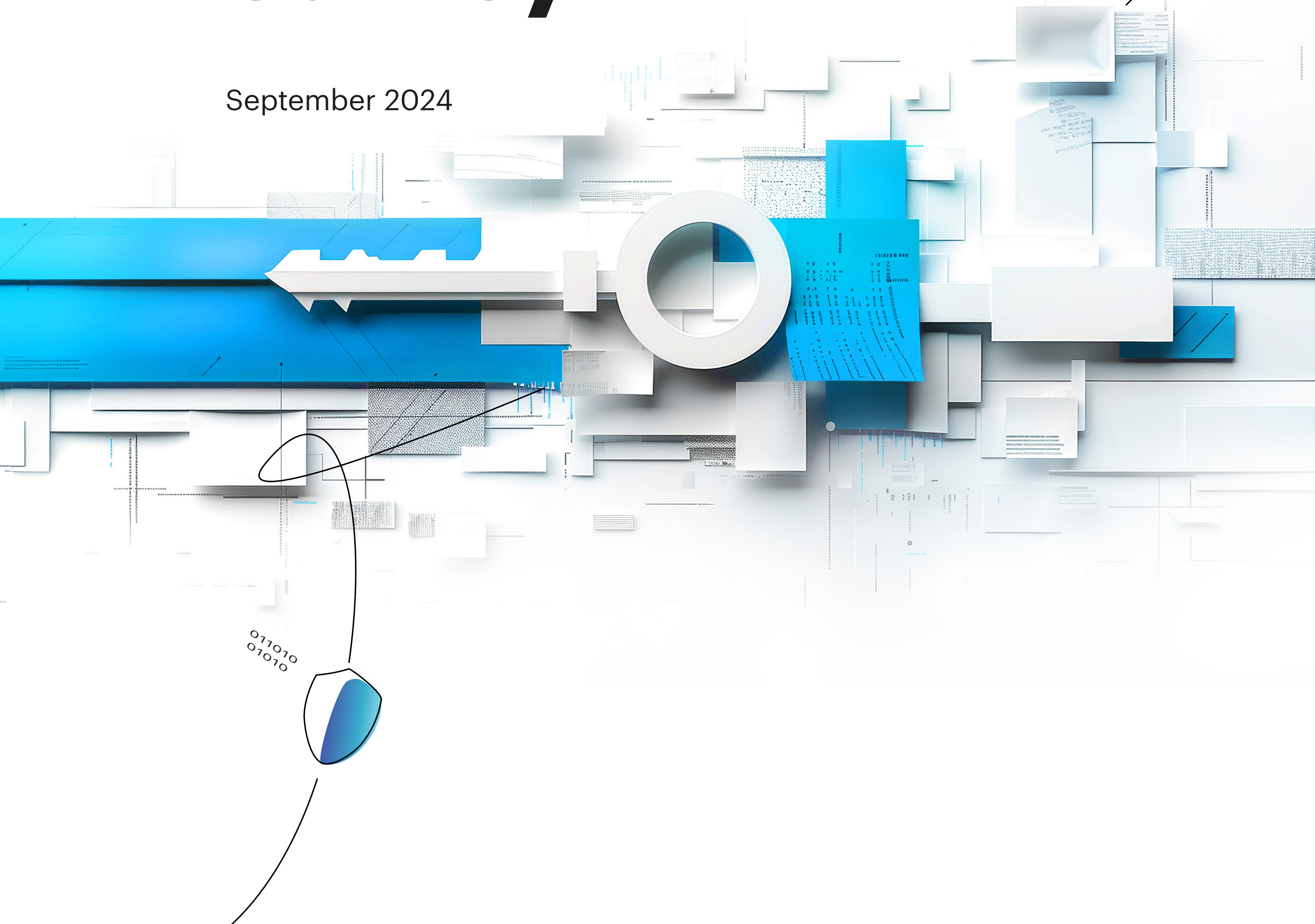
THE PULSE ON CYBERSECURITY

Key Findings from Team8's 2024 **CISO Village Survey**

September 2024



WRITTEN BY

Amir Zilberstein
Managing Partner,
Team8

Bobi Gilburd
Chief Innovation Officer,
Team8

Noa Hen
Strategy and Business
Operations Manager, Team8

Eidan Siniver
CTO, Team8

Kalman Heims
Strategy Manager,
Team8

Tal Blaustein
Business Research Intern,
Team8

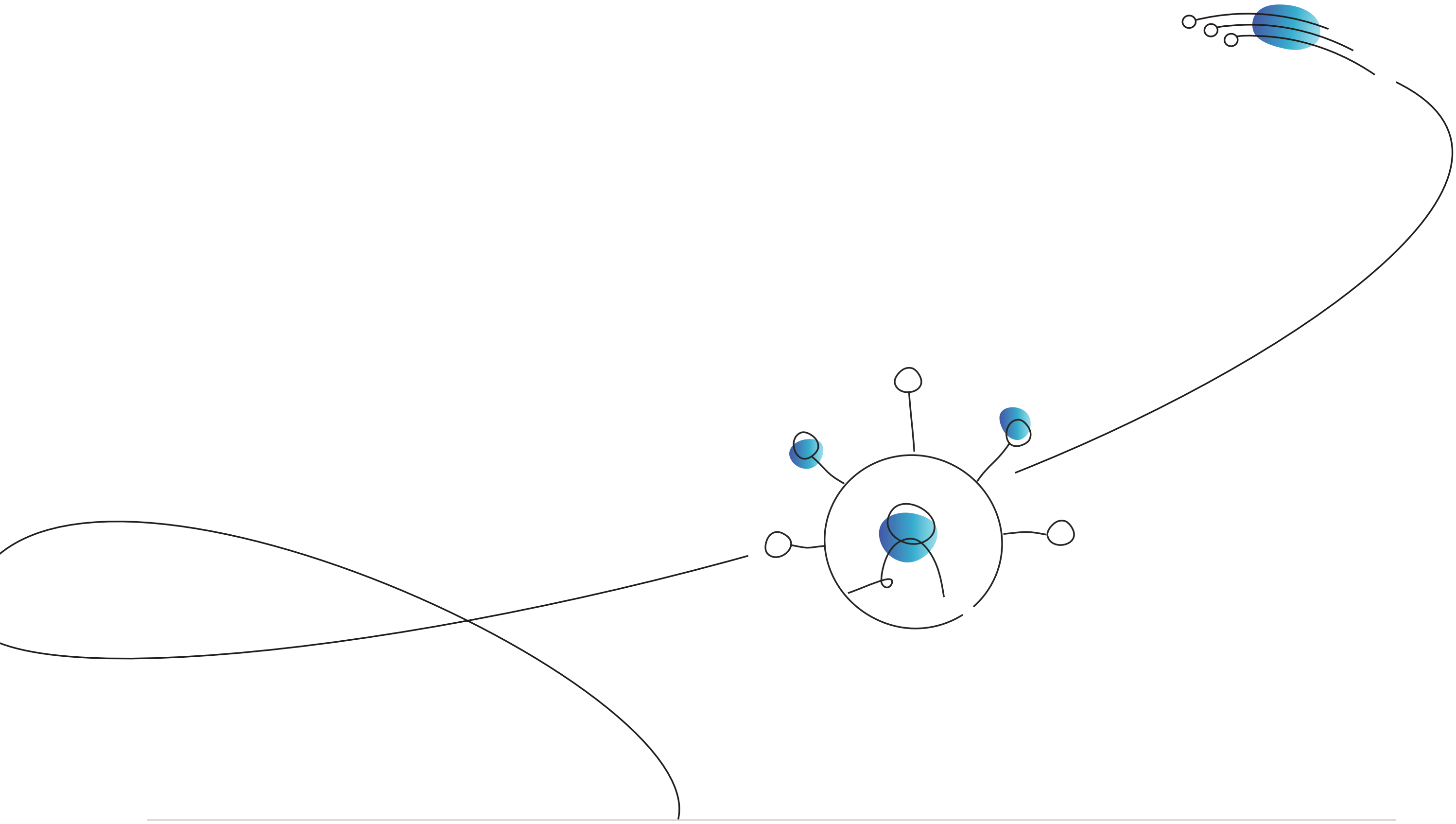
The Team8 CISO Village is a community of CISOs from the world’s leading enterprises. The primary focus of the Village is to facilitate collaboration among the world’s most prominent companies with the goal of sharing information and ideas, conducting intimate discussions on industry and technology trends 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

As geopolitical tensions soar and AI technology transforms our world, CISOs face unprecedented complexity. At the 2024 CISO Village Summit in California, themed "Secure by Nature," over 100 top cybersecurity leaders, including Fortune 500 execs, gathered to confront these challenges head-on. We conducted the 2024 CISO Village Survey to uncover the latest trends and insights. On the summit's final day, CISOs dissected the findings, sharing actionable strategies to fortify security.

Dive into our report to explore the cutting-edge survey results and exclusive data from the 2024 survey, designed to empower and elevate the entire cybersecurity community.

Key Takeaways

Amidst a rapidly changing threat landscape and heightened regulatory pressures, the report presents the critical trends, major challenges, and strategic imperatives shaping the future of cybersecurity.

Record budgets are being allocated to cybersecurity to secure critical technology investments amidst a stricter regulatory environment.

- **>70% of CISOs reported increases in their cybersecurity budgets** in 2024 - even more than in 2023.
- The verticals that demonstrated budget increases the most were financial services, technology and industrial/manufacturing, where over 55% of companies reported a significant budget increase in 2024.

While 70% of CISOs view AI as a major threat, 85% view it as an opportunity for defenders.

- **Sophisticated phishing attacks and deep-fakes** are viewed as the most critical AI-powered threats to organizational security.
- When it comes to defending AI systems, CISOs prioritize vulnerability management in AI development lifecycles, and data privacy for 3rd party AI systems.

Data Security and third party risk management are top of mind for cybersecurity executives

- Concerns over sensitive data leaking into AI models, combined with the proliferation of data from cloud migration and remote work, are heightening the focus on comprehensive and effective data security programs.
- The need for trusted enterprise-vendor exchanges is fueling interest in innovative TPRM solutions.

Cybersecurity regulations are becoming more stringent, placing greater compliance burdens on organizations and their security teams.

- CISOs are **facing increased personal liability** for security breaches, which is taking a toll on their personal well-being and job satisfaction.
- CISOs report **increased scrutiny from senior management**, requiring more frequent and detailed reporting on security postures and incident responses.

01

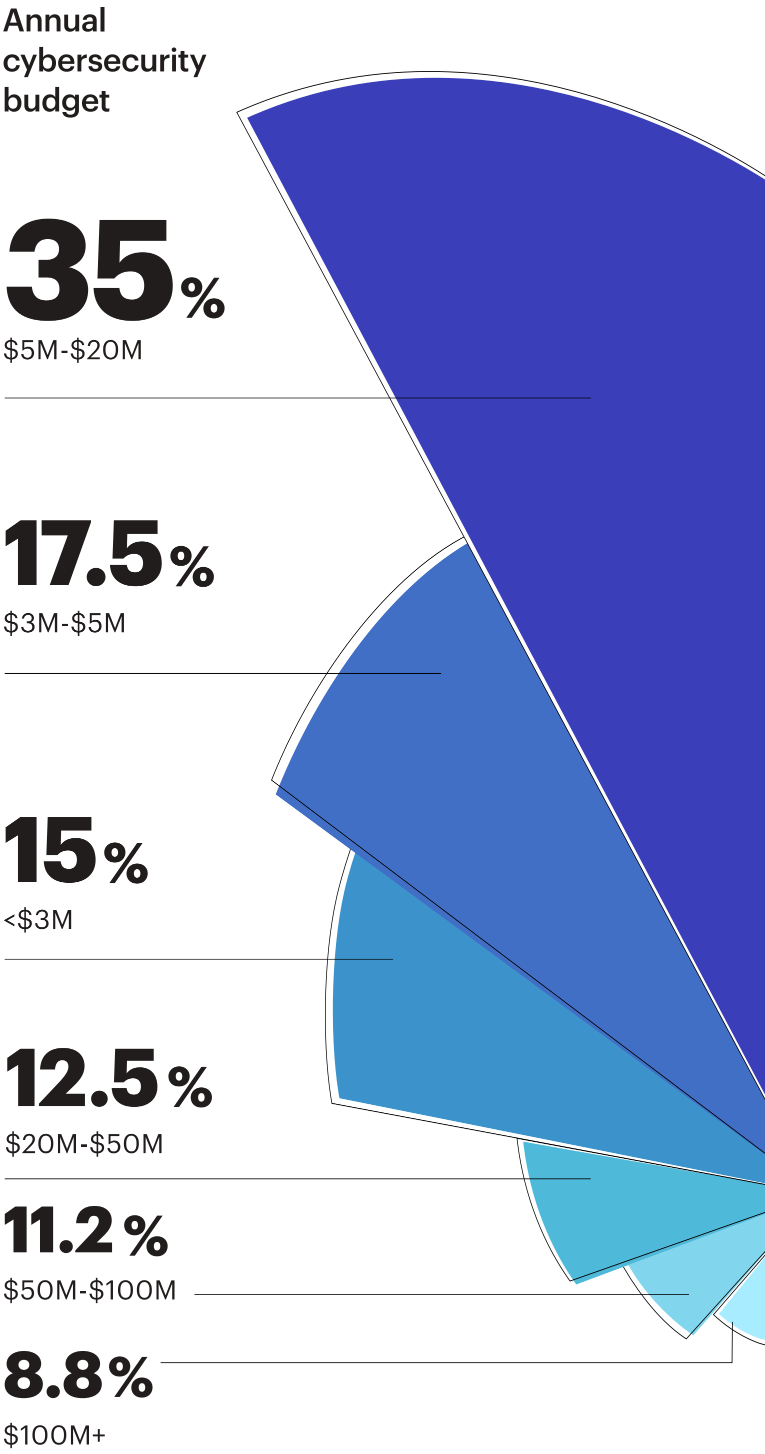
Security Budgets

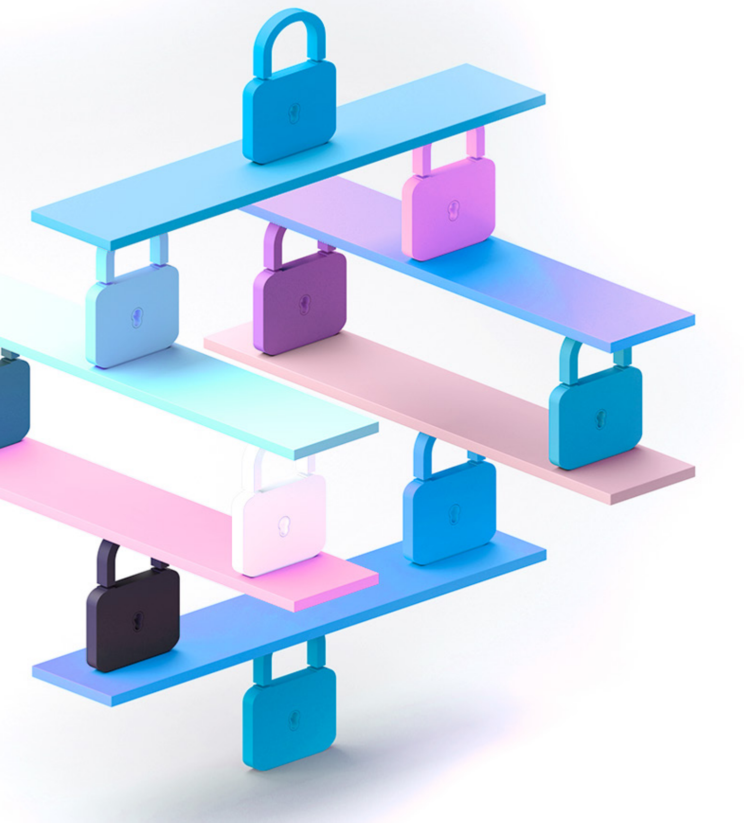
Benchmark: Budget ranges

The allocation of budgets within cybersecurity departments serves as a critical indicator of organizational priorities and preparedness against emerging threats. Understanding how different companies distribute resources sheds light on their strategic approach to safeguarding digital assets.

In 2024, the vast majority of survey respondents reported their team's budget to be under 20 million USD, with the largest share falling within the 5 to 20 million USD range.

The majority of companies with over 20 cybersecurity employees have an annual budget exceeding $5 million. Among companies with fewer than 20 cybersecurity employees, around 40 percent reported a cybersecurity department budget ranging from $3 million to $5 million, while a third reported a budget exceeding $5 million (Appendix 1).





Most CISOs report budget growth

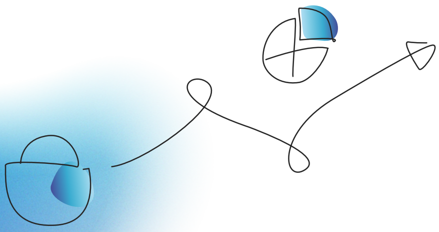
70% of respondents reported an increase in their cybersecurity budget for 2024, surpassing last year's total of surveyed organizations that increased spending. This is supported by a Gartner report projecting that global spending on security and risk management will reach $215 billion in 2024, a 14.3% increase from 2023.[1]

Several trends are driving this increase in cybersecurity budgets across all industries and companies of all sizes. First, the tightening regulatory burden on CISOs has garnered greater board attention, leading to increased budget allocations. Unlike other areas, cybersecurity budgets are more resilient to corporate budget cuts driven by economic pressures. For cybersecurity leaders, it is essential to proactively demonstrate how these budget allocations fortify defenses against evolving cyber threats and align with the organization's strategic business objectives.

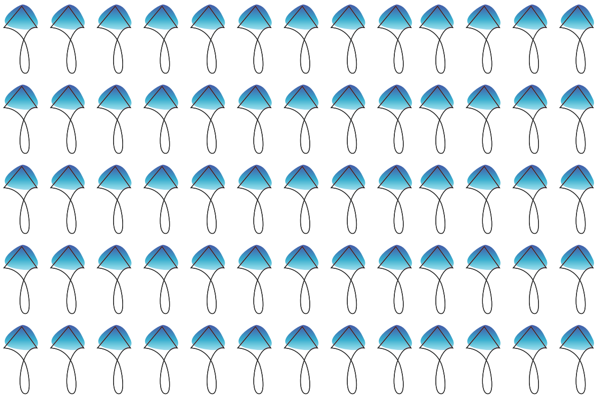
Second, AI is being leveraged by attackers to increase the velocity of attacks, creating a more challenging security landscape. Simultaneously, CISOs are being pushed by boards to incorporate advanced controls into their security stack to better defend against these threats. This dual pressure requires significant spending on infrastructure and tooling. As enterprise AI adoption rises, concerns grow about the effectiveness of current security frameworks in addressing evolving threats and data breaches. Looking ahead to 2025, Gartner predicts that the adoption of generative AI will significantly increase cybersecurity resource requirements, driving more than a 15% incremental spend on application and data security.[2]

Third, geopolitical shifts, such as the Russia-Ukraine conflict, the China-US trade war, and ongoing tensions in the Middle East, have heightened the threat from nation-state actors. This has prompted critical infrastructure players to implement tighter security measures.

Data from the survey respondents indicates a discrepancy in budget growth across industries, for the details see Appendix item 2.



70%
Increased
vs. 53% last year



15%
No Change
vs. 24% last year

15%
Decreased
vs. 22% last year

Smaller organizations saw budget decreases

Among surveyed CISOs, 14% reported budget cuts, down from 22% in 2023. The majority of these reductions occurred in companies with cybersecurity budgets under $20 million and security teams with fewer than 100 employees. It's safe to assume that enterprises with smaller budgets are more exposed to economic pressures and uncertainty due to macroeconomic conditions. As a result, they are prioritizing getting the most value from their current vendors before considering new ones.

02

Compliance and Liability

On July 12, 2024, AT&T announced in an SEC filing that hackers had stolen six months' worth of mobile phone customer data, revealing a massive breach with potential national security implications.

This breach, similar to the recent Ticketmaster incident, has been attributed to poor security practices in the Snowflake cloud storage accounts used by the companies (e.g., lack of MFA, or network allow lists). These high-profile, snowballing events are expected to increase pressure and scrutiny on CISOs. As organizations face increasingly aggressive attacks and a more complex regulatory landscape, CISOs must develop new strategies to protect their organizations while addressing the demands of various stakeholders and compliance issues.

> *As Group CISO, I view the evolving regulatory landscape as an opportunity for growth, resilience and responsible innovation. While the increased personal liability for breaches and intensified scrutiny from senior management can feel daunting, I believe they push us to elevate our game and strengthen our security postures. I'm excited about the potential for innovation in data security and third-party risk management (TPRM). With rising threats like phishing and deepfakes on the rise, we can implement solutions that protect sensitive data and build trust with our stakeholders.*
>
> **Alvaro Garrido,** Interim Group Chief Information Officer (CIO)
>
> standard chartered

2024: More regulation is introduced

In today's cybersecurity arena, regulatory frameworks have undergone significant evolution, creating a complex maze of compliance requirements for CISOs. Governments and regulatory bodies are increasingly enforcing stricter governance on cybersecurity, privacy, and data localization to protect sensitive information and promote transparency.

In 2024, several of these cybersecurity regulations are finally coming into effect, placing new demands on public and private organizations. This includes the new FTC Standards for Safeguarding Customer Information which have taken effect in May[3]; the new SEC breach disclosure rules effective from June; the EU AI Act, effective August 2024; the expanded NIS2 Directive effective October, and the newly formed Digital Operational Resilience Act (DORA), applied from January 2025.

Additionally, the U.S. Supreme Court's recent decision to overturn the Chevron doctrine may significantly affect the cybersecurity sector. The doctrine previously allowed courts to defer to federal agencies' expertise in interpreting ambiguous statutes. This may cause an increase in legal challenges to various agency cybersecurity requirements, such as incident reporting mandates and regulations for critical infrastructure sectors.[4]

Compliance with these regulations has become essential, introducing a new array of legal, financial, and reputational repercussions. This, in turn, intensifies board scrutiny on cybersecurity, driving CISOs to adopt comprehensive strategies that not only meet regulatory standards but also bolster the overall cybersecurity posture.

CISOs are under increased scrutiny by boards

The scrutiny CISOs face from senior management and the board of directors plays a pivotal role in shaping organizational cybersecurity strategies.

As regulations evolve and impose stricter requirements on data protection and cybersecurity practices, the level of scrutiny on CISOs intensifies. This scrutiny encompasses a range of factors, from compliance with regulatory standards to the effectiveness of cybersecurity measures.

The majority of survey respondents (54%) admitted that they are experiencing significantly tighter scrutiny by senior management and the board of directors, with an additional 30% experiencing more moderate oversight.

More CISOs feel personally impacted

As the role of the CISO grows more complex, the personal implications are becoming increasingly concerning. CISOs must not only enhance their organizations' security posture while meeting greater C-level and board demands, but they often also do so under a severe talent shortage and growing personal stakes.

Real-life examples, such as the SEC's charges against SolarWinds and its CISO[5], as well as the conviction of Uber's former CISO, Joe Sullivan, highlight the immense pressure and potential liability that CISOs are facing.

As a result, **over 54%** of survey respondents indicated that concerns about their liability in the event of a security breach have significantly affected their personal wellbeing.

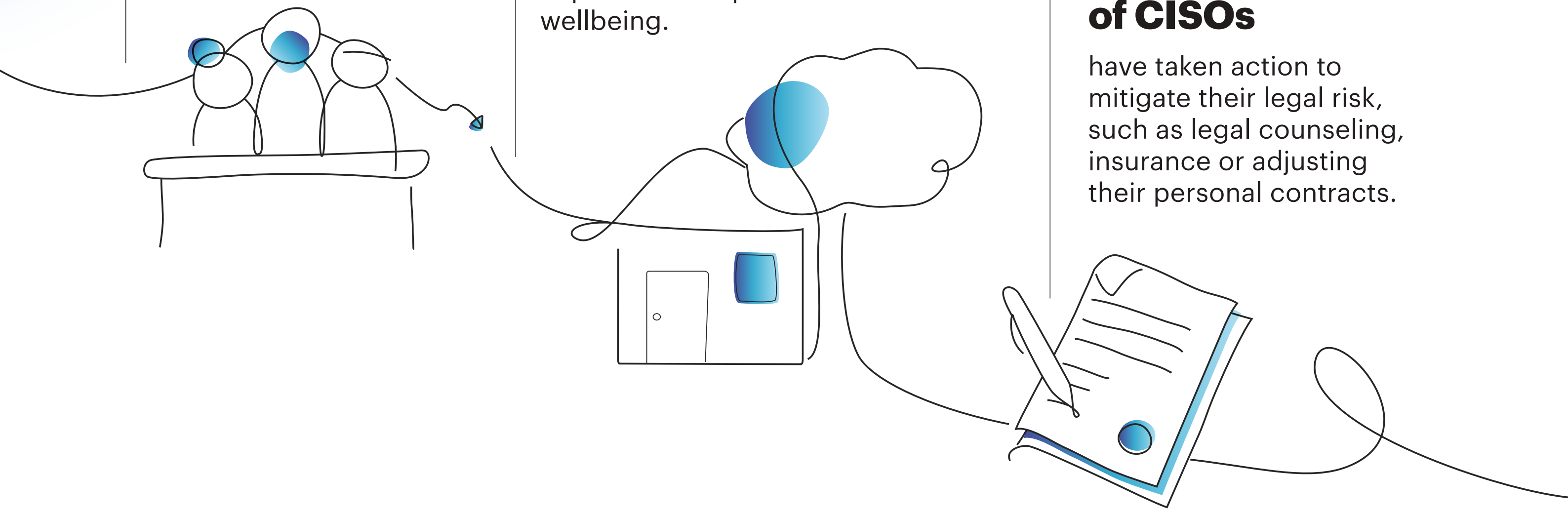
However, while CISOs currently bear the mental burden of their roles, they are slow to take action to secure their positions and reputations. **Only 32% of respondents** indicated they have taken proactive measures such as seeking legal counsel, purchasing liability insurance, or renegotiating contracts to protect themselves.

We anticipate that in the coming years, contract negotiation and liability insurance will become increasingly common as CISOs seek to mitigate personal liability risks.

54%
of CISOs
have experienced significantly tighter scrutiny by senior management and the board of directors.

>50%
of CISOs
report that concerns about their liability in case of a security breach have impacted their personal wellbeing.

only
32%
of CISOs
have taken action to mitigate their legal risk, such as legal counseling, insurance or adjusting their personal contracts.



03

AI

The rise of AI is transforming cybersecurity by enhancing defensive capabilities while also posing new challenges. As AI technologies become more sophisticated and accessible, they are being adopted by both cybersecurity professionals and malicious actors alike.

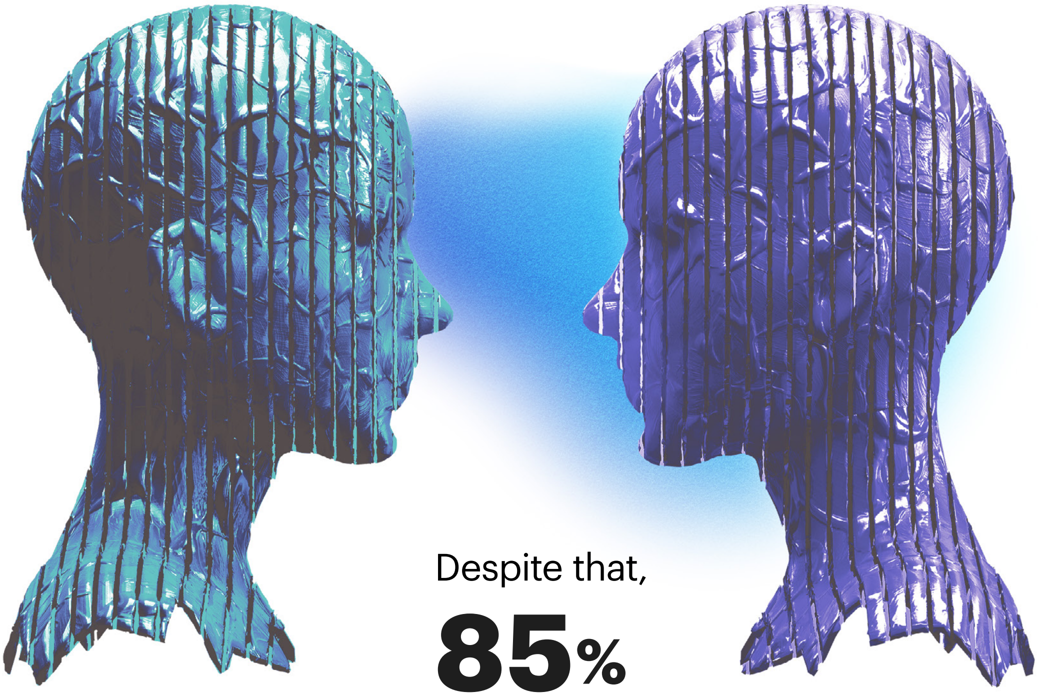
AI-powered tools are revolutionizing threat detection and response, enabling faster analysis of vast amounts of data and automating routine security tasks. However, this advancement also fuels the development of more complex cyber threats, such as AI-generated phishing attacks and deep fakes, which can deceive traditional security measures and employees. At this year's CISO Summit, nearly 70% of respondents reported viewing AI as a major security threat, while nearly 85% consider it an enabler for security.

For instance, the $25 million fraud case involving the UK engineering group Arup illustrates this threat. In this incident, fraudsters used a deep fake version of a senior manager during a video conference to trick the company into transferring the funds.[7] This case underscores how AI can be weaponized to exploit human trust and bypass conventional security protocols.

As a result, there's a growing demand for specialized cybersecurity solutions that can effectively counter these AI-driven threats. Companies are heavily investing in AI-integrated security platforms and technologies to maintain an edge in the ongoing arms race between defenders and attackers in cyberspace. This evolution signifies a pivotal shift towards leveraging AI as a critical component in securing digital infrastructures against emerging risks.

70%

of CISOs view AI as a major security threat.



Despite that,

85%

of CISOs consider AI as a key enabler for security

Top risks from attackers leveraging AI

While AI is certainly being leveraged to enhanced security tools, a notable surge in AI-powered attacks has become a formidable challenge for CISO. Recent data highlights the severity of these threats, with Bessemer reporting a staggering 1,265% increase in malicious phishing emails and a 967% rise in credential phishing since Q4 2022.[7]

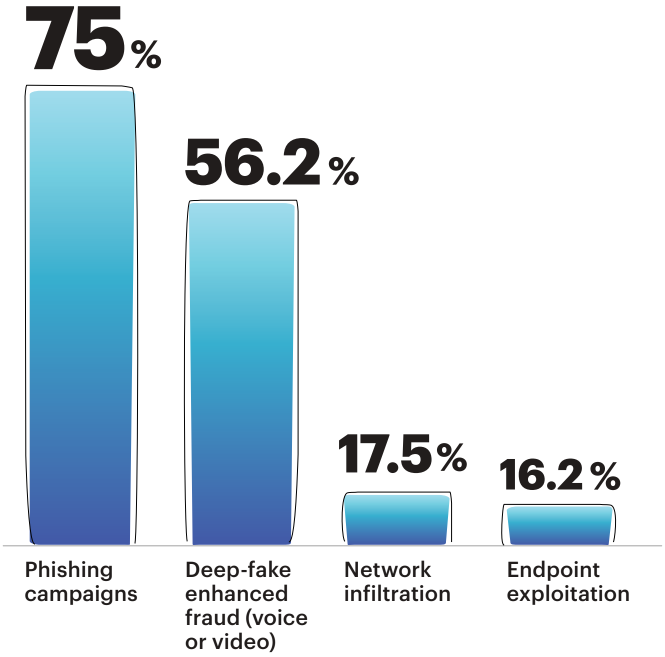
75% of respondents identify phishing as the most significant AI-powered threat to their organizations, highlighting its pervasive impact.

Additionally, 56% of respondents express concerns about deep fakes, which use AI to create convincing yet falsified media content, further complicating defense efforts.

These statistics emphasize the critical need for robust cybersecurity measures to counter AI-driven attacks and ensure resilience against emerging digital threats.

CISOs are increasingly pushed to adopt AI-powered tools to stay ahead of evolving threats, impacting all existing cybersecurity categories, including endpoint, cloud, network, and application security. The promise of GenAI-based automation in cybersecurity is especially potent given the immense skill shortage the industry is facing. AI is already beginning to augment human teams, aiming to accelerate detection, response and remediation efforts.

Which type of AI-powered attacks poses the biggest threat to your organization?



Challenges for defending AI

AI's impact on security teams goes beyond the cat and mouse chase of AI-based attacks and defenses. As enterprises adopt AI for critical business use-cases, AI models and development lifecycles are posing a new, novel attack surface, introducing a variety of security risks. Rapid adoption is forcing security teams to respond quickly and introduce robust safeguards and controls for AI systems. Survey respondents indicated top priorities for AI security solutions over the next two years (respondents were allowed to select a maximum of two categories).

In the next 1-2 years, do you expect to consider purchasing an AI security solution for any of the following purposes?

41.2%
Vulnerability management in AI development lifecycles

36.2%
Data privacy for 3rd party AI applications

32.5%
Shadow AI (discovery and mapping of AI usage)

28.8%
Only a platform combining several use-cases of the above

22.5%
Adversarial attacks against enterprise-owned AI applications

20%
Hallucinations, bias, copyright and other content liability issues

The top 3 risks ranked by CISOs include:

1. Vulnerability Management in AI Development Lifecycles

With the fast adoption of internally-built AI applications, such as fine-tuned models and RAG-based use-cases, companies must integrate robust vulnerability management practices from development to deployment. In order to ensure the security and reliability of AI systems, companies are primarily relying on a range of red teaming techniques to surface both known and emerging vulnerabilities. New solutions aim to automate the red teaming process through various scanning techniques across application code, models, notebooks, and datasets to detect vulnerabilities at different stages of the development process.

2. Data Privacy for 3rd Party AI Applications

As employees leverage 3rd party AI services for a variety of use-cases, from ChatGPT to Github copilot, CISOs are facing growing IP and data leakage risks. Proper access controls, and data leakage prevention solutions are in order, especially in light of regulatory requirements such as GDPR and CCPA.

3. Shadow AI (Discovery and Mapping of AI Usage)

Shadow AI refers to unauthorized AI deployed within organizations without IT or security department approval or oversight. As developers can import an open-source model with a few short lines of code, and business users can "chat" with a new copilot at the click of a button, detecting and mapping these instances is critical for CISOs and security teams to mitigate potential security and compliance risks. Investing in AI discovery solutions can help identify unauthorized deployments and assess their impact on security posture.

Naturally, amidst a skills shortage and record-breaking threat landscape, CISO teams are struggling to respond to such a fast-paced technology shift. Survey respondents reported that the top barrier to defending AI systems is the lack of expertise within existing security teams, who were not trained on generative AI and the new vulnerabilities it introduces. In light of the scarcity of security and AI talent, this is a particularly challenging problem.

Such expertise is especially important given the second biggest challenge in defending AI systems - the need to balance security with usability. As boards push enterprises to incorporate AI features in order to remain competitive, security teams cannot get away with stringent, boycott policies. Precision is needed, and precision requires true expertise. We expect a new ecosystem of advanced solutions to help security teams fill this gap in the coming years.

What are the biggest challenges your organization faces in defending AI systems?

57.5%

Lack of expertise

56.2%

Balancing security with usability

31.2%

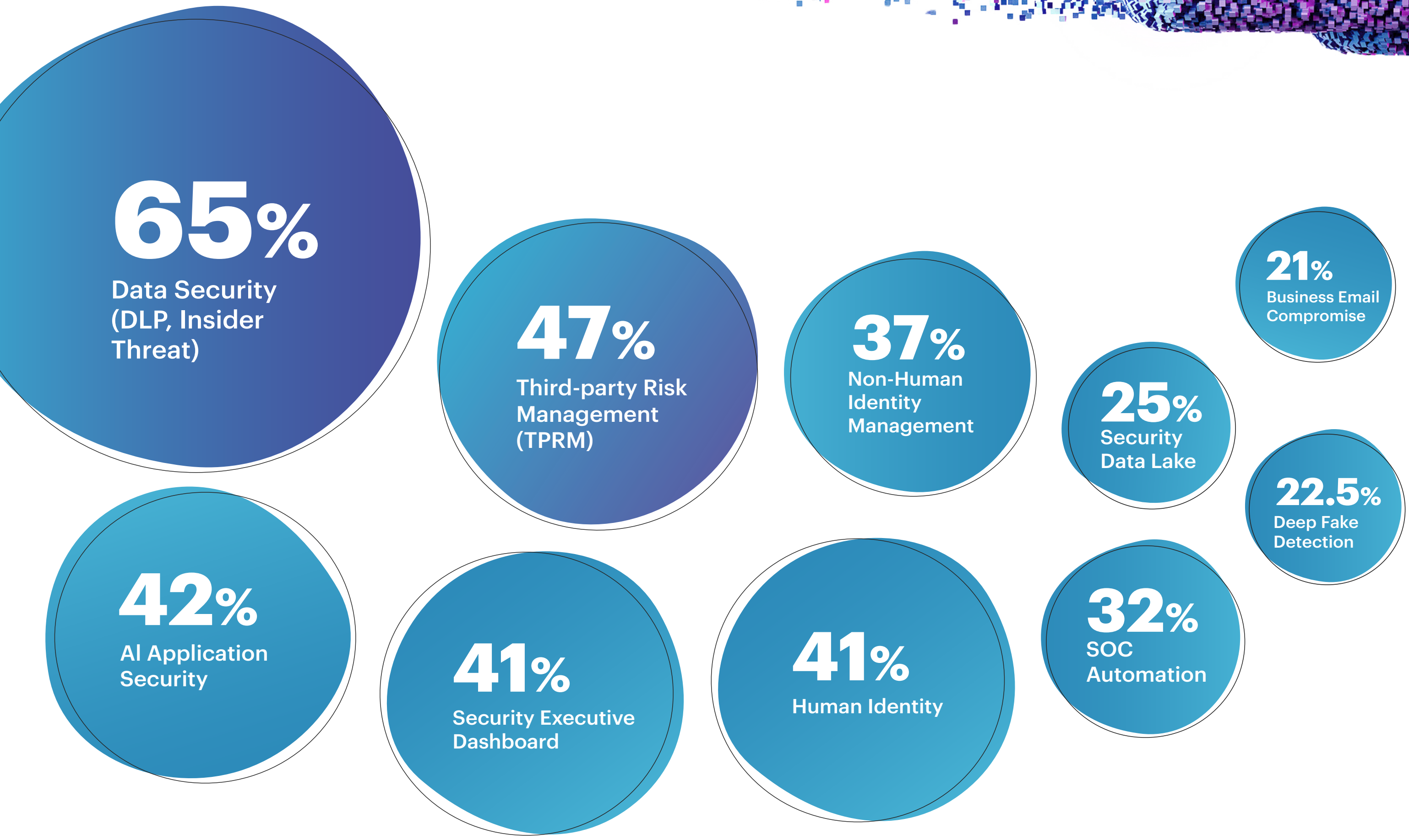
Regulatory uncertainty

04

2024 Top CISO Pain Points

Organizations face a range of cyber-security challenges, with survey respondents highlighting data security, third-party risk management, and AI security as the most pressing issues where current solutions fall short.

What are the most acute problems you face, where existing solutions are not meeting needs?



Data Security is the main pain point

Over the past decade, organizations have increasingly embraced cloud technology, resulting in an influx of vast and diverse types of new data. This shift has fundamentally transformed how businesses operate and manage their information. The adoption of cloud solutions has brought numerous benefits, such as scalability and flexibility, but it has also introduced new complexities and vulnerabilities.

Simultaneously, the rise of SaaS applications and the shift to remote work have eroded traditional data perimeters, making it more challenging to secure sensitive information. The adoption of AI further complicates this landscape, as it poses significant risks for sensitive data leakage. These developments underscore the need for robust data security frameworks.

Consequently, **65% of CISOs** surveyed identify data security, including data loss prevention (DLP) and insider threats, as the most pressing issue lacking adequate solutions. This trend aligns with ongoing concerns highlighted in Cisco's 2023 CISO Survival Guide, where 70% of CISOs prioritize DLP and Data Access.[8]

> *Data Security is a huge challenge because of the vast, diverse and ubiquitous set of use cases we handle; it is also a top priority that traditionally hasn't been optimally addressed by the market both from a security and a compliance perspective. New intelligent classification and labeling systems, comprehensive user and entity behavior analytics and simple ways to enable the use of huge datasets by AI systems in a secure manner could be part of the solution. Fostering AI to build these new solutions will be for sure part of the approach.*
>
> **David Corral,** Head of IT/OT Cybersecurity Architecture
>
> REPSOL

TPRM: A pain point for nearly 1 in every 2 CISOs

Third-Party Risk Management (TPRM) involves assessing and managing the risks associated with sharing data and granting system access to third parties. As enterprises increasingly integrate third-party services, from on-prem software to SaaS vendors, the demand for effective TPRM tools has grown significantly. According to a 2023 Deloitte report, **60% of organizations currently work with over 1,000 third parties**, a number expected to rise as business ecosystems expand and become more complex.

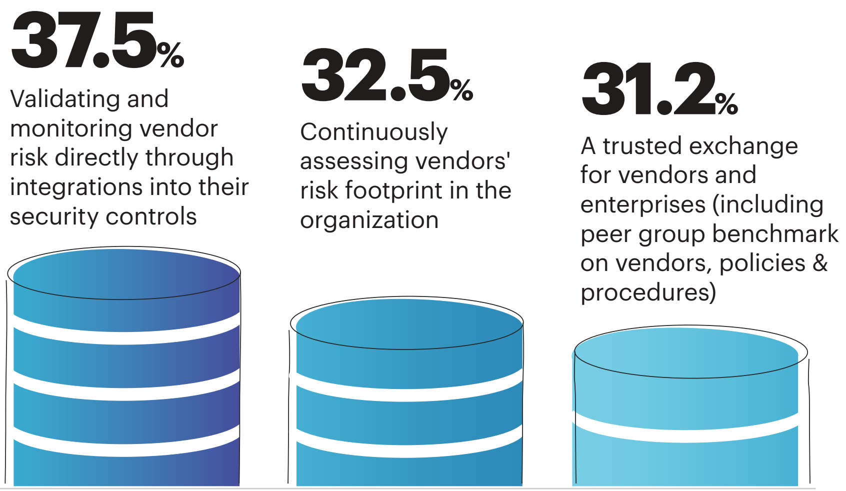
Accordingly, 47% percent of surveyed CISOs have identified TPRM as a critical pain point with insufficient current solutions. TPRM is increasingly crucial to enterprise security as organizations rely heavily on external vendors and partners.

Two new innovations are shaping the future of TPRM. First, the automation of TPRM workflows is streamlining processes, enhancing efficiency, and ensuring consistency in risk assessments and management. Second, there is a shift from mere compliance to proactive and ongoing security measures. This approach not only addresses current threats but also anticipates and mitigates future risks, thereby strengthening overall resilience and trustworthiness in organizational operations.

Accordingly, survey respondents have indicated that they would consider replacing their current TPRM solution given either a continuous monitoring solution, tracking vendor risk or vendor footprint in the organization, or a trusted exchange between enterprises and vendors.

The majority of respondents indicated that a trusted exchange for vendors and enterprises is important (40%) or highly important (38%). Such an exchange could reduce repetitive questionnaires by automatically updating/receiving attestation of compliance certifications and connecting enterprises with 'approved or verified' vendors.

What would make you purchase or replace your Third-Party Risk Management (TPRM) product?



AI Application Security

As mentioned above, the growing penetration of AI into professional environments requires a comprehensive security approach equipped with the right tooling to address both consumption and creation aspects of AI adoption.

Enterprises are going beyond playing with ChatGPT, and are already building critical AI-based applications: from chatbots to underwriting models. These models are exposed to new, novel threats, including:

- Prompt Injection - Malicious inputs which overwrite system instructions, leading to a variety of hazards, from harmful content to code execution.
- Evasion - Attackers can craft an input to be misclassified by the model, leading to an incorrect output during inference. For example, this could lead a facial detection system to grant access to an unauthorized party.
- Data poisoning - An adversary could plant malicious information inside the training or RAG data to affect the resulting model behavior, leading to bias, inaccuracies or “backdoors” in AI systems.
- Model extraction - Hackers could attempt to reproduce model weights via several hundreds of sophisticated prompts. When the model itself is your company’s IP, this can be a top concern.
- Model inversion - Manipulative prompts could lead a model to disclose private training data, or uncover the membership of a specific individual in the training data.

A new category of AI security solutions is emerging to meet these challenges, introducing discovery, vulnerability scanning and runtime protection solutions.

> *The evolving role of a CISO demands that we enable the business by balancing innovation with protection in the fast moving world of AI adoption by building guardrails, not gates.*
>
> **Reet Kaur,**
> Executive Director Digital IT
> Risk Management & Security

Human Identity

The expanding attack surfaces and shift to zero-trust architectures are driving the need for modern, identity-centric cybersecurity measures. Attackers are using sophisticated techniques to exploit weaknesses in identity management, making traditional security measures less effective. At the same time, a rapid increase in the number of human and non-human identities, along with increasing decentralization, has made it increasingly difficult to see the big picture. Human Identity emerged as a top pain point among surveyed CISOs, with **41% highlighting it as a priority**. These challenges underscore the top trends in the identity security space: Identity Fabric and Zero Trust Security.

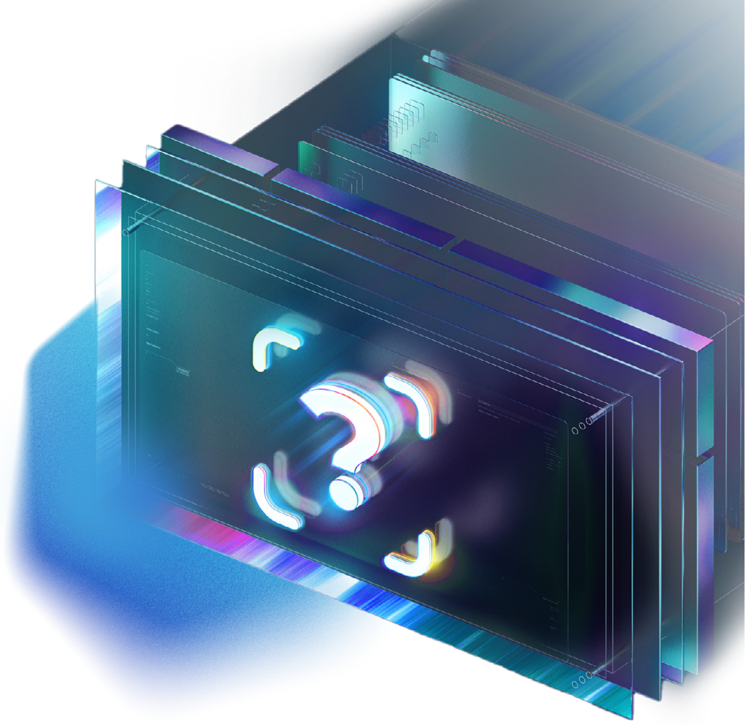
Identity Fabric

In 2023, survey respondents highlighted increased investment in IAM, and in 2024, both Human and Non-Human Identity emerged as top priorities for CISOs. Identity fabric solutions address the fragmentation within identity security by integrating Identity Access Management (IAM), Identity Governance and Administration (IGA), and Privileged Access Management (PAM) into a unified platform. This approach ensures centralized governance, providing organizations with high level control over identities and access rights across all applications and environments. Platforms like Team8 portfolio company Orchid emphasize full visibility and control over legacy and homegrown applications, which are often neglected by current solutions. By incorporating these applications into the identity fabric, organizations enhance overall security and compliance, ensuring robust protection and streamlined identity management.

Zero Trust Security

The zero trust security model is emerging as a trend in the face of increasingly complex and distributed networks, cloud adoption, and an expanding attack surface. The principle of "never trust, always verify" mitigates the potential for bad actors to access sensitive information within the company's data stack. As companies increasingly adopt cloud, SaaS, BYOD, and hybrid models, there is a growing shift towards identity-focused cybersecurity. This approach is essential as cloud-based workflows expand and networks confront more sophisticated cyber threats.[10]

Methodology & Survey Respondents



We conducted our annual CISO Survey during the 2024 CISO Village Summit in California. This event convened over 100 top cybersecurity executives from major global companies, including many Fortune 500 firms. This year's summit theme, Secure by Nature, provided a focused platform for senior security leaders to address current challenges, share best practices, and explore emerging cybersecurity trends.

To capture and analyze the emerging trends discussed at the summit, Team8 facilitated the 2024 CISO Village Survey. During the summit's final day, CISOs convened to review and discuss the survey findings, enhancing security trends from a peer-group perspective, and providing actionable insights.

This report presents the survey results and insights to the broader security community, aiming to enrich both CISOs and the cybersecurity industry at large. It also includes previously unpublished data from the 2023 CISO Village Survey, offering a comprehensive view of ongoing trends and challenges within the field.

Alongside insights into cybersecurity, the report also provides information about the companies of the participating CISOs. By examining the aggregated data, the following findings were uncovered:

Approximately 60 percent of survey respondents reported having a cybersecurity department with **over 20 employees**. Among these, approximately 30 percent have 21-100 employees and 23 percent have 101-500 employees.

Moreover, the majority of CISOs come from the **financial services, technology, and industrial/ manufacturing** industries. Following these, health & pharma and retail & e-commerce are the most common industries represented.

Cybersecurity Department Size

Among the respondents, the industries that showed the larger cybersecurity department sizes were financial services and industrial and manufacturing, with 35% and 55% of respondents reporting more than 100 employees, respectively.

What is the current size of your cybersecurity team?

0-20
38.8%

21-100
31.2%

101-500
22.5%

500+
7.5%

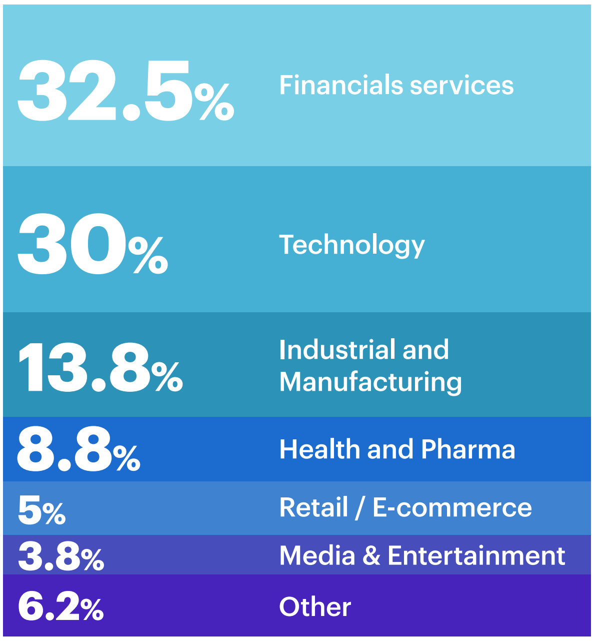
Industry

Among the surveyed CISOs, the majority work in either financial services (33%) or technology (30%) sectors. Industrial and manufacturing sectors follow, accounting for about 14% of the respondents. About 9% work in the health and pharmaceutical industry and 5% work in retail and e-commerce sectors.

When comparing industry-specific budget changes, significant disparities emerge. In the financial services sector, 58% of respondents reported an increase in their cybersecurity budgets. This figure is notably lower than the overall 70% of respondents across all industries who reported budget increases.

Conversely, the technology sector exhibited a more pronounced growth in budget allocation, with approximately 79% of respondents indicating an increase. This stark contrast highlights how the tech sector is prioritizing and investing in cybersecurity more aggressively than the financial services sector.[11] Supply chain attacks, such as those targeting SolarWinds, Okta, and Snowflake, are potential drivers of this increased focus and investment in cybersecurity within the tech sector. Additionally, as capital markets reward the tech sector for the fast adoption of AI, budget increases are more likely across departments. As technology companies prioritize rapid growth, this necessitates a more robust cybersecurity posture.

What is your Industry

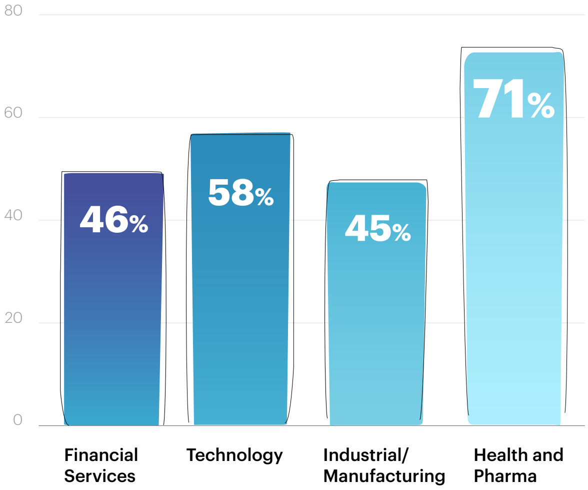


Scrutiny

Scrutiny vs. Industry

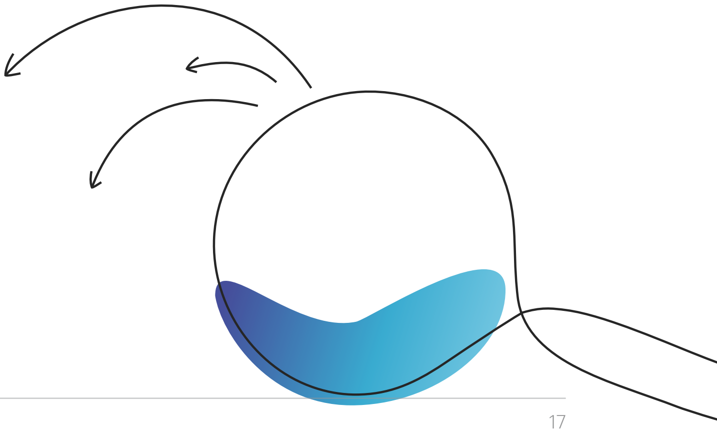
The data reveals that the health and pharmaceutical sector experiences the highest level of scrutiny, with 71% of respondents reporting significantly tighter scrutiny by their board of directors. The technology sector follows closely, with 58% of respondents indicating similar scrutiny. This significant concentration suggests that these industries face greater internal pressure compared to others.

% of CISOs who reported experiencing significantly higher scrutiny by the board of directors, by industry



Scrutiny vs. Budget

CISOs managing large budgets over 100 million USD overwhelmingly reported high levels of scrutiny from senior leadership and the board of directors. With 86% of these respondents indicating high scrutiny, it is evident that the more financial responsibility a CISO takes on, the more oversight they receive from senior executives, leading to increased levels of scrutiny.

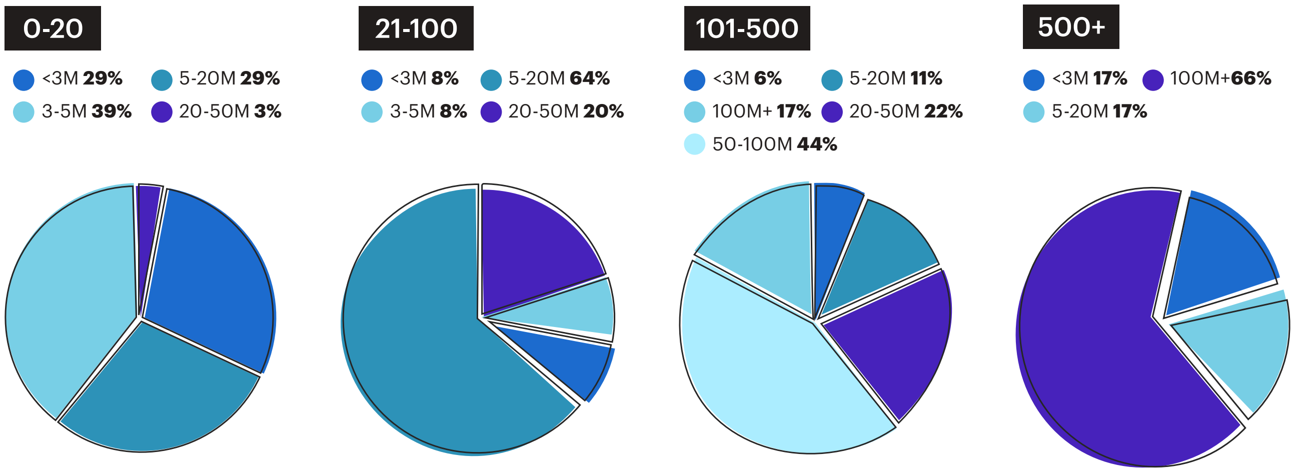


Appendix

A. Department Size vs. Budget

The majority of CISOs overseeing security departments with 21-100 employees reported annual budgets ranging from 5 to 20 million USD, with 64% falling within this range. Meanwhile, 20% of these CISOs managed larger budgets between 20 to 50 million USD. For companies with security departments of 101-500 employees, 44% had budgets in the 50 to 100 million USD range, and 17% had budgets exceeding 100 million USD.

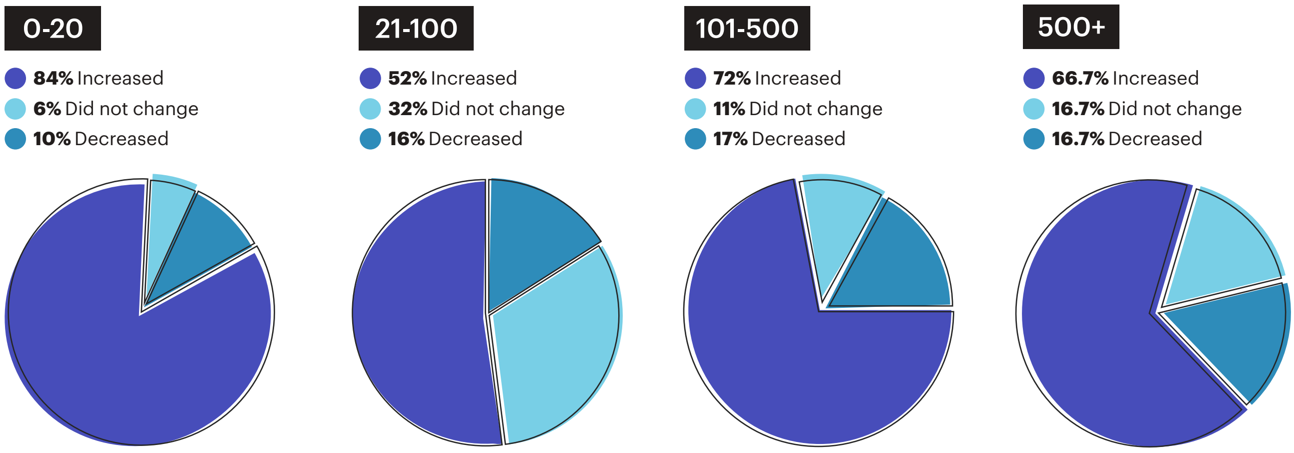
Budget Distribution by CISO Organization Size (# Employees)



B. Department Size vs. Budget Change

Our survey results indicate that departments with 0-20 employees experienced the highest percentage of budget increases, with 84% of CISOs reporting increased budgets and only 10% reporting decreases. Additionally, approximately 72% of companies with 101-500 employees reported budget increases, while only 17% reported decreases.

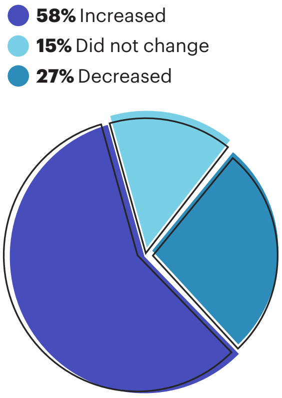
Budget Change for CISO Organizations (# Employees)



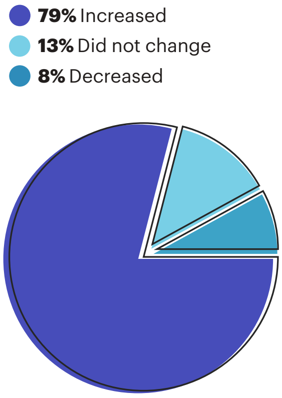
C. Budget Change by Industry

Overall, 70% of survey respondents reported an increase in their cybersecurity budgets. However, this varied significantly by industry: 58% of those in financial services saw budget increases, compared to 79% in technology and 91% in industrial and manufacturing sectors.

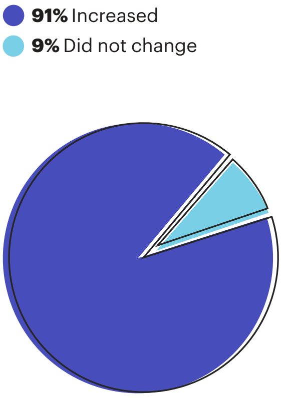
Financial Services



Technology



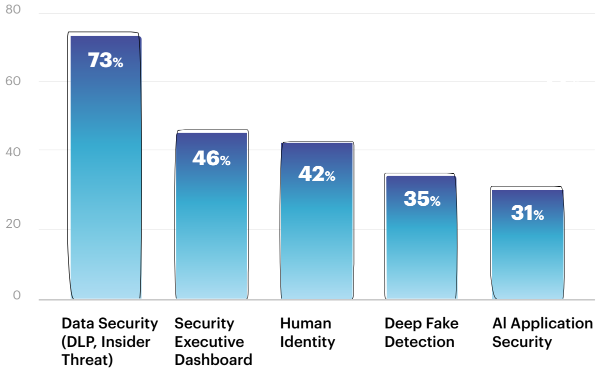
Manufacturing



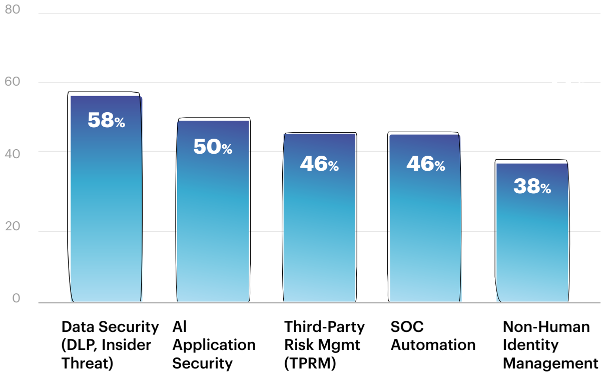
D. Pain Points by Industry

Across the top three industries—financial services, technology, and industrial & manufacturing—Data Security emerged as the primary concern for all. However, each industry prioritized additional pain points differently: financial services identified Security Executive Dashboard as the second most pressing issue, technology focused on AI Application Security, and industrial and manufacturing emphasized Third-Party Risk Management.

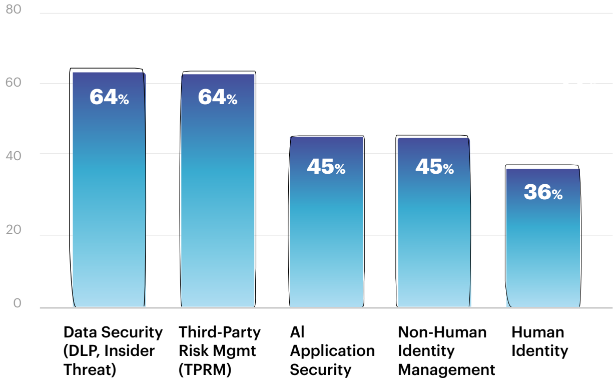
Financial Services



Technology



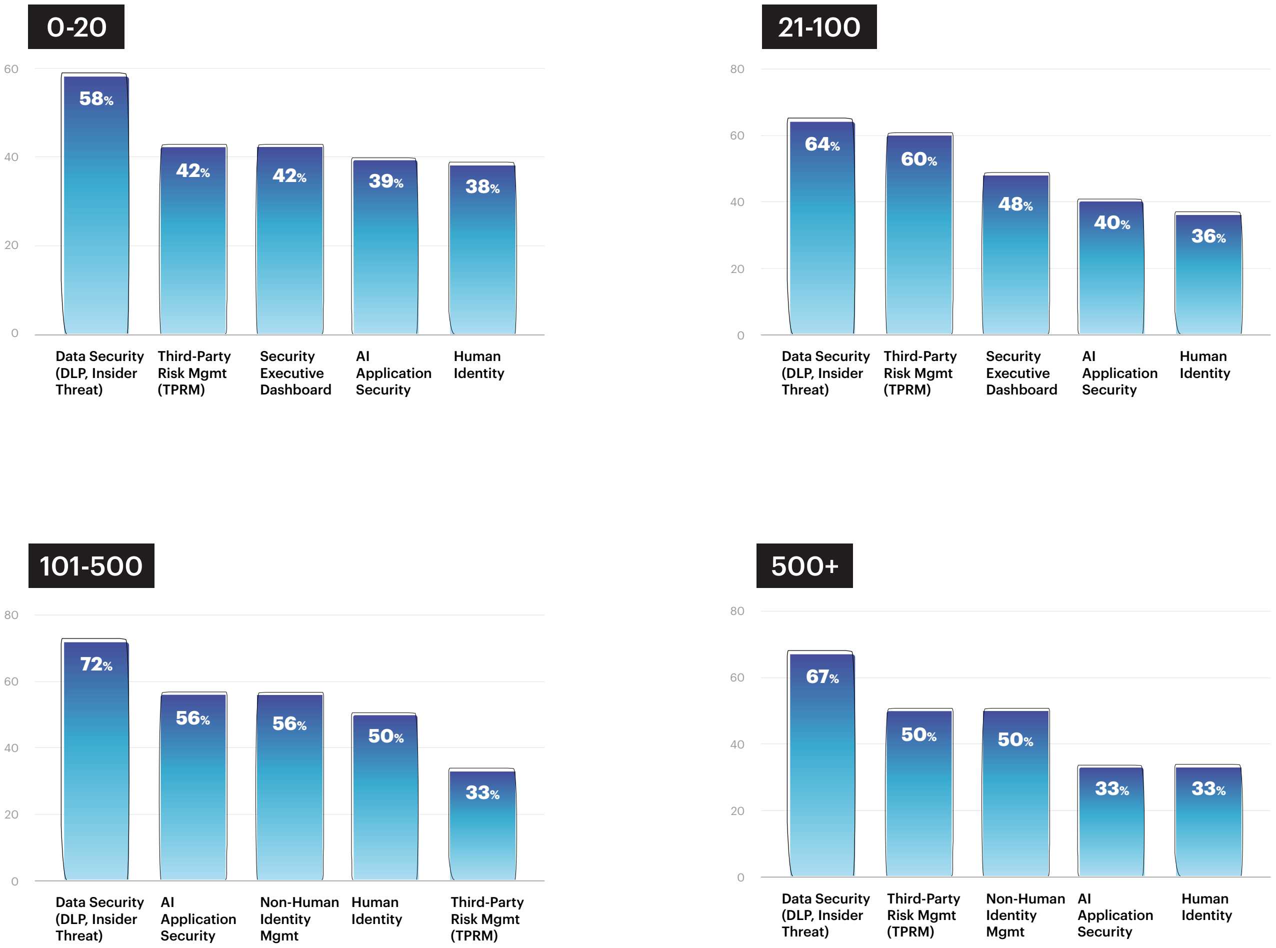
Manufacturing



E. Pain Points by Department Size

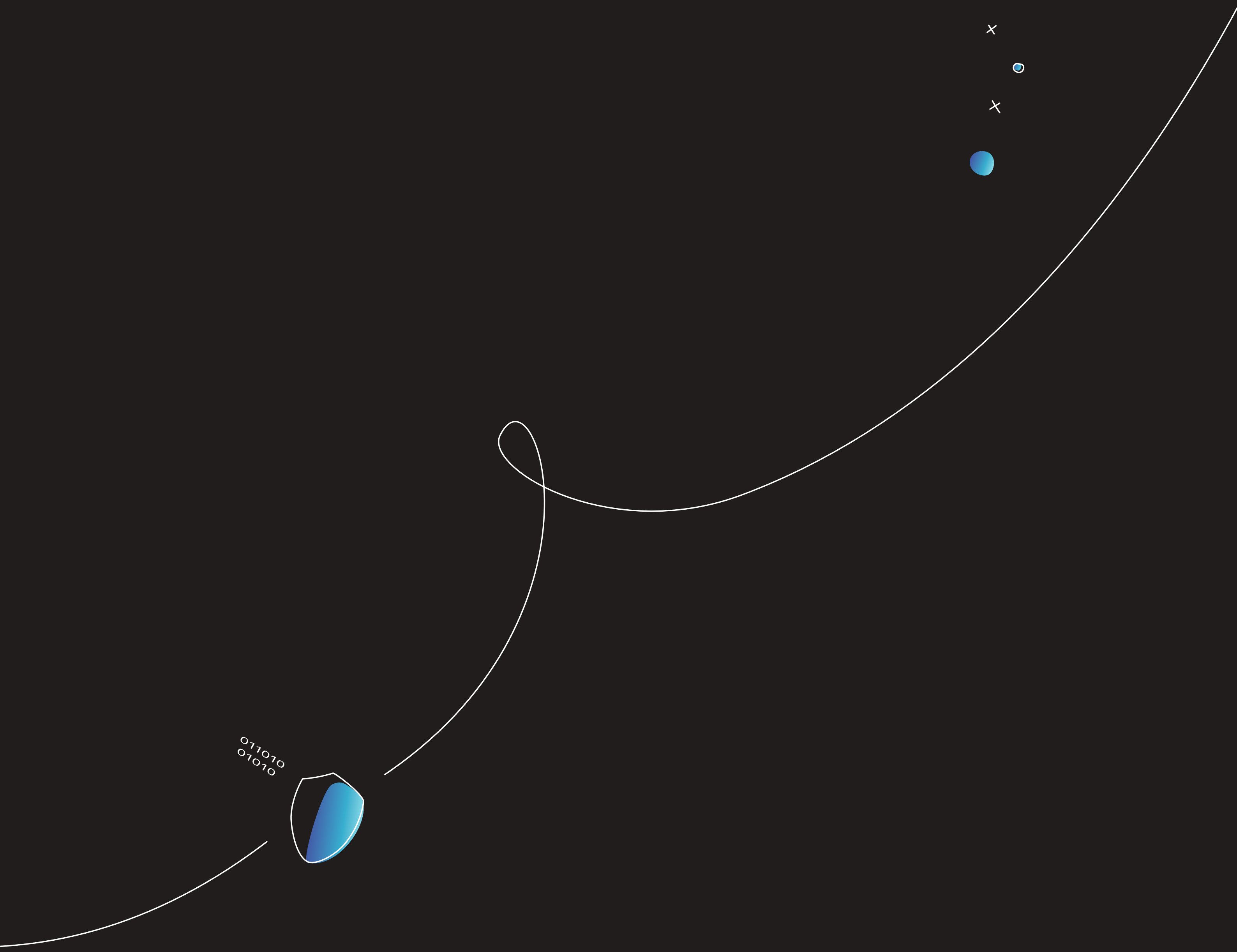
Surveyed CISOs consistently identified Data Security as the top pain point across all department sizes. Meanwhile, Third-Party Risk Management was typically ranked as the second most pressing concern across most department sizes. However, for security departments with 101-500 employees, it fell to fifth place, with only 33% of CISOs in this category considering it a top priority.

Pain Points for CISO Organization Size (# Employees)



Endnotes

1. Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024, 2023
2. Top Trends in Cybersecurity for 2024, Richard Addiscott, Jeremy D'Hoinne, etc., Gartner, 2024
3. Safeguards Rule Notification Requirement Now in Effect, Lesley Fair, Federal Trade Commission (FTC)
4. Supreme Court Ruling on Chevron Doctrine May Upend Future Cybersecurity Regulation, David Jones, 2024
5. SolarWinds Corporation and Timothy G. Brown, SEC
6. Deepfake Fraud Directed at Banks on The Rise, Liz Lumley, The Banker, 2024
7. Cybersecurity Tends in 2024, Mike Droesch, Amit Karp, and Yael Schiff, Bessemer Venture Partners, 2024
8. 2023 CISO Survival Guide, Collaboration Between Cisco Investments, Forgepoint Capital, NightDragon, Team8, 2023
9. The Rising Importance of Third Party Risk Management (TPRM), Daniel Soo, Suzanne Denton, etc., Deloitte, 2023
10. The Next Generation of Cloud Security Startups, Joel De La Garza, Andreessen Horowitz, 2019
11. Budget Change by Industry Chart



For more information

Contact us at: cisovillage@team8.vc | www.team8.vc

TEAM8™