White paper

Cybersecurity Annual Research Report 2022

Cybersecurity is still the leading concern, and less than half of companies feel prepared.

Solve

rackspace technology®

Table of contents

rackspace technology

Introduction and key findings

Are companies well positioned when it comes to data/asset protection and cybersecurity threats?

The second annual Rackspace Technology® cybersecurity survey polled 1,420 IT leaders across industries, including manufacturing, finance, retail, government and healthcare in the Americas, Europe, Asia, Australia and the Middle East.

Our research found that while a majority (59%) of respondents cite cybersecurity attacks as the top business concern in the C-suite, less than half (43%) say that they are protecting critical data and assets from threat.

At the same time, despite sizable increases in their cybersecurity investment, greater board visibility and increased collaboration between the security team and the C-suite, most IT executives report being either unprepared or only somewhat prepared to respond to major threats.

The study also revealed that while overall investment in cybersecurity has increased, there is a lack of preparation, and concern from CEOs is perceived to be relatively lacking.

This report discusses main insights and implications based on responses from our industry peers regarding cybersecurity adoption, challenges, investment and preparedness.

A high-level review of our annual survey reflects the following trends:

1. **Cybersecurity is the number one business concern.** Right now, the topic outweighs even price inflation, supply chain/logistics and the global IT talent shortage.

2. **A majority of companies are less than fully prepared to address major threats/attacks.** Respondents most frequently cited downtime (59%) and loss of intellectual property/data (50%) as the primary risks.

3. **Tied for the top priority in cybersecurity: "Knowing your vulnerabilities" and "protecting data."** This makes sense, as 43% agree that both identifying the gaps and taking action to close them would outrank risk management (42%), as companies strive to locate and remediate security gaps.

4. **More CEOs may wish to consider communicating the urgency/importance of cybersecurity on a more even par with other C-suite colleagues.** While 17% of respondents chose the CIO as likely to be the most concerned about cybersecurity, only 8% of those surveyed named the CEO.

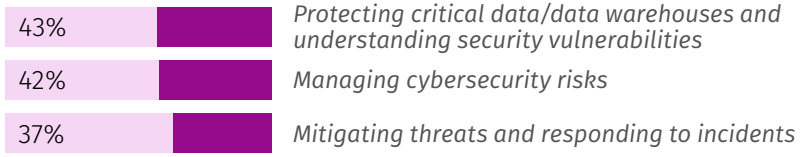
As survey results demonstrate, cybersecurity continues to be far and away the leading business concern and a major focus of IT investment. But with talent at a premium, more organizations are looking outside their four walls for guidance in this new cloud-first world.

Top priorities

As more organizations migrate their IT infrastructure away from data centers and advance their cloud transformation initiatives, they are increasingly focused on how these changes may affect their security posture.

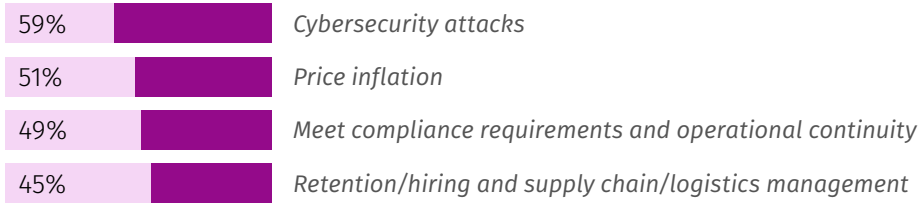
Companies who can take a more proactive approach to cybersecurity — one that includes broader visibility and higher levels of security — can control and detect threats earlier, rather than having to constantly react to issues as they arise. There's work to be done, as the study suggests.

Top priorities for cybersecurity



Cybersecurity is the top business concern for respondents, outweighing economic concerns such as inflation, supply chain and logistics management, and even the IT talent shortage.

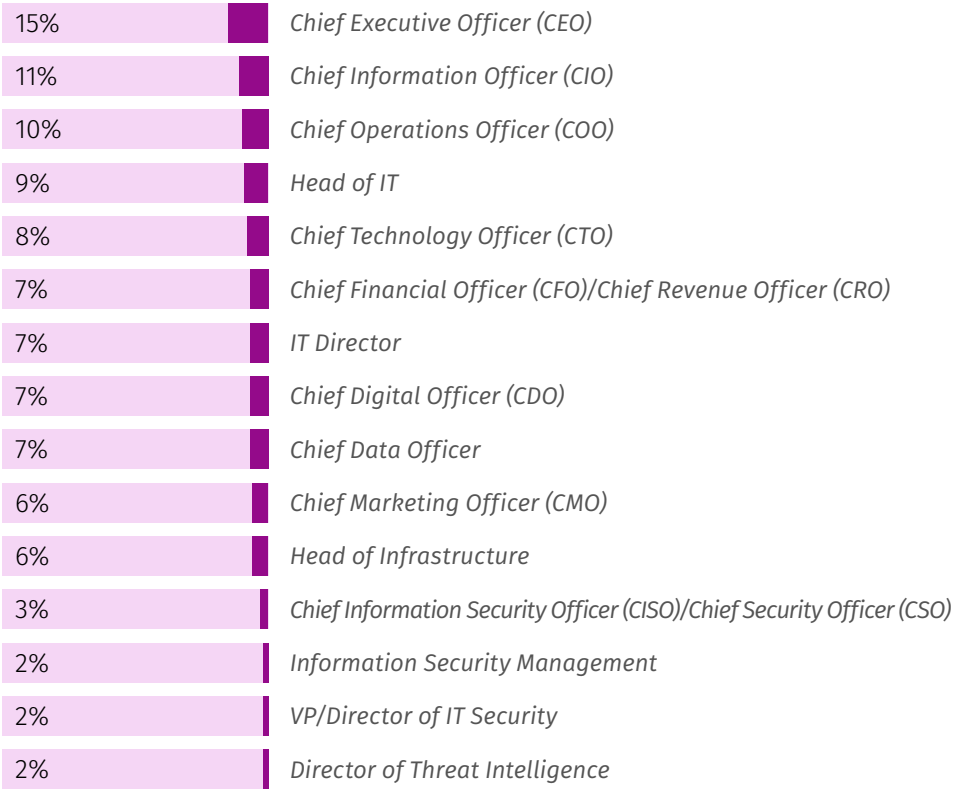
Top business concerns for your C-Suite



CEOs cannot afford to downplay or delay

As cybersecurity threats evolve and cloud adoption proliferates, enterprises must accelerate the shift left to add security earlier in IT processes. Those companies and C-suite leaders who manage (and communicate) cloud risks more proactively, with sound strategies and stronger tools to protect cloud data and resources, will reap the benefits sooner.

Who in the C-suite is more likely to challenge cybersecurity initiatives or funding?



Clarity regarding security coverage is also key

Organizations are changing the way they allocate resources to counter threats, even as budgets increase. Along with this is a growing recognition that the cloud brings with it a new array of security challenges. These challenges require new expertise, and often reliance on external partners that can help implement cloud native security tools, automate security, provide cloud native application protection, offer container security solutions and other capabilities.

Yet, customers are sometimes confused about which security features the different hyperscalers provide.

> "We do business with Amazon Web Services (AWS), isn't that safe enough, already?"

The answer is: "Yes, partially — but not necessarily."

Often customers still need to take an active role in keeping their own IT environments safe. Their company may have basic security in place, but perhaps the customer mistakenly believes all services are inherently secure when they aren't. Companies need additional expertise and staff to work together to ensure that they are optimally prepared and protected.

Approach to cloud security architecture

How is your organization's current approach to cloud security architecture currently distributed, and where would it likely be in three years?

Today	*In three years*	
33.3%	33.0%	*Traditional Security — We mainly use data center network security, along with VM-centric security*
21.8%	22.8%	*Cloud-centric — We use native tooling mixed with third party tooling*
21.5%	21.9%	*DevSecOps Integration — Our security processes are built into our DevOps processes, run by applications and cloud management teams*
20.5%	20.7%	*Intermediate — We use third-party tools built for cloud security*

Infrastructure distribution

How is your current infrastructure distributed, and how will it change in the next 3 years?

Today	*In three years*	
30.6%	31.5%	*On-premises data center — A group of servers that your organization privately owns*
24.2%	23.2%	*Hyperscaler/Public cloud — Multi-tenant cloud computing owned and administered by a service provider*
23.4%	23.3%	*Managed hosting service — A service provider handles the management, setup, administration and overall support of servers*
21.8%	22.0%	*Colocation — Servers and other computing hardware that is rented from another company*

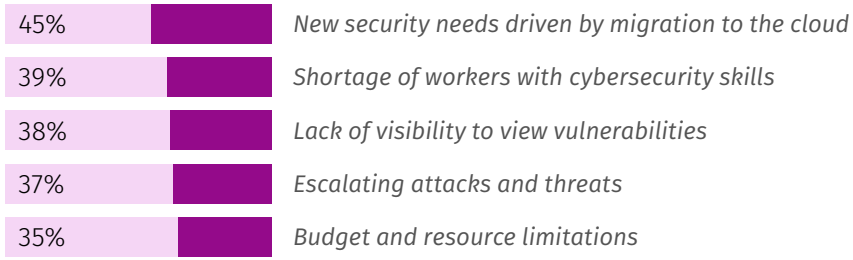
Challenges

As the cloud becomes more ubiquitous, every business, in turn, becomes a target. As a result, cybersecurity threats are now so sophisticated that it's no longer difficult (or incrementally expensive) for a bad actor to scan the internet until they encounter something that is unprotected.

To avoid compromise while meeting budgetary and strategic requirements, organizations' response must be robust.

Greatest cybersecurity challenges

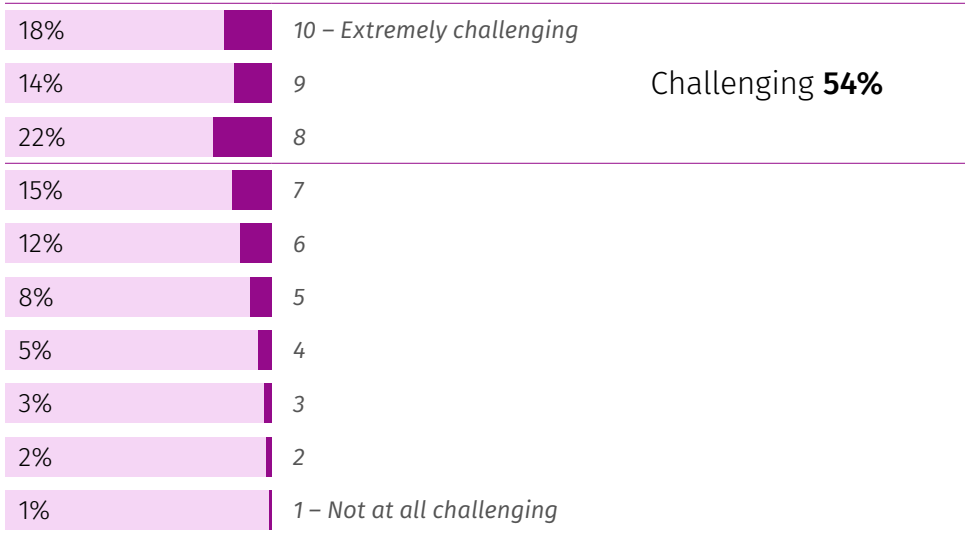
When asked to name the top three cybersecurity challenges their organization faces, migrating and operating apps to the cloud led the way.



Challenges in recruiting and retaining cybersecurity talent

In our research, 54% of technology leaders confirmed that confronting the difficulties in hiring and retaining IT talent remains a major challenge.

How challenging are you finding it to recruit and retain cybersecurity talent/skills currently?



Training

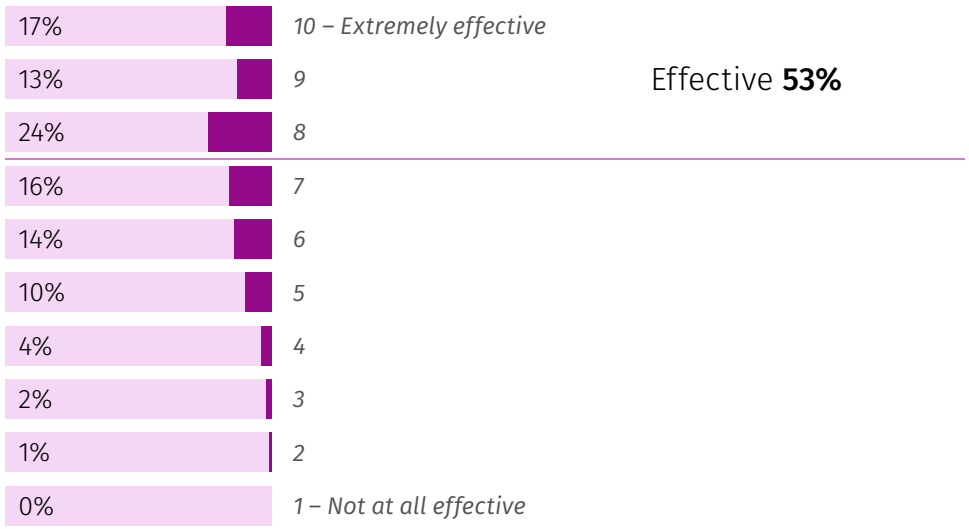
When using public cloud infrastructure, organizations need to be confident that they can recognize and halt a cloud breach that could expose critical data.

Some **53% said their internal training initiatives are currently effective** in retaining cybersecurity talent.

To thwart primary threats such as ransomware, it goes without saying that all organizations must provide employees with cybersecurity training at the time of hiring and on a regular basis to refresh understanding. This is critical not only for security awareness, but also for talent retention.

Effectiveness of internal training initiatives to retain talent

How effective are your internal training initiatives in terms of cybersecurity talent retention currently?



Effective **53%**

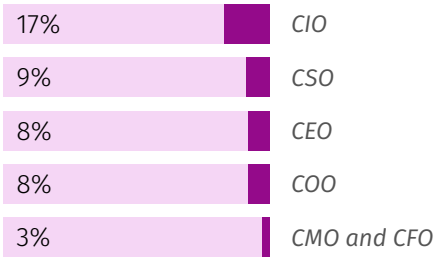
The C-suite

Who in the C-Suite is most supportive of cybersecurity investments?

Not surprisingly, respondents named the CIO (19%) as the most supportive.

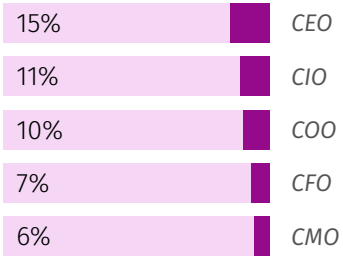
Who within your leadership is most concerned about cybersecurity?

Remarkably, however, **only 8% said the CEO was most concerned** — indicating a gap between a company's perceived and actual readiness to counter cybersecurity threats and actual attacks.



Most likely to challenge cybersecurity funding initiatives?

When it comes to funding, the CEO (15%) was cited as an IT organization's most common challenger to funding cybersecurity investments, followed by the CIO (11%).



Investment

Cloud security tops investment priorities

Even with the economic challenges the pandemic posed, organizations are showing no signs of reducing their cybersecurity investments, with 70% of respondents reporting their budgets have increased over the past three years.

The top recipients of this new investment are cloud native security (59%), data security (50%), consultative security services (44%) and application security (41%).

Companies are **most likely to rely on the expertise of an external partner involving cloud native security**.

Technology investment to protect business from cyberattacks

Which forms of technology are your organization investing in to protect your business from cyberattacks?

59% *Cloud Native Security*

Cloud native security tools, security automation, DevSecOps, infrastructure as code security services, cloud native application protection, cloud native application security as code, container security solutions, cloud security posture management, cloud workload protection, cloud access security broker (CASB) software

50% *Data Security*

Encryption software, enterprise data loss prevention software, tokenization software, database security tools

44% *Consultative Security Services*

Offensive security and assurance services, integrated risk management services, security professional services, continuous attack simulation testing and optimization, security hygiene and vulnerability management, security strategic advisory services, security assessments, hardware support, cloud security and tool implementation, IT outsourcing

41% *Application Security*

App sec testing software, vulnerability scanning, web application firewall solutions, DDoS and Bot mitigation, API attack protections

37% *Infrastructure Detection and Response*

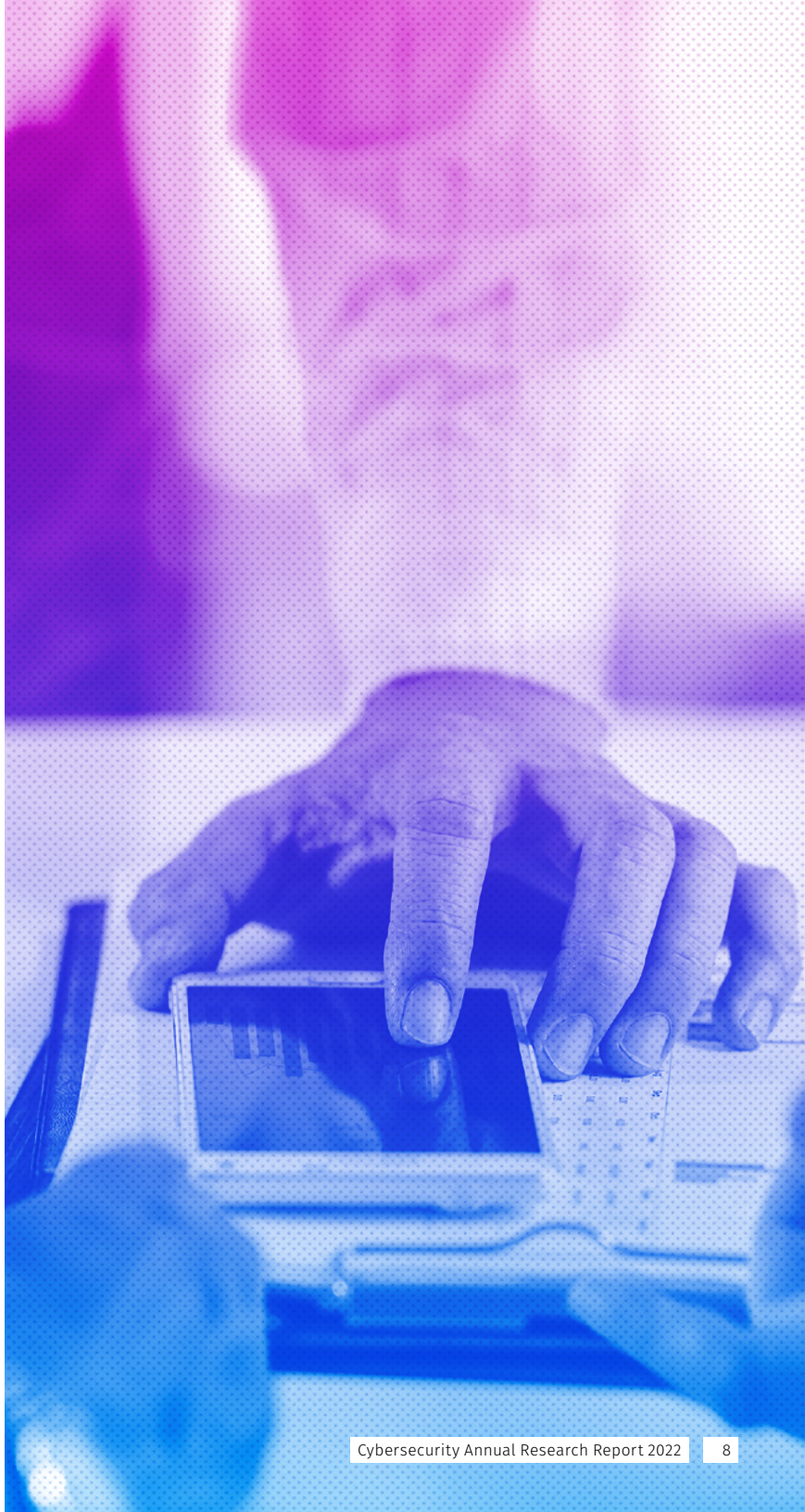
Endpoint management and protection tools, secure e-mail gateway software, security information and event management (SIEM) software, threat intelligence software, extended detection and response (XDR)

29% *Identify Access Management (IAM)*

Access management software, identity governance and admin software, privileged access management software, user authentication software

19% *Next-Gen Networking*

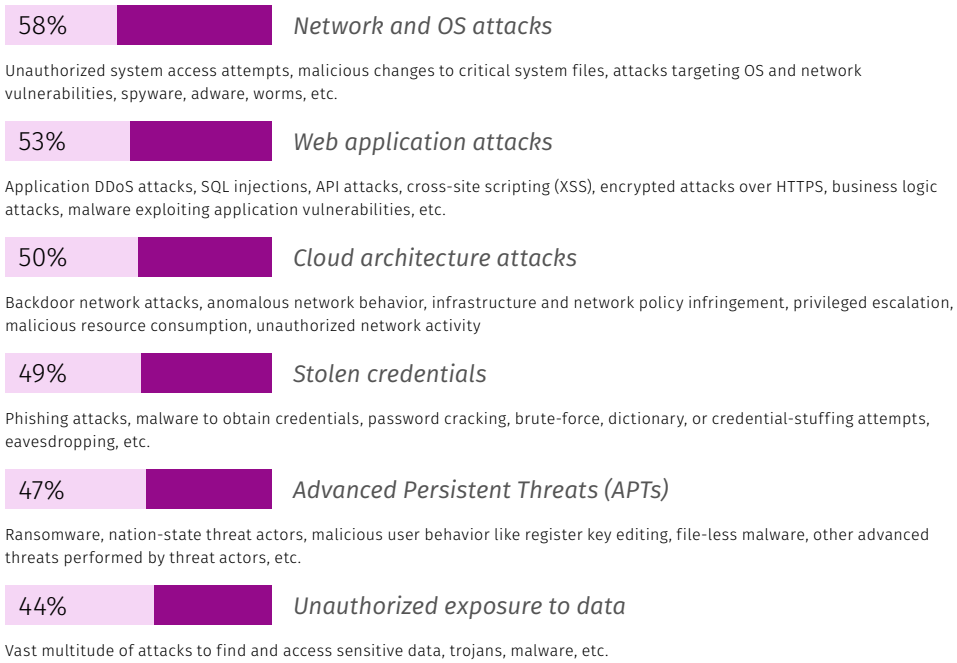
Secure Access Service Edge software, Zero Trust architecture management software, zero trust network access, secure web gateway, SD-WAN



These investments align closely with the areas where organizations perceive the greatest concentration of threats, **led by network security** (58%), and closely followed by web application attacks (53%) and cloud architecture attacks (50%).

Top cybersecurity threats

Please rank the top three cybersecurity threats that are the highest risk for your organization



Increasing budgets

Companies could spend more to prepare — **83% spend between 9% and 14% of their IT budget on cybersecurity**. Happily, their cybersecurity budgets are increasing.

Our research showed that nearly half of respondents invested less than $1 million in cybersecurity last year — with nearly two-thirds (66%) of all surveyed spending less than $5 million.

Amount invested in cybersecurity last year

Change in cybersecurity budget over last 3 years

When it comes to cybersecurity budgets, **69% said their cybersecurity budget increased in the past three years**.

Security teams and the C-suite

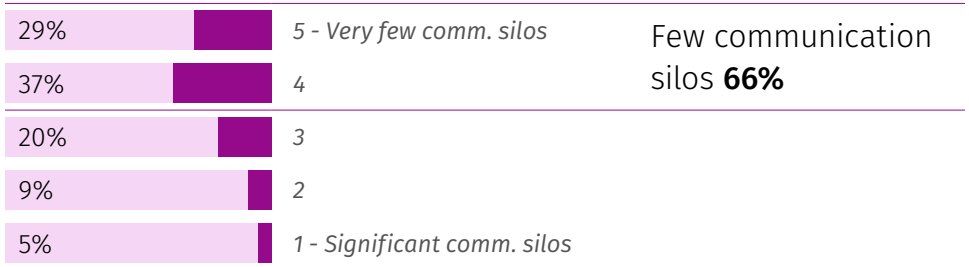
IT security and leadership teams have made progress in breaking down silos and facilitating better communication about threats and priorities.

Examining the relationship between security teams, boards and C-suite executives, 70% of respondents said there has been an increase in board visibility for cybersecurity over the past five years, while 69% cited better collaboration between the security team and C-suite members.

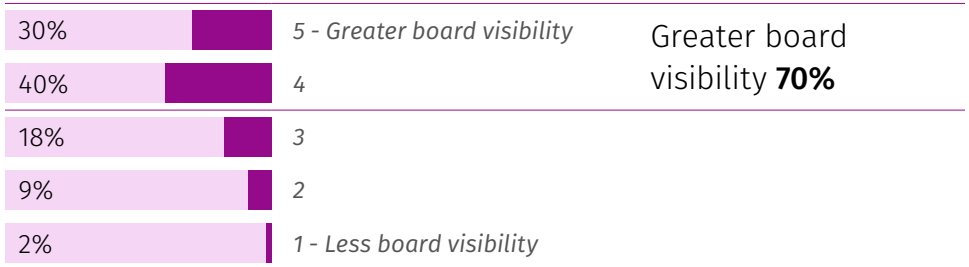
Change in relationships due to increased cybersecurity threats

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

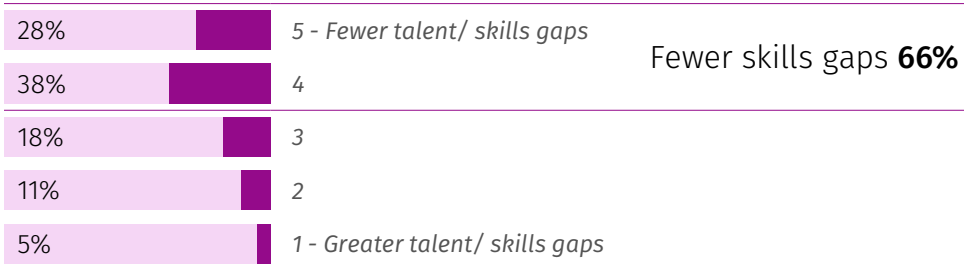
When it comes to communication silos between the C-suite and the security team, there are...



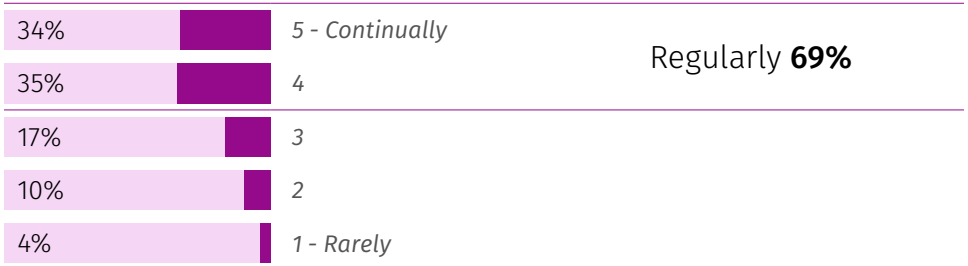
In terms of board visibility for the security team in my organization, compared to 5 years ago there is...



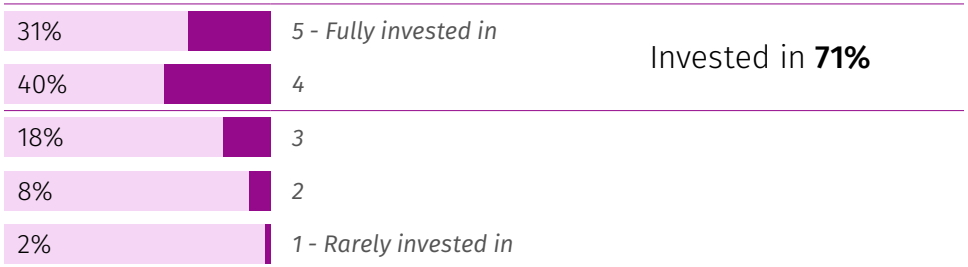
In relation to security skills and talent, the approach taken by the C-suite in my organization has resulted in...



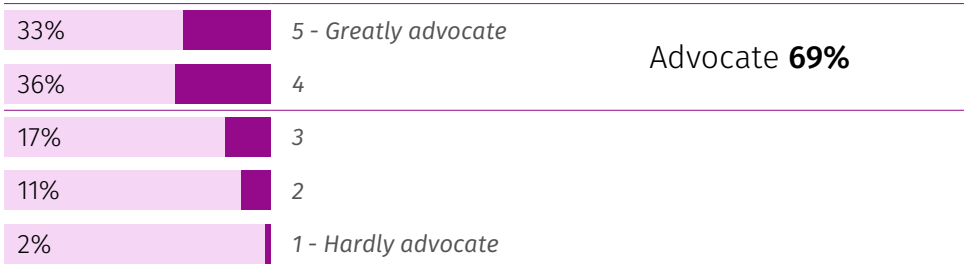
C-suite and the Security collaborate...



The relationship between the C-suite and the security team is...



The support from the C-suite indicates that with cybersecurity, the C-suite...



Only 13% of respondents said there were significant communications gaps between the security team and C-suite, while 69% of IT executives view their counterparts in the C-suite as advocates for their concerns.

Regarding investment in cybersecurity the C-suite in my organization are making...

31%	*5 - More investment*
40%	*4*
18%	*3*
9%	*2*
2%	*1 -Less investment*

More investment **71%**

The current relationship between the C-suite and the security has resulted in a...

31%	*5 - Increase in career opportunities*
38%	*4*
19%	*3*
10%	*2*
2%	*1 - Decrease in career opportunities*

Increase in career opportunities **69%**

Communications between the C-suite and the security team is characterized by...

32%	*5 - Very few comm. gaps*
36%	*4*
19%	*3*
10%	*2*
3%	*1 - Significant comm. gaps*

Few communication gaps **67%**

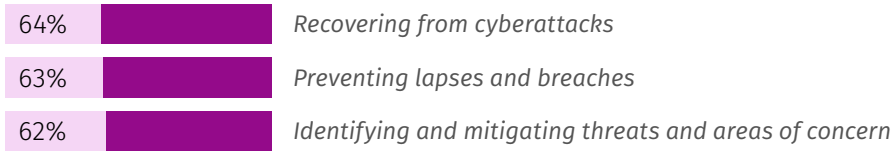
Overall, organizations are much more sophisticated when it comes to cybersecurity and have a better understanding of where they face challenges. At the same time, given the shortage of IT talent and the new skills that the cloud requires, they also know where they need expert guidance.

Preparedness

Commitment to cybersecurity

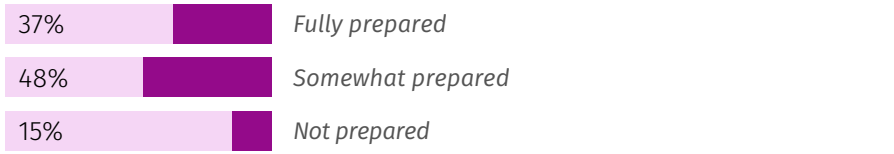
Most organizations are less than fully prepared to address major threats. Despite sizable increases in their cybersecurity investment, greater board visibility, and increased collaboration between the security team and the C-suite, most IT leaders say they are either unprepared or only somewhat prepared to respond to significant threats.

How prepared is your organization to address each of the following...

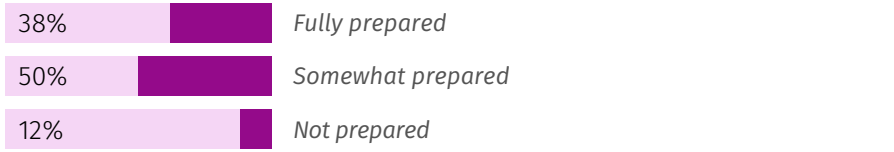


Preparedness of organization

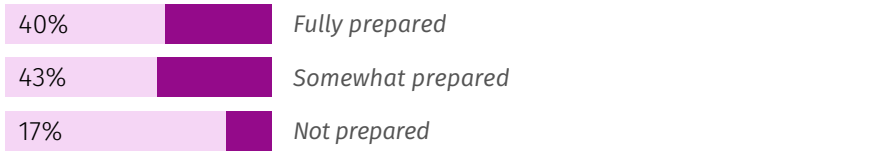
Prevent cybersecurity lapses and breaches



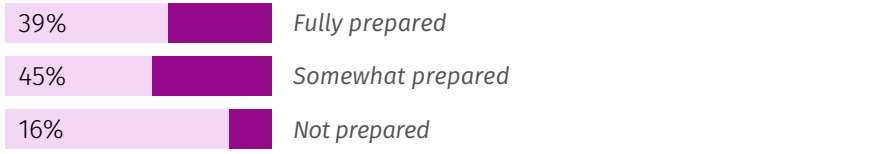
Identify and mitigate threats and areas of concern



Respond to attacks and potential threats

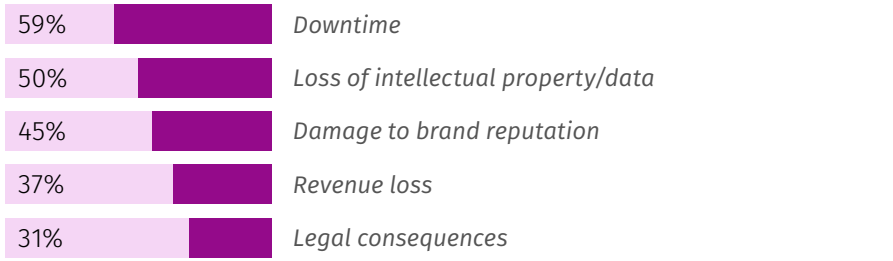


Recover from attacks



What are the consequences of a cybersecurity threat/attack?

As cloud usage soars worldwide and enterprise cloud security efforts fall short of needs, security risks increase. Respondents most frequently cited **operational downtime** and **loss of intellectual property/data**.

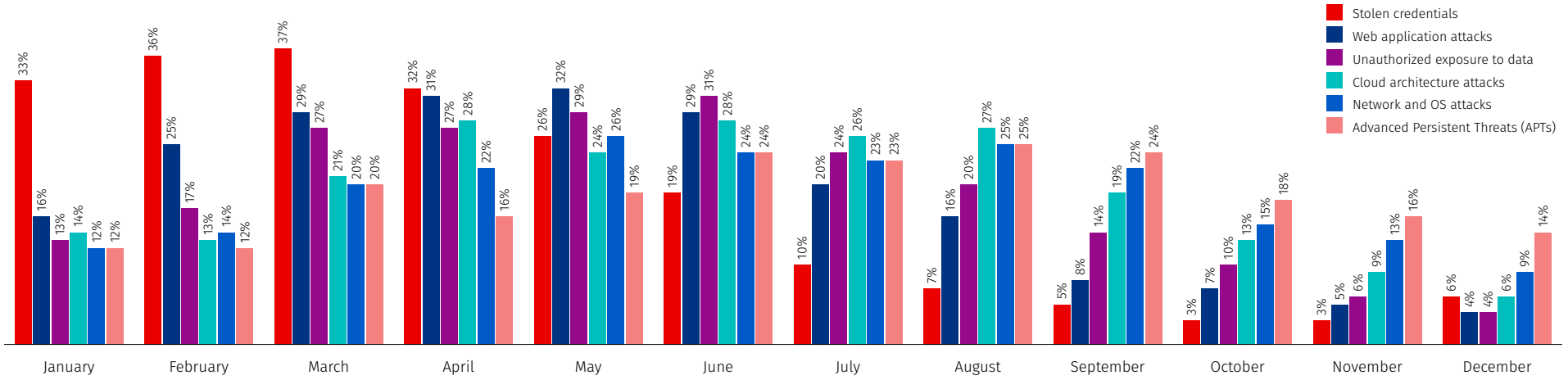


Seasonality

In the survey, 61% of organizations said they do associate seasonality with the frequency and severity of cybersecurity attacks. Activity peaks during Q1 and gradually diminishes over the calendar year to a December low.

Increased occurrences of cybersecurity attacks

When are you most likely to see an increase in cybersecurity attacks?

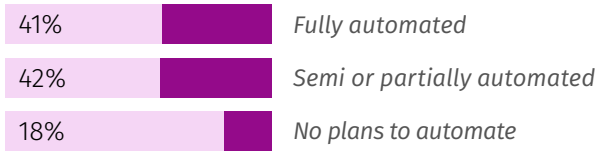


Security automation

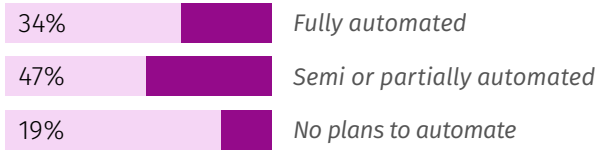
Cybercriminals have shifted tactics from the opportunistic attacks of the past to the more deliberate, persistent threat attacks we see today. Recognizing that bad actors have built capabilities into malware so that it spreads automatically across networks, most organizations are employing automation to combat these threats.

To what degree are your security processes currently automated?

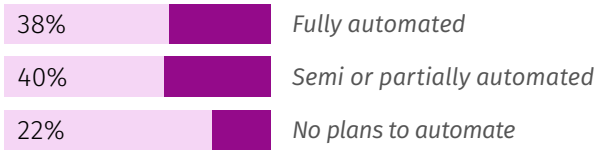
Prevention of lapses and breaches



Detection of threats or areas of concern



Responding to attacks and potential threats



Advise, transform, manage and optimize with Rackspace Technology

Cybersecurity: Think beyond clouds for better outcomes

The cloud enhances your abilities to innovate, create new revenue streams, build better customer experiences and establish new models for work and collaboration. We'll help you accelerate digital transformation through a zero trust, secure-by-design approach to governance, risk and compliance (GRC) that:

- Aligns your security and compliance posture across all clouds environments
- Detects, correlates and responds to security events across cloud environments at scale
- Provides secure access to cloud applications to users anywhere on any device
- Secures cloud native applications without slowing development

We're here to help ensure that all of your technologies work together to move you forward at any stage of our engagement model:

Advise	Transform
• Assess your current needs • Explore your options • Build your transformation plan for cloud, data, application and security solutions	• Modernize your applications • Automate workloads • Implement unified security across multiple clouds
Manage	**Optimize**
• Public, private, multicloud • Data center operations • Cloud networks	• Application performance • Data analytics • Customer experience

rackspace technology®

About Rackspace Technology

Rackspace Technology is the multicloud solutions expert. We combine our expertise with the world's leading technologies — across multicloud, applications, data and security — 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 optimizing 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 our obsession with our customers' success — our Fanatical Experience® — so they can work faster, smarter and stay ahead of what's next.

Learn more at www.rackspace.com or call 1-800-961-2888.

Rackspace-White-Paper-Cybersecurity-Research-Report-2022-TSK-7112_v4 :: August 31, 2022