White paper

The 2023 Cybersecurity Research Report

Despite security concerns, C-suite and IT leaders raise budgets, explore AI

Solve

rackspace technology | Microsoft

Table of contents

rackspace technology. | Microsoft

Introduction and key findings

In the face of escalating cyber threats, organisations are intensifying their cybersecurity initiatives and investments, with a particular emphasis on leveraging AI as a vital instrument in bolstering their defenses. A heightened awareness and proactive stance have fostered increased engagement and involvement from members of the C-suite and corporate boards. The findings outlined in this report are based on our recent survey, which highlights the critical concerns and adaptive strategies that are shaping cloud and cybersecurity technologies.

To obtain a deeper understanding of the contemporary cybersecurity landscape, Rackspace Technology® commissioned the 2023 Cybersecurity Research Report. This report is built on insights from a comprehensive survey of 1,420 IT executives across varied sectors that include manufacturing, finance, retail, government and healthcare. The IT leaders we engaged with represent a global IT perspective in regions spanning the Americas, Europe, Asia, Australia and the Middle East.

Our objective with this research was to gather the perspectives and priorities of global IT leaders who are considering leveraging cybersecurity best practices to spur growth in their organisations. Through the survey, we were able to pinpoint areas of investment, operational challenges and potential threats while gauging an outlook on the future.

The research highlights two crucial measures businesses need to implement to enhance their resilience against cyberthreats:

1. crafting a comprehensive cybersecurity strategy that aligns with organisational objectives, and
2. mitigating the IT talent shortage through strategic, long-term solutions.

This report provides insights into the core findings and implications extracted from the feedback of industry peers. It offers a detailed examination of the trends influencing cybersecurity adoption, the hurdles encountered, current investment trajectories and the overall readiness of organisations to confront evolving threats. A high-level review of our annual survey uncovers the following predominant trends:

Cybersecurity is embedded in business operations and a top priority at the board level. In our research, 63% of C-suite and board members ranked cybersecurity as their number one business concern, marking a 5% increase from last year — when cybersecurity also ranked as their top concern.

As a top C-suite and board priority, cybersecurity (63%) currently outranks:

57%	*Digital transformation*
52%	*Sustainability*
48%	*Inflation/interest rates*
43%	*Retaining/hiring talent*
38%	*Supply chain and logistics management*

AI is increasingly driving organisations' security posture and motivation for investment

While 62% of respondents said AI has increased the need for cybersecurity, AI has also become embedded in security tooling with 81% of firms stating they have a formal policy on AI governance and security. Leading concerns included data privacy (64%) and compliance and legal considerations (58%).

Organisations are increasing their cybersecurity budgets accordingly

Some 62% of respondents revealed that their companies have increased dedicated budgets over the past year, while just 3% have made cuts. Furthermore, 33% of these organisations have raised budgets by more than 14% or more, with 48% of these dedicating more than 14% of their total IT budget to cybersecurity efforts.

Cloud-native security gains prominence as IT boundaries blur

Among the most significant areas of investment — cloud-native security (57%), data security (51%), and application security (48%) — application security has seen a 7% increase year-over-year. This emphasis on cloud-native security is in sync with the survey participants' perceived primary threat vector: cloud architecture attacks, which have surged by 12% compared to last year's survey.

The IT talent shortage persists despite short-term changes in the job market

Companies are elevating salaries to attract skilled professionals in a marketplace where the demand for AI specialists significantly exceeds the supply. A notable strategy adopted by organisations is engaging with external cybersecurity service partners for consultation or support — a top priority for 43% of respondents — driven primarily by a lack of internal expertise (48% of respondents).

Cybersecurity concerns grow despite surging investments

Despite sizable increases in their cybersecurity investment, greater board visibility and increased collaboration between the security team and the C-suite, **69% of global IT executives reported that their level of concern for cybersecurity has increased over the past 12 months.**

As we forge ahead into final months of 2023, IT leaders find themselves at a critical juncture where prioritising, preparing and investing in robust cybersecurity strategies is more vital than ever. The escalation of cyberthreats necessitates a vigilant and proactive approach to security that's anchored in collaboration and strategic foresight.

The shift toward utilising AI is already becoming apparent as it establishes itself as an indispensable tool, steering organisations in honing their cybersecurity postures and guiding investment strategies. Encouragingly, we are witnessing a surge in engagement from C-suite executives and board members, fostering a collaborative environment marked by increased visibility and buy-in. This proactive engagement is mirrored in budget augmentation that's allocated toward application security, cloud-native security, and data security, indicating a significant shift in organisational priorities.

Looking at the road ahead, 2023 will likely stand as a pivotal year for cybersecurity. It represents a time where organisations are not merely reacting to cyberthreats but seizing control of their risk management agendas.

A closer look at survey data

Top priorities

Cybersecurity remains the top business concern

Survey respondents view cybersecurity as more important than digital transformation, sustainability and economic concerns such as inflation volatility, the talent shortage and supply chain and logistics management woes.

What are the top 3 business concerns your c-suite is likely to have currently?

63%	*Cybersecurity (was also top-ranked in 2022, at 59%)*
57%	*Digital transformation*
52%	*Sustainability*
48%	*Inflation/interest rates*
43%	*Retaining/hiring talent*
38%	*Supply chain and logistics management*

IT executives face a diverse range of cybersecurity risks daily. IT leadership can help strengthen its defenses by investing in tools that protect against multiple threat vectors. Companies should address risks proactively: train their workforces, increase their cybersecurity budgets and give security a more prominent role in organisational cultures.

Please rank the top priorities for your organisation's current cybersecurity strategy:

43%	*Protecting critical data/data warehouses and understanding security vulnerabilities*
42%	*Integrate cyber risk into enterprise risk management*
35%	*Integrating strategic security measures into your new processes*
34%	*Mitigating threats and responding to incidents*
33%	*Modernise/rationalise security tooling*

Top priorities for cybersecurity strategy today vs. two years ago:

2023	2021	
43%	39%	*Protecting critical data and data warehouses*
42%	39%	*Integrate cyber risk into enterprise risk management*
35%	36%	*Integrate strategic security measures into new processes*

Integrating cybersecurity in the organisation

To foster a more secure organisation, it's essential to integrate people, processes and technology effectively. Survey data reveals that organisations are steadily embedding cybersecurity measures, although further progress is necessary.

How well has your organisation integrated cybersecurity into the following areas?

People

51% *"Staff at levels of the business have wide knowledge of cybersecurity best practices."*

Process

45% *"Security contributes to decision-making at both business and IT levels."*

Technology

45% *"The firm accounts for state-of-the-art technologies for new purchases and projects."*

Growing concern

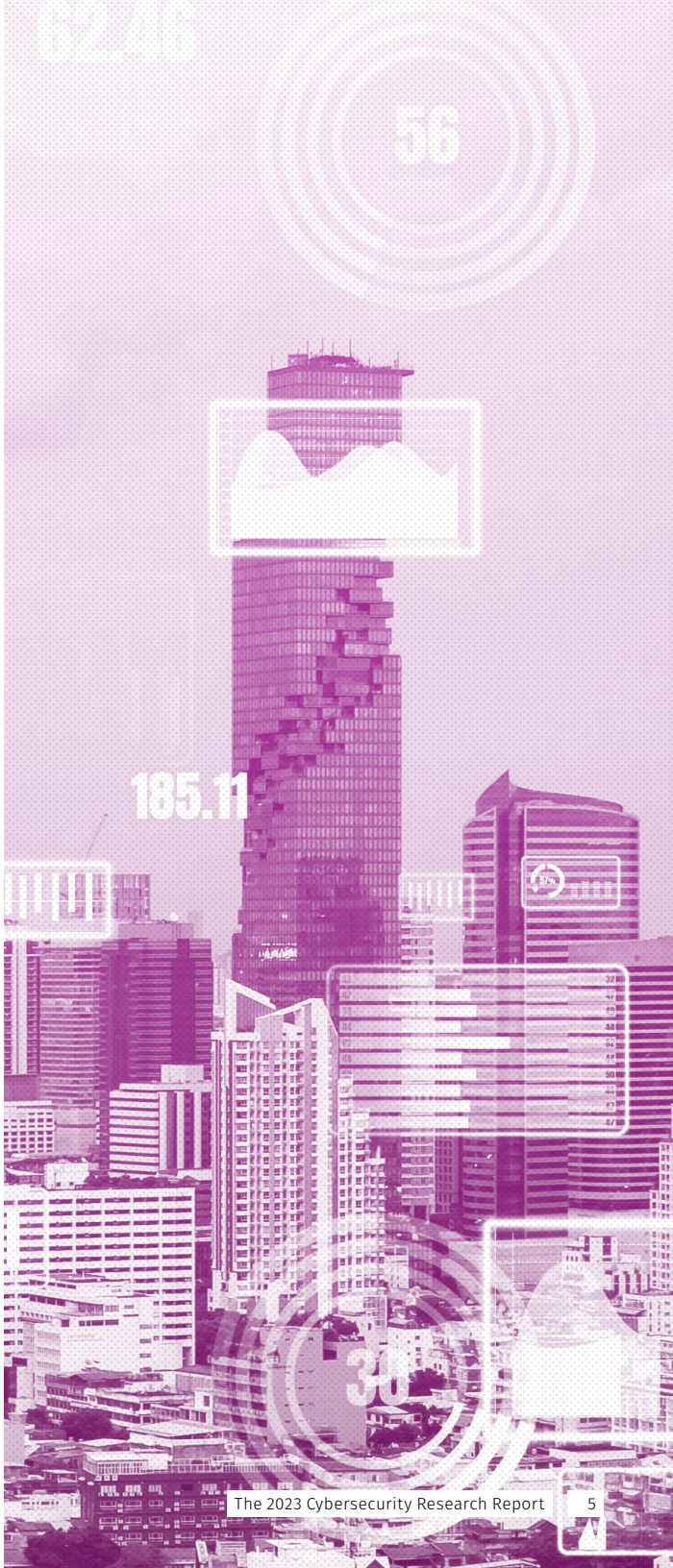
The research reveals a growing concern among global IT executives regarding cybersecurity. Nearly seven out of 10 (69%) reported that their level of concern has increased over the past 12 months.

Top security measures

59% *Integrate security fundamentals into business objectives by implementing organisation-wide best practices for security hygiene*

55% *Partner with a cybersecurity services provider for expert support*

48% *Automate security operations and incident response with AI to simultaneously improve both*



The reality these leaders recognise

Global IT leaders are fully aware that while effective cybersecurity can help detect threats and secure data, no system can guarantee complete security. Evolving technologies and ever-changing hacking techniques make protecting against cyber threats a major challenge.

Top cybersecurity challenges

When asked to identify the top cybersecurity challenges their organisation faces, migrating and operating applications in the cloud led the way for the second consecutive year.

What are the greatest cybersecurity challenges your organisation is facing currently?

35%	*New security needs driven by migrating and operating cloud applications*
32%	*Cybersecurity skills in short supply among workforce*
32%	*Legacy applications create security exposure*
31%	*Cannot view vulnerabilities across all infrastructure*
28%	*Optimise the value of cyber insurance*
27%	*Compliance; budget and resource limitations*

The C-suite

The C-suite is also taking the lead

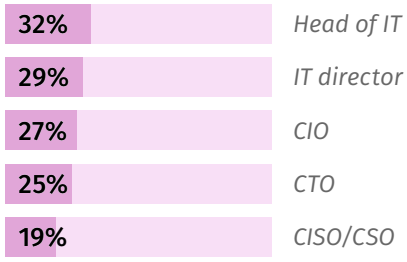
Just as cyberthreats have evolved from an IT problem to a business problem, cybersecurity strategies are shifting from IT to the C-suite to align with strategic business goals and growth. And the link between cybersecurity and cost efficiency is becoming increasingly clear.

Not surprisingly, when asked to identify the primary advocate for cybersecurity investment and initiatives within their leadership, 16% of respondents most frequently named the Chief Information Officer (CIO).

Who in your organisation is the strongest advocate of cybersecurity investments and initiatives?

Prevention and ultimate responsibility

C-suite leadership and IT operations recognise the importance of creating tight relationships to bridge the gap between risk and prevention of cyber attacks. According to 32% of respondents, the Head of IT bears the primary responsibility for preventing cyberattacks.

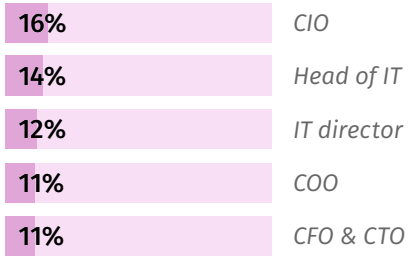


The buck stops with the CIO

Due to resource and funding constraints, leaders must forgo a backlog of initiatives and investments. Cyber investment is still an area of growth, so leaders must maximise investments to address their outstanding risks.

The majority of cybersecurity responsibility lies with the CIO; 16% of respondents identified them as the primary figure accountable for preventing cybersecurity attacks. And he or she is also seen as the most likely individual to challenge cybersecurity initiatives or funding:

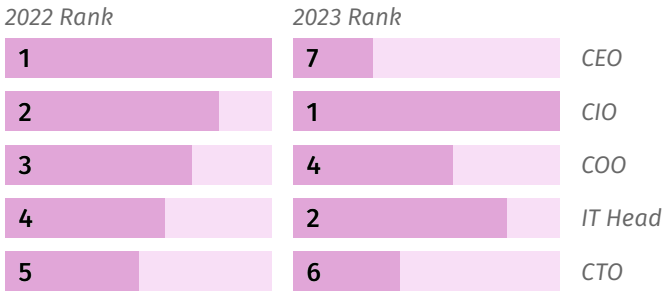
And who in your organisation is ultimately accountable for preventing cyberattacks?



The CIO is ultimately accountable

In a significant departure from last year, when CEOs were viewed as the primary initiators of challenges to cyber initiatives, the 2023 research paints a different picture. Now, CEOs have a reduced influence rate of 14%, placing them seventh in the hierarchy — trailing behind the CTO, CFO, COO, IT Director and Head of IT. Leading the pack with a 21% influence rate is the CIO.

Who is most likely to challenge cybersecurity initiatives or funding?



Engagement between security teams and the C-suite

There is a notable consensus regarding the commitment of leadership teams to cybersecurity. We found that 74% of survey participants either strongly agree or agree that their leadership is fully vested in bolstering cybersecurity measures. Moreover, 73% of executives in the C-suite are actively advocating for the needs of the cybersecurity team, a sentiment echoed by the surge in investment, collaboration and dialogue between IT security professionals and leadership teams on cybersecurity risks and priorities.

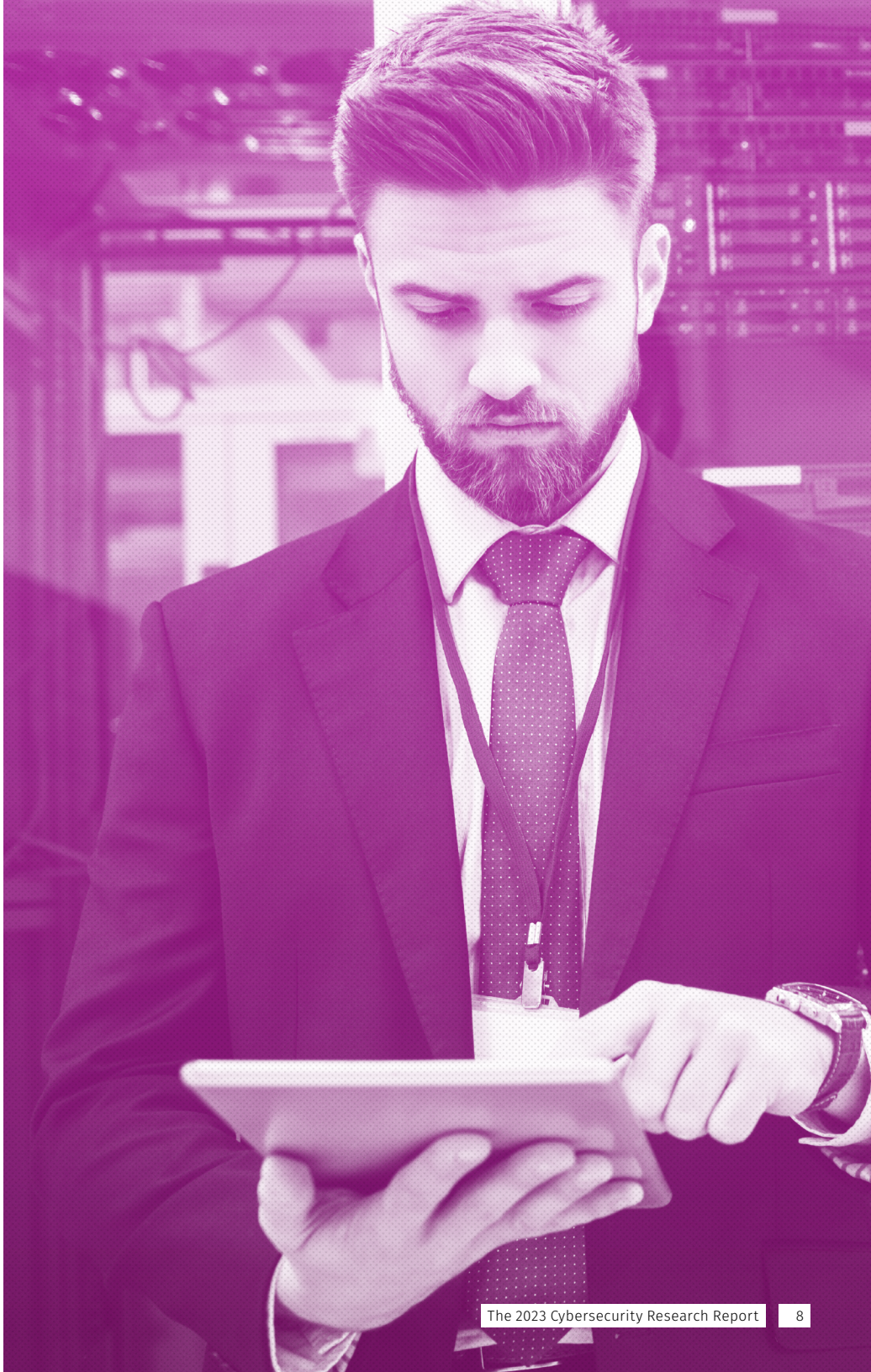
How has the relationship with the security team and the C-suite within your organisation changed as a result of an increase in cyberthreats?

[Strongly agree + Agree]

74%	*C-suite is fully invested in its relationship with the security team*
73%	*C-suite greatly advocates for the security team*
71%	*C-suite and security team collaborate continually*
71%	*C-suite is increasing its investment in cybersecurity*
70%	*Greater board visibility compared to five years ago*
70%	*The collaboration has created new security career opportunities*
65%	*C suite approach to security skills and talent has reduced gaps*

Strong communication and collaboration

A mere 13% of respondents reported significant communication silos between the security team and the C-suite in their organisations. In contrast, a substantial 67% of global IT executives noted very few communication gaps with their C-suite counterparts.



Realising the potential of AI

Businesses are increasingly recognising the vital role AI can play in enhancing their cybersecurity operations. A notable 62% report that surge in accessibility to AI technologies has heightened their need for more stringent cybersecurity measures.

AI-enabled technologies are becoming increasingly used in security tooling. Both C-suite and board members are progressively acknowledging AI's transformative potential, fostering enhanced visibility, buy-in and collaboration across organisational tiers. This shift in perception and approach might be attributed to the anticipation that generative AI can significantly boost productivity, potentially adding trillions of dollars to the global economy.

Has AI increased or decreased the need for cybersecurity in your organisation?

62% of respondents say it's slightly increased or significantly increased *the need for cybersecurity.*

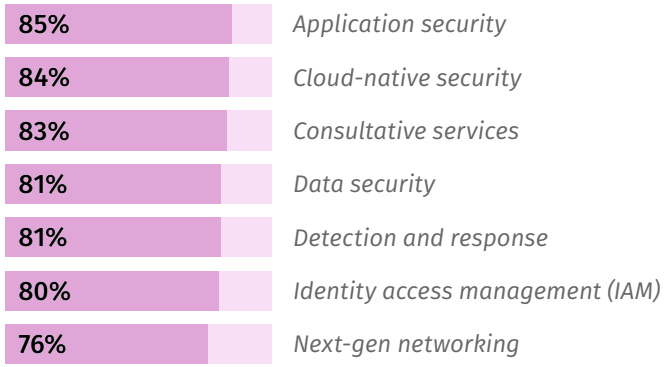
Does your organisation have a formal policy on AI governance and security?

81% of respondents confirm *that they do have a formal policy.*

With a large majority of organisations adopting formal AI governance and security policies, the focus now shifts to refining specific areas within this framework. Moving forward, there are three critical tasks that organisations must complete:

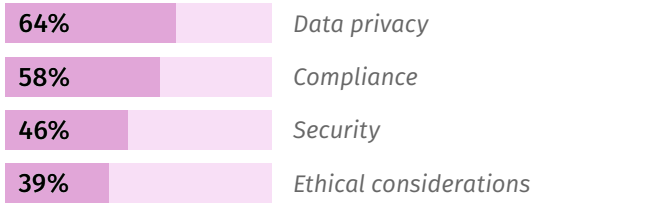
- **Prioritise data protection:** AI serves as a potent tool in reducing risks and enhancing the protection of an organisation's data. However, it's critical to remember that securing data is a continual endeavor demanding consistent attention and evaluation.
- **Continue to work toward AI integration:** AI is steadily evolving as a vital component of cybersecurity. Organisations should remain abreast of the burgeoning developments in AI technologies within the cybersecurity realm and establish policies and procedures that heighten security levels.
- **Promote comprehensive understanding:** It seems that a comprehensive understanding of AI governance and security among employees is still in its early stages, as revealed by the survey. Respondents indicated that 43% of employees have a fair amount of comprehension regarding the company's AI governance and security measures, compared to 39% possessing a great deal of understanding.

To what extent is AI being leveraged within each of these forms of technology?

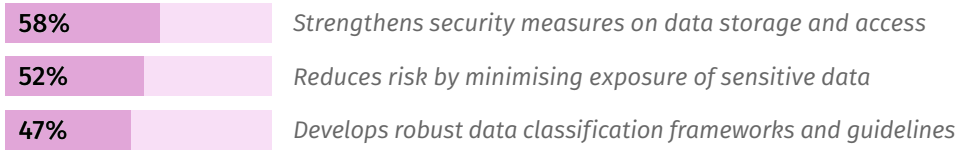


Companies must proactively embrace AI technologies to detect AI-driven threats and adapt to AI-related changes. Otherwise, they risk becoming outdated and facing multiple issues.

What are the main underlying concerns that led to the formalisation of your organisation's AI governance and security policy?



Regarding data security and AI, in what ways does a formal policy address any security concerns?



Which forms of technology is your organisation using to protect you from cyberattacks?

Cloud-native security

As IT boundaries increasingly diffuse, companies are focusing on implementing robust cloud-native security measures to safeguard their evolving infrastructures.

Escalating focus on cloud-native security

As the IT landscape evolves, the emphasis on cloud-native security is intensifying. It now accounts for the majority of cybersecurity investment at 57%, followed by data security at 51%, and application security at 48%. There has been a 7% increase in application security compared to the prior year.

This heightened focus is a response to the perceived increase in cloud architecture attacks, now accounting for a substantial 62% of identified threats, up 12% from the previous year. To counteract these threats, 53% of organisations are now relying on specialised partners for cloud-native security.

rackspace technology. | Microsoft

Funding increases in cybersecurity

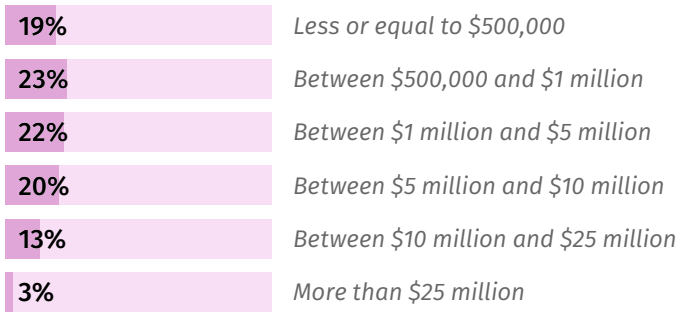
Increasing cybersecurity budgets

With cyberthreats persistently looming over governments and businesses, the objective shifts from complete avoidance, which may be unfeasible, to building substantial cyber resilience. This approach aids in mitigating disruptions during an attack and lessening the potential for long-term damage.

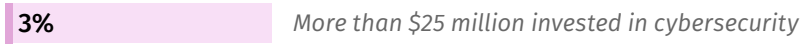
To gear up for this, companies are allocating more resources; 62% have reported an increase in their IT budget allocated for cybersecurity.

Spending is on the rise. Our research showed that 81% of respondents spent more than $500,000 on cybersecurity investment in the last 12 months.

How much does your organisation invest in cybersecurity in the last year estimated in U.S. dollars?



A small percentage in 2023 reported investment of more than $25 million.



What's driving cybersecurity investment?

Mitigating potential risk is the top driver of cyber investment while past incidents/breaches is ranked lowest overall. That is counterintuitive, given that respondents also indicated that addressing potential risks was their highest driver for investment.

Top threat vectors

As companies are usually the primary targets of cyberattacks, they recognise the importance of investing to improve security. Consequently, cybersecurity budgets are just as vital to them as are their investments in cloud and AI technologies.

Budget allocations should align closely with the areas where organisations perceive the greatest concentration of threats, led by cloud architecture attacks (62%), and closely followed by advanced persistent threats (APTs) (56%) and insecure infrastructure (50%).

Obstacles to recruiting and retaining cybersecurity talent

The process of recruiting and retaining cybersecurity talent continues to present significant challenges. According to our research, a majority of technology leaders (56%) acknowledge that navigating the complexities of hiring and retaining IT talent is a prominent concern.

Organisations find themselves grappling with several common obstacles:

- A substantial proportion of staff depart for better salary packages, work culture and professional growth opportunities elsewhere (54%)
- A struggle to continually adapt training and development programs to meet employee expectations (48%)
- A high demand but low supply of skilled personnel (44%)
- A notable skills gap in specialised areas (39%)
- The fast-paced nature of cybersecurity (36%)
- Inexperience (29%)

Maximising opportunities amid challenges

Increasingly, companies are focusing on retention efforts through the adoption of various strategies. These strategies include adopting a positive working environment, offering professional development opportunities and building a strong brand reputation.

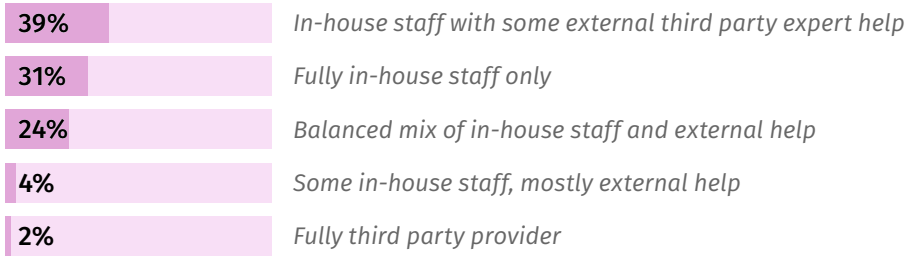
Notably, 53% of organisations report finding success with internal training initiatives for cybersecurity.

Seeking external assistance

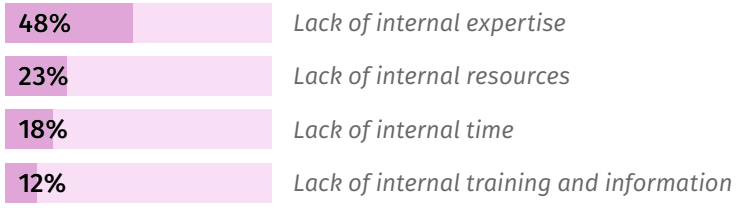
Due to the ongoing talent shortage, companies are finding it challenging to significantly expand their cybersecurity teams. Instead, many are prioritising collaboration with external cybersecurity service partners for consultation or support, a step motivated by a deficiency in internal expertise.

Who do you rely on to manage your cybersecurity?

To seamlessly integrate security into their operational fabric while maintaining a culture of innovation, many companies are opting for varying degrees of external assistance. Here is how they are distributing the responsibility:



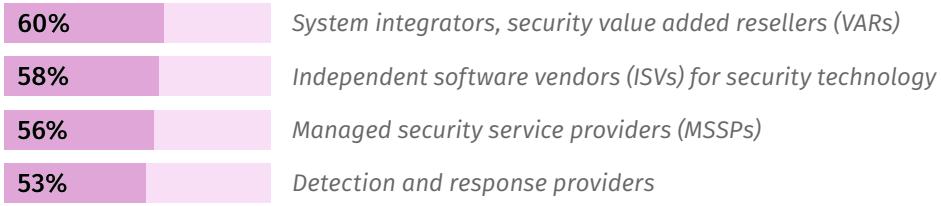
What is the top reason to work with external cybersecurity providers?



Looking to external partners

As cybersecurity complexity grows, with workloads and data deployed across multiple platforms, organisations find it increasingly difficult to 'go it alone.' Respondents prioritised engaging with outside cybersecurity service partners for consultation or support (43%), primarily due to a shortage of internal expertise (48%). This indicates that finding adequate cybersecurity talent continues to be difficult and suggests companies are turning to partners to fill the gap.

What types of cybersecurity partner are you likely to engage with?

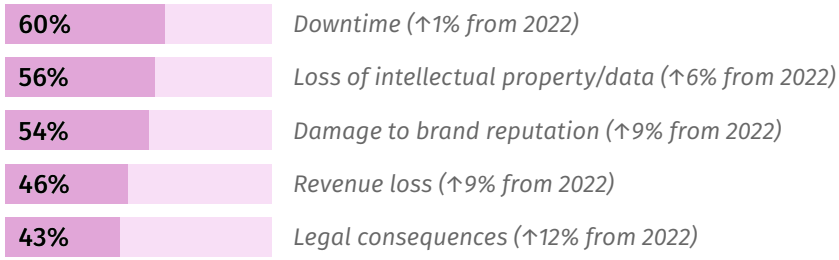


Enhancing preparedness

The global surges in cloud usage and enterprise cloud complexity have brought a deeper understanding of associated security risks. Companies are more aware of the potential repercussions of a cyberattack, which extend beyond operational downtime and data loss to encompass legal ramifications, revenue loss and damage to reputation.

Our year-over-year survey results indicate **a growing recognition of the impact of threats including legal, revenue and reputational threat potential:**

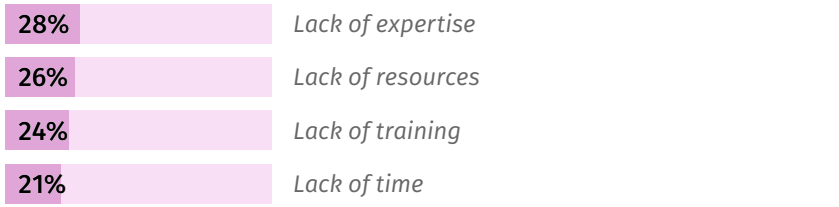
If cybersecurity defenses were breached, what are the top three potential risks to organisations in your industry?



Compliance challenges

Cybersecurity compliance requires organisations to adhere to stringent regulations and standards. This can be challenging, as organisations must continuously monitor security threats, implement appropriate security controls and undergo regular security audits.

Rank the following cybersecurity and compliance challenges for your business:



Security automation

As attacks increase in sophistication, so does automation to protect against ongoing threats.

- Of the survey respondents, **92% automate either some or all of their prevention process** for lapses and breaches, an increase of 9% from the previous year.
- Similarly, **87% are automating some or all of their response to attacks and potential threats**, an increase of 9% over 2022.
- This year, **83% of survey respondents utilised threat detection automation**, which is an 2% increase from the 81% who used it a year ago.

Navigating toward a secure future

Organisations will soon exponentially increase the amount of their applications in the cloud introducing a host of new security vulnerabilities and challenges. Our research underscores that cybersecurity continues to be a primary business concern and a major focal point of IT investment among IT professionals globally. The good news is that companies are exhibiting a heightened degree of cybersecurity acumen. There exists a more profound understanding of security threats, with business leaders adopting a collaborative approach to share both accountability and responsibility in the decision-making processes that impact security. Businesses are also investing in policy and security measures to implement AI, increasing security budgets, adopting cloud-native tools and automation, and eliminating silos in order to facilitate strong communication regarding risks and priorities.

In the face of an acute shortage of specialised talent in the cybersecurity sector, organisations are becoming increasingly reliant on external assistance. Simultaneously, many are reinforcing their security capabilities through an increased focus on nurturing talent and refining existing strategies. These commitments support efforts to maintain business continuity, even when faced with potential attacks or breaches, and to safeguard vital assets. By consistently investing in both personnel and processes, companies are becoming better prepared to manage potential data breaches while steering toward a future where resilience is a cornerstone in the evolving landscape of cybersecurity.

Strengthen your security posture with a full suite of multicloud solutions

No matter where you are on your cloud journey, Rackspace Technology is here to help secure that journey. We offer a comprehensive portfolio of services and solutions aimed at the seamless integration of your data, applications, and security objectives, and rely on a premier security partner ecosystem that helps enhance our expertise to move you forward while helping to ensure robust IT security through proven practices and expertise.

- 850+ Security certifications earned by experts worldwide
- 250+ Security analyst and professional certifications
- 100+ Employees with cloud security technical certifications

Through our Advise/Transform/Manage/Optimise approach to service delivery, Rackspace Technology can be your trusted partner to deliver modern, secure and robust IT operations to your organisation.

Advise	**Transform**
• Assess your security needs • Explore your options • Build your transformation plan for cloud, data, application and security solutions	• Implement unified security across multiple clouds • Modernise and secure your applications • Automate workloads
Manage	**Optimise**
• Protect your multicloud environments • Utilise data centre and security operations • Leverage cloud networks	• Deploy advanced, AI informed security to further protect your assets • Improve application performance • Get industry-leading solutions from a proven delivery partner • Enhance customer experience

rackspace technology | Microsoft

About Microsoft

Rackspace Technology and Microsoft® have been partners for more than a decade, collaborating closely to cultivate a relationship focused on helping global businesses make the most of Microsoft technologies. The company launched its offerings on the Microsoft Azure® platform in 2016, and since then its partnership with Microsoft has taken off, particularly in the areas of analytics and AI. A six-time Microsoft Hosting Partner of the Year recipient with over 700 Microsoft Certified Professionals, Rackspace's excellence in product delivery, service, and support across the Microsoft portfolio has helped to raise the bar in design and deployment of customised, integrated Microsoft solutions.

Learn more at www.microsoft.com

About Rackspace Technology

Rackspace Technology is a multicloud solutions expert. We combine our expertise with the world's leading technologies — across Security, AI, applications, and data — to deliver end-to-end solutions. We have a proven record of advising customers based on their business challenges, designing solutions that scale, building and managing those solutions, and optimising returns into the future.

As a global, multicloud technology services pioneer, we deliver innovative capabilities of the cloud to help customers build new revenue streams, increase efficiency and create incredible experiences. Named a best place to work, year after year according to Fortune, Forbes and Glassdoor, we attract and develop world-class talent to deliver the best expertise to our customers. Everything we do is wrapped in Fanatical Experience® — our obsession with our customers' success that drives us to help them work faster, smarter and stay ahead of what's next.

Learn more at www.rackspace.com or call +44 (0) 800 988 0100

Capitalize on the power of AI, quickly and responsibly

Foundry for AI by Rackspace (FAIR™) offers a roadmap to responsible AI adoption through three solutions: Ideate, Incubate and Industrialize. With FAIR, your organization can quickly tap into the transformative potential of AI to help unlock enhanced creativity, minimize errors, amplify productivity and achieve new levels of cost efficiency.

Learn more at: fair.rackspace.com

FAIR™

© 2023 Rackspace US, Inc. :: Rackspace®, Fanatical Support®, Fanatical Experience® and other Rackspace marks are either service marks or registered service marks of Rackspace US, Inc . in the United States and other countries . All other trademarks, service marks, images, products and brands remain the sole property of their respective holders and do not imply endorsement or sponsorship.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS A GENERAL INTRODUCTION TO RACKSPACE TECHNOLOGY SERVICES AND DOES NOT INCLUDE ANY LEGAL COMMITMENT ON THE PART OF RACKSPACE TECHNOLOGY.

Rackspace Technology cannot guarantee the accuracy of any information presented after the date of publication.

Rackspace-White-Paper-Q3-2023-Cybersecurity-SOL-EMEA-9450 :: September 25, 2023

rackspace technology® | Microsoft