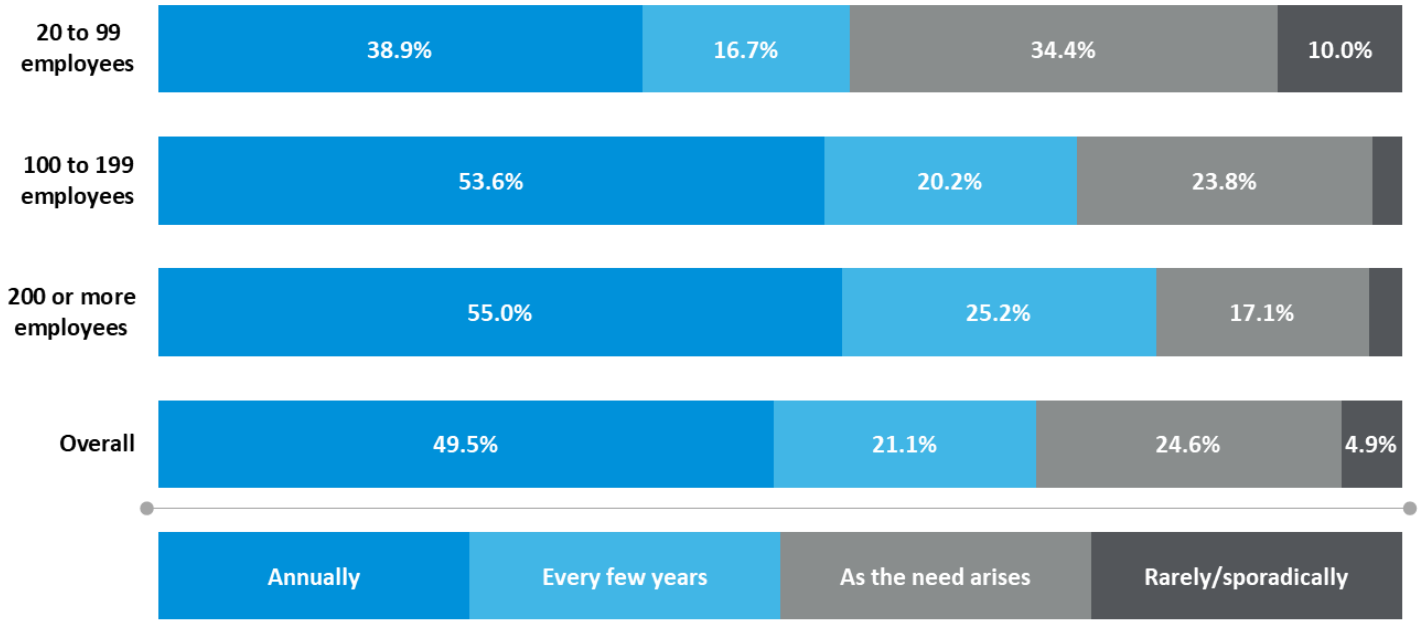


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

SD-WAN provider reviews were also relatively uncommon

How often do you review the suitability of your SD-WAN provider (software-defined networking in a wide area network) for your organisation's needs?



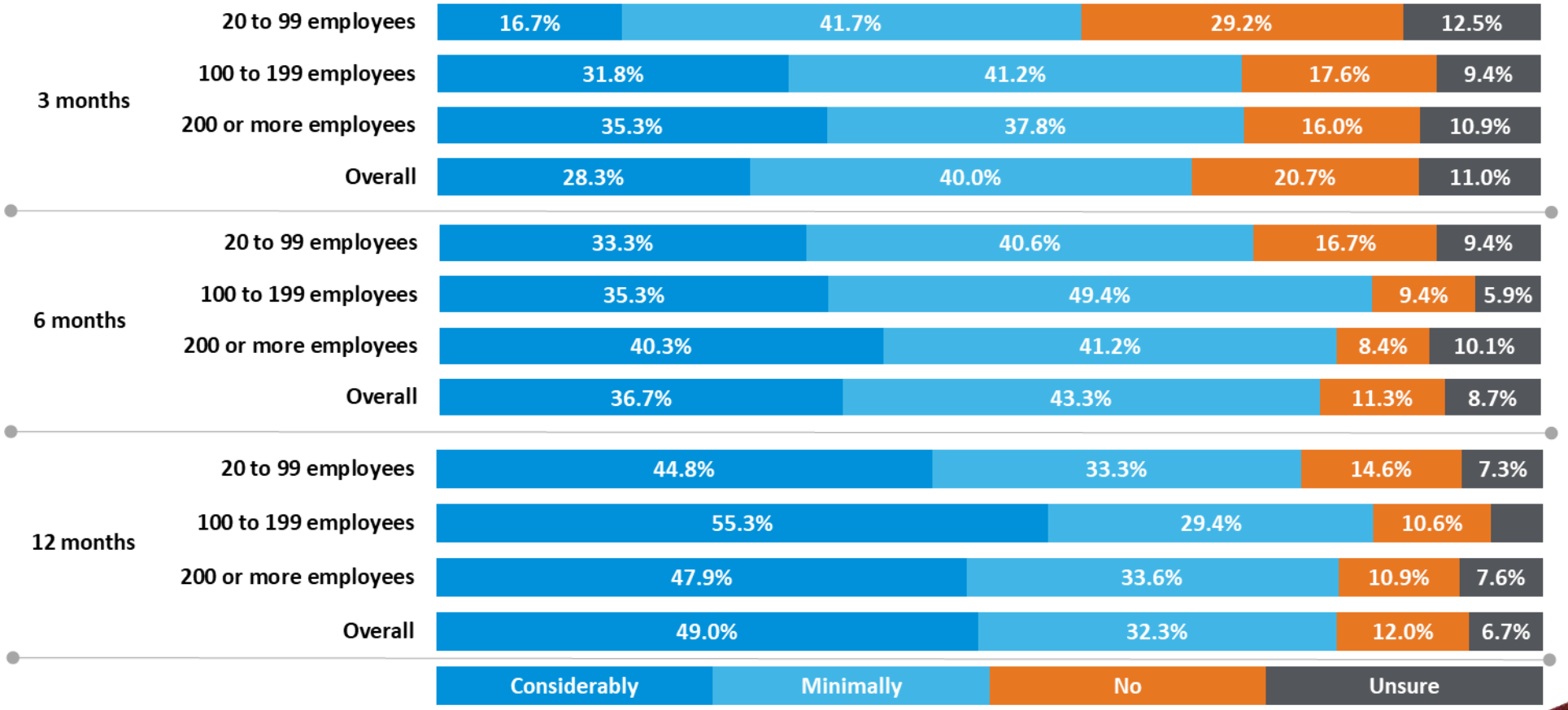
n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Beyond the index: investment and adoption

Considerable IT infrastructure investment was evident over the last year

Have you invested in your IT infrastructure in the last…?

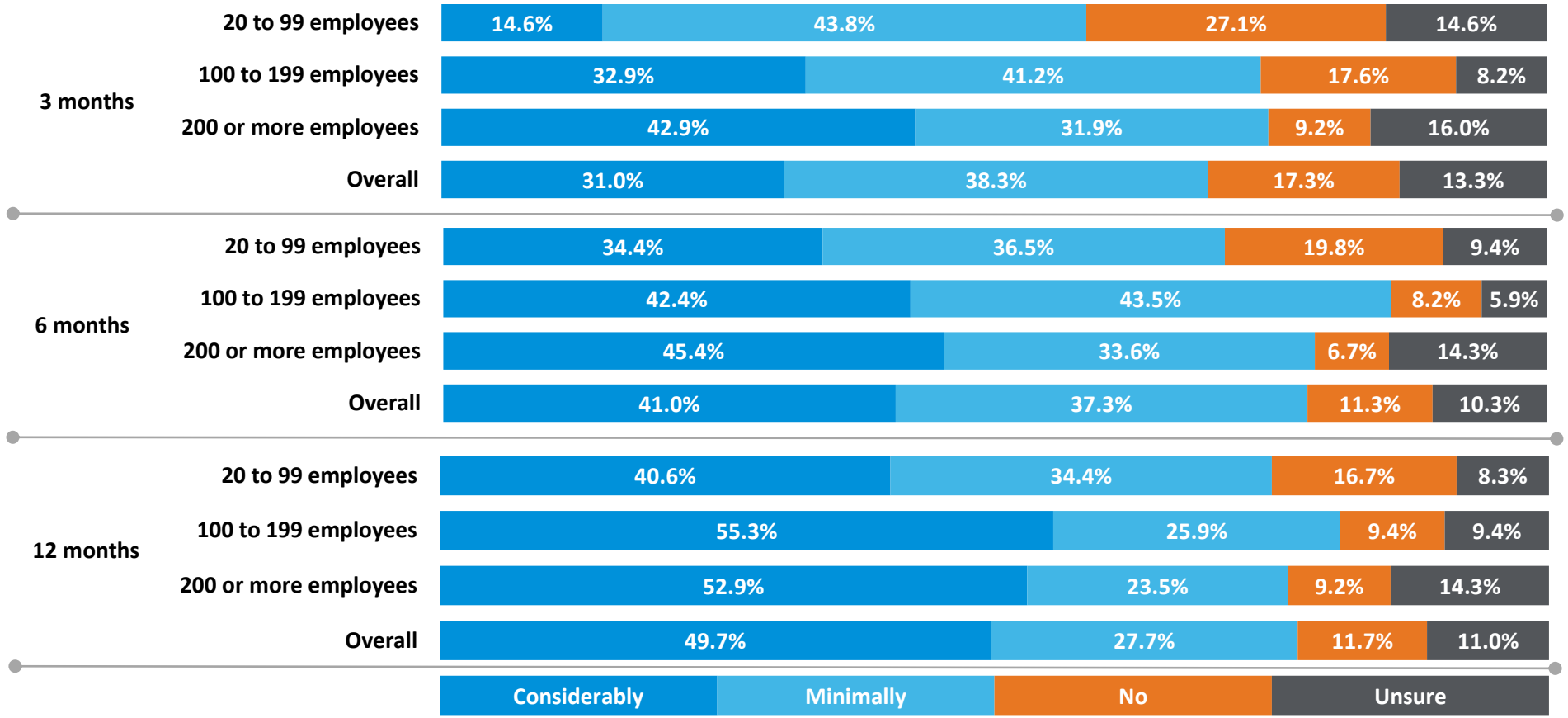


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

This level of investment appeared to be ongoing over the next year

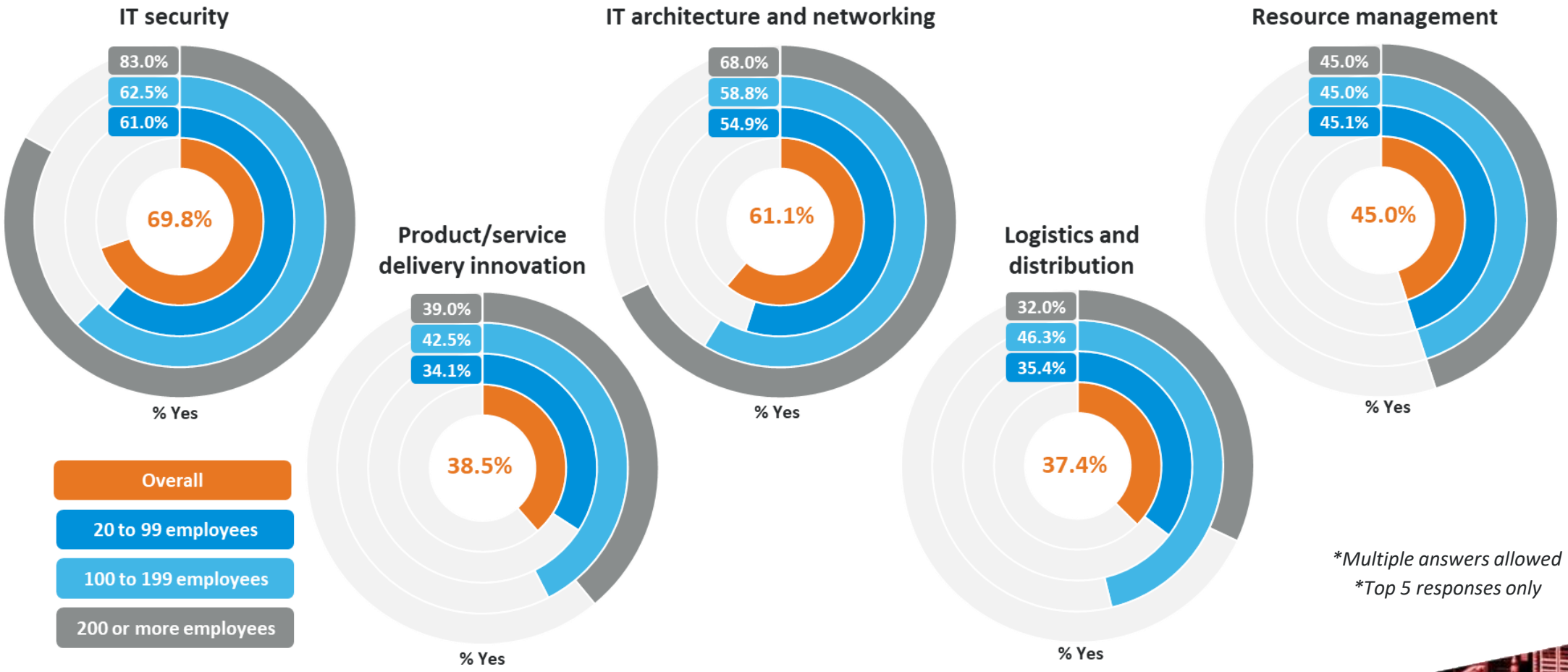
Are you planning to invest in your IT infrastructure in the next…?



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

IT security and architecture were the two main investment priorities

What areas will likely be the next IT infrastructure investments for your business?

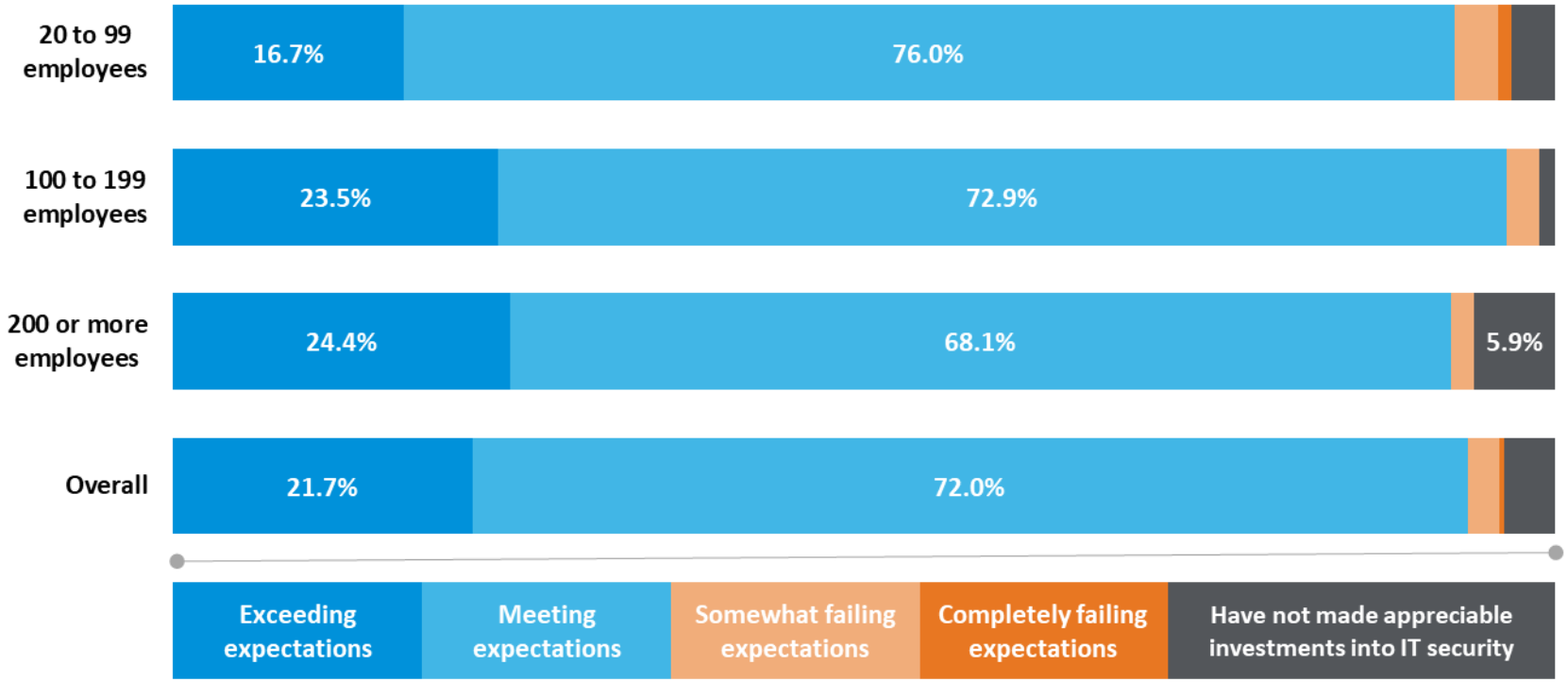


*Multiple answers allowed
*Top 5 responses only

n = 262, senior IT decision-makers who are planning to invest in IT infrastructure in the next 3-12 months
n = 82, organisations with 20 to 99 employees; 80, 100 to 199 employees; 100, 200 or more employees

Most IT security investment mets or exceeded expectations

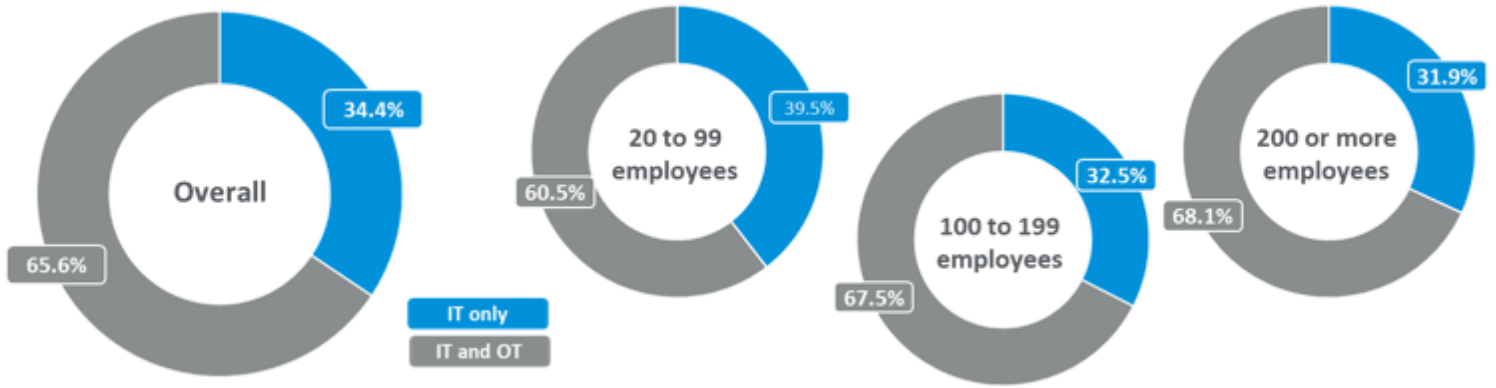
To date, have you seen the business benefits expected from your IT security investment? (e.g. key risks mitigated, operational efficiencies and improved performance metrics.)



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

About one third of companies had an IT-only environment

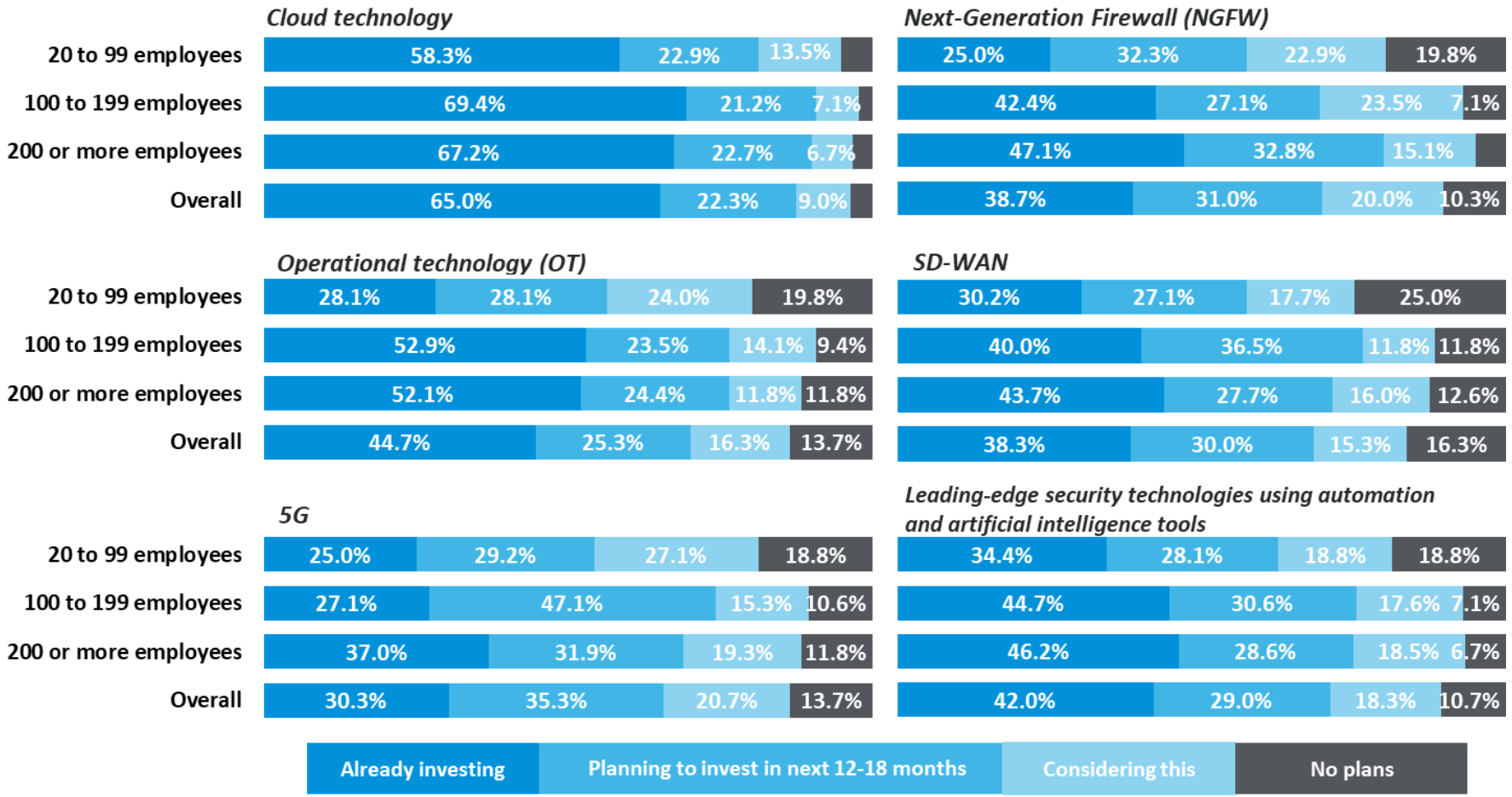
Does your business support both an IT and OT (operational technology) environment?



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Cloud technology headlined future infrastructure plans

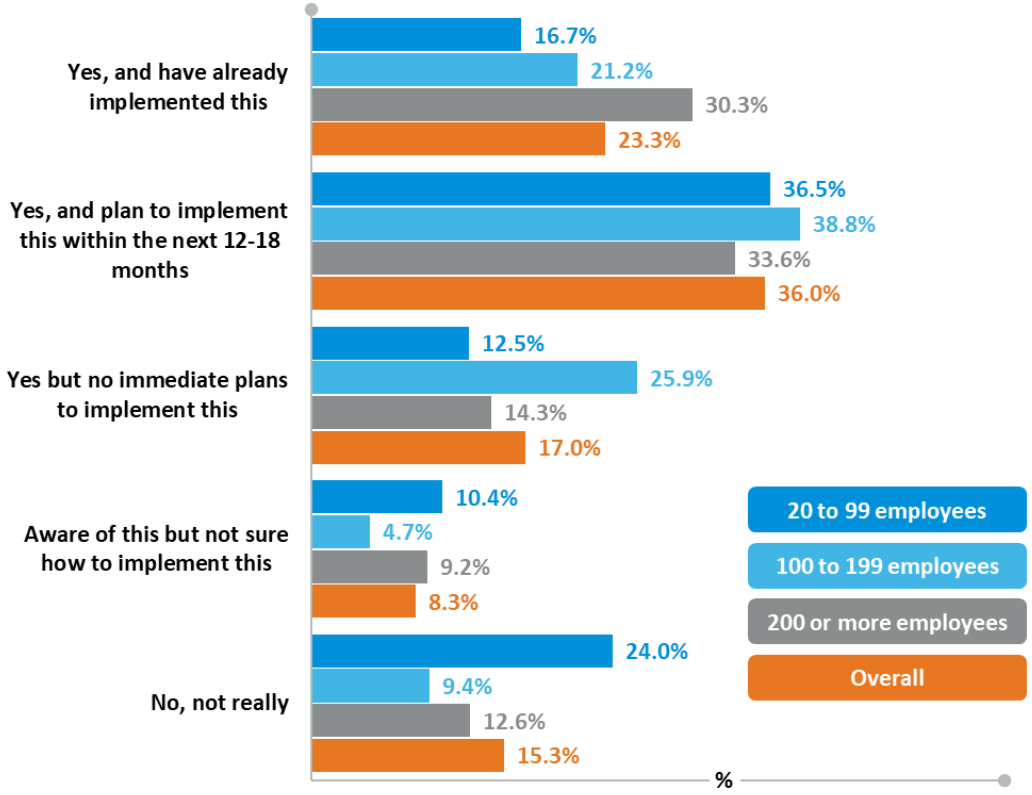
Is your organisation currently or planning to invest in any of the following technologies?



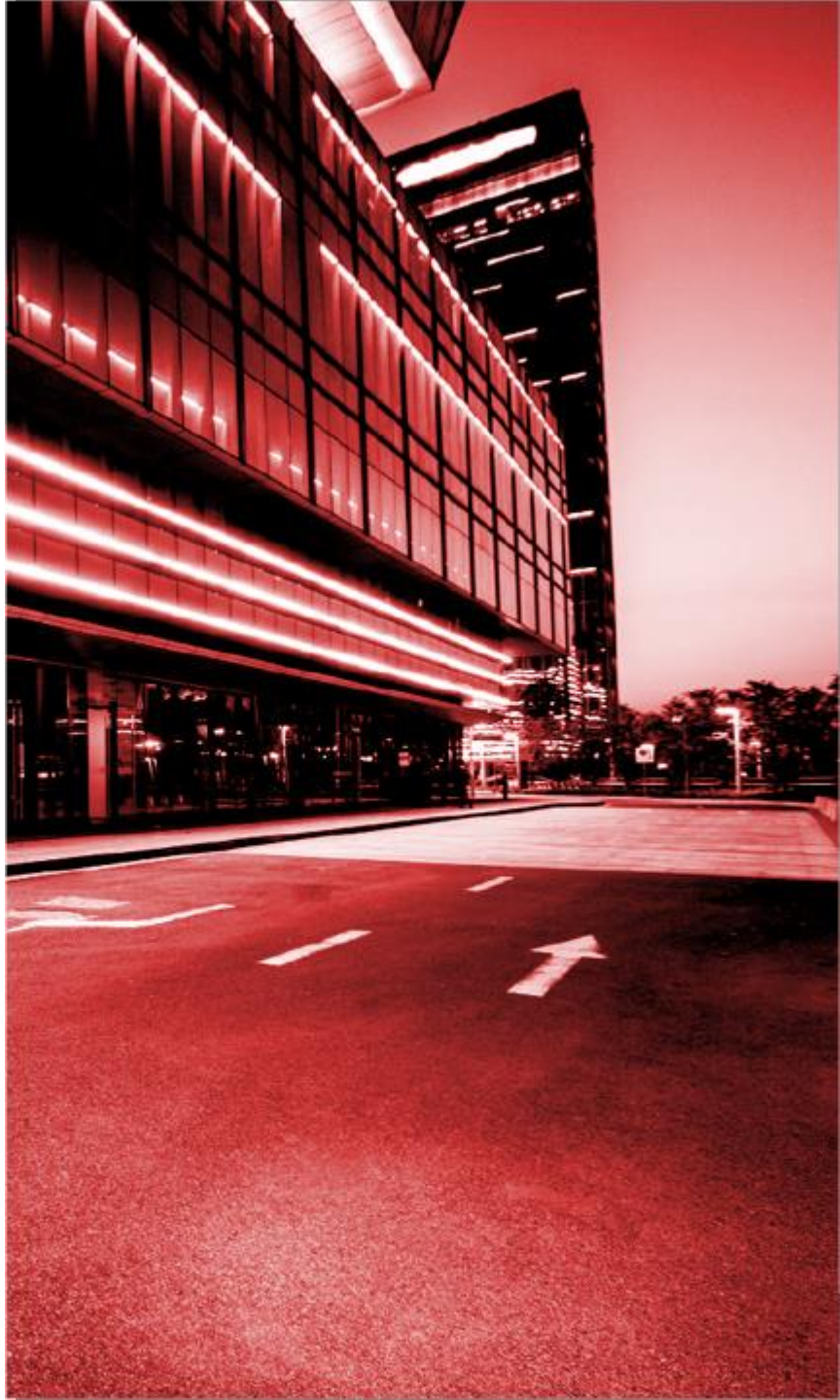
n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Zero trust security had strong awareness but implementation remained low

Are you aware of zero trust security and how to implement it into your organisation?

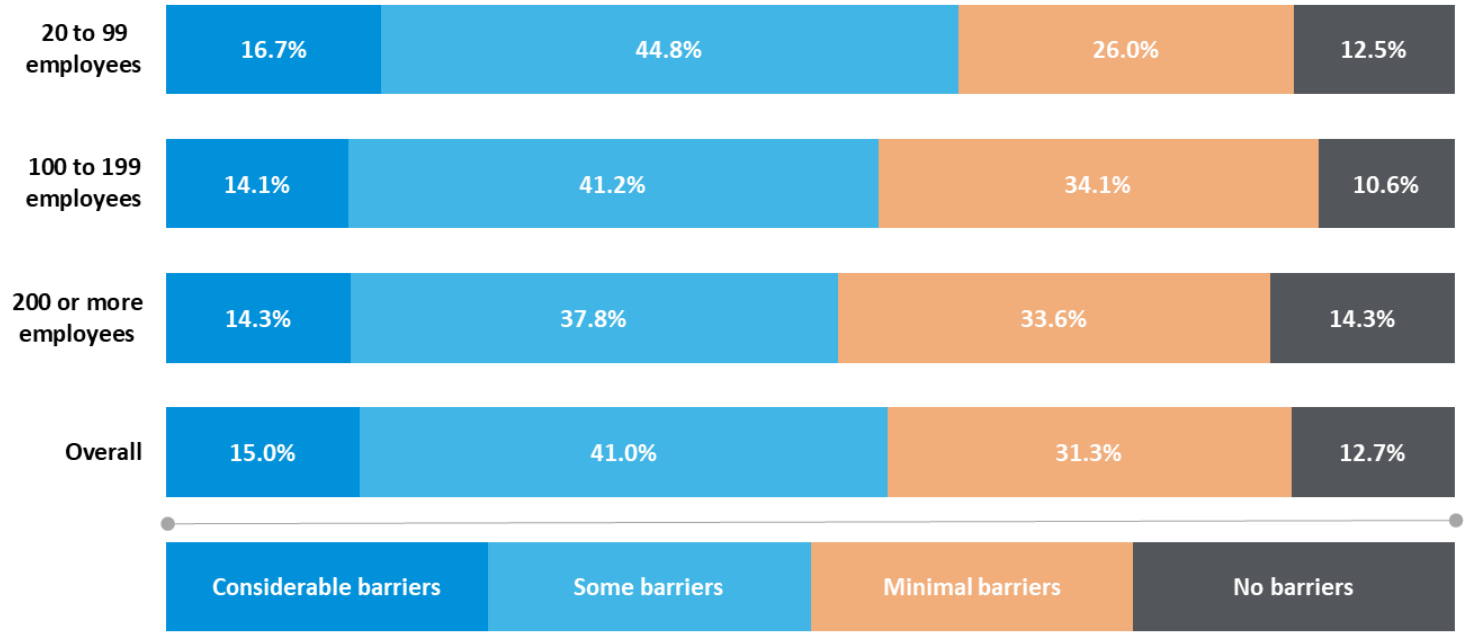


n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees



Most companies faced at least some barriers in cybersecurity upgrades

Do you feel there are barriers to upgrading your cybersecurity systems and processes as required?

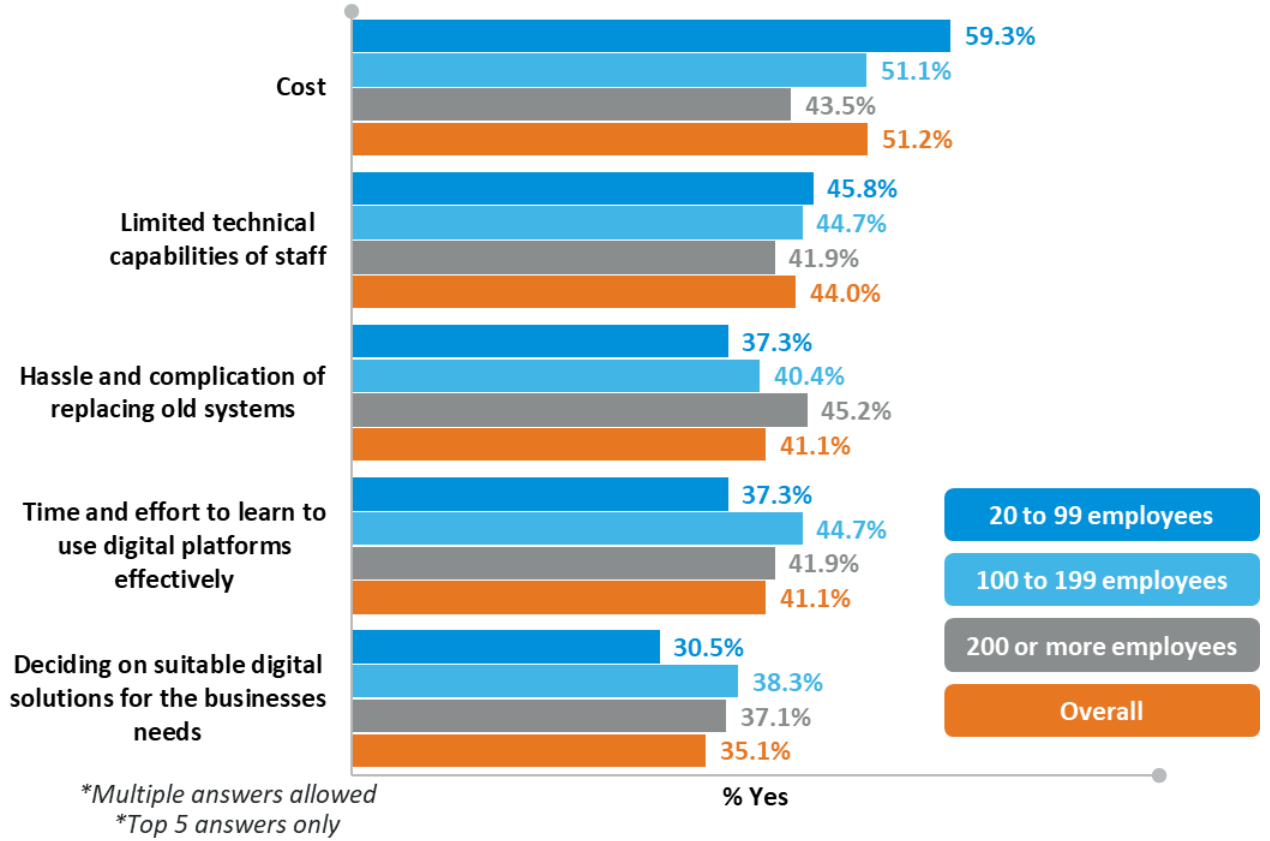


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

The effort and hassle of technological upgrade were the biggest barriers for larger companies, while smaller companies worried more about cost

What are the main barriers to upgrading your cybersecurity systems and processes?



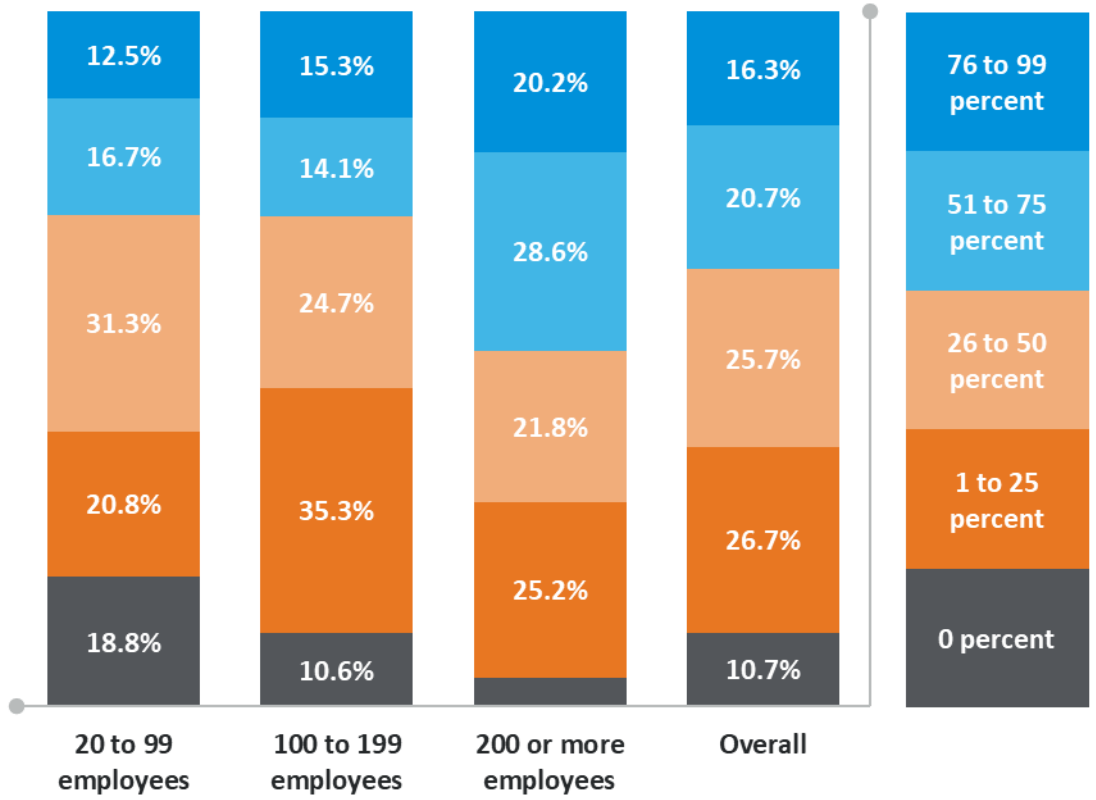
*Multiple answers allowed
*Top 5 answers only

n = 168, overall (senior IT decision-makers who think there are barriers in upgrading their cybersecurity systems)
n = 59, organisations with 20 to 99 employees; 47, 100 to 199 employees; 62, 200 or more employees

Beyond the index: vulnerabilities

Most companies had a sizeable proportion of employees working remotely

Approximately what percentage of your current workforce is working remotely to at least some degree? Indicate 0 if none.

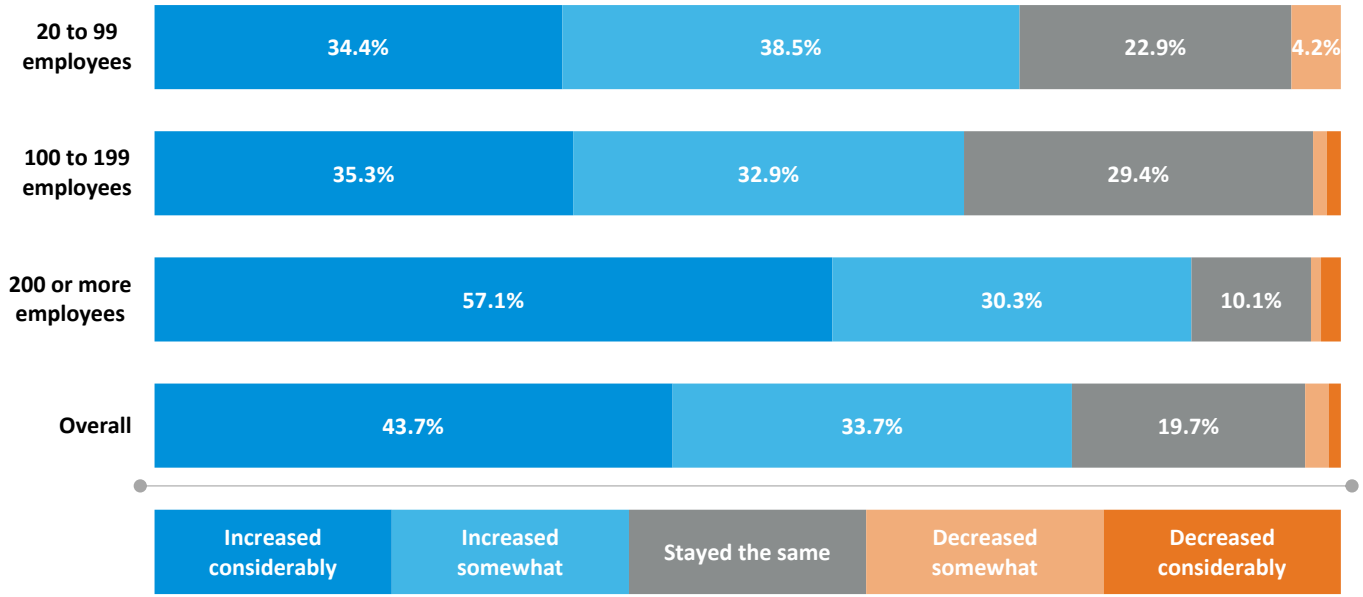


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees;
85, 100 to 199 employees; 119, 200 or more employees

Most companies saw a large increase in their remote workforce

Has this increased, decreased or stayed the same compare to 12 months ago?

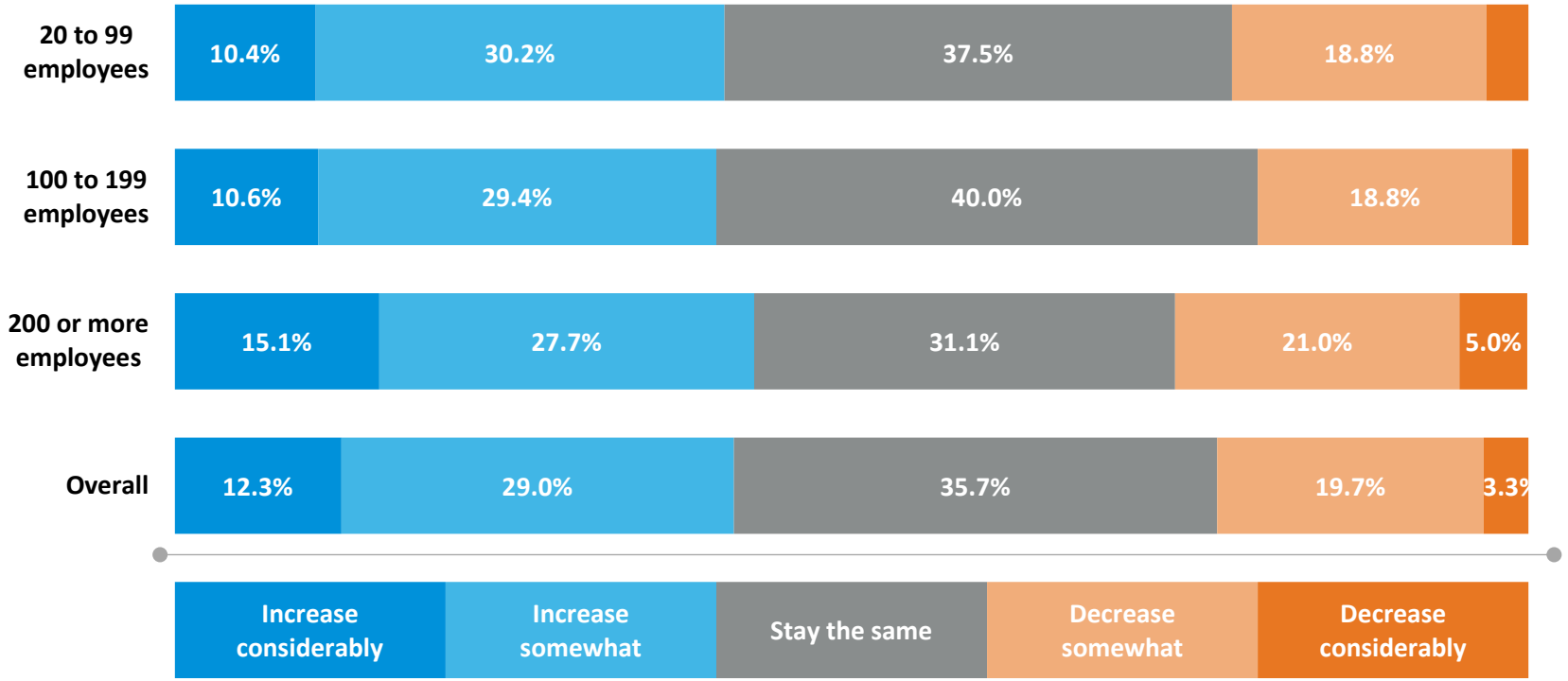


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Few forecast their remote workforce would decrease

Do you anticipate this to increase, decrease or stay the same over the next 12 months?

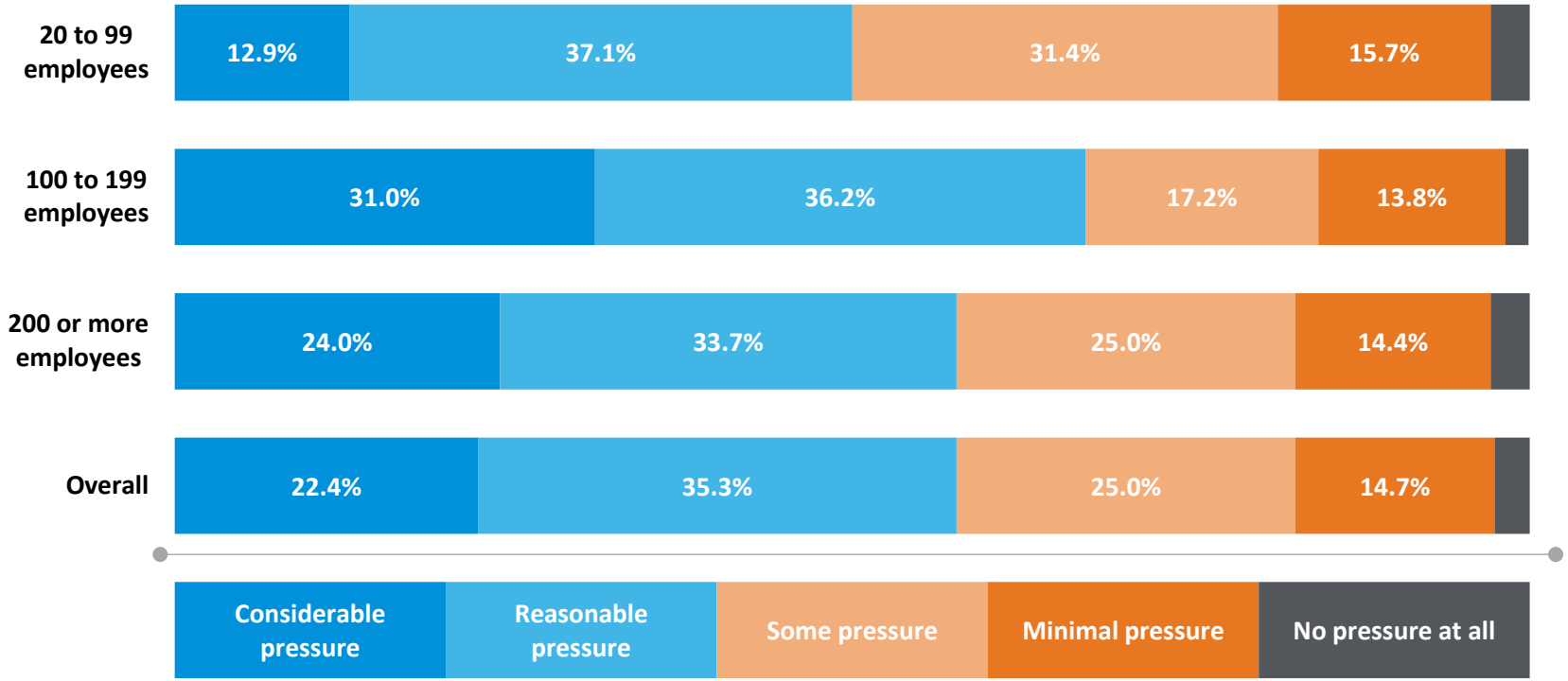


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

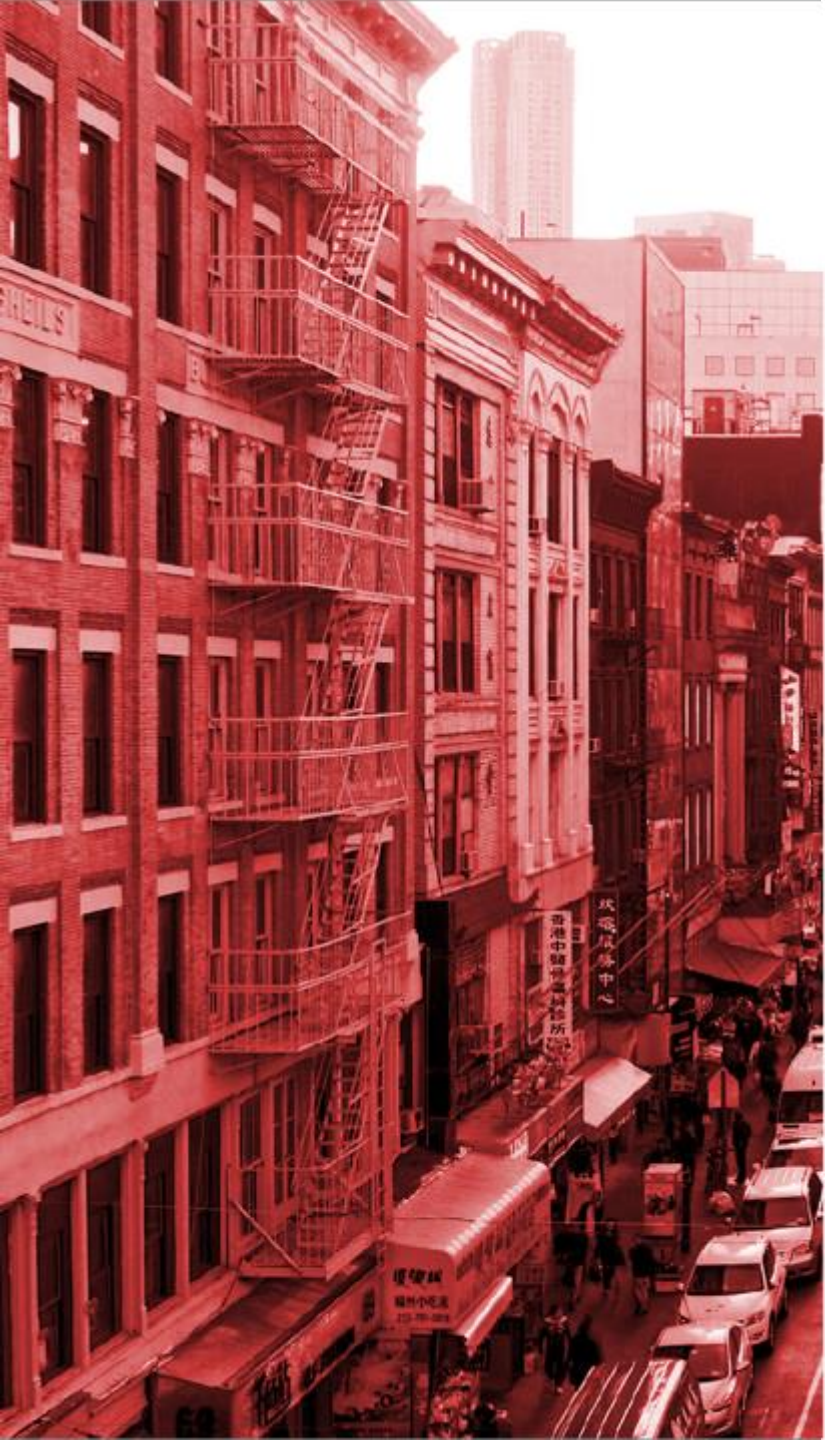
Most agreed it had put pressure on their current infrastructure

Has a move to a distributed workforce put additional pressure on your IT infrastructure?



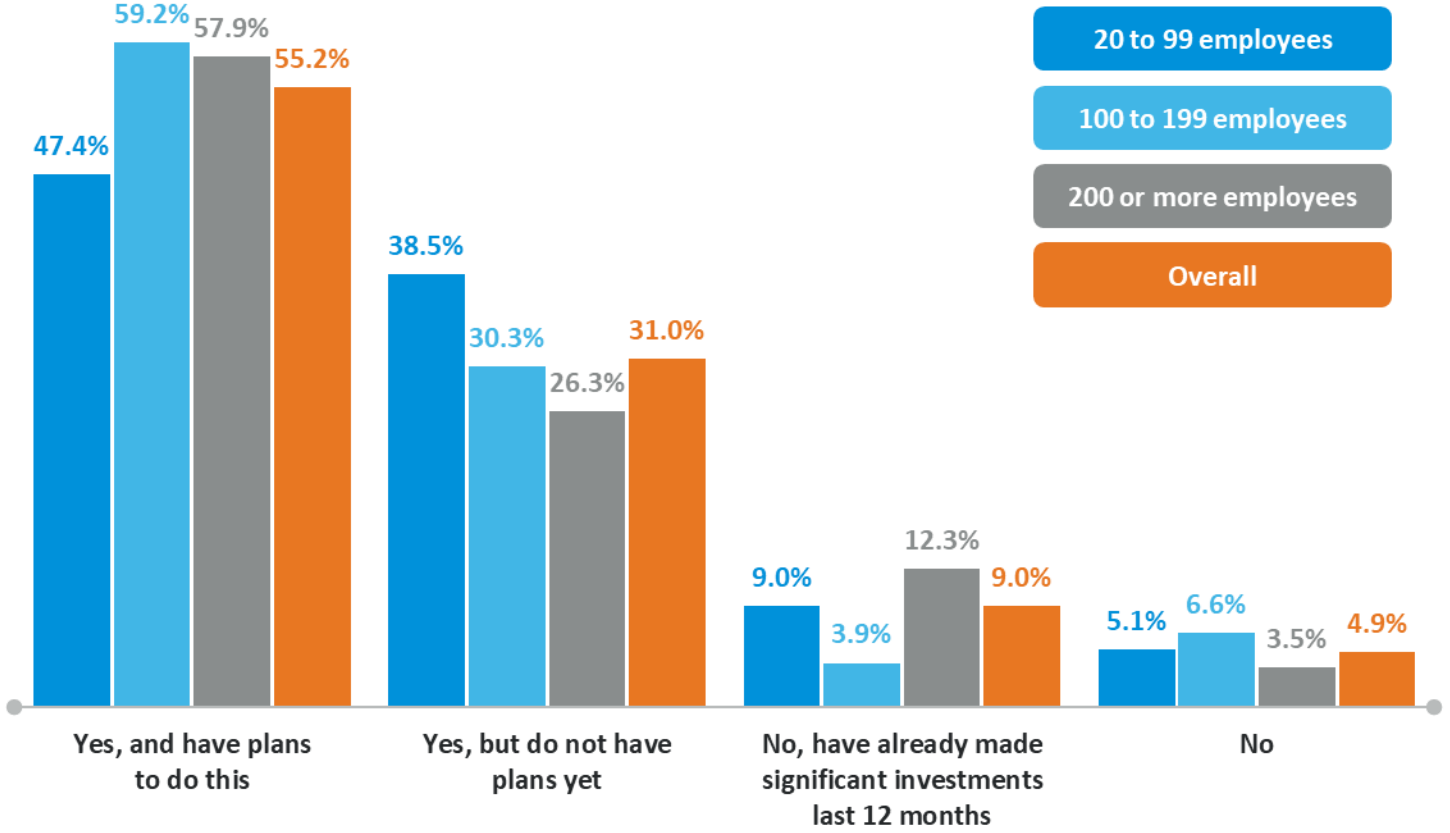
n = 232, overall (those whose remote workforce has increased in the past 12 months)

n = 70, organisations with 20 to 99 employees; 58, 100 to 199 employees; 104, 200 or more employees



Most agreed IT investment was needed to better protect their remote workforces

Do you anticipate investing more in IT security to better protect your remote workforce in the next 12 months?

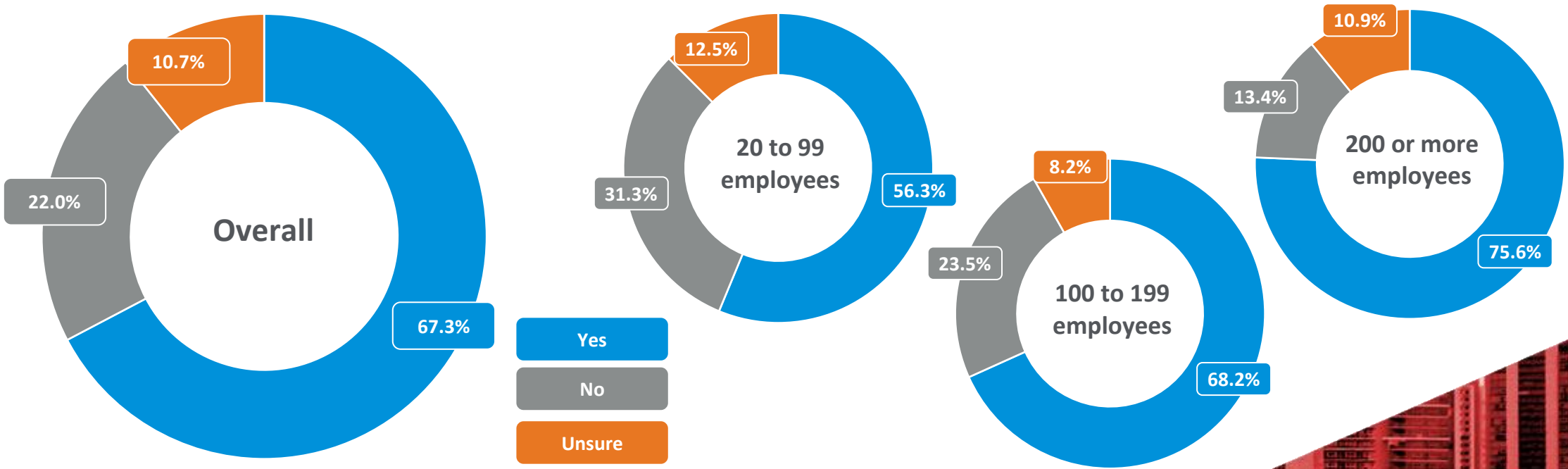


n = 268, overall (senior IT decision-makers whose organisations had a remote workforce)

n = 78, organisations with 20 to 99 employees; 76, 100 to 199 employees; 114, 200 or more employees

A significant IT breach is a major risk to most business operations

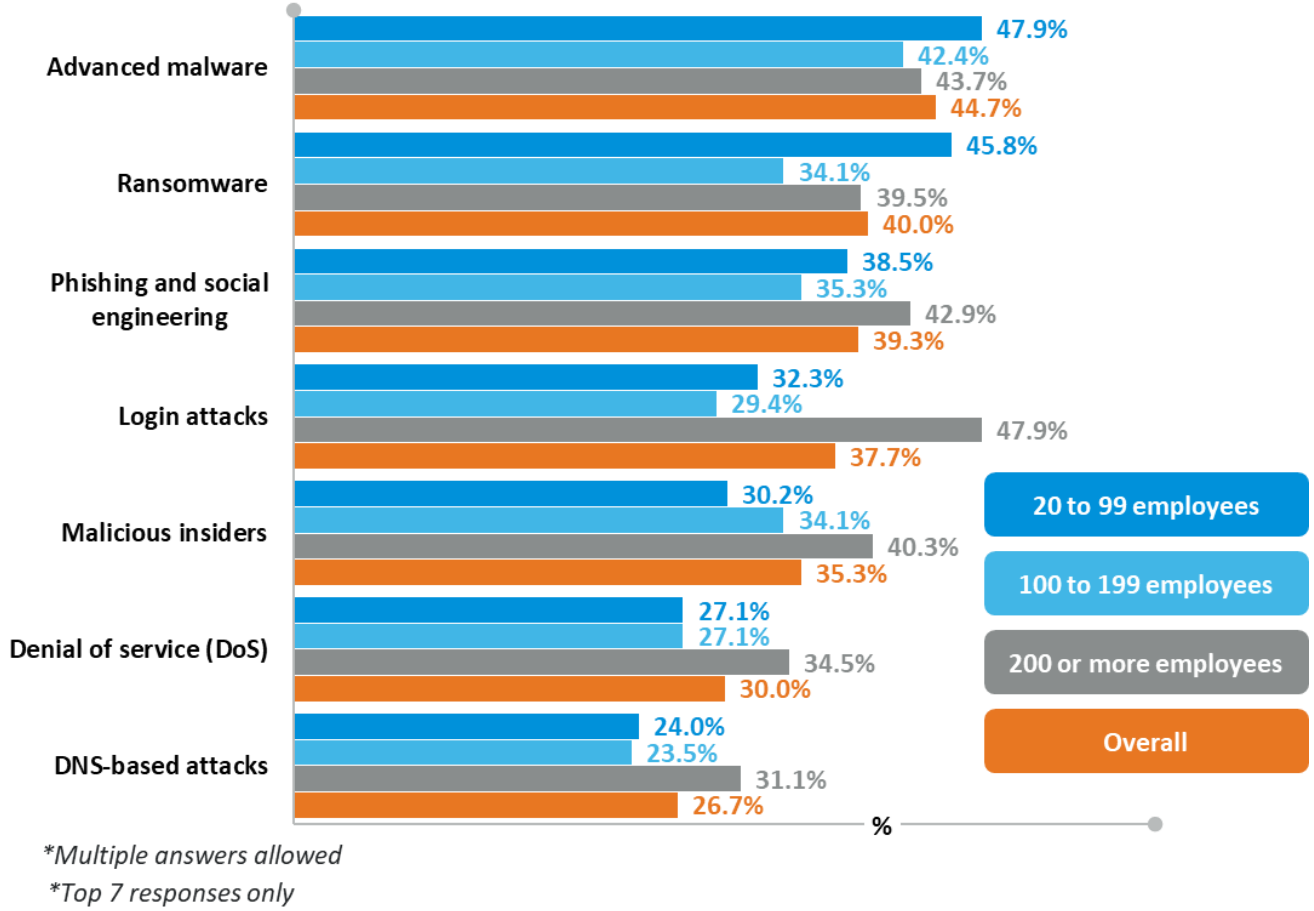
Do you believe a significant IT security breach can cause your business to cease operating over time and/or incur a significant cost?



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Malware and ransomware were the main concerns for smaller organisations, with larger ones more concerned about login attacks

What are the IT security threats you are most concerned about for your organisation in 2021?



*Multiple answers allowed

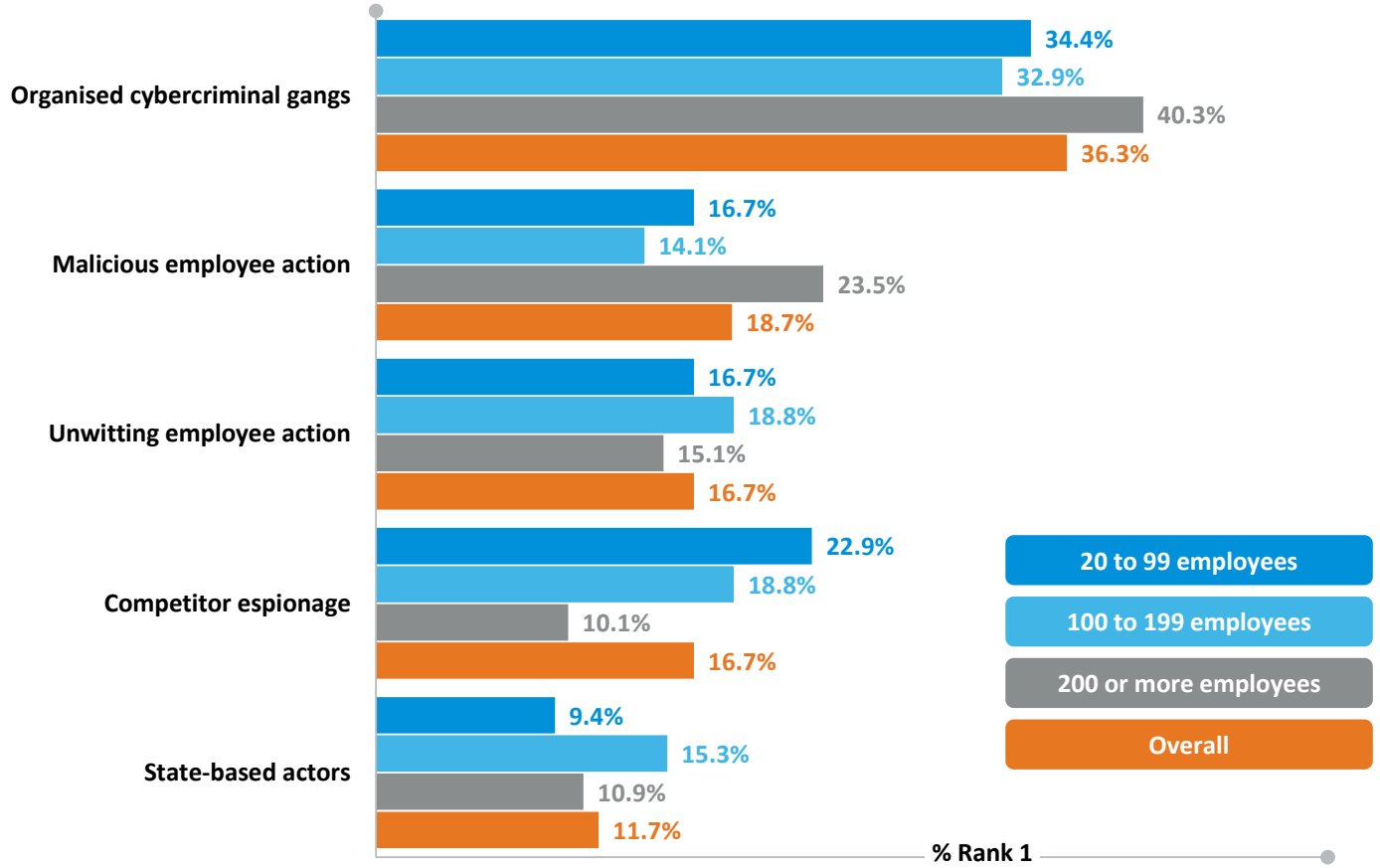
*Top 7 responses only

n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Cybercriminals and employee actions were the main perceived threats

In order of concern, rank where you believe your greatest IT security threats come from?

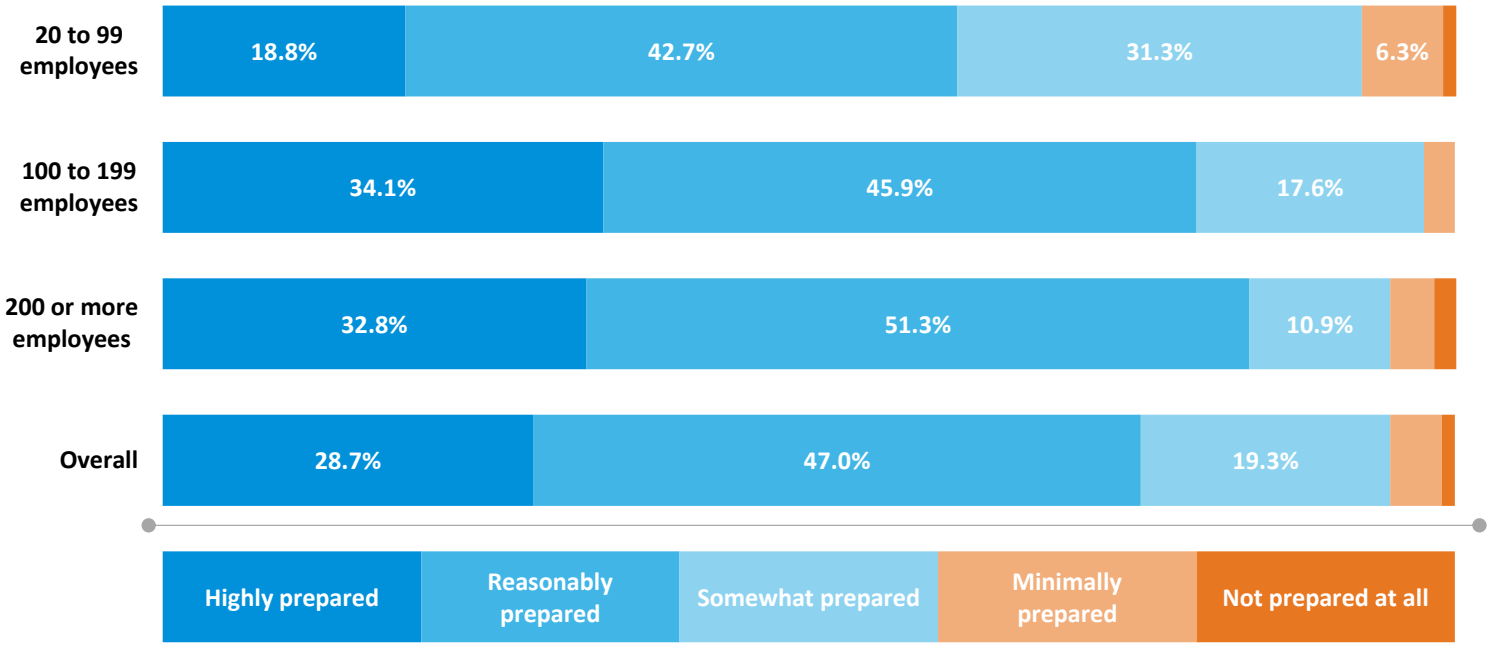


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Most companies still felt at least reasonably prepared for a security threat

Overall, how prepared for an IT security threat do you think your organisation currently is?



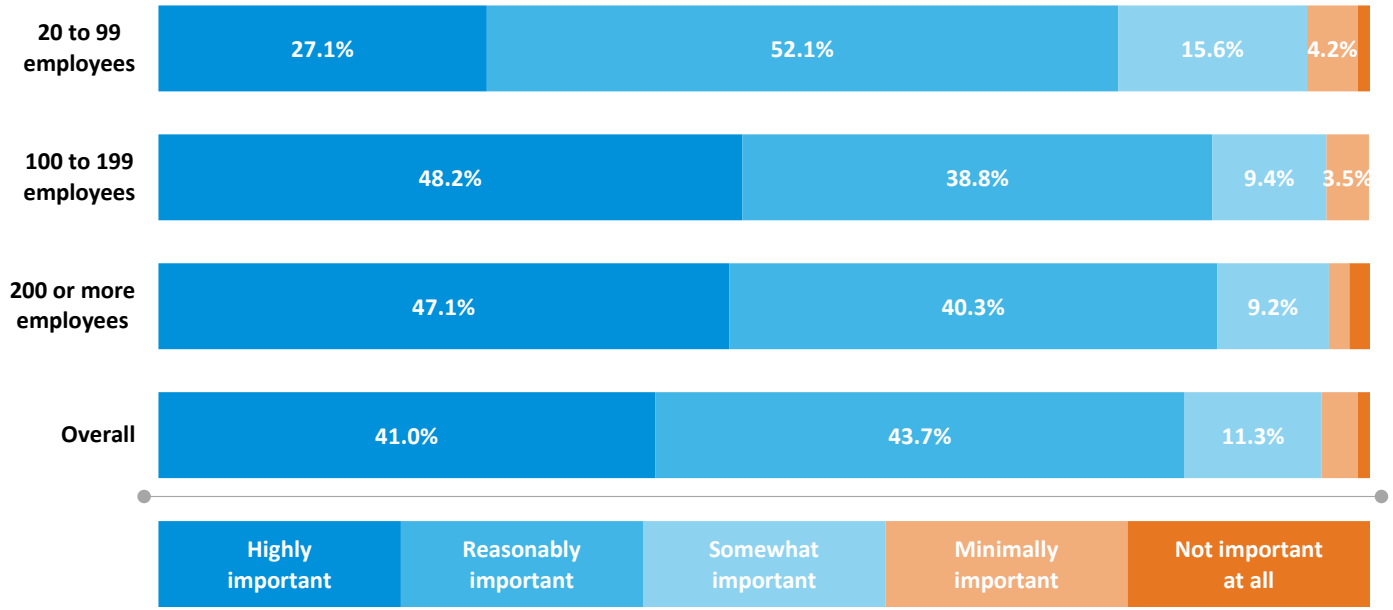
n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Beyond the index: decision-making

Network efficiency ranked high as a priority for Australian organisations

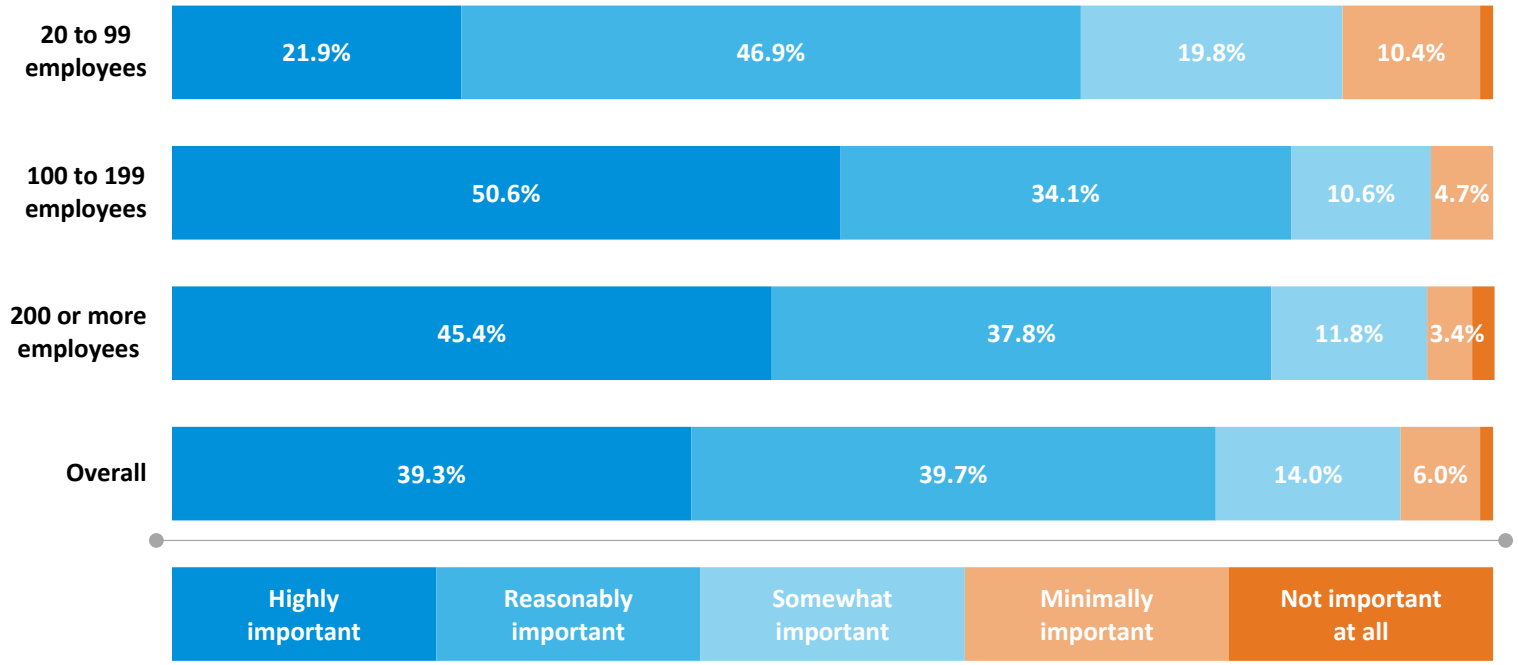
How important to your organisation is introducing efficiency into network operations?



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Companies placed high importance on simplifying their IT operations

How important to your organisation is simplifying IT complexity in network operations?

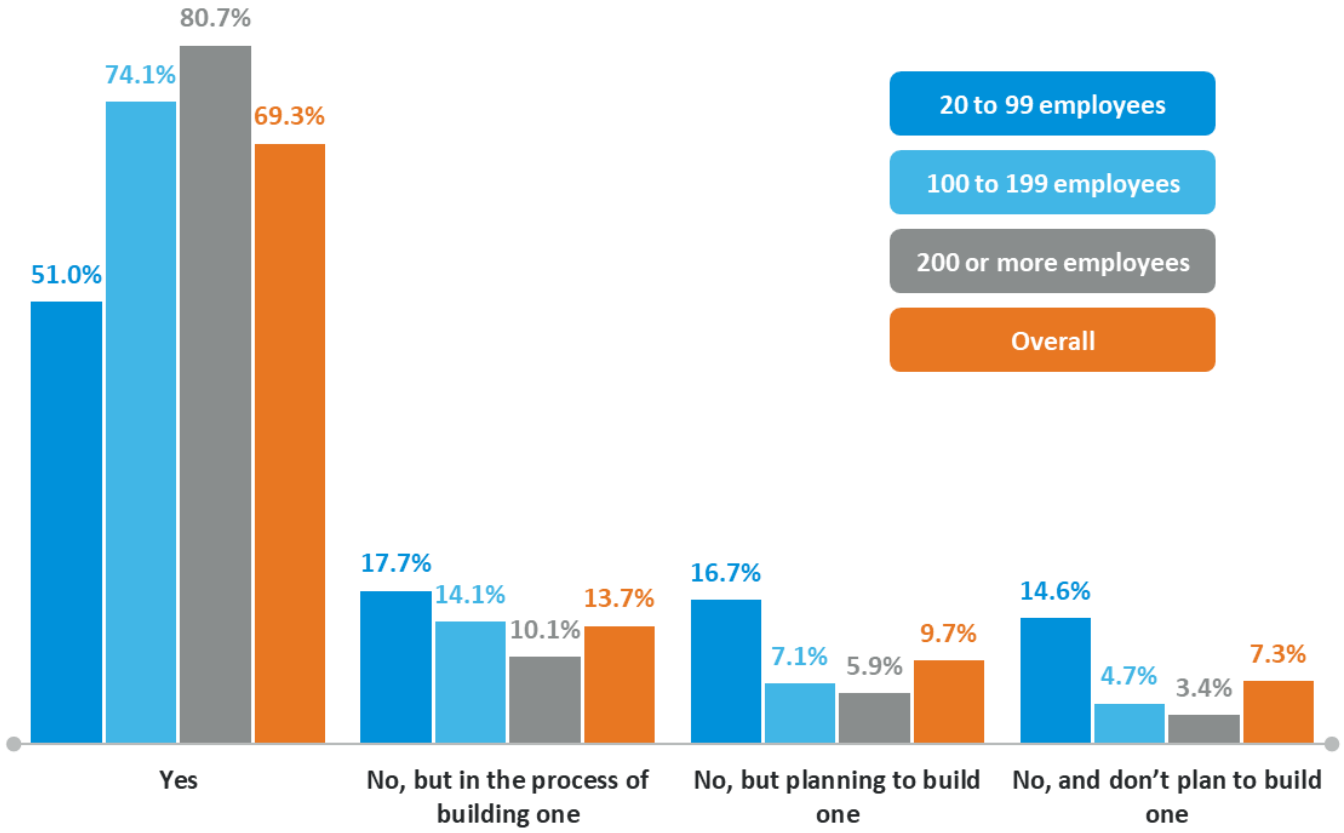


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Larger companies were more likely to have dedicated security management

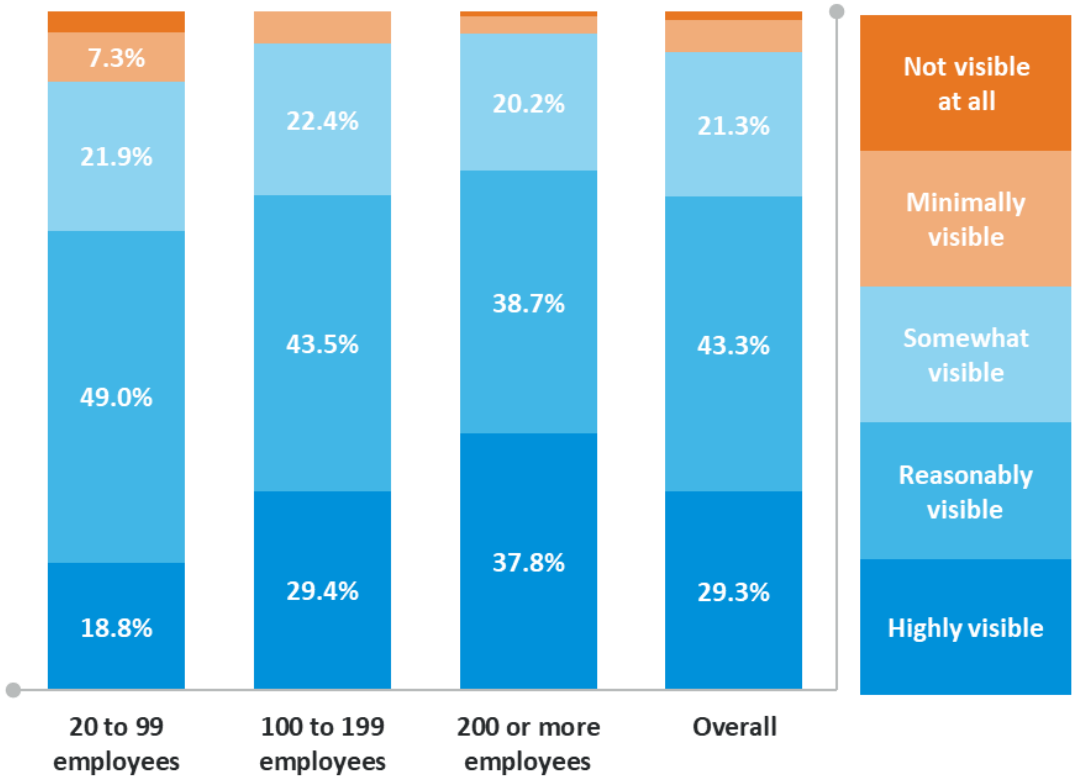
Do you have a dedicated security management centre or team?



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

More than 1 in 5 lacked reasonable executive visibility for IT security

How much visibility does IT security have within the executive leadership team?

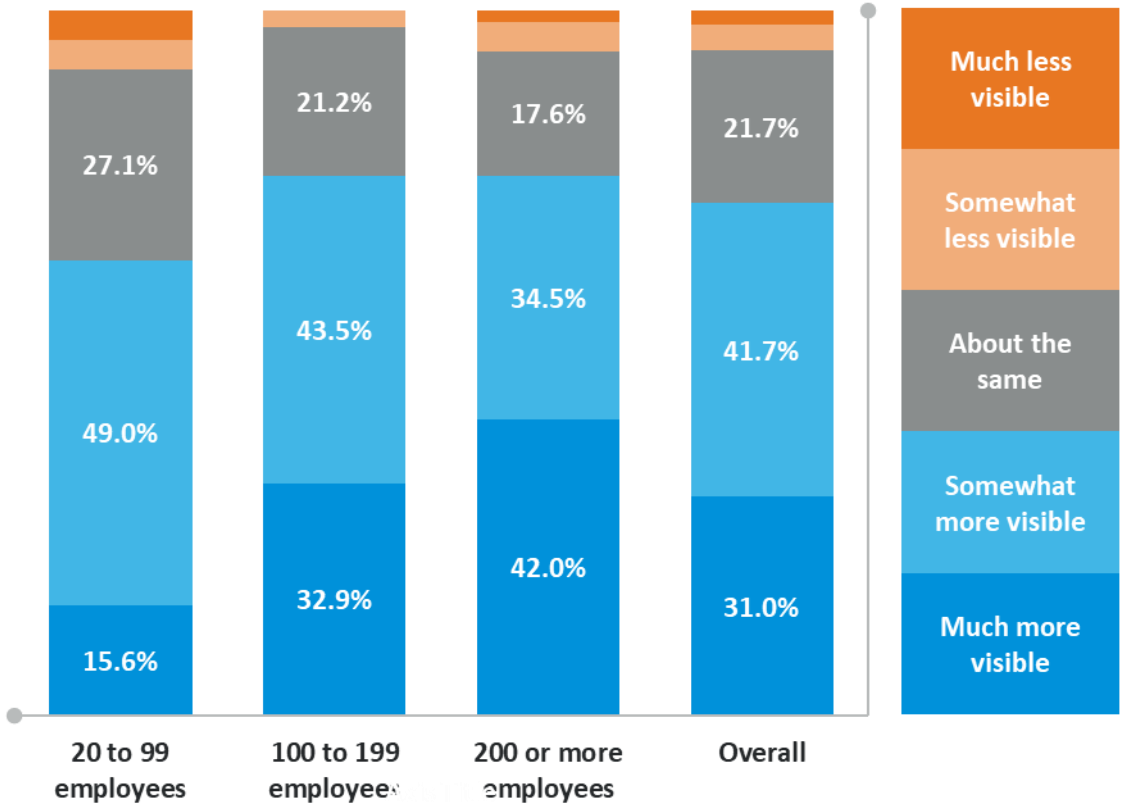


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

IT security decisions were more visible to leaders than other organisational decisions

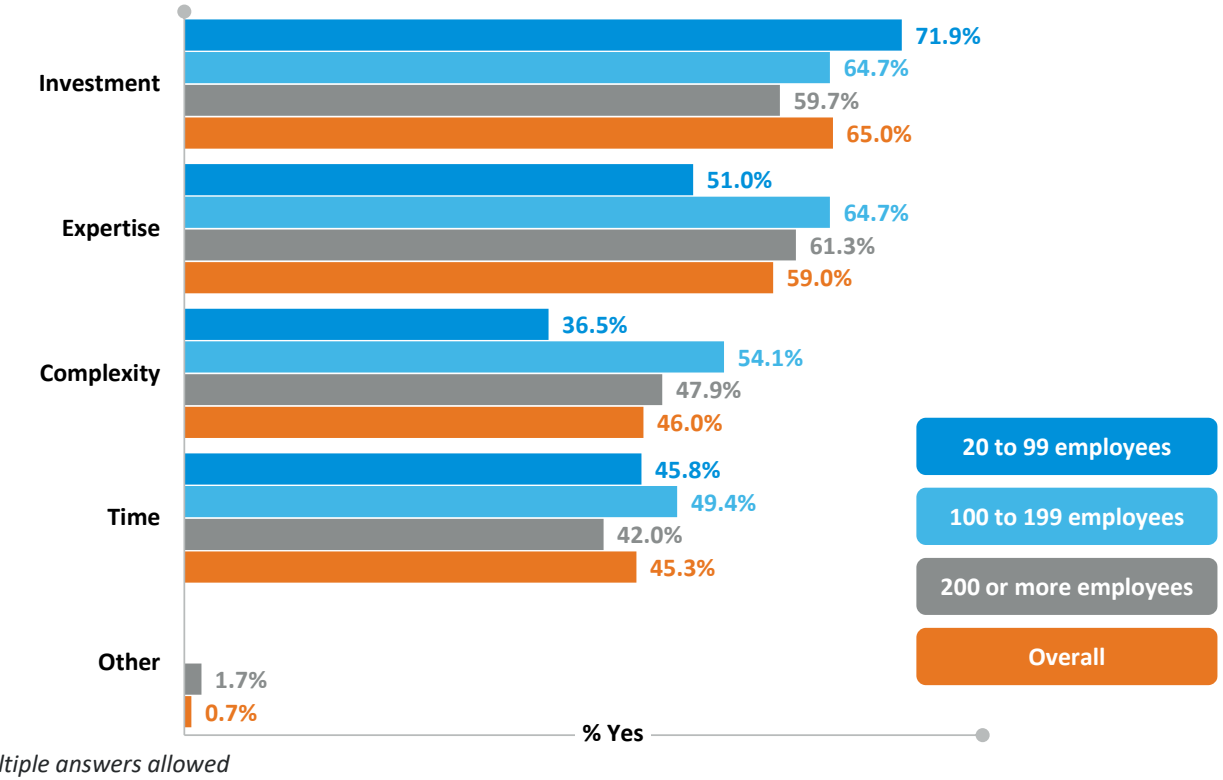
How visible are IT security decisions to the executive leadership team compared to other key operational areas of the business?



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees;
85, 100 to 199 employees; 119, 200 or more employees

Cost remained the biggest cybersecurity challenge for small companies, with time and complexity troubling larger organisations

What are the greatest challenges in choosing and integrating a cybersecurity framework into your business practices?



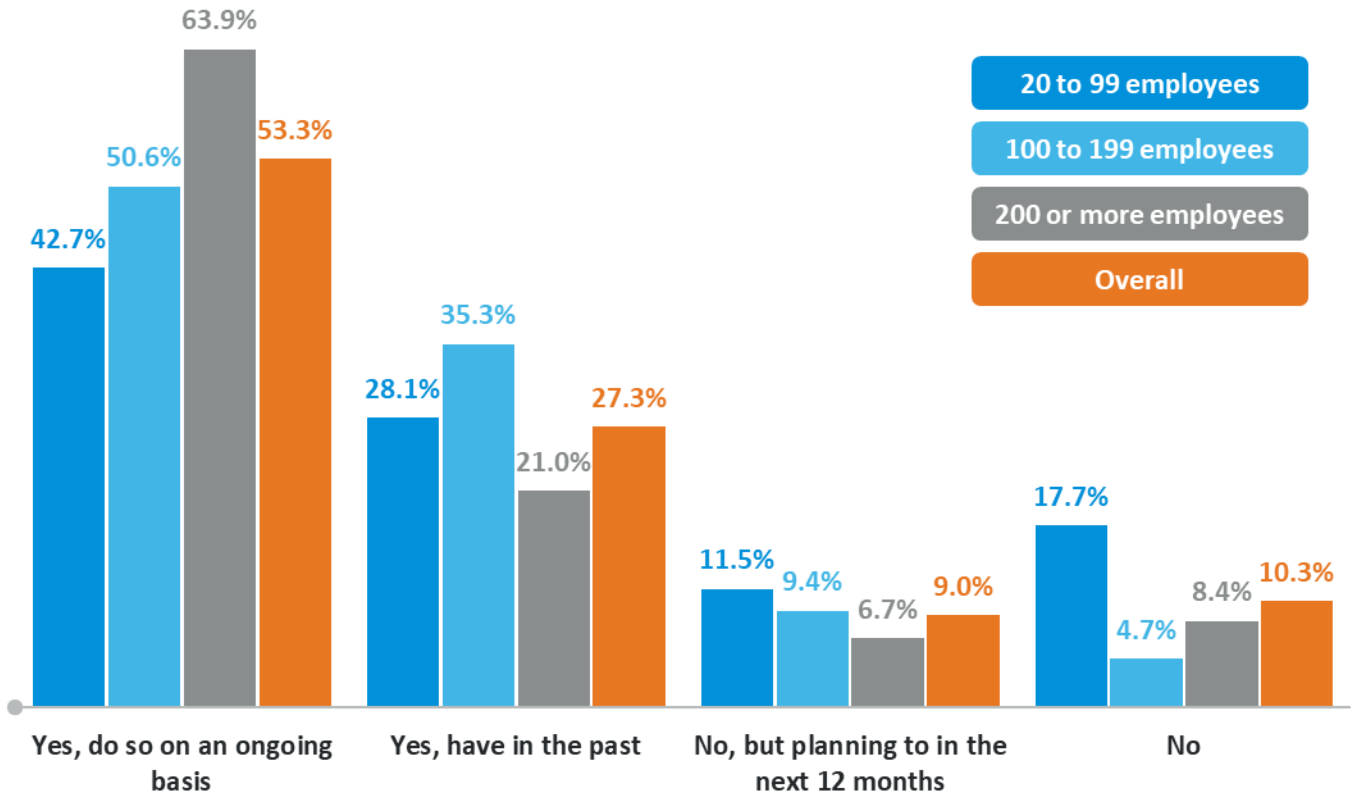
*Multiple answers allowed

n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

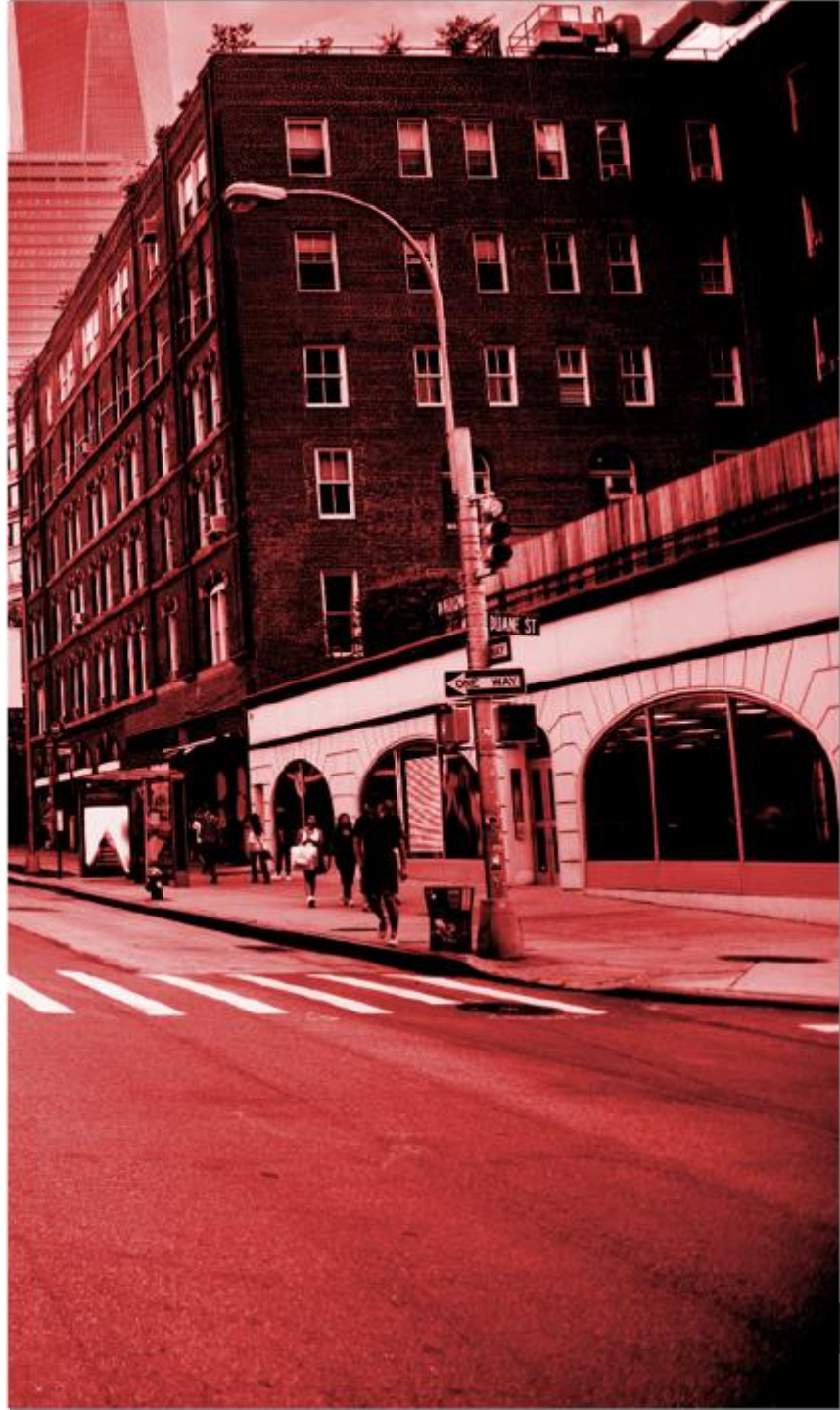
Almost two in three large companies employed ongoing IT security consultants

Do you employ specialist consultancies to help formulate your IT security strategy?



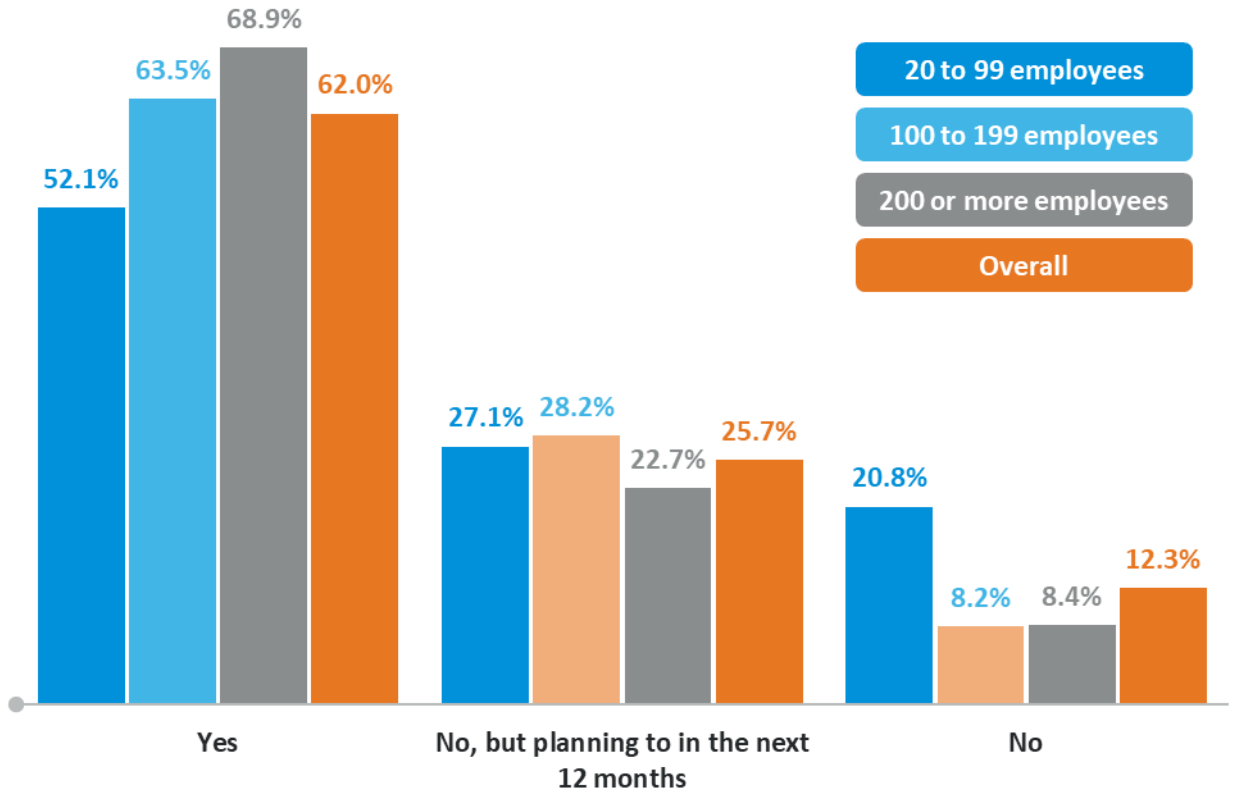
n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees



Most companies had a managed security provider

Do you have a managed security provider working with your organisation?

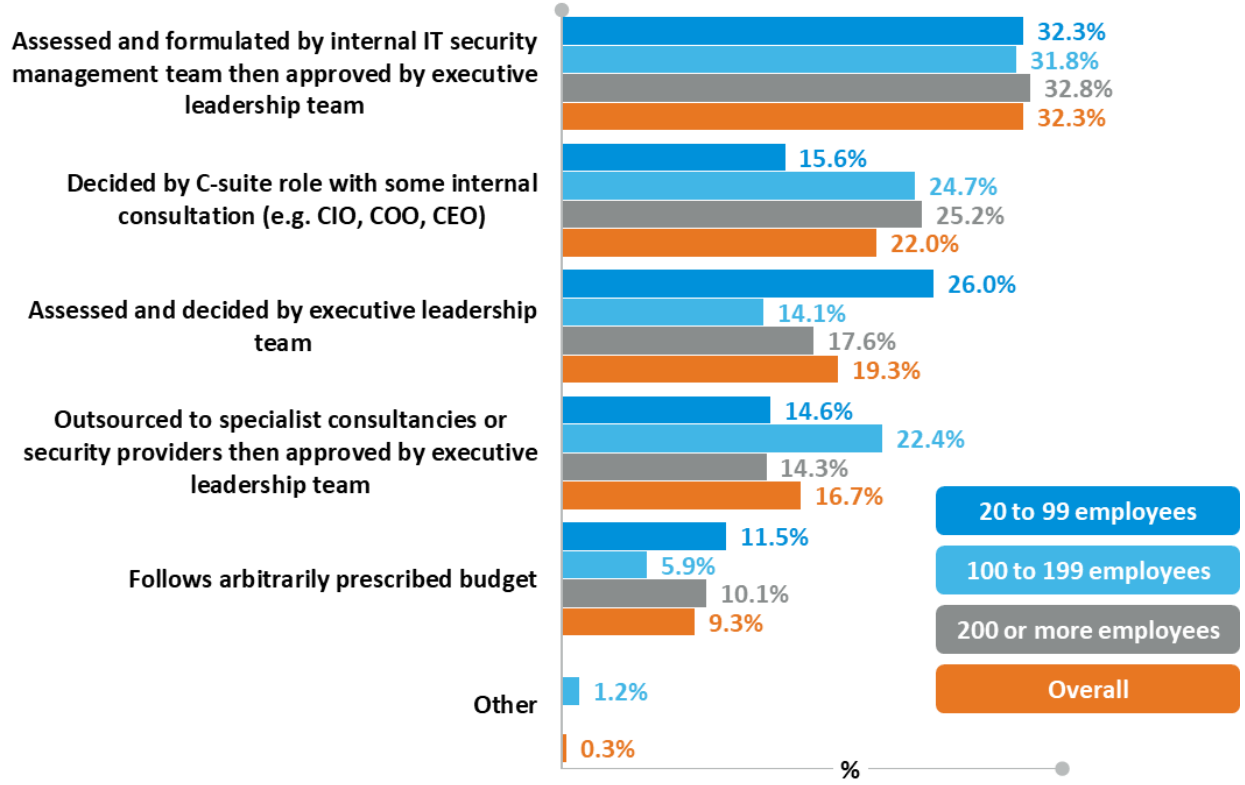


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Executive leadership consistently played a role in IT decision-making

What best describes how your organisation makes decisions about investment in security, including which areas it will invest in (e.g. adoption, planning and preparedness, training)?



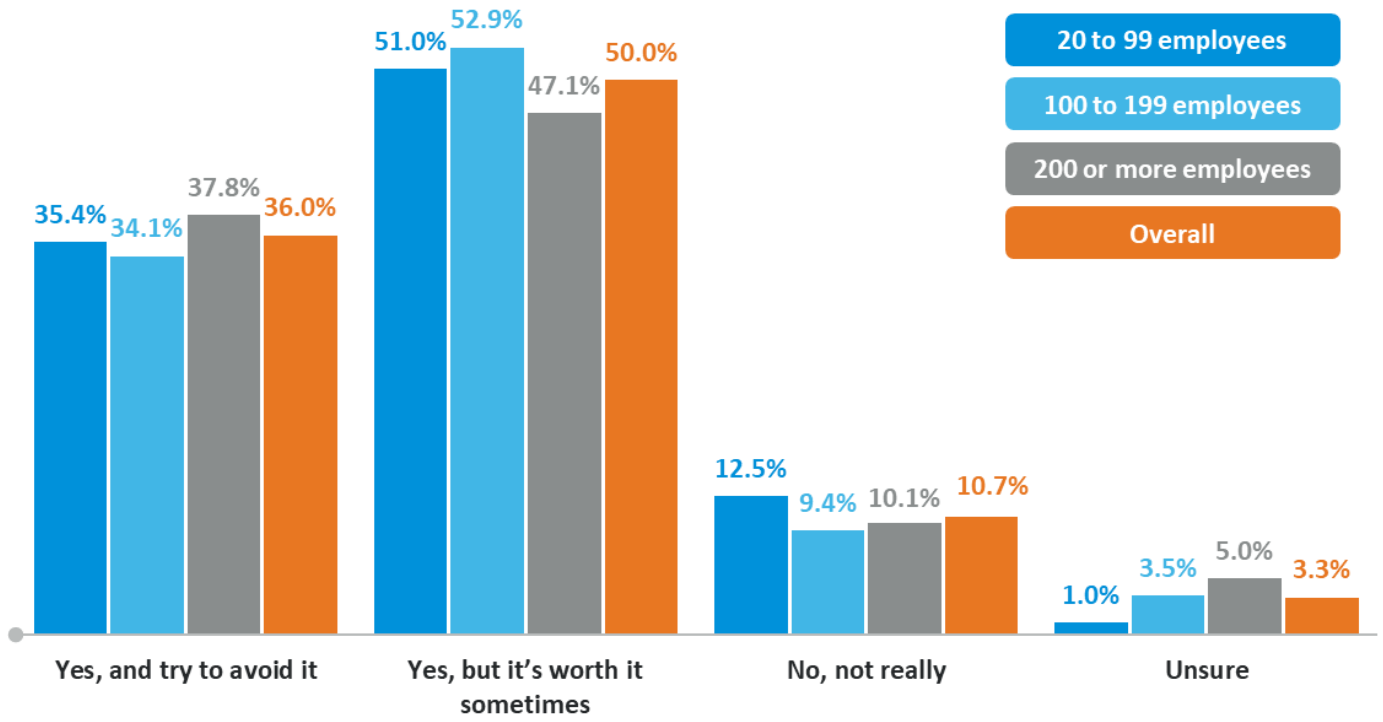
n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Beyond the index: provider preference

Most companies believed the complexity of having multiple IT vendors could be worth it

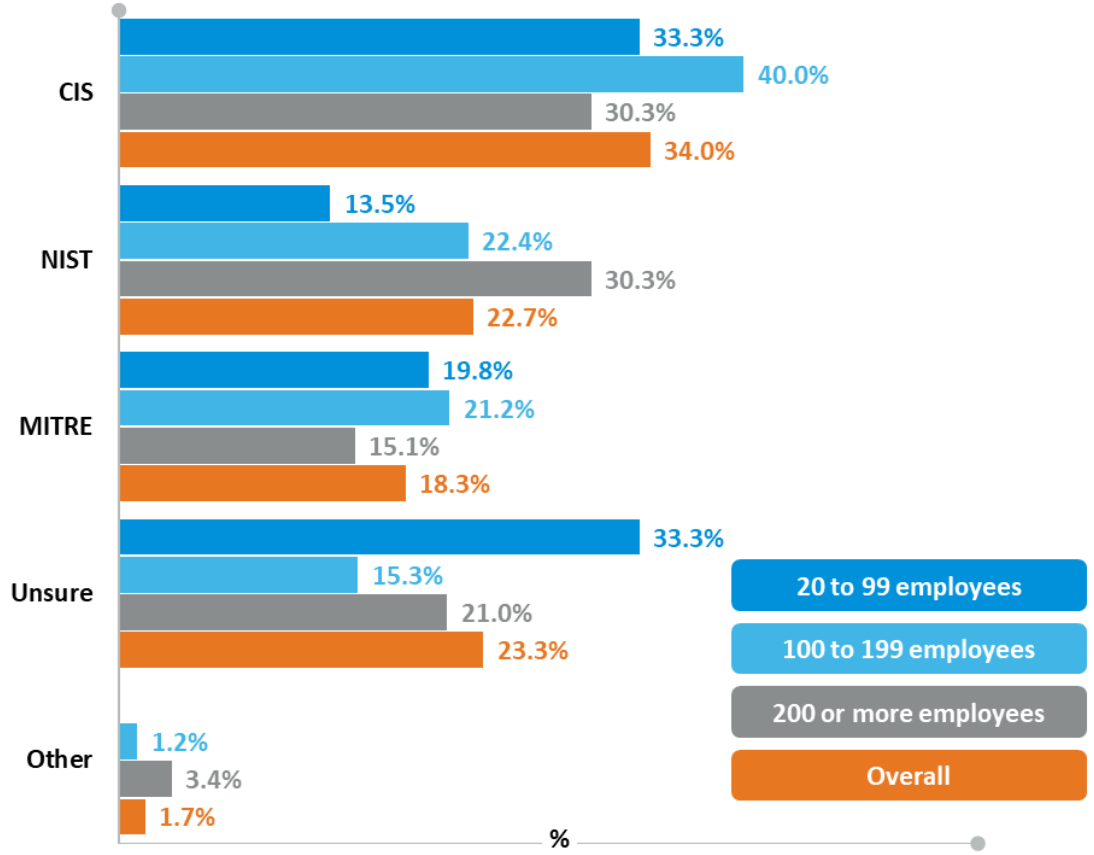
Do you feel multiple vendors and technologies add cost and complexity to your IT environment?



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

CIS had a strong foothold in small companies, while NIST was the first preference of larger organisations

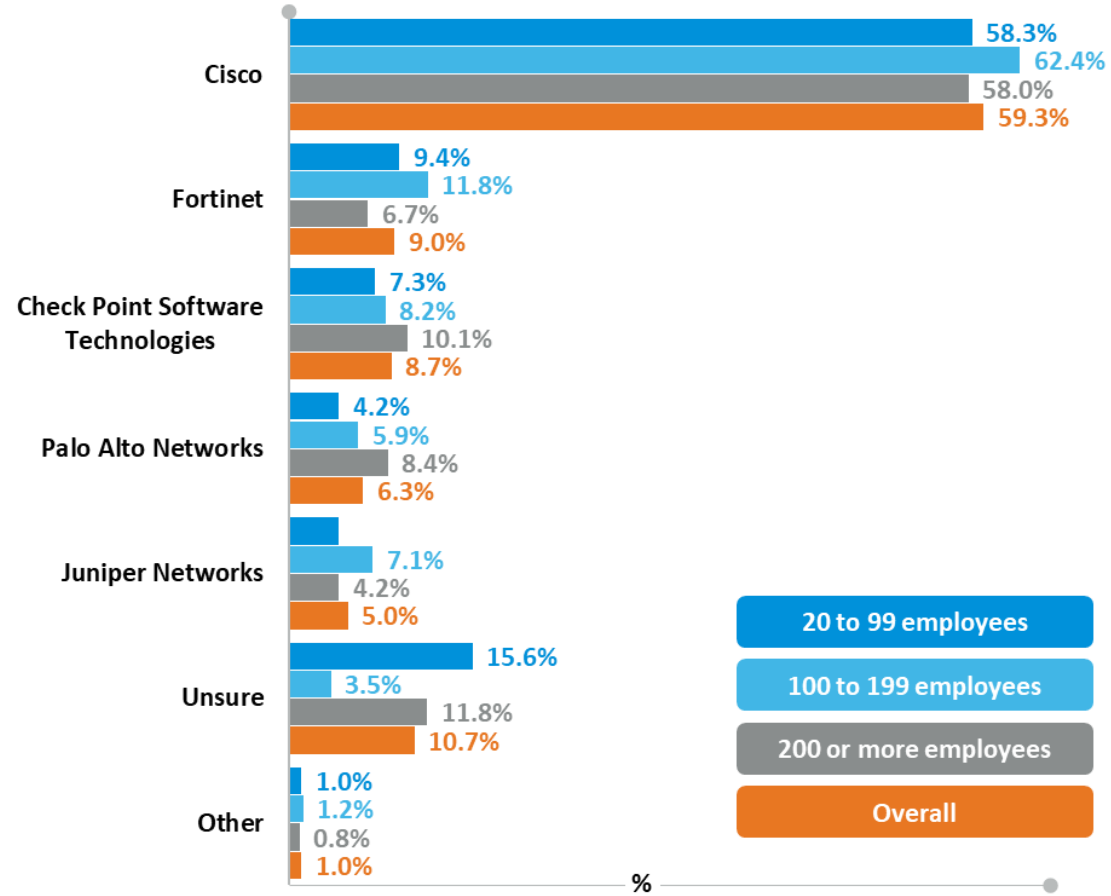
Which of the following is your primary cybersecurity framework?



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

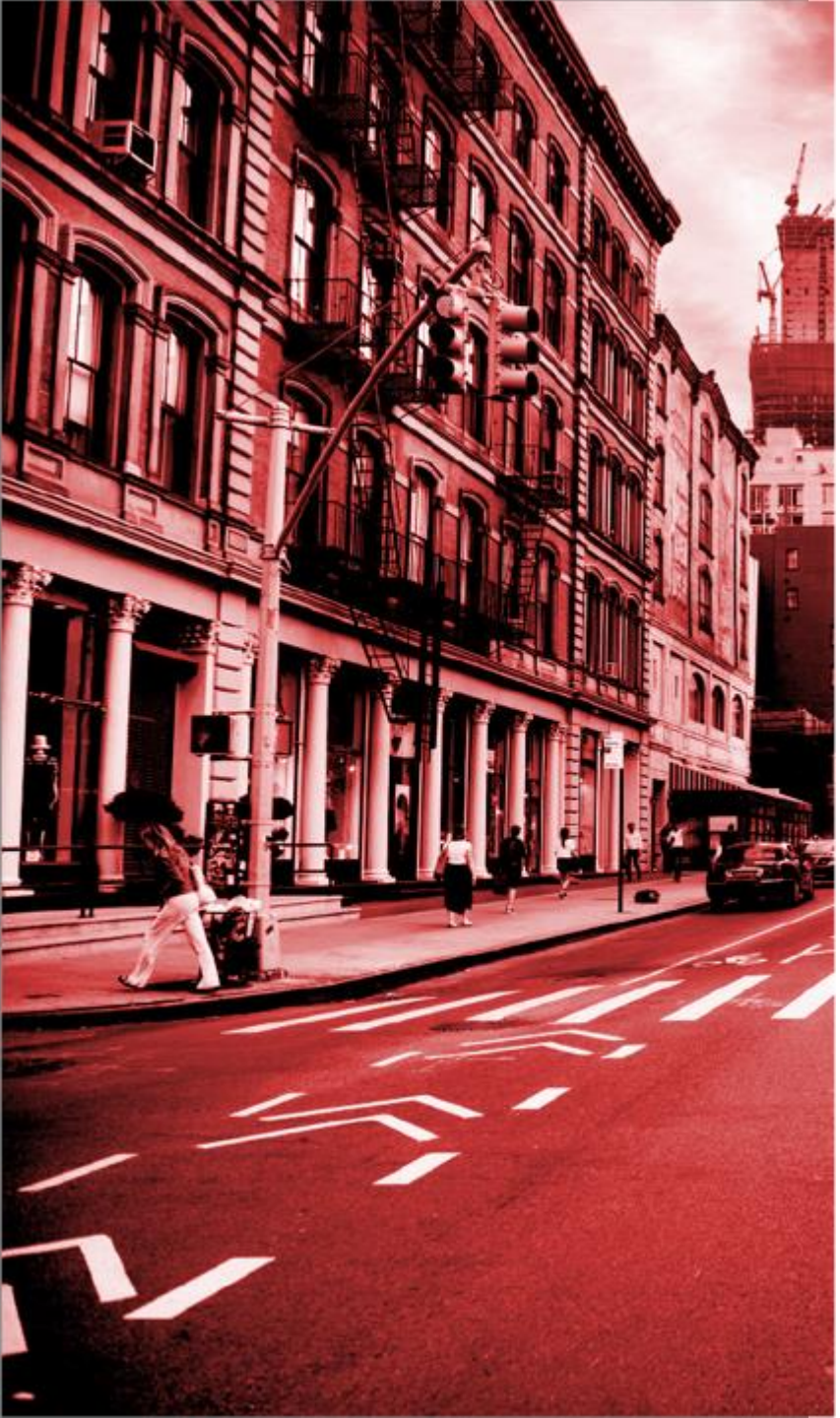
CISCO had a very strong hold on the firewall market in Australia

Who do you use as your primary firewall provider?



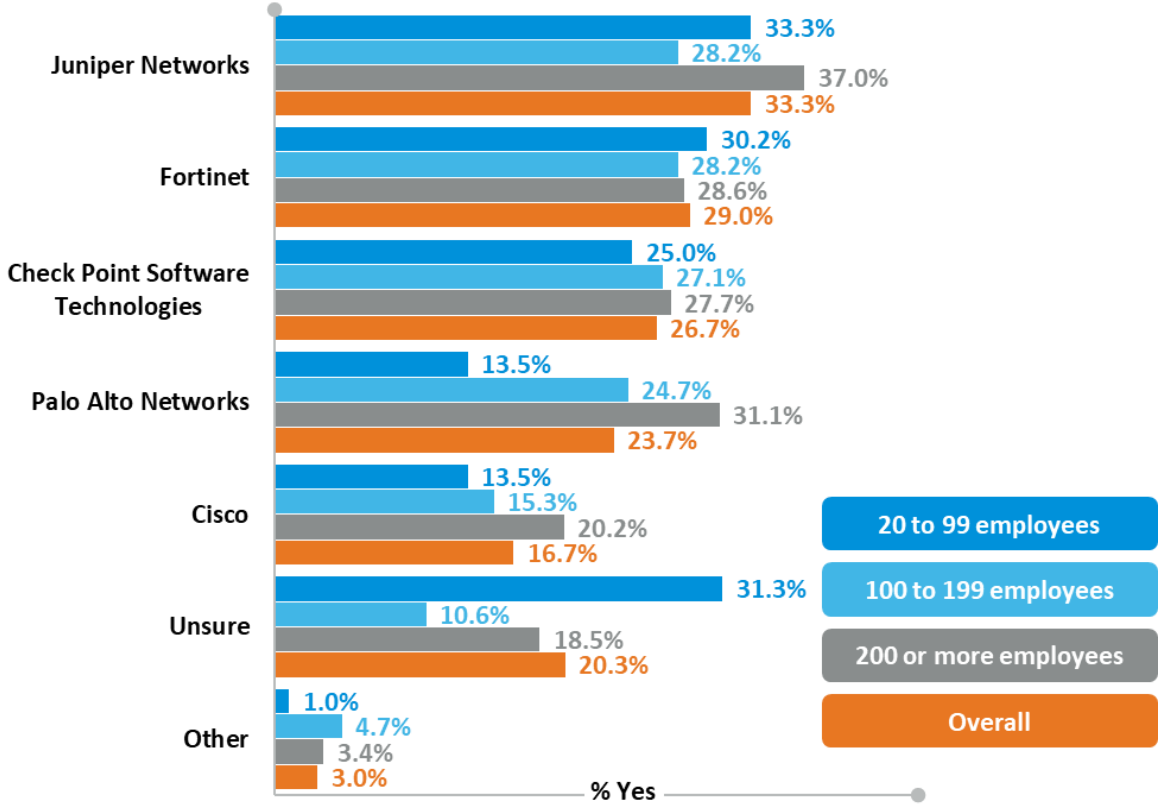
n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees



Fortinet was among the top primary firewall providers considered

Who would you consider using as your primary firewall provider?

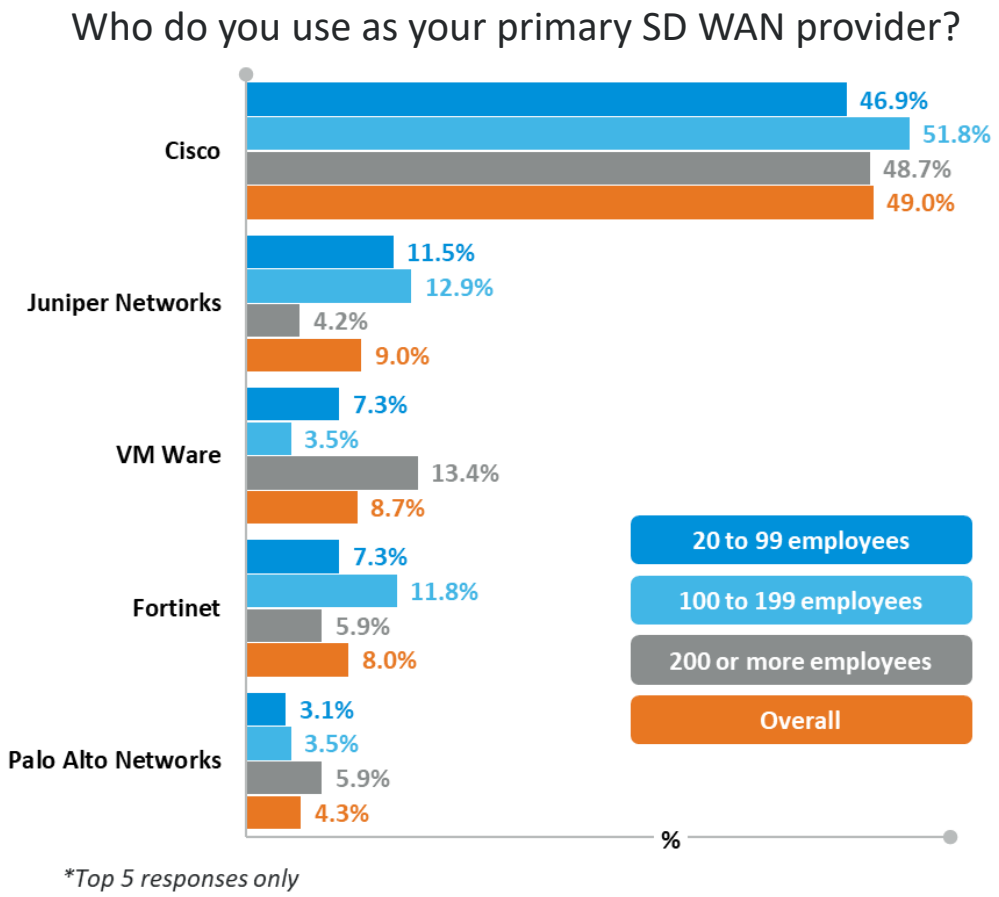


*Multiple answers allowed

n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

CISCO also had a strong hold over the SD-WAN market in Australia

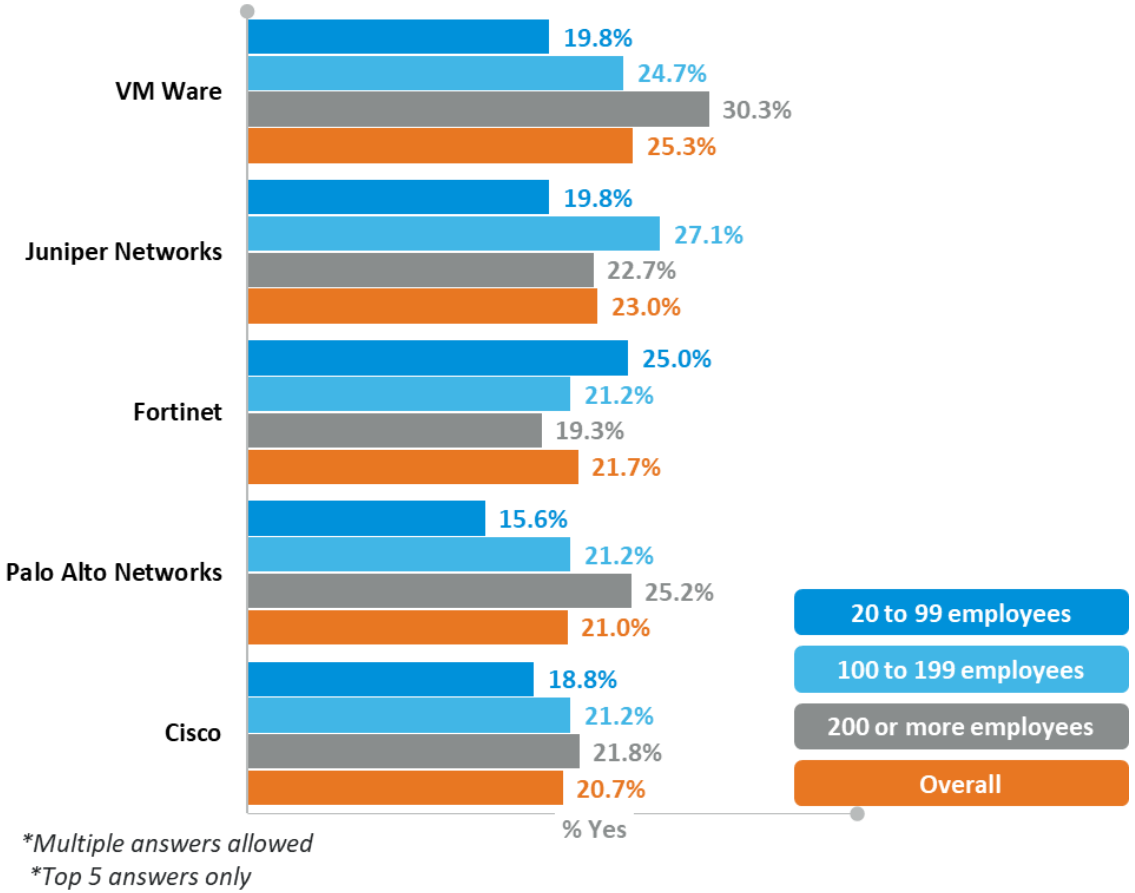


*Top 5 responses only

n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees;
85, 100 to 199 employees; 119, 200 or more employees

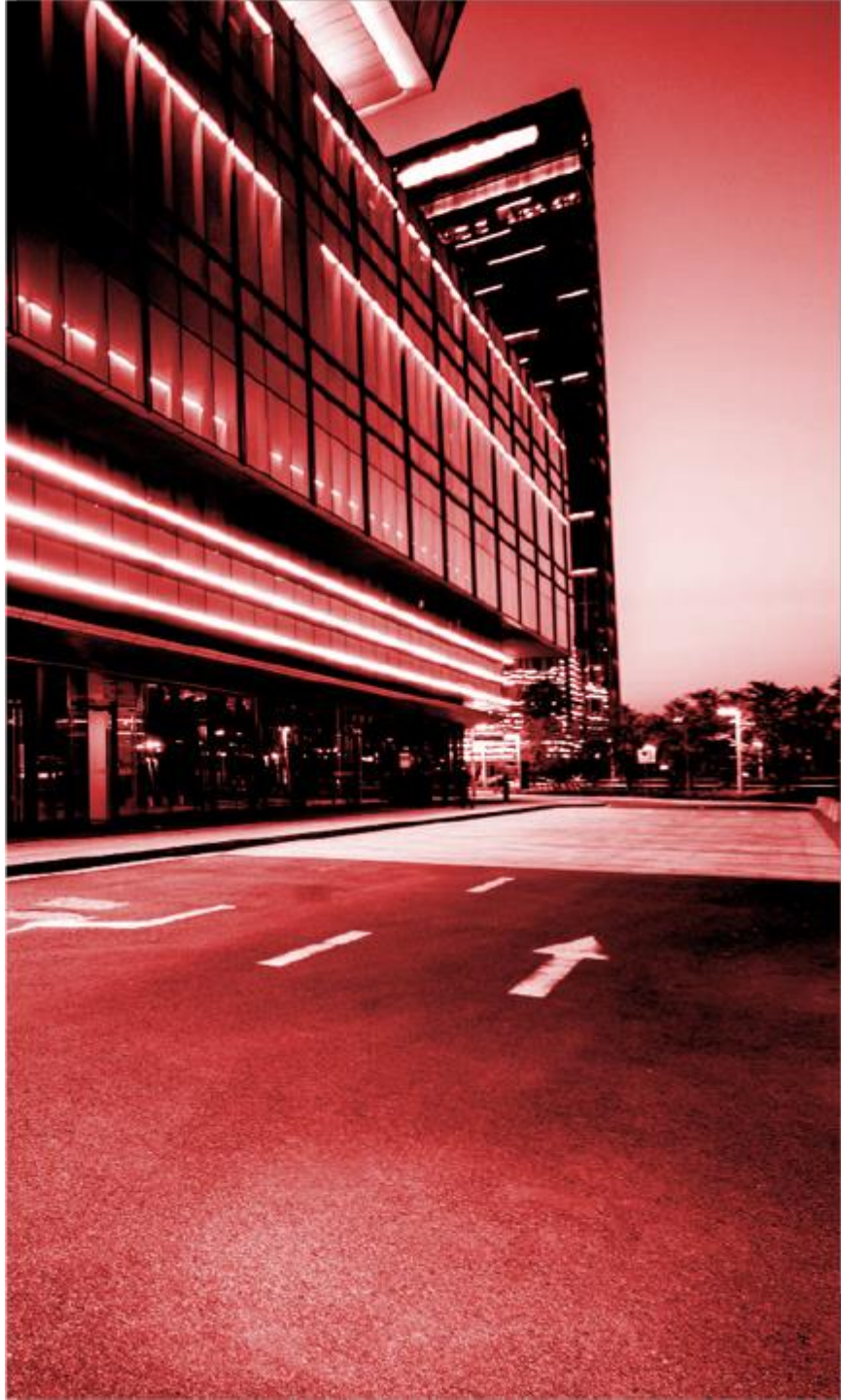
Fortinet also figured highly in the SD-WAN consideration set

Who would you consider using as your primary SD-WAN provider?



*Multiple answers allowed
*Top 5 answers only

n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees



Profile and demographics

Profile

Which of the following best describes your current employment status?

	Overall	20 to 99 employees	100 to 199 employees	200 or more employees
Full-time paid employment	85.3%	79.2%	89.4%	87.4%
Part-time paid employment	11.3%	15.6%	7.1%	10.9%
Self-employed	2.7%	4.2%	3.5%	0.8%
Casual employment	0.7%	1.0%	0.0%	0.8%

Which of the following best describes the seniority of the role you mostly work in?

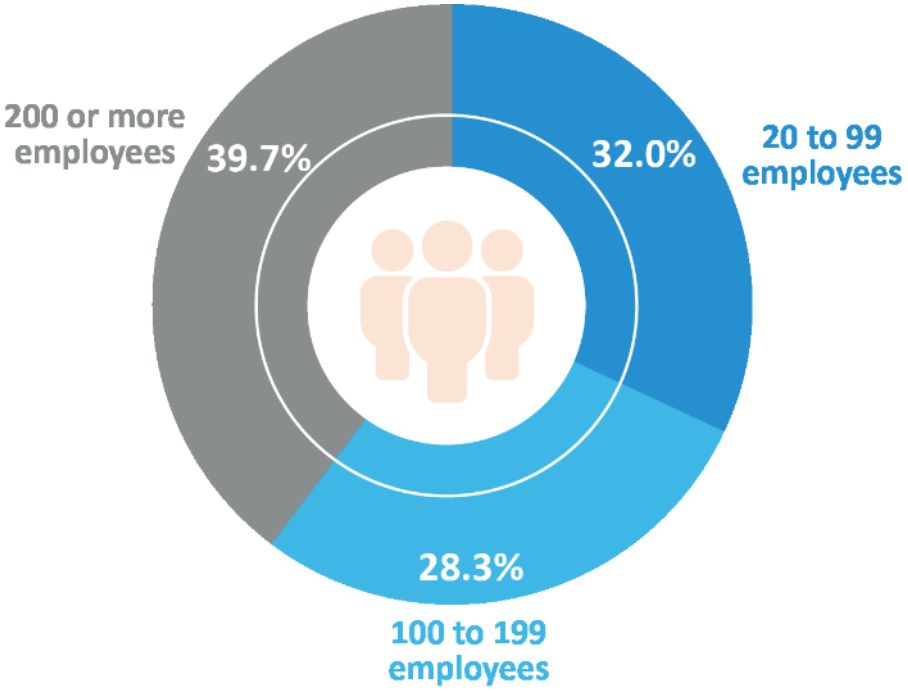
	Overall	20 to 99 employees	100 to 199 employees	200 or more employees
Mid-level (non-management)	11.0%	12.5%	8.2%	11.8%
Senior (non-management)	15.0%	19.8%	12.9%	12.6%
Middle management	25.7%	19.8%	27.1%	29.4%
Senior management	31.3%	32.3%	34.1%	28.6%
Executive management	17.0%	15.6%	17.6%	17.6%

n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Profile

How many people are employed by your business?



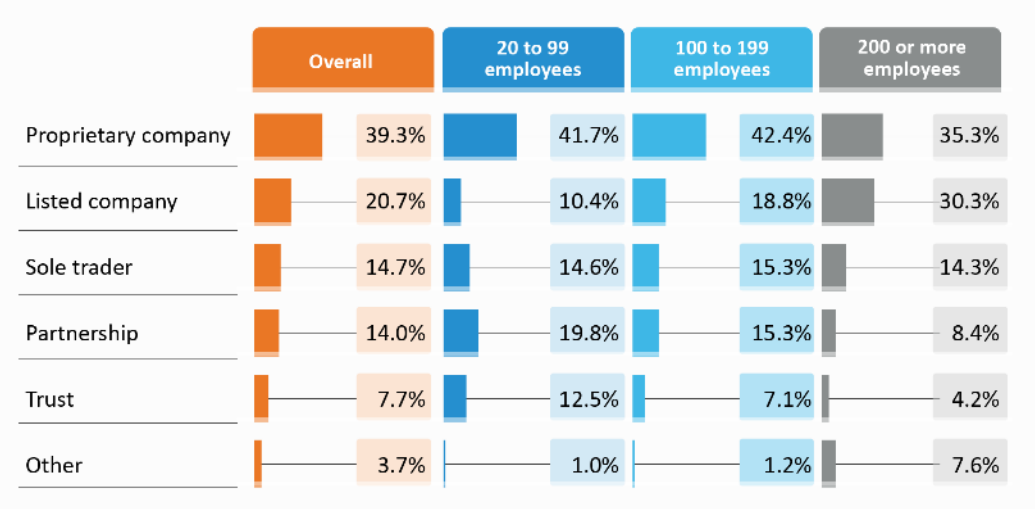
In broad terms, what is the annual turnover of your organisation?

	Overall	20 to 99 employees	100 to 199 employees	200 or more employees
Less than $2 million	5.0%	9.6%	2.4%	2.9%
$2 million to less than $5 million	13.6%	20.2%	17.1%	4.9%
$5 million to less than $15 million	13.6%	26.6%	8.5%	5.8%
$15 million to less than $25 million	11.5%	12.8%	14.6%	7.8%
$25 million to less than $50 million	11.1%	13.8%	9.8%	9.7%
$50 million to less than $100 million	10.8%	5.3%	17.1%	10.7%
$100 million to less than $150 million	7.5%	5.3%	8.5%	8.7%
$150 million to less than $200 million	7.9%	4.3%	12.2%	7.8%
$200 million to less than $250 million	5.4%	1.1%	7.3%	7.8%
$250 million or more	13.6%	1.1%	2.4%	34.0%

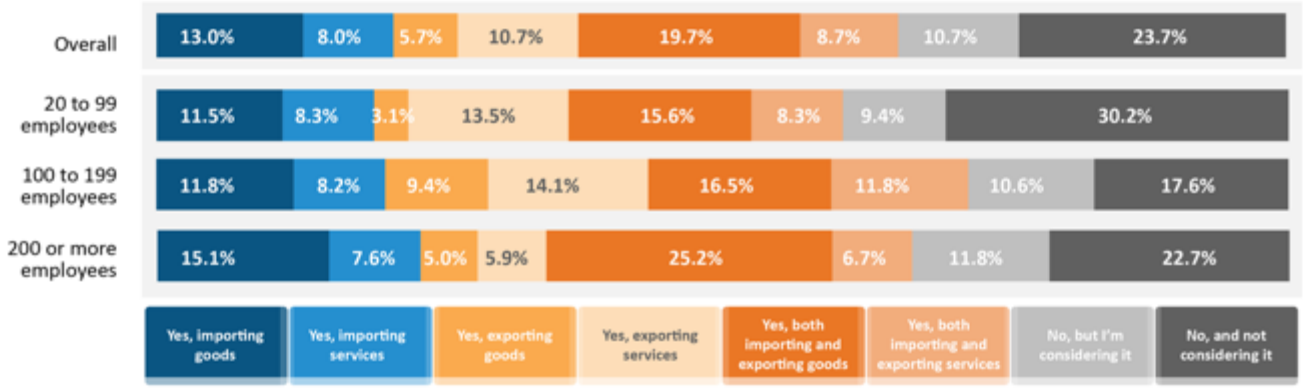
n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Profile

Which of the following best describes your organisation?



Does your organisation trade internationally (importing or exporting)?

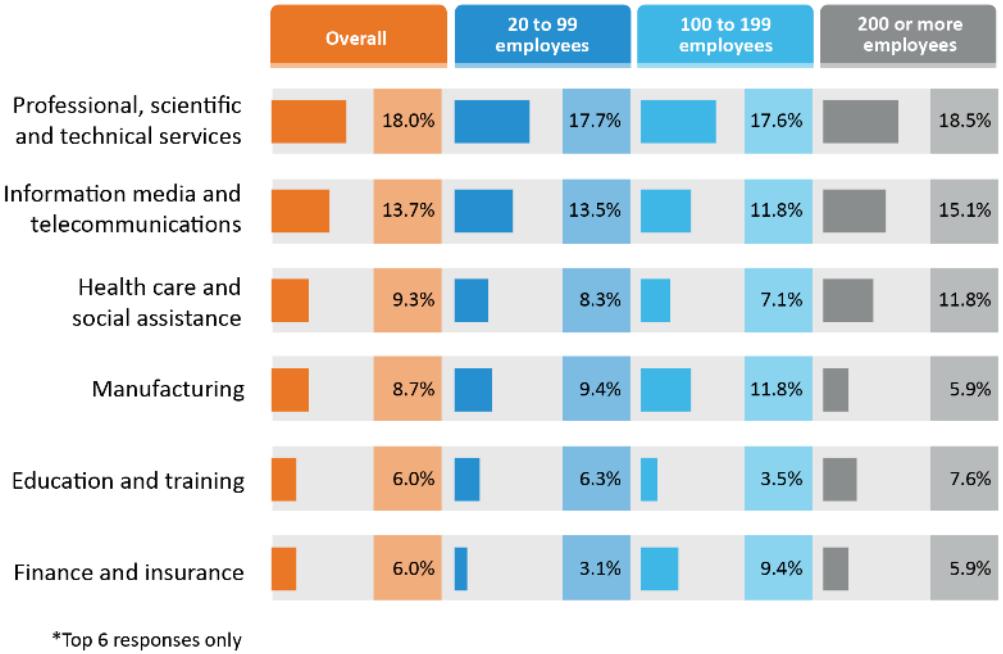


n = 300, overall (senior IT decision-makers in organisation)

n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

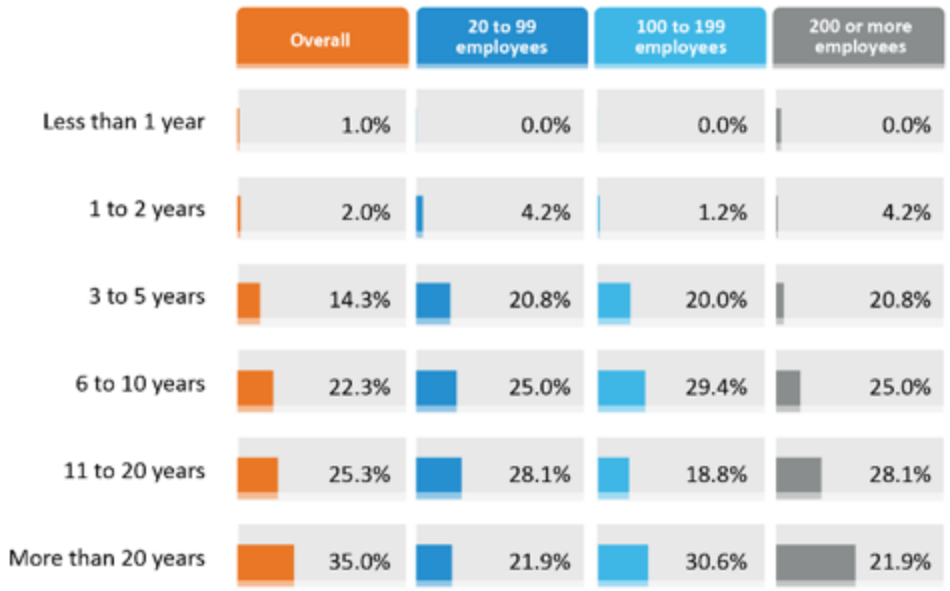
Profile

Which of the following best describes the industry sector in which your organisation operates?



*Top 6 responses only

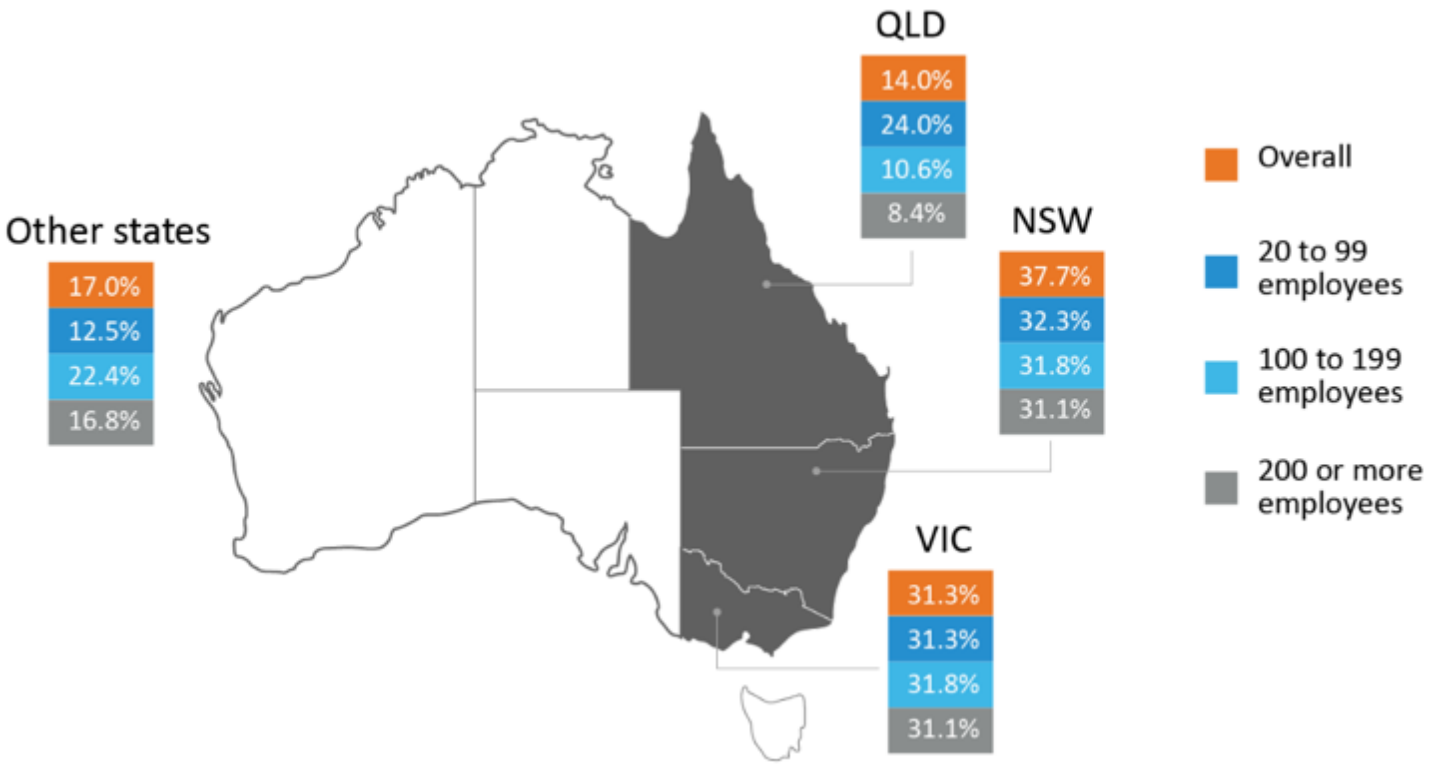
How long has your organisation been in operation?



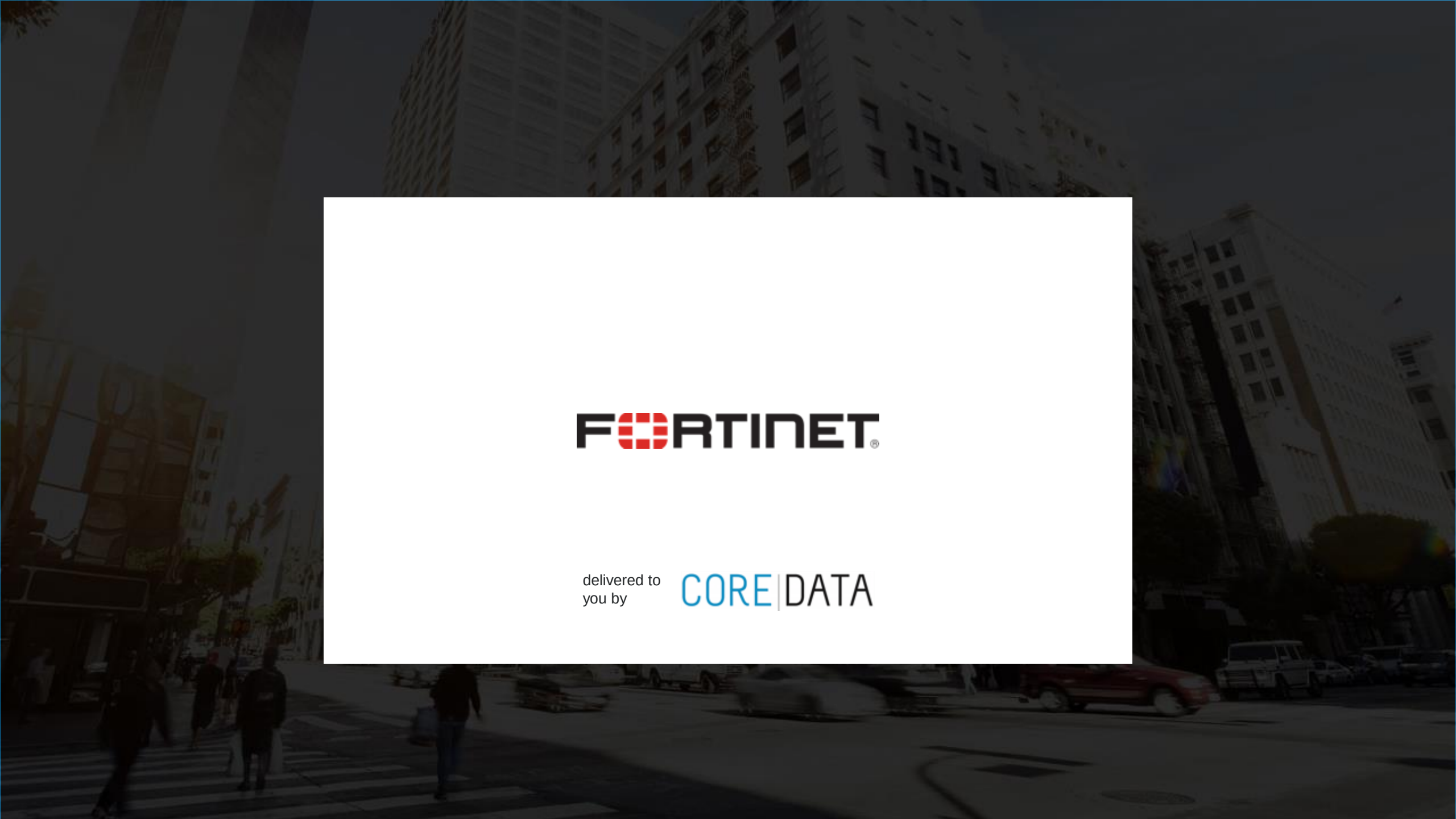
n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees

Profile

In which state/territory is your organisation headquartered?



n = 300, overall (senior IT decision-makers in organisation)
n = 96, organisations with 20 to 99 employees; 85, 100 to 199 employees; 119, 200 or more employees


FORTINET
delivered to
you by
CORE DATA