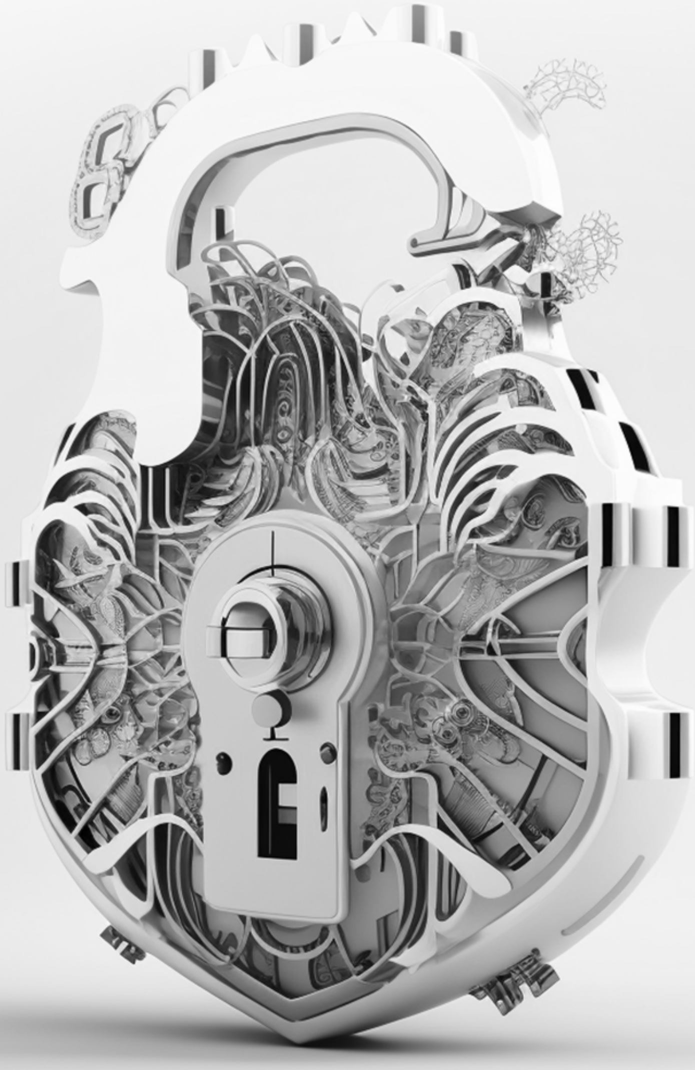
TEAM8™

THE PULSE ON CYBERSECURITY:

Key Findings from Team8's 2023 **CISO Village Survey**

September 2023



WRITTEN BY

Amir Zilberstein

Managing Partner,
Team8

Bobi Gilburd

Chief Ideation Officer,
Team8

Tom Sadon

Director of Marketing,
Team8

Shirly Ozer

Director of Strategy,
Team8

Sarah Levin

Business Research Intern,
Team8

Many thanks to Team8 CISO Village members for filling out the survey and for their valuable comments and fruitful discussions on the survey results and insights.

The Team8 CISO Village is a community of CISOs from the world's leading enterprises. The primary focus of the Village is to facilitate collaboration among the world's most prominent companies with the goal of sharing information and ideas, conducting intimate discussions on industry and technology trends and needs, and generating value and business opportunities for all parties.

By helping Team8 to identify real pain points and understand the requirements of large organizations,members of the Village are first in line to leverage solutions that are purpose-built by Team8's portfolio companies to support their needs.

To contact the Team8 CISO Village, please email cisovillage@team8.vc

DISCLAIMER: **These materials are provided for convenience only and may not be relied upon for any purpose. The contents of this document are not to be construed as legal or business advice; please consult your own attorney or business advisor for any such legal and business advice. The contributions of any of the authors, reviewers, or any other person involved in the production of this document do not in any way represent their employers.**

Table of Contents

Executive Summary &Key Takeaways 4
Security Budget 5
Budget Line Expansion Expectations 7
Organizational Cybersecurity Problems 10
Product Removal & Replacement 12
Build vs. Buy 13
Questions to Fellow CISOs 14
Survey Respondent Information 16
Appendix 18

Executive Summary & Key Takeaways

This report presents analysis of insights gathered from 130 leading CISOs who participated in the 2023 Team8 CISO Village TLV Summit, an exclusive and intimate gathering of CISOs from global prominent enterprises, many of which are Fortune 500 companies.

The 2023 Summit focused on the theme of personal and professional resilience. Throughout five days, industry experts discussed their evolving roles, trends in technology, mutual opportunities, and common challenges.

To capture insights into the emerging trends discussed at the conference, Team8 conducted the 2023 CISO Village Survey. On the final day of the summit, CISOs gathered to discuss the survey results. The discussion helped strengthen the CISO Village members' understanding of current trends in security, and supported Team8's ideation as part of Team8's unique company-building model. The survey results and insights are now being shared with the wider public through this report to contribute to both the CISO community and the broader cybersecurity ecosystem.

Additionally, this report incorporates previously unpublished information gathered from the 2022 CISO Village TLV Summit Survey.

In a year filled with economic and geopolitical instability, the theme of resilience is prevalent throughout the report, which presents insights on prevailing trends, challenges, and strategies in the cybersecurity landscape.

- Despite predictions suggesting cybersecurity spending would be impacted by recent economic challenges, **most organizations continue to increase their cybersecurity budgets.**
- **As expected, enterprises also continued transitioning to the cloud.**

The COVID-19 pandemic, the volatile economic environment, and the rise of remote work created new challenges in the cybersecurity landscape that have simultaneously instigated new opportunities for growth.

- To adapt to the new era of work and data management, the surveyed CISOs **felt the need to expand their budget lines, especially for spending on Identity and Access Management (IAM) and cloud security services.**

Amidst changes in the threat landscape, CISOs are eager to adopt further innovation.

- As companies have increased integration with third-party infrastructure, **CISOs expressed a strong desire for improved third-party risk management solutions.**
- Staffing shortages in the cybersecurity industry, alongside the evolving threats posed by insiders working alone or cooperating with cybercrime groups, have also pushed CISOs to seek **solutions that help reduce human error and mitigate insider threats.**
- As enterprises adopt AI solutions, CISOs also expressed the need for **innovation in AI security** to keep up with the changing landscape of threats.

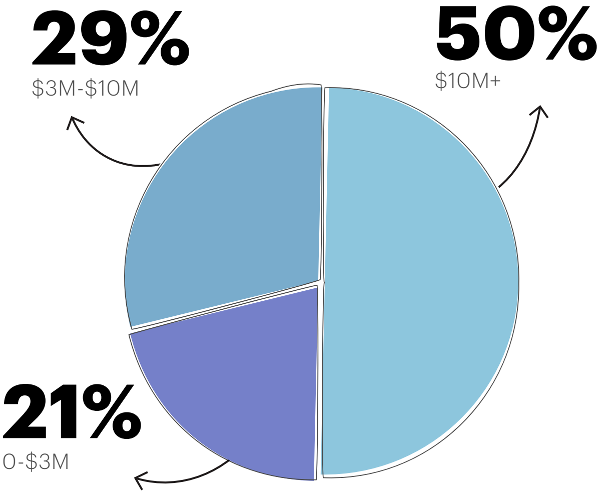
Security Budget

1.1 Budgets

The majority of companies with over 50 employees working in their cybersecurity department have an annual budget exceeding $10 million. Among the companies with fewer than 50 employees in the cybersecurity department, around 47 percent of respondents reported a budget ranging from $3 million to $10 million, while 13 percent reported a budget exceeding $10 million.

For more details, see also Appendix A.1 Budget by CISO organization size (no. of employees)

Annual cybersecurity budget:



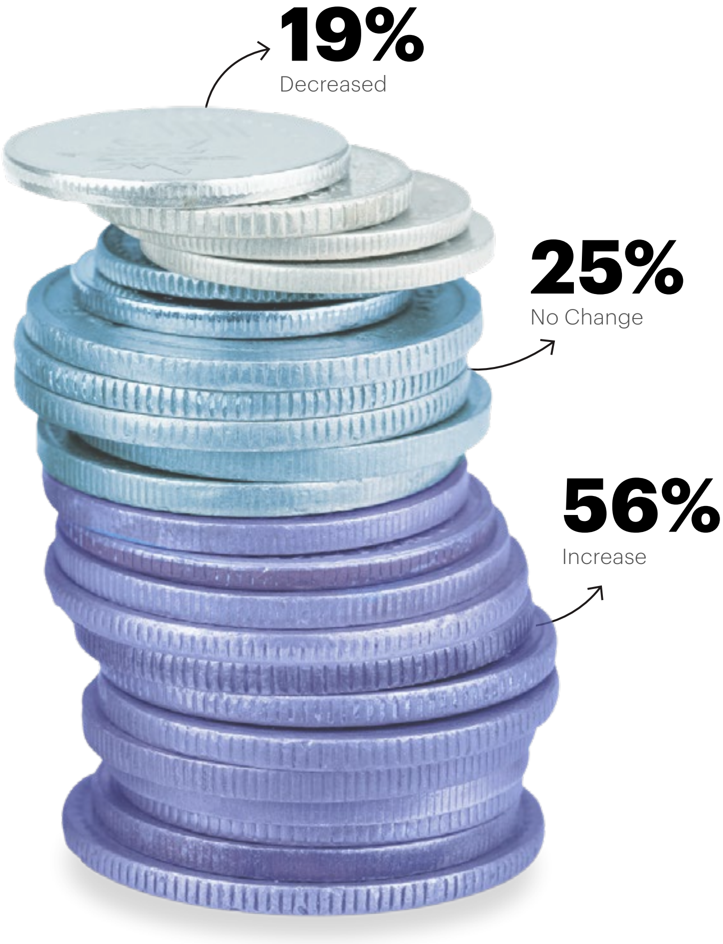
1.2 Budget Change

Around 56 percent of survey respondents reported a budget increase from 2022.

In the 2022 CISO Survey, 65 percent of respondents reported an increase in their budget compared to 2021. Our survey results align with the global trend that cybersecurity spending has not been as severely impacted by recent geopolitical and economic challenges as expected. On average, cybersecurity spending worldwide has increased since 2022.[1] Additionally, a 2022 McKinsey report projects an annual rise of 13 percent in spending on cybersecurity until 2025.[2]

For more details, see also Appendix A.2 Budget change by CISO organization size (no. of employees).

Budget Change:

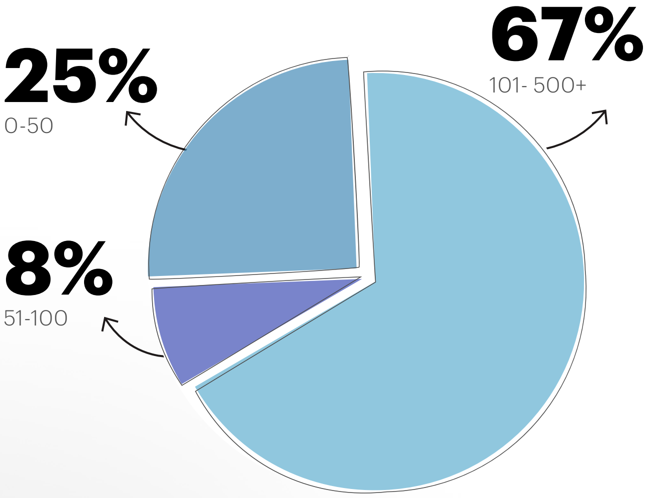


1.3 Budget Decreases

Among the CISOs surveyed, 19 percent reported budget decreases, with the majority of these cuts observed in larger companies with over 100 cybersecurity employees and budgets exceeding $10 million.

While most organizations have been expanding their cybersecurity budgets despite economic challenges, some cybersecurity departments have not been immune to budget cuts. Cybersecurity plays a crucial role in business outcomes by ensuring regulatory compliance, safeguarding intellectual property, and enabling faster and safer growth. However, cybersecurity leaders often struggle to adequately justify budget allocations and communicate the direct impact of cybersecurity on business outcomes to C-suite executives and the board of directors.[3] Benchmarking cybersecurity staff and formalizing strategic planning can help bridge the communication gap and reduce vulnerability to budget cuts.[4] Although cybersecurity spending is projected to grow, potential economic challenges in the upcoming year may put resource pressure on companies, further heightening the possibility of budget cuts. It is crucial for cybersecurity leaders to take proactive measures to safeguard their budgets. By demonstrating links between spending and business outcomes, CISOs can help ensure the necessary resources are allocated to protect against evolving cyber threats.[5]

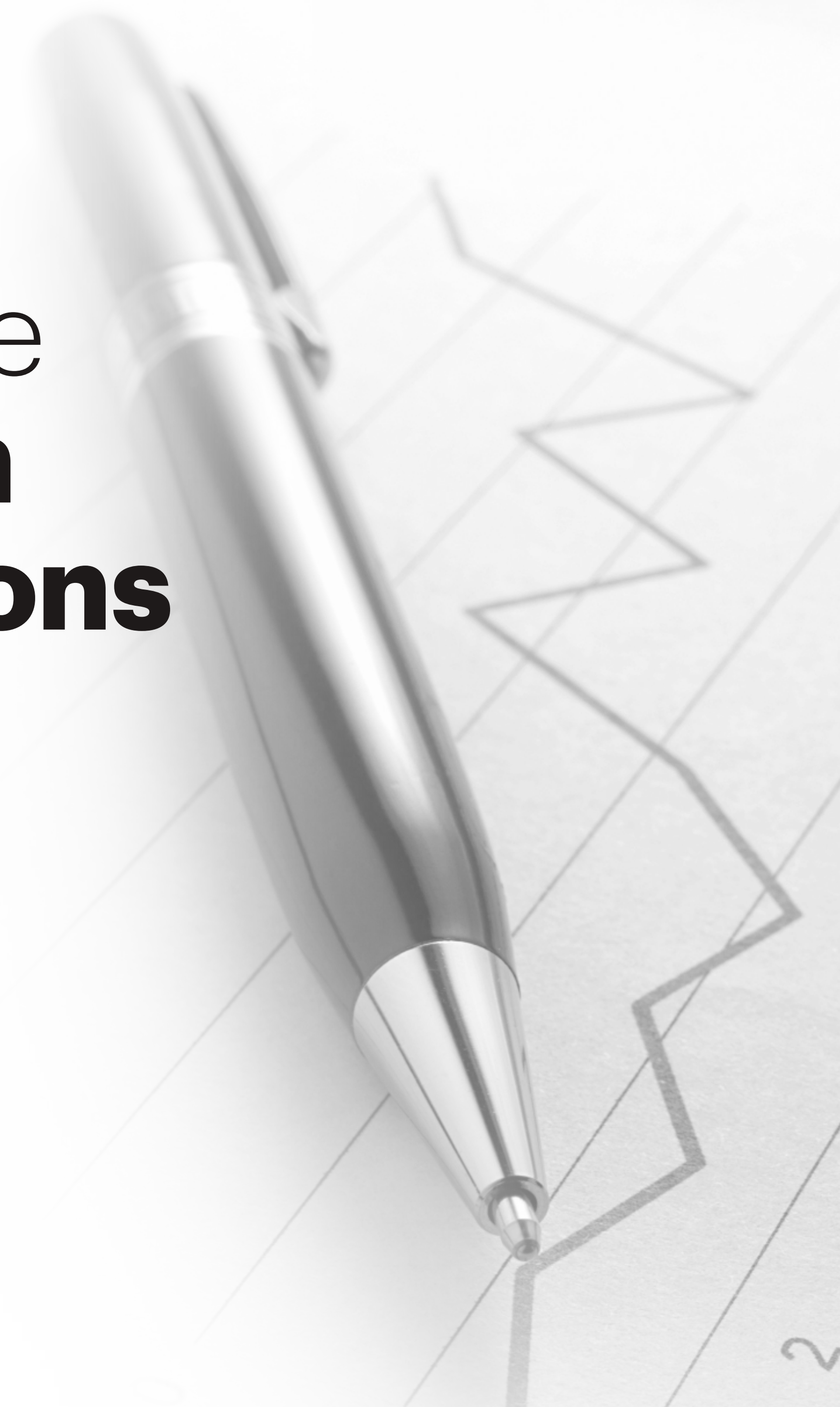
Budget Decreases - Organization size:



> In a world rife with economic and geopolitical challenges, cybersecurity takes center stage as enterprises recognize the critical necessity of increasing investment in robust defense measures to protect their most valuable assets."
>
> **ADM Michael S. Rogers,** Former Director, NSA

02

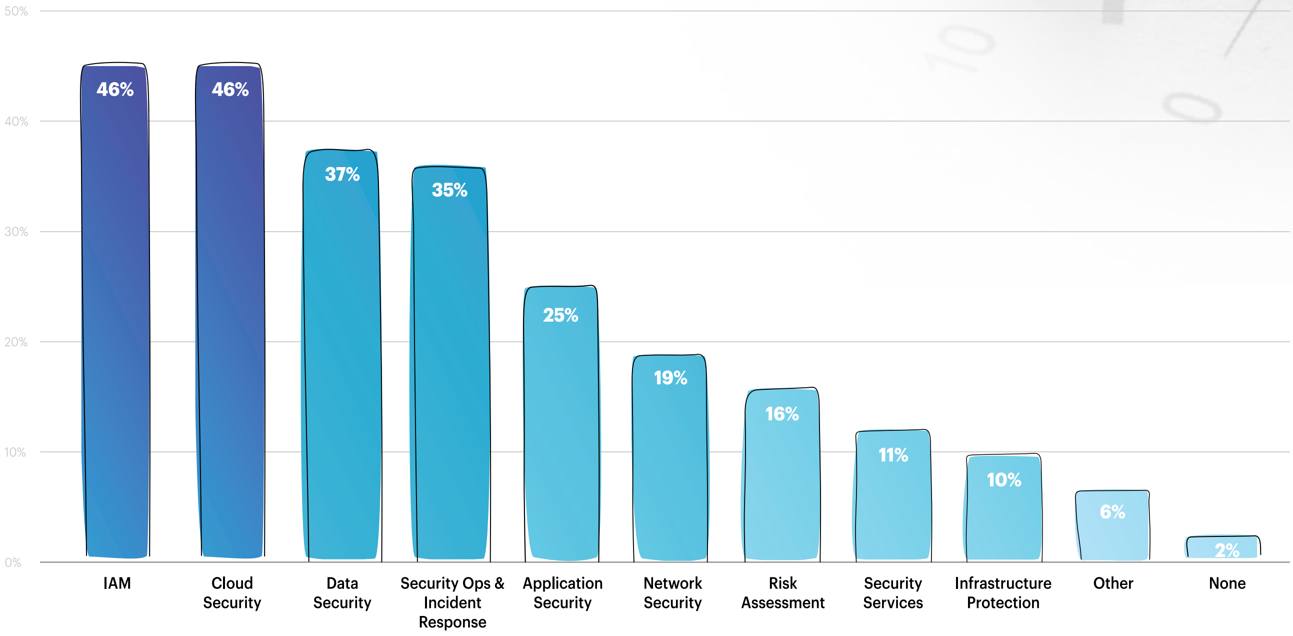
Budget Line **Expansion Expectations**



Our survey indicates that budget expansions are widely anticipated in two categories. The first is IAM (Identity and Access Management) which encompasses IGA (Identity Governance and Administration), PAM (Privileged Access Management), authentication, machine identity management, etc. The second category is cloud security which encompasses CNAPP (Cloud Native Application Platform), CSPM (Cloud Security Posture Management), CWPP (Cloud Workload Protection Platform), and CDR (Cloud Detection and Response).[6]

On the other hand, risk assessment, security services, and infrastructure protection are less frequently listed as anticipated categories for budget expansion.

Budget Line Expansion Expectations:



IAM (Identity & Access Management)

IAM is ranked as one of the top categories for budget expansion, alongside cloud security. CISOs have shared their insights into why IAM is listed as one of the primary areas for budget expansion in the coming year. The COVID-19 pandemic and the rapid adoption of remote work have created unmet needs in existing IGA tools and programs, resulting in increased friction between security teams and employees. Furthermore, with the accelerated adoption of cloud technologies, IAM needs to extend its capabilities to encompass both on-premise and cloud products. The consensus among the CISOs is that IAM has untapped potential, providing opportunities for further development and innovation.

> Identity and access management is a decades old challenge that requires clear prioritization and investment to address the protection of cloud, SaaS and IoT environments. Companies will need to embrace emerging technology including AI based identity solutions that will more effectively – and at scale - validate identity, support compliance and enable the detection and response of behavioral anomalies of its employees, third parties, and IoT systems.”
>
> **Renee Guttmann,** Founder and CISO, CisoHive; Former CISO, Campbell Soup Company, Royal Caribbean Cruises and Coca-Cola

Cloud Security

Cloud adoption is rapidly increasing. By 2025, over 85% of enterprises are projected to adopt a cloud-first approach and will not be able to execute their strategies without the use of cloud technology.[7] The shift to cloud infrastructure, especially multi-cloud, introduces added security complexities that were not needed with standard on-premises environments. The dramatic spike in cloud usage has increased the need for dedicated cloud security solutions. The demand for more advanced cloud security tools, including CSPM and CWPP, which have expanded into the broader CNAPP concept, along with CIEM (Cloud Infrastructure Entitlement Management) tools and the emerging category of CDR, has never been higher.

> Businesses are rapidly migrating their data and applications to the cloud to take advantage of the innovation and security benefits that are difficult to achieve in on-premise environments. They are equally seeking out cloud security best practices, technologies and solutions to assist in this transition from the traditional datacenter skills, experiences and processes”
>
> **David Cross,** SVP, CISO SaaS Cloud Security, Oracle

Data Security

Data security solutions play a crucial role in digital transformation and cloud migration processes. As organizations store an increasing volume and diversity of data across various infrastructures and no longer have a clearly defined on-premises perimeter, they face heightened risk of data attacks.[8] Therefore, there is a pressing need for data security solutions that prioritize data discovery, classification, and protection for both on-prem and cloud scenarios.

Budget Line Expansion Expectations by Cloud Deployment

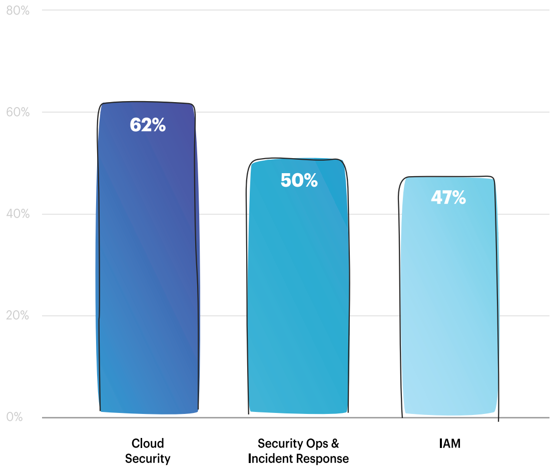
The distribution of expected increased budget lines varies depending on cloud deployment status.

Hybrid Infrastructure

Around 56 percent of survey respondents list their cloud deployment status as hybrid, with an ongoing transition towards greater coud adoption (see also section 7.1 - Survey Responded Cloud Deployment Status).

Among respondents from hybrid companies, 66 percent expect increases in spending on cloud security. CISOs speculated that these hybrid companies, already on their digital transformation, require team rescalling to effectively manage incident response in the cloud. This necessitates increased spending on both cloud security and security operations.

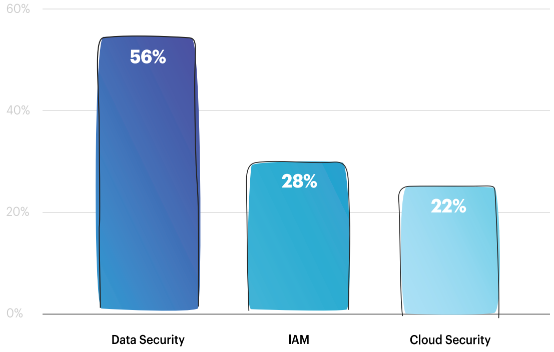
Hybrid: Top 3 Budget Expansion Categories



Born in Cloud / Mainly Cloud

Among companies that predominantly operate in the cloud, data security emerged as the category with the highest anticipated budget expansion. However, only 22 percent of respondents indicated an expectation to increase spending on cloud security. This lower percentage may be attributed to these companies' more advanced cloud deployment status, suggesting that they have already invested in robust cloud security measures. Additionally, it reflects the need for data security solutions that align with the evolving cloud landscape. In the past, companies with on-prem computing could build a perimeter and trust their data was contained.[9] However, many companies now lack a clearly defined perimeter. In addition, the data flows between on-prem solutions, public, and private clouds have increased security complexity prompting the need for more agile data security solutions.[10]

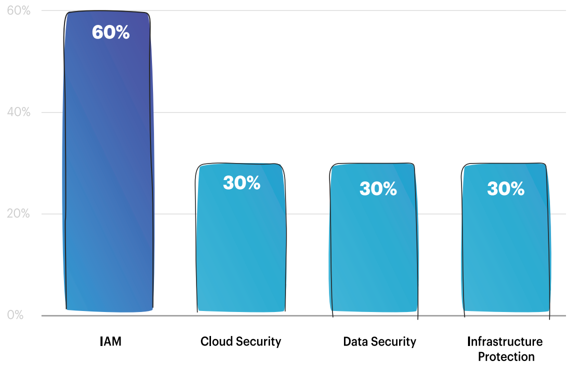
Born in the Cloud & Mainly Cloud: Top 3 Budget Expansion Categories



On-Premises

Even among companies primarily operating on-premises, 30 percent of respondents listed cloud security as an expected budget expansion category. This suggests that despite a slower rate of cloud adoption, there is a recognition of the need for cloud security and potential for further expansion.

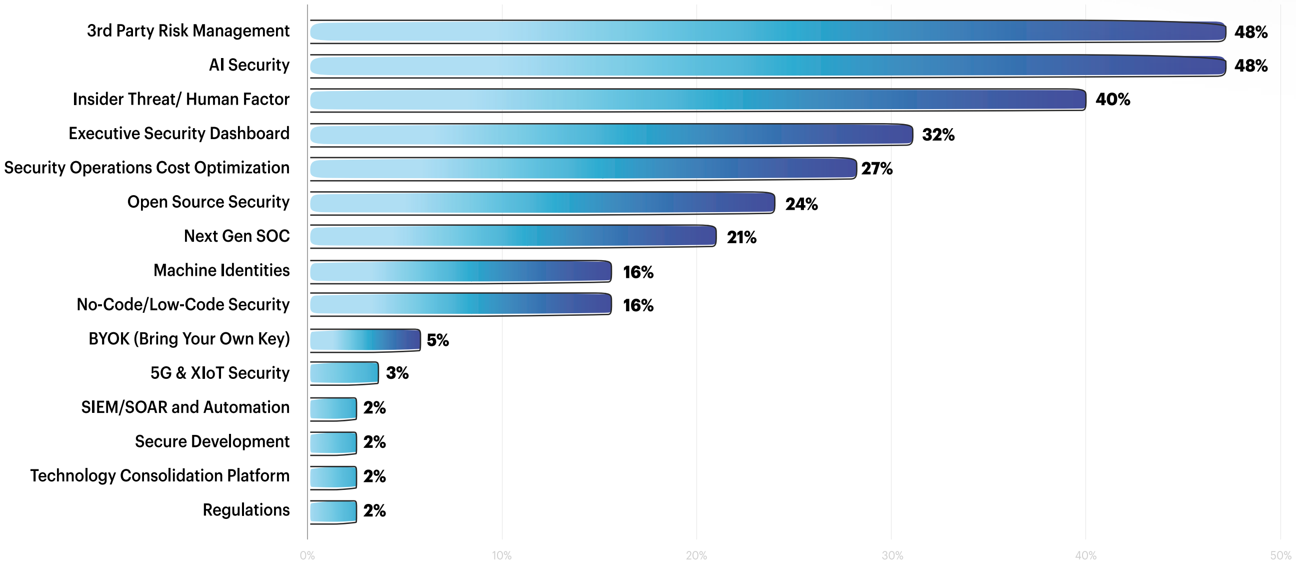
Mainly On Prem: Top 3 Budget Expansion Categories



03

Organizational Cybersecurity Problems

While organizations face a range of challenges, survey respondents overwhelmingly listed third-party risk management, AI security, and Insider threats as the most acute problems the organization is facing where existing solutions are not meeting needs.[11]



Third-Party Risk Management

Among the survey respondents, 48 percent identified third-party risk management as one of the most pressing challenges they face in their organizations. The increased integration with third-party infrastructure, including SaaS (Software as a service), PaaS (Platform as a Service), and LaaS (Logging as a Service) products, has heightened companies' vulnerability to third-party risks.[12] Amidst the volatile economic environment and staffing shortages, companies across various industries have shown a growing interest in third-party risk management programs.[13] However, the market for third-party risk management solutions remains fragmented, which forces CISOs to make compromises when selecting their risk management products.[14] Our survey results reinforce the need for innovation in third-party risk management to address these challenges efficiently.

AI Security

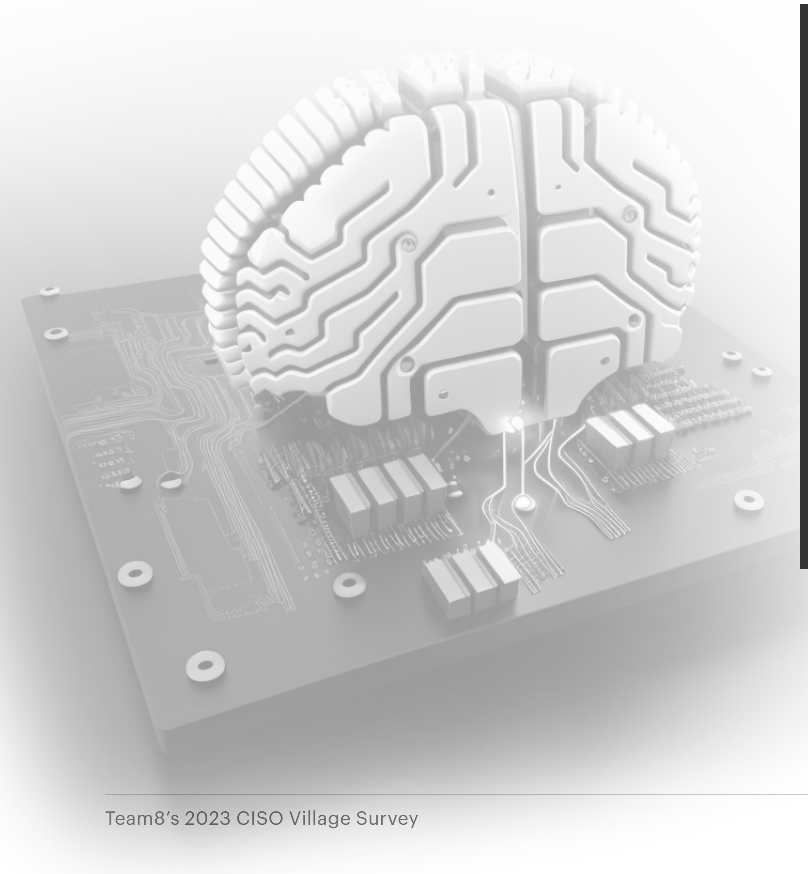
GenAI adoption has surpassed expectations, outpacing the adoption of all other technologies worldwide and has become accessible and intuitive for almost everyone to use. However, this rapid adoption of AI across industries has given rise to new security risks, with AI privacy breaches and security incidents quickly becoming widespread.[15] Currently, the limited number of providers creates the potential for concentration risk.

The risk associated with third-party SaaS is amplified by GenAI, as users are enticed by the convenience and high-value proposition of inputting sensitive data into AI platforms.

GenAI has the potential to assist cyber defenders by focusing attention and intelligence on the attack surface. At the same time, GenAI also introduces new risks that are not yet fully understood. For instance, attackers may exploit GenAI to identify vulnerabilities at a faster pace than defenders can effectively respond to.

Another challenge is ensuring that the AI agent/model performs as intended. The data that the agent or model is based on must be secure and reliable, and there is a growing need for solutions that will address threats such as data tempering or manipulations.

As AI technology continues to evolve, our understanding of its impact is still developing. However, there is no doubt that there is an urgent need for innovations in AI security solutions.



Human Threat

Insider threats and human factors ranked as one of the top problems among the surveyed CISOs. According to a 2023 Nuspire survey, 41 percent of CISOs reported that human error and lack of internal employee training remained the number one IT system vulnerability, which was a decrease from 50 percent in 2022.[16] It is projected that by 2025, over half of significant cyber incidents will be attributed to either a shortage of skilled personnel or human error.[17] Troublingly, around 90% of employees who admitted to engaging in unsecure actions during work were aware that their actions increased the organization's risk.[18] However, they proceeded due to the perceived benefits of speed and convenience that outweighed potential risk.[19] In addition, the risk of deliberate harm or sabotage by an employee always remains a concern for enterprises.

The number of organizations with formal insider risk management programs is expected to rise from 10 percent today to 50 percent by 2025 to fill this need.[20]

> **Safely recognizing the benefits of GenAI requires a whole-firm view of the risks and rewards. In this regard, the CISO is well positioned to partner with internal AI specialists in support of GenAI**
>
> **Steve Sparkes,** CISO, Scotiabank

Product **Removal & Replacement**

Survey respondents most frequently listed SIEM (Security Information and Event Management) as a product they would like to remove or replace in the coming year. Managed services and legacy scanning tools were also among the frequently mentioned products to remove or replace.

SIEM

The effectiveness of SIEM products depends on several critical factors including staffing, funding, and a robust data stack.[21] Our survey findings indicate that many CISOs find SIEM lacking in performance due to these constraints. This finding is also aligned with the results of the previous question, where both SIEM and SOAR (Security Orchestration, Automation and Response) were identified as among the least pressing issues faced by enterprises, with only 2 percent of respondents indicating that SIEM is a pain point that lacks solutions capable of meeting the requirements of CISO.

The prevalent desire to remove SIEM highlights the need for innovative solutions that can address the limitations associated with traditional SIEM implementations. Respondents expressed interest in alternative approaches, including exploring XDR (Extended Detection and Response) tools and data warehouse technology, or transitioning to other modern SIEM products.

05

Build vs. Buy

The percentage of respondents who indicated a preference for building their own solutions, rather than purchasing them, has decreased from 56 percent in 2022 to 44 percent in 2023. Furthermore, the types of products that respondents considered building has also changed. In 2023, automation tools, AI, and dashboards were the most frequently listed tools. In contrast, in 2022, automation was frequently listed, but dashboards were not. AI was also not mentioned in 2022, highlighting the rapid adoption of AI technology.

Analytics Tools and Dashboards

CISOs have shown a strong interest in building analytics tools and dashboards internally rather than buying them. This trend is particularly notable among CISOs from companies with hybrid cloud adoption status. Enterprises with hybrid environments are seeking a unified platform for visibility into their IT environment, driving the demand for analytics products and dashboards.[22] However, there has also been a trend toward greater visibility across different IT infrastructure elements. This trend suggests that the need for dashboard and analytics tools is evolving and may become secondary to other forms of monitoring. [23]

Automations

Survey respondents also indicated an interest in building automation solutions internally rather than relying on purchasing them. The desired automation capabilities encompass a wide range, including automation of processes and integration of Gen AI tools to support security operations. With the increased availability of automation, machine learning, and AI tools accessible to attackers, cybersecurity teams must be prepared for high-speed attacks.[24] By increasing the use of automation, cybersecurity teams can build their overall resilience to attacks by increasing their response speed and effectiveness.[25]

Questions to **Fellow CISOs**

A fundamental aspect of Team8's CISO Village is the intimate discussions among CISOs that foster knowledge sharing and the exchange of common challenges and ideas.

With that in mind, the final survey question posed to participants was:

> **IF YOU COULD ASK YOUR FELLOW CISOS ONE QUESTION, WHAT WOULD IT BE?**

Best ROI

One of the most frequently asked questions focused on **identifying the best ROI** (Return on Investment) **tools, projects, and processes** that CISOs had utilized or experienced in the past year. The survey presentation provided an opportunity for crowd respondents to discuss their notable ROI successes.

One respondent highlighted the impact of reserving time to act as "**cyber janitors** of the company." The CISO explained that implementing a **clean up** of their legacy environments, virtual machines, and virtual tenants significantly enhanced the overall efficiency and security within their department. Their approach was based on the principle that what isn't present cannot be attacked. CISOs were then able to use the freed up resources to explore and implement new ideas and processes. Additionally, other participants in the discussion also emphasized the importance of maintaining network hygiene, asserting that it offers the best value investment for hybrid companies.

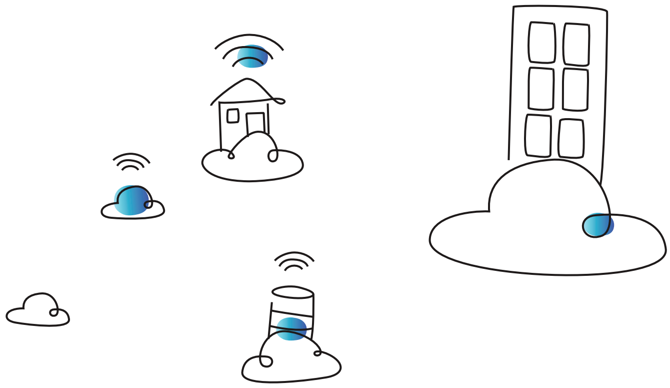
Additional respondents discussed **visibility into legacy solutions.** They stated that around 30 percent of their time is spent looking into 20 different dashboards. Finding cloud providers they never heard of was manual and boring work that was challenging to automate.

Other respondents suggested that their best ROI was achieved through **highly strategic projects** that involved embedding security teams in development teams. This approach allowed them to front-load security efforts and "shift-left" in the development process.

An additional high-ROI process mentioned is team building and training. CISOs who invest in continuously growing their team's knowledge and building a positive team culture are able to cultivate more skilled and efficient teams.

Creativity

One survey respondent asked the question of how to **gain more control over developers** without impeding them and their creativity? Typically, IT policies are implemented to limit risky behavior, such as downloading and installing new software or accessing cloud services.[26] While these restrictions can prevent malware, they also impose limitations on developers' creative freedom, hinder innovation, and reduce efficiency if developers are prohibited from adopting open source or third-party code. In addition, improved developer experience is a driving factor in attracting and retaining talent.[27] CISOs are often viewed as hindering creativity in the name of security. However, CISOs can promote creativity while maintaining security by utilizing developer sandboxes on virtual machines. These sandboxes restrict access to host operating systems, allowing developers to experiment with open source tools without compromising the organization's overall security posture.[28] This question aligns with our firm belief that cybersecurity is not limited to a gatekeeper role that solely imposes boundaries on employees, but rather a crucial business enabler that empowers teams to achieve their objectives securely.



Personal Questions

Personal issues and stress emerged as a primary category of questions posed by survey respondents, which is consistent with reports of burnout associated with the CISO role. A 2023 Gartner CISO survey found that 71 percent of respondents reported stress as the most significant personal risk they face, and 54 percent reported burnout.[29] Predictions indicate that approximately 50 percent of cybersecurity leaders will change jobs by 2024, with 25 percent citing work-related stressors as the primary reason for seeking new opportunities.[30] They assert that work-related stressors including psychological pressure, staff shortages, and budgetary constraints may contribute to essential employees leaving the field.[31]

For these reasons, we selected "personal and professional resilience" as the theme for the 2023 Team8 CISO Village TLV Summit. Addressing the personal aspects of being a CISO, including insights and strategies to avoid burnout and cultivate personal resilience, is essential for ensuring the success and overall well-being of cybersecurity leaders.

> **It’s very clear that Fighting today's cybersecurity threats requires a village, but anticipating and preparing for tomorrow's disruptive challenges requires the magic of Team8's CISO Village"**
>
> **Paul Branley,** CISO, TSB Bank

Survey **Respondent Information**

In addition to cybersecurity-related insights, this report also presents findings from the analysis of general information about the participating CISOs' companies and teams. Analyzing the aggregated data revealed the following findings:

The majority of CISO survey respondents report **hybrid cloud deployment** status and are in the process of transitioning more fully to the cloud.

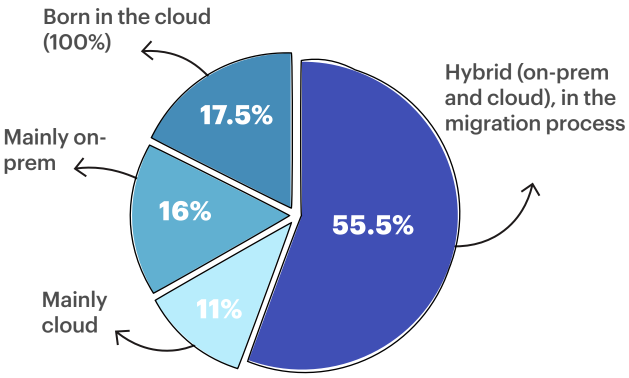
Approximately 50 percent of survey respondents reported having a cybersecurity department with **over 50 employees.** Among the companies with zero to 50 employees, over 60 percent reported experiencing budget increases. Around 27 percent of respondents manage departments with 50 to 250 employees, while 22 percent manage departments with over 251 employees.

In addition, the majority of CISOs come from either **technology or financial service industries.** Among companies with 251-500+ employees, approximately 38 percent are in technology, 25 percent in industrial and manufacturing, and 12.5 percent in financial services.

7.1 Survey Responded Cloud Deployment Status

A 2022 Mckinsey study found that only a small number of surveyed companies currently host more than half of their applications on public cloud platforms.[32] Most survey respondents report a hybrid state of cloud adoption where they have some data on-prem and in the cloud and are currently in the migration process to the cloud. However, a significant majority of companies anticipate having more than half of their applications in the public cloud within three years.[33]

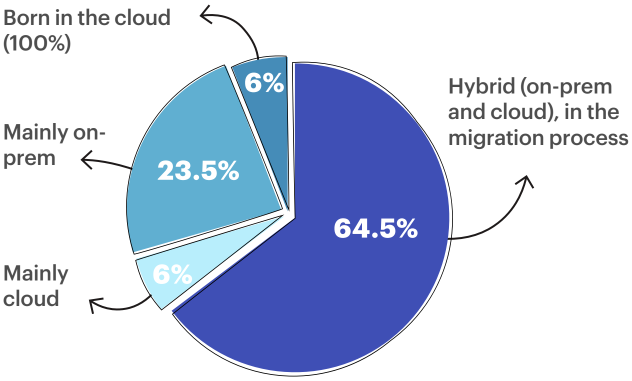
Cloud Deployment Status



Cloud deployment by industry

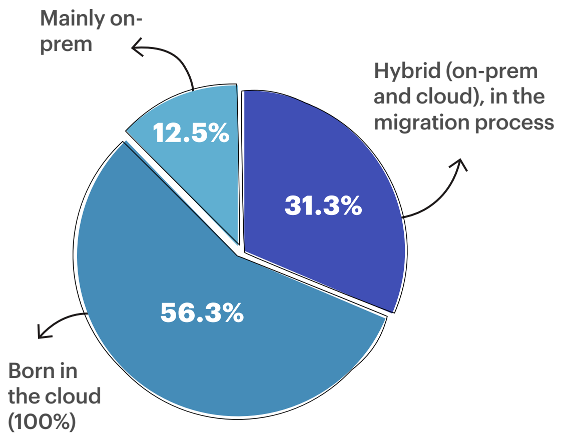
Nearly 65 percent of the surveyed CISOs who work in the financial services sector report adopting a hybrid approach, with only about 12 percent stating that they are primarily or fully in the cloud. The relatively low cloud adoption in the financial services industry leaves significant potential for greater cloud impact, particularly in improving IT resilience through increased cloud adoption.[34]

Financial Services



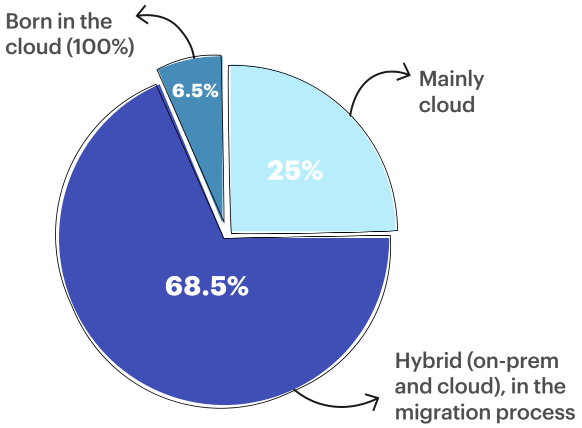
There is a notable contrast in the **technology sector**, as 60 percent of CISOs at technology companies report complete adoption of cloud technology, 33 percent report hybrid adoption, and only 7 percent primarily rely on on-premises solutions. Technology and software companies have made significant progress in adopting cloud technologies and now face the challenge of finding ways to benefit from the enormous scale of their cloud capabilities.[35]

Technology



The power and natural gas industry shows a preference for on-premise computing, resulting in a slower motivation for cloud migration.[36] However, our survey indicates that the industrial and manufacturing industry demonstrates high levels of adoption, with only 6.3 percent of respondents reporting a primarily on-prem approach.

Energy, Industrial & Manufacturing



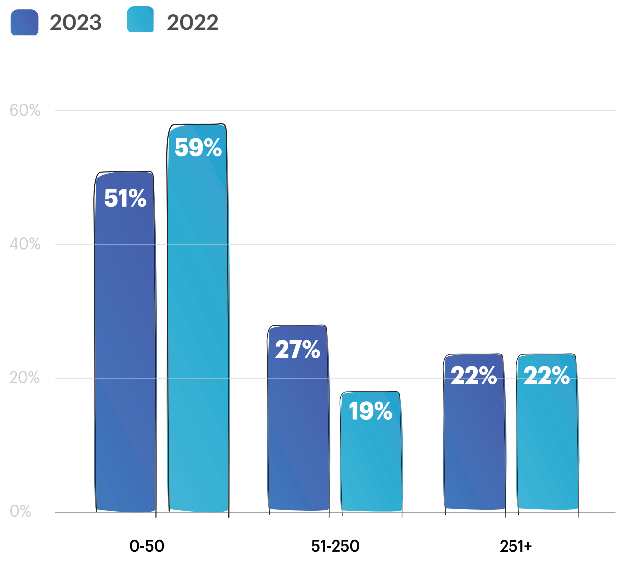
7.2 Cybersecurity Department Size

In 2023, the percentage of teams with 0-50 employees decreased from 59 percent in 2022 to 50.8 percent.

The percentage of departments with 251-500+ employees remained stable, yet there was an increase in teams with 50-250 employees, rising from 18.8 percent in 2022 to 27 percent.

Our results suggest potential growth in the size of cybersecurity teams, aligning with the broader trend of a growing cybersecurity workforce. Despite tech firms undergoing layoffs, cybersecurity teams have continued to hire, indicating a sustained demand for cybersecurity employees. The growth in cybersecurity team sizes is expected to continue. The U.S. Bureau of Labor Statistics predicts a significant growth rate of 35 percent for Information Security Analysts between 2021 and 2031, far surpassing the average growth rate for all occupations in the U.S.[37]

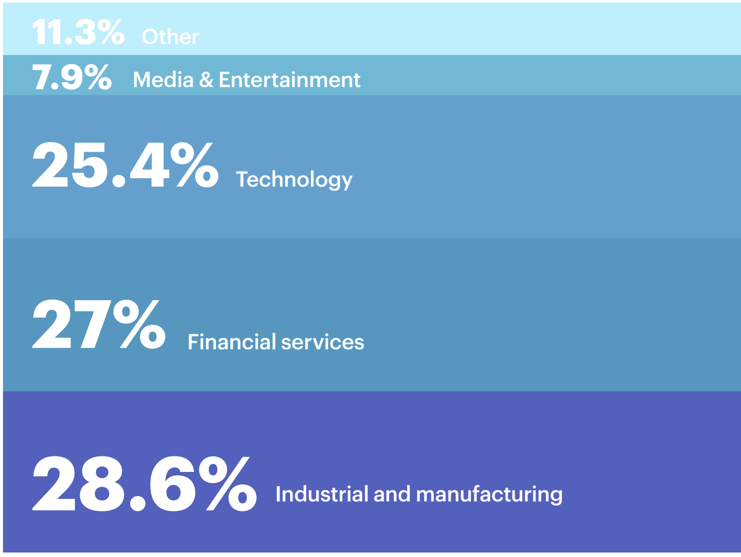
Cybersecurity department's employee headcount



7.3 Industry

Most of the surveyed CISOs work in either financial services, the industrial and manufacturing sector, or technology. Only about eight percent state that they work in media and entertainment, and around three percent work in health and pharma.

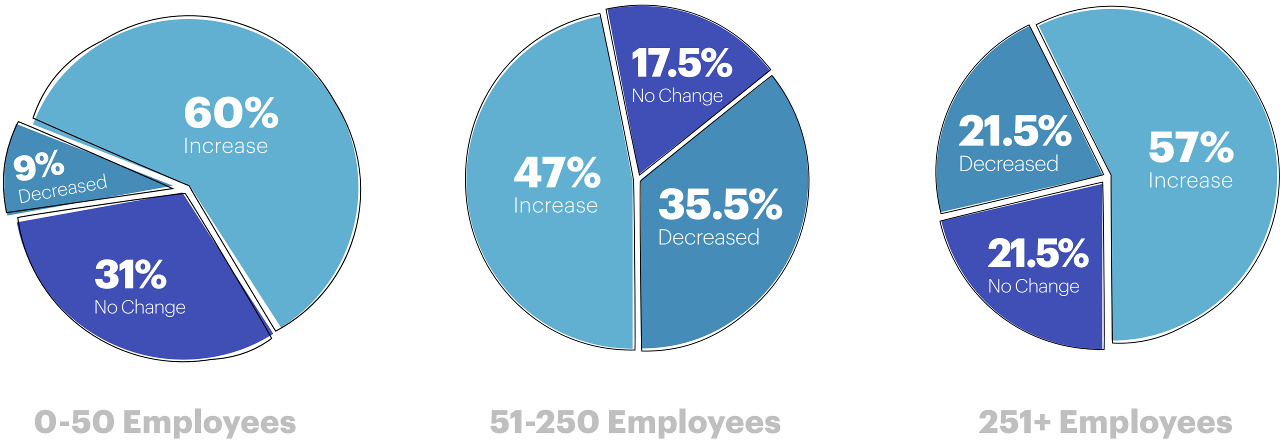
Industry



Appendix: **Budget**

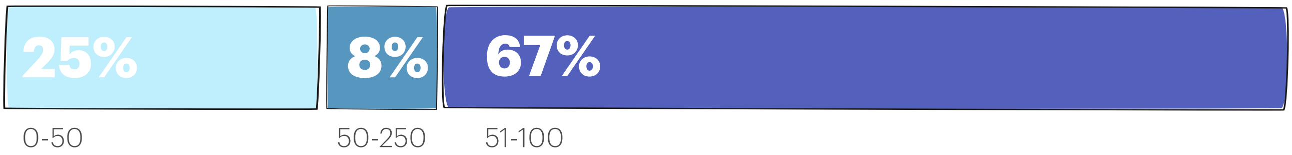
A. Budget change by CISO organization size (no. of employees)

Our survey results show that departments with 0-50 employees experienced the greatest percentage of the increases, with almost 60 percent of CISOs reporting that the budget increased and only 9 percent reporting budget decreases. Approximately 57 percent of companies with 251-500+ employees also reported budget increases, and only 21 percent reported decreases.



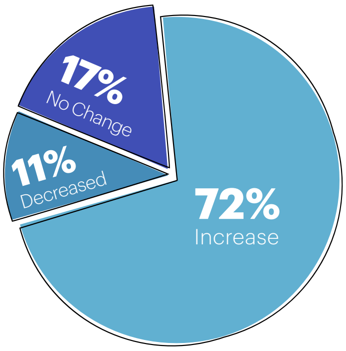
B. Budget decrease by CISO organization size (no. of employees)

Larger security departments were most affected by budget decreases, With 42 percent of organizations with security departments of 101-250 employees reporting budget decrees. Additionally, 25 percent of organizations with security departments of 251-500+ employees faced decreases.

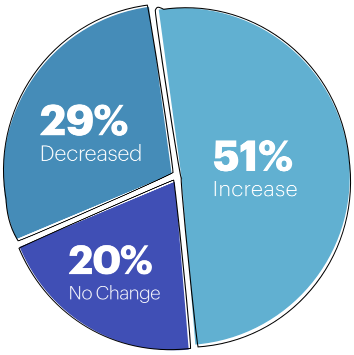


C. Budget change by cloud adoption

Our survey results find that organizations with higher levels of cloud adoption experienced more budget increases. For example, 72 percent of CISOs that report 100 percent cloud adoption and 51 percent of organizations with hybrid cloud status experienced budget increases. In contrast, 40 percent of organizations with on-prem infrastructure had budget increases, while the rest experienced no change in their budget.



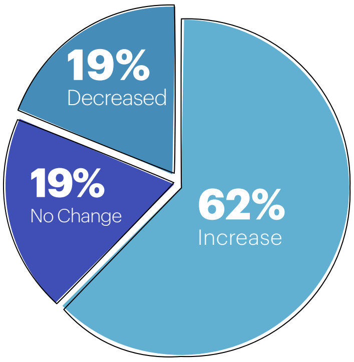
Born in the cloud/ mainly cloud



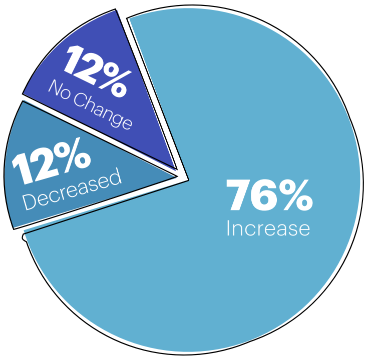
Hybrid

D. Budget change by Industry

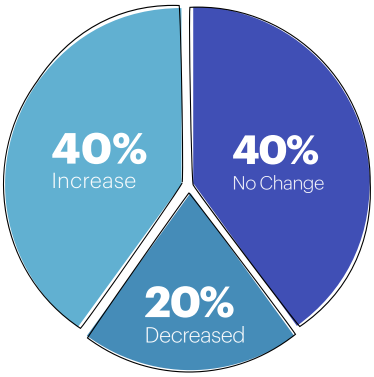
Around 62 percent of CISOs who operate in the technology domain reported budget increases. Around 76 percent of CISOs from industrial, manufacturing, mobility and energy domains also reported budget increases. However, in media, gaming, and telco companies, the percentage of organizations that experienced an increase was almost the same as the percentage of organizations that had no change in their budget.



Technology



Industrial, Manufacturing, Mobility & Energy



Media, Gaming & Telco

Endnotes

1. Quick Answer: How to Responsibly Defend Cybersecurity's Budget During Economic Headwinds, William Candrick and Richard Addiscott, Gartner, 2023
2. New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers, Bharath Aiyer, Jeffrey Caso, Peter Russell, and March Sorel, McKinsey, 2022
3. Quick Answer: How to Responsibly Defend Cybersecurity's Budget During Economic Headwinds, William Candrick and Richard Addiscott, Gartner, 2023
4. Quick Answer: How to Responsibly Defend Cybersecurity's Budget During Economic Headwinds, William Candrick and Richard Addiscott, Gartner, 2023
5. Quick Answer: How to Responsibly Defend Cybersecurity's Budget During Economic Headwinds, William Candrick and Richard Addiscott, Gartner, 2023
6. Surveyed CISOs could select 1-2 budget lines
7. Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences, Gartner, 2021
8. The Evolution of Data Security Solutions, Dan Benjamin, Cybersecurity Insiders
9. The Evolution of Data Security Solutions, Dan Benjamin, Cybersecurity Insiders
10. The Evolution of Data Security Solutions, Dan Benjamin, Cybersecurity Insiders
11. In this question, the surveyed CISO could select multiple options from a list
12. Gartner Identifies Three Factors Influencing Growth in Security Spending, Gartner, 2022
13. Market Guide for Third-Party Risk Management Solutions, Luke Ellery, Joanne Spencer, Christopher Ambrose, Cian Curtin, Koray Kose, Nicholas Sworek, and Zack Hutto, Gartner, 2022
14. Market Guide for Third-Party Risk Management Solutions, Luke Ellery, Joanne Spencer, Christopher Ambrose, Cian Curtin, Koray Kose, Nicholas Sworek, and Zack Hutto, Gartner, 2022
15. AI Models under Attack; Conventional Controls are not Enough, Avivah Litan, Gartner 2022
16. https://www.nuspire.com/resources/second-annual-ciso-research-report-on-challenges-and-buying-trends-a-focus-on-optimization/
17. Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, Deepti Gopal, Leigh McMullen, Andrew Walls, Richard Addiscott, Paul Furtado, Craig Porter, Oscar Isaka, and Charlie Winckless, Gartner, 2022
18. Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, Deepti Gopal, Leigh McMullen, Andrew Walls, Richard Addiscott, Paul Furtado, Craig Porter, Oscar Isaka, and Charlie Winckless, Gartner, 2023
19. Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, Deepti Gopal, Leigh McMullen, Andrew Walls, Richard Addiscott, Paul Furtado, Craig Porter, Oscar Isaka, and Charlie Winckless, Gartner, 2022
20. Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, Deepti Gopal, Leigh McMullen, Andrew Walls, Richard Addiscott, Paul Furtado, Craig Porter, Oscar Isaka, and Charlie Winckless, Gartner, 2022
21. Hype Cycle for Security Operations 2022, Andrew Davies, Gartner, 2022
22. Market Guide for Infrastructure Monitoring Tools, Pankaj Prasad, Matt Crossley,and Mrudula Bangera, Gartner, 2022
23. Market Guide for Infrastructure Monitoring Tools, Pankaj Prasad, Matt Crossley,and Mrudula Bangera, Gartner, 2022
24. Maverick Research: Risk Management Produces Bad Cybersecurity, Andrew Walls, Leigh McMullen, Jay Heiser, and Deepti Gopal, Gartner, 2023
25. Innovation Insight: Cybersecurity Continuous Control Monitoring,
26. The Evolving CISO: From Naysayer to Enabler, Charles Blauner, 2021
27. Innovation Insight for Internal Developer Portals, Manjunath Bhat, Mark O'Neill, and Oleksandr Matvitskyy, Gartner, 2022
28. The Evolving CISO: From Naysayer to Enabler, Charles Blauner, 2021
29. 2022 Global Chief Information Security Officer (CISO) Survey, Matt Aiello, Scott Thompson, Max Randria, Camilla Reventlow, Guy Shaul, and Adam Vaughan, Heidrick, 2022
30. Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, Deepti Gopal, Leigh McMullen, Andrew Walls, Richard Addiscott, Paul Furtado, Craig Porter, Oscar Isaka, and Charlie Winckless, Gartner, 2022
31. Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, Deepti Gopal, Leigh McMullen, Andrew Walls, Richard Addiscott, Paul Furtado, Craig Porter, Oscar Isaka, and Charlie Winckless, Gartner, 2022
32. Five learnings from CTOs and tech leaders on their cloud strategies, Brendan Campbell, Mark Gu, Venkatesh L, and Kaavini Takkar, McKinsey Digital, 2023
33. Five learnings from CTOs and tech leaders on their cloud strategies, Brendan Campbell, Mark Gu, Venkatesh L, and Kaavini Takkar, McKinsey Digital, 2023
34. Projecting the global value of cloud: $3 trillion is up for grabs for companies that go beyond adoption, McKinsey, 2022
35. Projecting the global value of cloud: $3 trillion is up for grabs for companies that go beyond adoption, McKinsey, 2022
36. Projecting the global value of cloud: $3 trillion is up for grabs for companies that go beyond adoption, McKinsey, 2022
37. Information Security Analysts, U.S. Bureau of Labor Statistics, 2022