TLP: Clear

CISO BENCH MARK

2026 | 8TH EDITION

RETAIL & HOSPITALITY ISAC | IANS

Table of Contents

Executive Summary

In 2025, tariffs and shifting consumer sentiment increased supply chain costs, tightened margins across retail and hospitality (RH), and forced many firms to reduce budgets. Growing adoption of AI offers a path toward productivity gains, yet high implementation costs present an added challenge for already strained budgets.

This report provides a current state assessment of cybersecurity organizations amid these circumstances. It offers detailed insight into budgets and staffing; CISO responsibilities and challenges; and the use, challenges and budget implications of AI for cybersecurity[1]. The research is based on the responses from 201 CISO respondents to this year's annual RH-ISAC CISO Benchmark survey. The report is produced in partnership between RH-ISAC, member companies and IANS.

Key findings

Security budgets grow incrementally

IT and security budgets grew modestly in 2025, reflecting incremental expansion rather than a fundamental shift in how organizations prioritize security spending. Expectations for budget growth heading into 2026 are cautiously positive, with more CISOs expecting increases than in the prior year. CISOs attribute their expectations to anticipated company performance, routine annual adjustments and digital transformation initiatives.

AI emerges as top friction point

AI has overtaken ransomware and phishing as the top CISO friction point—not because ransomware and phishing have been solved, but because AI has added an entirely new layer of uncertainty on top of an already demanding threat landscape. Accordingly, CISOs' key initiatives for 2026 are shaped by AI; though, execution remains limited by familiar structural issues such as cyber vs. IT prioritization tensions and budget constraints.

Security organizations' adoption of AI advances

Security teams are finding real but measured value in AI, mainly in threat detection, analysis and reporting. AI governance is advancing—only 3% of organizations have no AI policy in place—yet concerns about data leakage, insider misuse and weak controls persist. Nearly 90% of CISOs expect AI security spending to rise, largely by reallocating existing budgets.

CISOs expect to keep staffing levels stable

Staffing levels are expected to hold steady in 2026, with most security organizations maintaining headcount and using AI to boost team efficiency rather than reduce roles. Contractors face more risk, with 20% of CISOs projecting cuts, especially at firms exceeding $10 billion in revenue.

1. *This report is published as the 2026 edition and reflects survey data collected in December 2025. Budget figures labeled "2025" refer to respondents' current-year budgets at the time of the survey; figures labeled "2024" refer to the prior year. Projections labeled "2026" reflect respondents' expectations for the coming budget year."*

By the Numbers: Key Highlights

Security Spending

Security budgets evolve incrementally – making room for AI investments

54% | **anticipate budget increases** and **33%** anticipate no change

43% | of CISOs expert significant increases in AI-related investments

Security Workforce

Cybersecurity full-time employees expected to grow in 2026

35% | plan to **grow full-time cybersecurity staff** in 2026

55% | of InfoSec FTEs work on **IT, security operations, IAM, security engineering, GRC, or fraud prevention**

CISO Responsibilities

CISO scope continues to expand

70% | of CISOs saw **AI** added to their responsibilities.

8pp* | rise in product security as a CISO area of responsibility

Challenges & Concerns

AI Is both a friction point and a friction multiplier

Top 3 | Friction points cited: AI (**71%**), supply chain attacks (**54%**), and vulnerability identification and remediation (**41%**)

Top 2 | Challenges cited: Cyber vs IT prioritization (**70%**) and budget constraints (**68%**)

74% | Say **data leakage through public AI tools** is a key concern regarding AI security

CISO Responsibilities

Actual NIST CSF score improvements fall behind expectations

0% | change in average NIST scores across functions in 2024–2025 — with an 11% rise projected for 2026

66% | rise in product security as a CISO area of responsibility

Budget Trends

Budgets grew incrementally, without a strategic rebalance.

IT and security spending trended upward in 2025, with average IT spend rising from 3.2% to 3.9% of revenue, and average security spend increasing from 0.57% to 0.75%. Security investment as a share of IT budget remained relatively stable (5.7% to 5.8%, on average), suggesting incremental growth, rather than a structural shift in prioritization.[2]

For CISOs, the data reflects modest budget expansion, but not a step-change in how organizations allocated resources toward cybersecurity relative to overall IT. A notable creative trend also emerged, where some security leaders are offloading certain budget items—like compliance assessments—to business units, effectively stretching their security dollars without formally growing their budgets.

Budget metrics: Midpoint averages* and median brackets

		2024	2025
IT spend as % of revenue	Average	3.2%	3.9%
	Median bracket	3%	3%
Security spend as % of revenue	Average	0.57%	0.75%
	Median bracket	0%–0.5%	0%–0.5%
Security spend as % of IT budget	Average	5.7%	5.8%
	Median bracket	6%–7%	6%–7%

** Averages are weighted averages (mean values) of the midpoints of the brackets and do not include "10%+" brackets for IT spend as percentage of revenue and security spend as percentage of IT budget.*

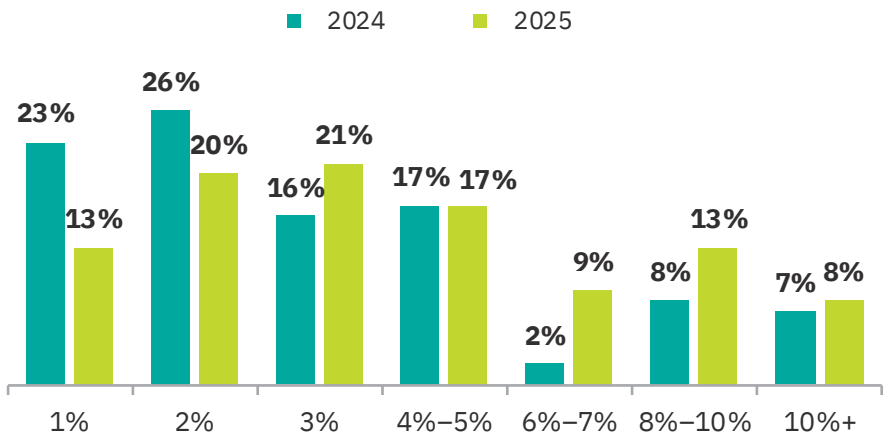
> *"I've actually saved some money because I've transferred it to the business as well. … The work is still being done, but it doesn't have to be in our budget."*
>
> **— CISO, Retail, $2B–10B revenue**

2. *Readers may notice that calculating security spend as a percentage of IT spend using the two related metrics (IT spend as a percentage of revenue and security spend as a percentage of revenue) does not fully correspond to the percentages shown in the bottom right table in the figure "IT and Security Spend Relative to Revenue, 2024–2025". This discrepancy is likely due to two factors: Respondents may have estimated their answers rather than calculated exact figures, and the derived percentages are based on bracket midpoints, excluding the "more than 10%" bracket (which has no midpoint). As a result, these figures are directionally indicative but should not be treated as exact figures.*

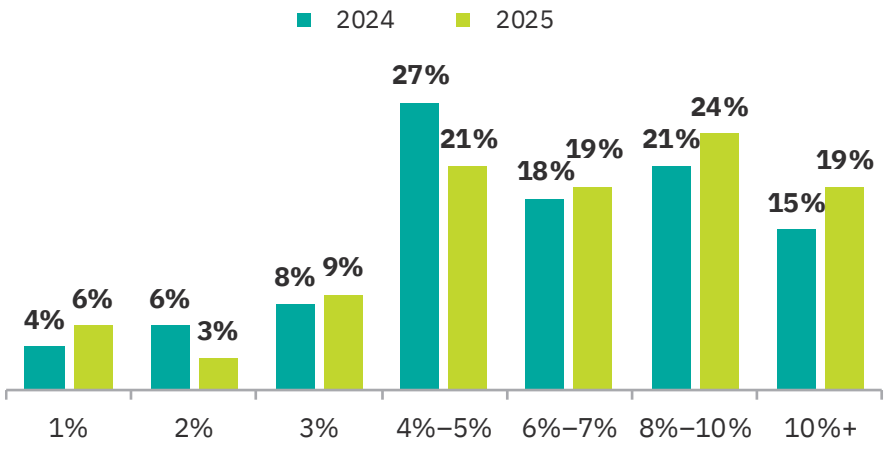
IT and Security Spend Relative to Revenue, 2024–2025

What are your approximate annual IT spend as percentage of annual revenue, security spend as percentage of annual revenue and security spend as percent of the overall IT budget?

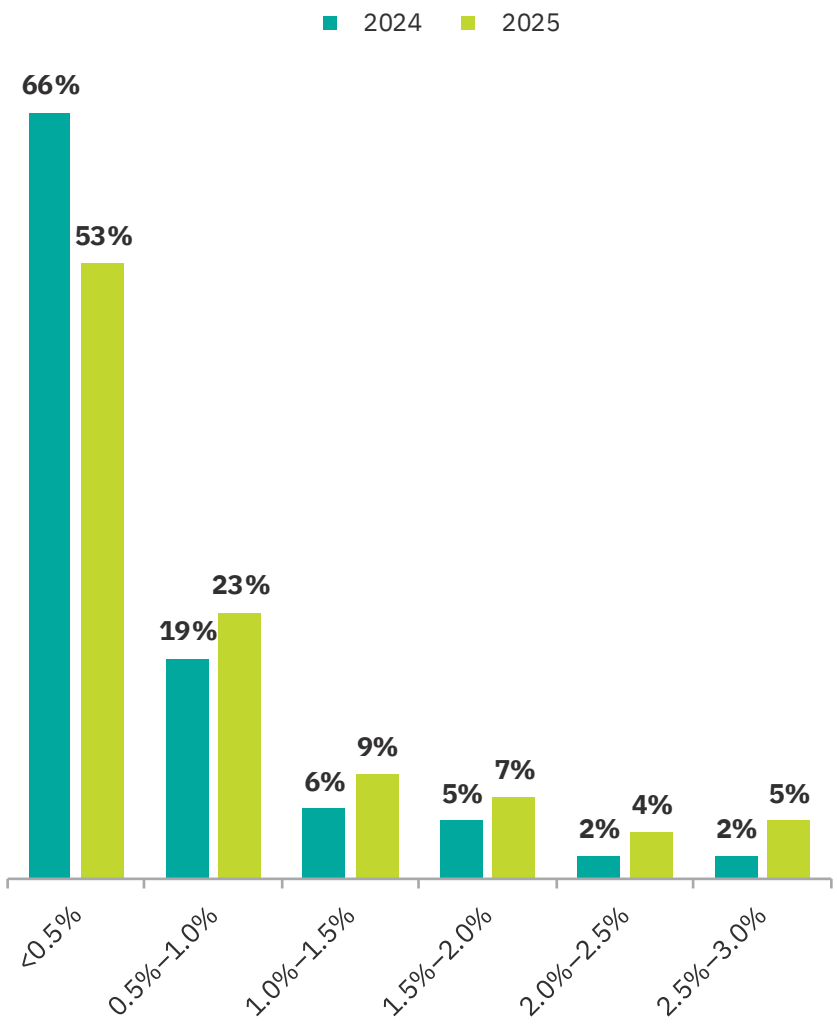
IT spend as percentage of revenue



Security spend as percentage IT budget



Security spend as percentage of revenue



Security investment growth extends across sizes and sectors

Security budget growth expectations strengthen heading into 2026, with 54% of CISOs anticipating increases, compared to 44% the prior year. The share expecting flat budgets declined by 10 percentage points.

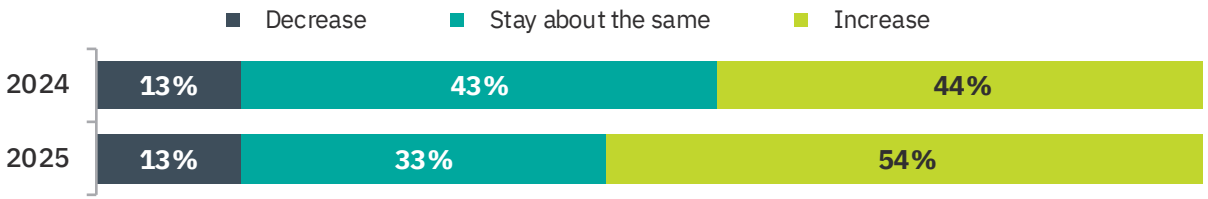
The share of respondents with expected increases is largest among organizations under $2 billion in revenue, where a majority anticipate increases of 1% to 10%, or more, whereas larger enterprises more frequently report stable budgets.

Across sectors, expected increases outpace decreases, particularly in hospitality, retail and consumer-focused industries, indicating continued, but measured, expansion in cybersecurity investment rather than dramatic funding shifts.

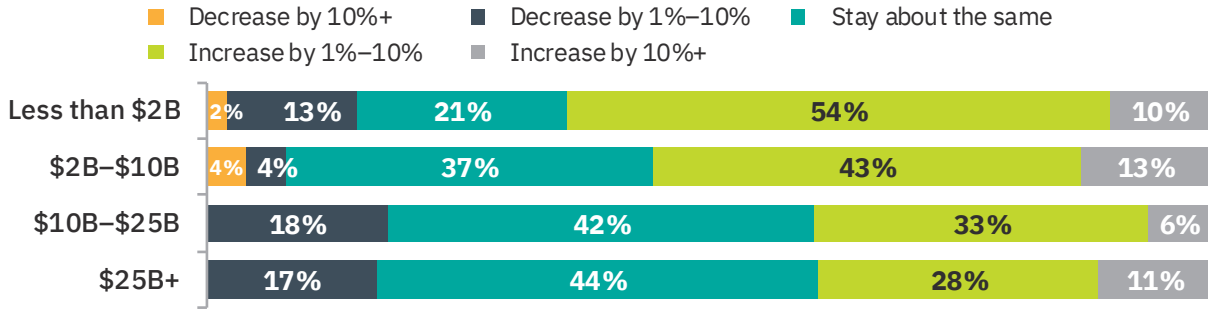
Expected Security Budget Change in 2026

How do you expect your organization's total security budget to change in the coming year compared to the current year?

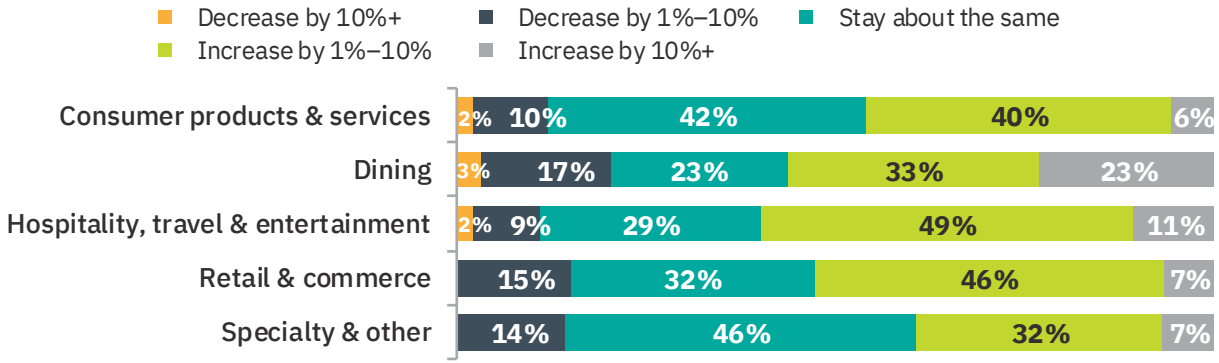
By year, 2024–2025



By revenue segment, 2025



By sector group, 2025



Totals may not sum to 100% due to rounding.

Security budget increases are tied to growth; decreases reflect cost controls

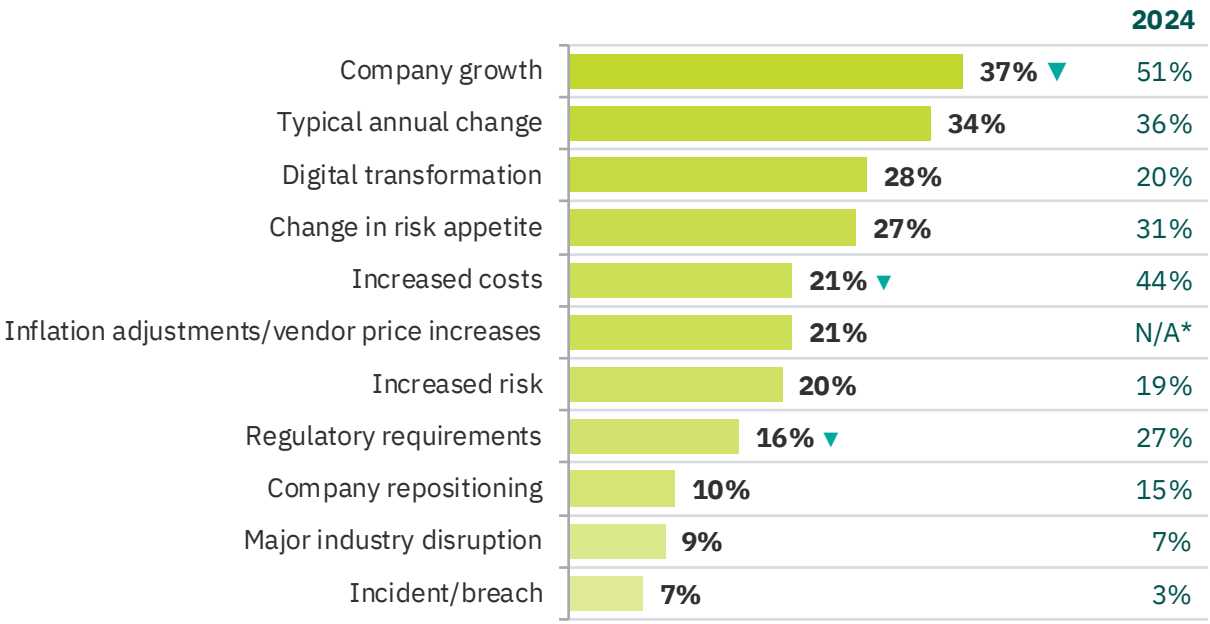
Security budget increases are most attributed to company growth, routine annual adjustments and digital transformation initiatives. Anecdotally, CISOs also point to AI-related initiatives as key drivers of budget increases. Notably, incident-driven funding remains relatively rare, suggesting the security investment is becoming more planned and programmatic rather than reactive.

Conversely, when budgets decrease, the primary reasons are organizationwide cost reduction and broad macroeconomic pressures, indicating cybersecurity spend can be impacted by negative business performance.

Key Drivers of Security Budget Change

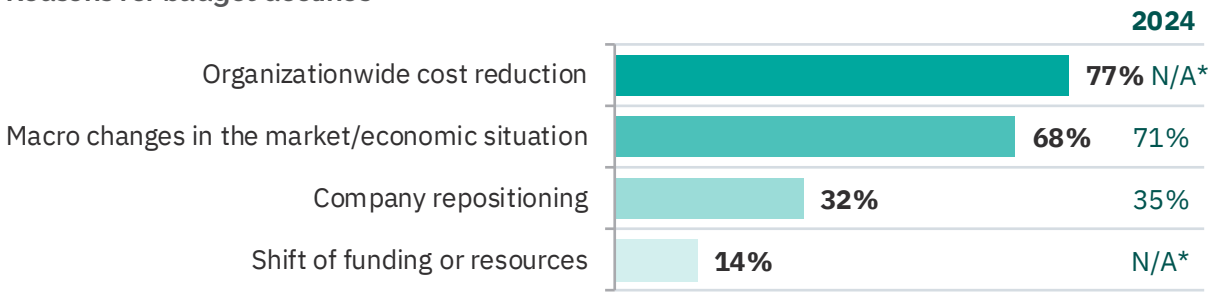
What are the top three reasons you anticipate this change, if any, in your budget? Up to three answers selected.

Drivers of budget increases



▼ YOY decrease by at least 10 percentage points

Reasons for budget declines



** Not asked in 2024*

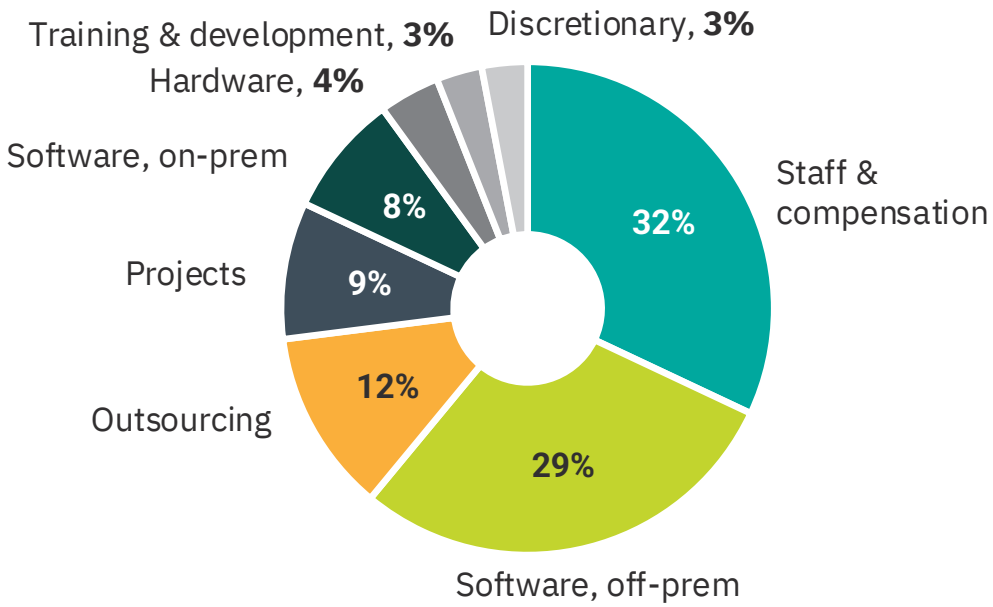
Security budgets lean toward talent and cloud tools

Security budgets remain heavily concentrated on staff & compensation (32%) and off-prem software (29%), underscoring the continued prioritization of talent and cloud-based security capabilities. Outsourcing and project-based spending represent secondary allocations, while hardware, training and discretionary spending are comparatively small.

Larger organizations allocate a greater share to personnel and on-prem investments, whereas smaller companies dedicate relatively more to outsourced services and off-prem software, reflecting differing operating models and maturity levels.

Security Budget Breakdown

How does your company's annual information security budget break down approximately?



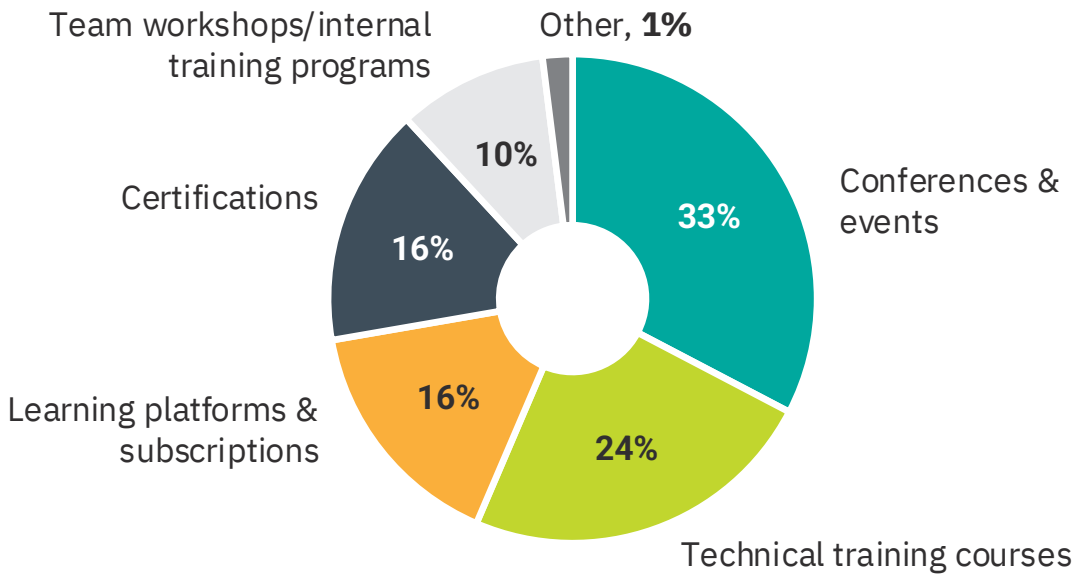
Security training budgets prioritize external exposure and technical skills

Security training budgets are primarily directed toward conferences and events (33%) and technical training courses (24%), signaling a strong emphasis on external engagement and hands-on skill development. Learning platforms, certifications and internal workshops represent secondary allocations, with consistent patterns across revenue segments.

Larger organizations dedicate slightly more budget to formal technical training, while smaller firms more heavily lean into conferences and learning subscriptions, reflecting differing approaches to workforce development and capacity building.

Security Training & Development Budget Breakdown

For the training and development portion of your information security budget, how is that budget allocated?



The Evolving CISO Role

Traditional reporting lines prevail

Most CISOs continue to report into technology leadership, with 40% reporting to the CIO and 27% reporting to the chief technology officer (CTO). Overall, 81% report through a tech function, compared to 19% reporting into business roles such as CEO, chief operating officer (COO) or chief financial officer (CFO).

Smaller organizations are more likely to have CISOs reporting outside of IT, while larger enterprises show more traditional tech reporting lines.

That said, CISOs note that where a CISO reports matters less than the relationships and influence they build within the organization. The one structural caveat raised by CISOs is that if the CISO is a peer to the CIO or CTO rather than reporting to them, it is critical they share the same manager; otherwise, conflict escalation becomes unwieldy.

> *"If they don't have the same boss, the same manager, then you're going multiple levels up to escalate where there is contention. And that never goes well."*
>
> **— CISO, Retail, $10B–$25B revenue**

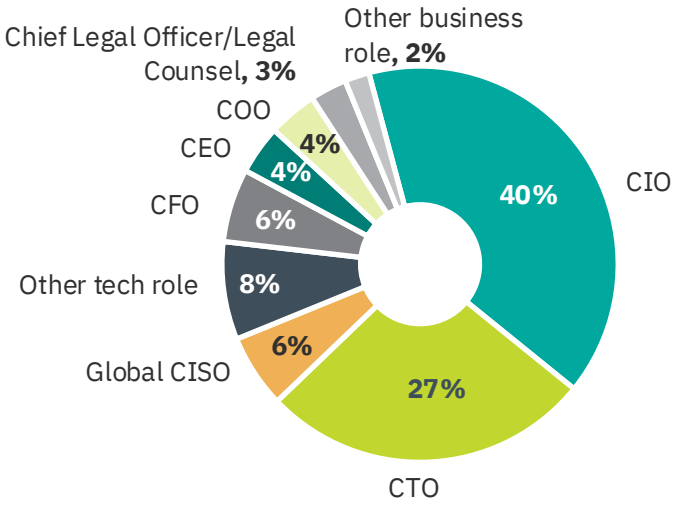
CISO scope continues to broaden

Besides their broad ownership across core security functions, oversight increasingly extends into business risk domains, such as third-party risk and business continuity, as well as emerging areas including AI and IoT/OT security.

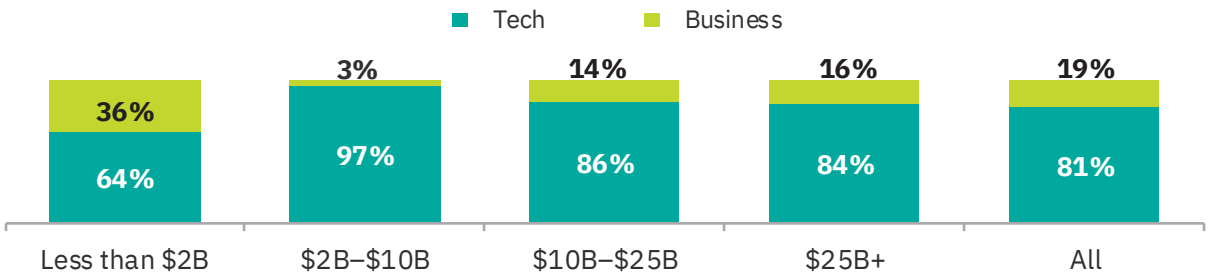
At the same time, many CISOs continue to carry traditional IT responsibilities, particularly network security and IT compliance, highlighting the role's continued blend of security leadership and operational IT oversight.

CISO Reporting Lines

Which of the following executives do you report to?



What function do you report into?

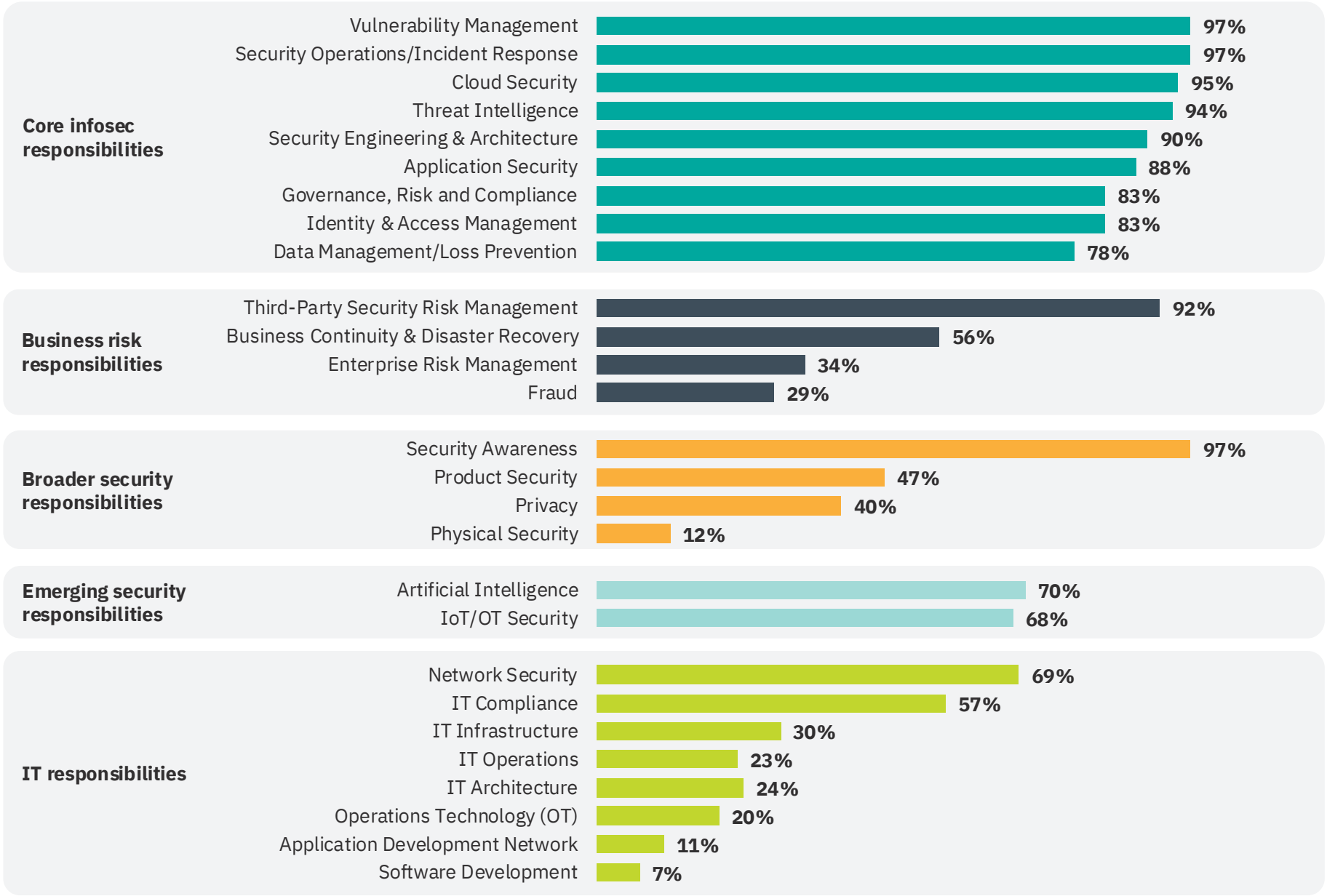


Tech: CIO; CTO; global CISO; and other tech functions including chief security officer, chief technology and digital officer, and head of IT.

Business: CEO; president; general manager; COO; CFO; CRO; legal counsel; and other business functions such as chief digital officer, chief product officer and chief administration officer.

CISO Responsibilities

In your current role, what is included in your security ownership?

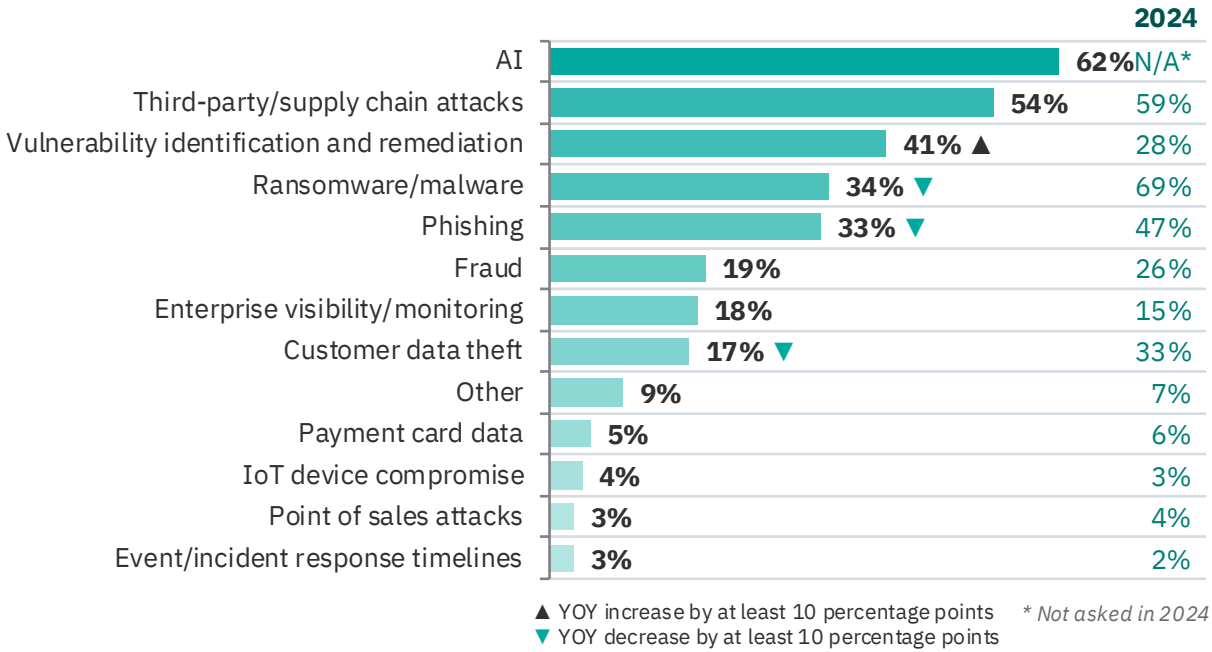


AI emerges as CISO top friction point

The top three areas of friction are AI (62%), third-party/supply chain risk (54%), and vulnerability identification and remediation (41%). Compared with the prior year, ransomware and malware dropped 35 percentage points to 34%, and phishing fell 15 points to 33%, but neither has receded as a real threat. AI is actively amplifying both by expanding the attack surface and accelerating adversarial capabilities. Ransomware is increasingly viewed as an outcome of other vectors, including phishing, third-party compromise and unpatched vulnerabilities, rather than a stand-alone friction point, which explains its ranking decline. AI, by contrast, remains an open question: widely recognized as consequential, but still lacking concrete governance answers.

CISOs' Top Friction Points

What are the top three information security friction points your organization currently faces? Up to three answers selected.



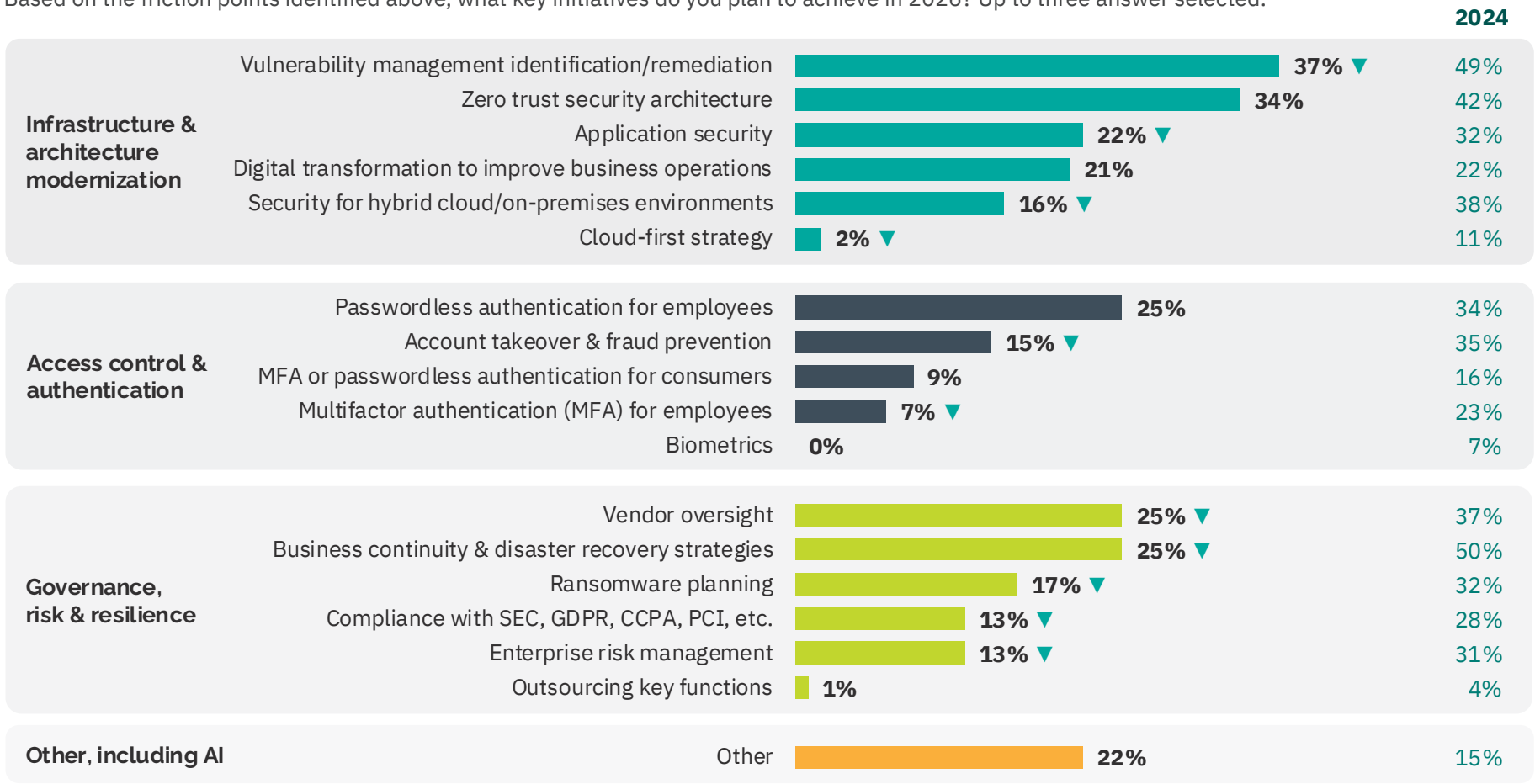
> *Ransomware and data extortion are still absolutely top of mind. AI hasn't overtaken them; it's just added another area of exposure to an already full plate.*
>
> **— CISO, Travel, $25B+ revenue**

AI shakes up CISOs' top 3 security initiatives

Based on the main friction points, the most common key initiatives for 2026 are related to infrastructure & architecture modernization. However, compared to the prior year, most categories saw a decline in prioritization. The "Other" category was the notable exception with year-over-year (YOY) growth and the written-in responses overwhelmingly centering on AI.

Key Security Initiatives in 2026

Based on the friction points identified above, what key initiatives do you plan to achieve in 2026? Up to three answer selected.



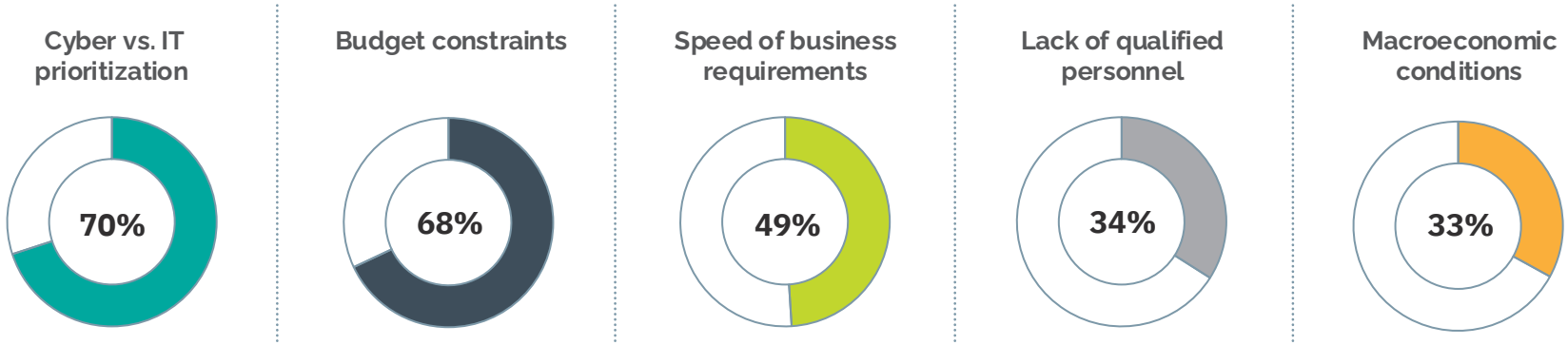
▼ YOY decrease by at least 10 percentage points

CISOs point to structural challenges as key barriers to achieving initiatives

CISOs' top challenges in executing 2026 initiatives are largely structural rather than technical, including tensions between security and broader IT prioritization, budget constraints and the pace of business demands. This highlights that execution risk is driven as much by internal alignment and funding dynamics as by the threat landscape itself.

CISOs' Top Challenges

What are the top three challenges (i.e., internal or external) you currently face in achieving those initiatives? Multiple answers possible.



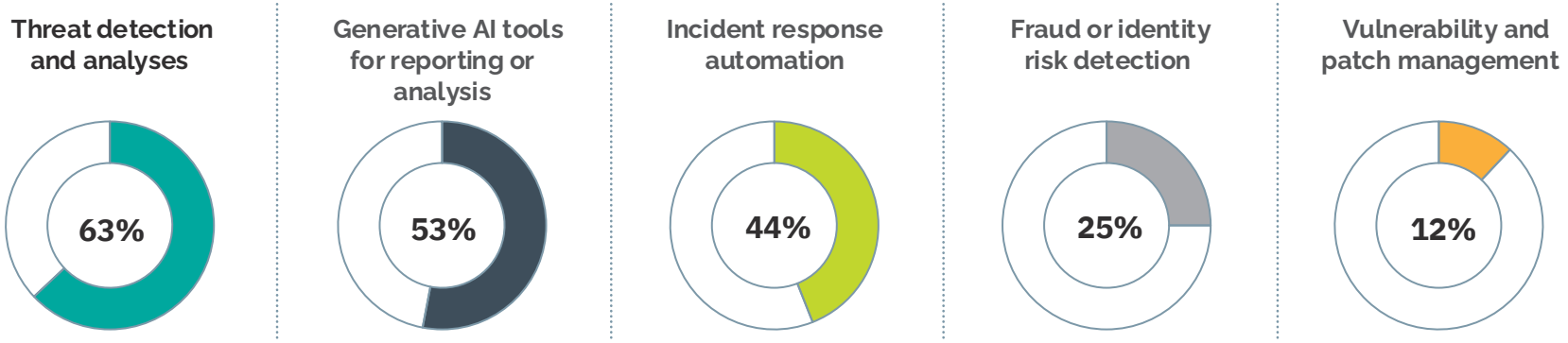
The Impact of AI on the Security Function

Security teams in the retail and hospitality sector are finding the most traction with AI in areas like threat detection, analysis and reporting functions. For example, using AI to streamline threat modeling—a process that traditionally required lengthy workshops between security and application teams, by routing structured inputs through a pre-staged AI prompt to generate a solid baseline risk assessment in minutes rather than hours. Anecdotally, CISOs caution against chasing flashy AI solutions, instead advocating for "boring AI," meaning the unglamorous but high-return application of automation and machine learning to existing workflows.

> *"The highest-return AI initiatives aren't about acquiring a company or buying a product just because it has AI in the name, expecting it to magically solve all your problems."*
>
> **— CISO, Retail & Apparel, $2B–$10B revenue**

How Security Functions Currently Use AI

How is your organization currently using AI or machine learning within the security function? Multiple answers possible.



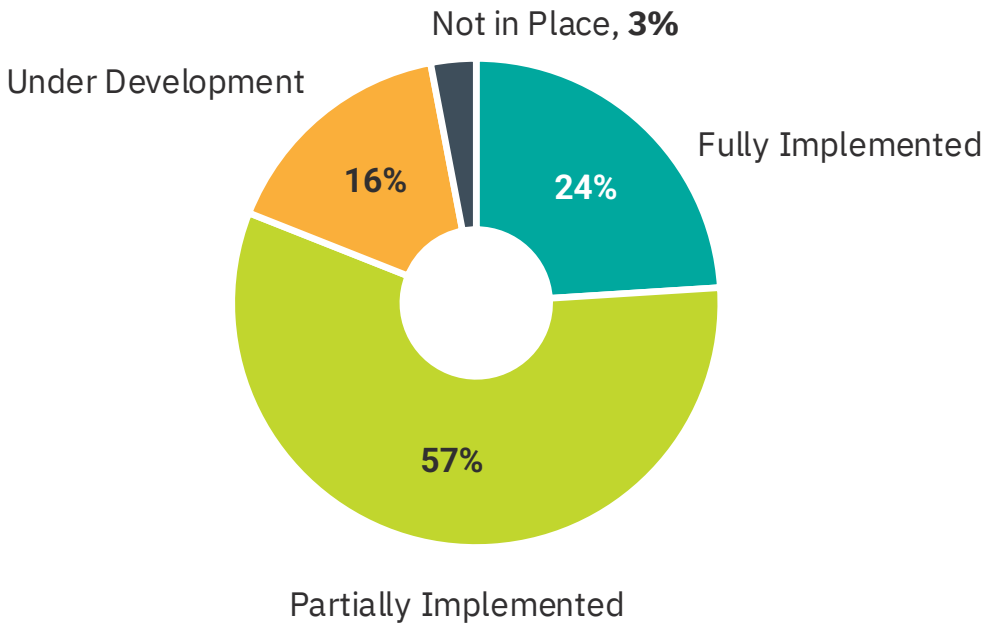
Formal AI frameworks reduce, but do not eliminate risk

AI governance frameworks have quickly gained traction—81% of organizations have at least partially implemented policies. But formalized frameworks have not eliminated core security concerns. Data leakage, insider misuse and weak governance controls remain top risks, and even among organizations with fully implemented frameworks, fears around model reliability and prompt-based attacks persist.

The data suggests that while governance maturity reduces uncertainty, it does not fully mitigate operational AI risk, leaving CISOs managing exposure even in more structured environments.

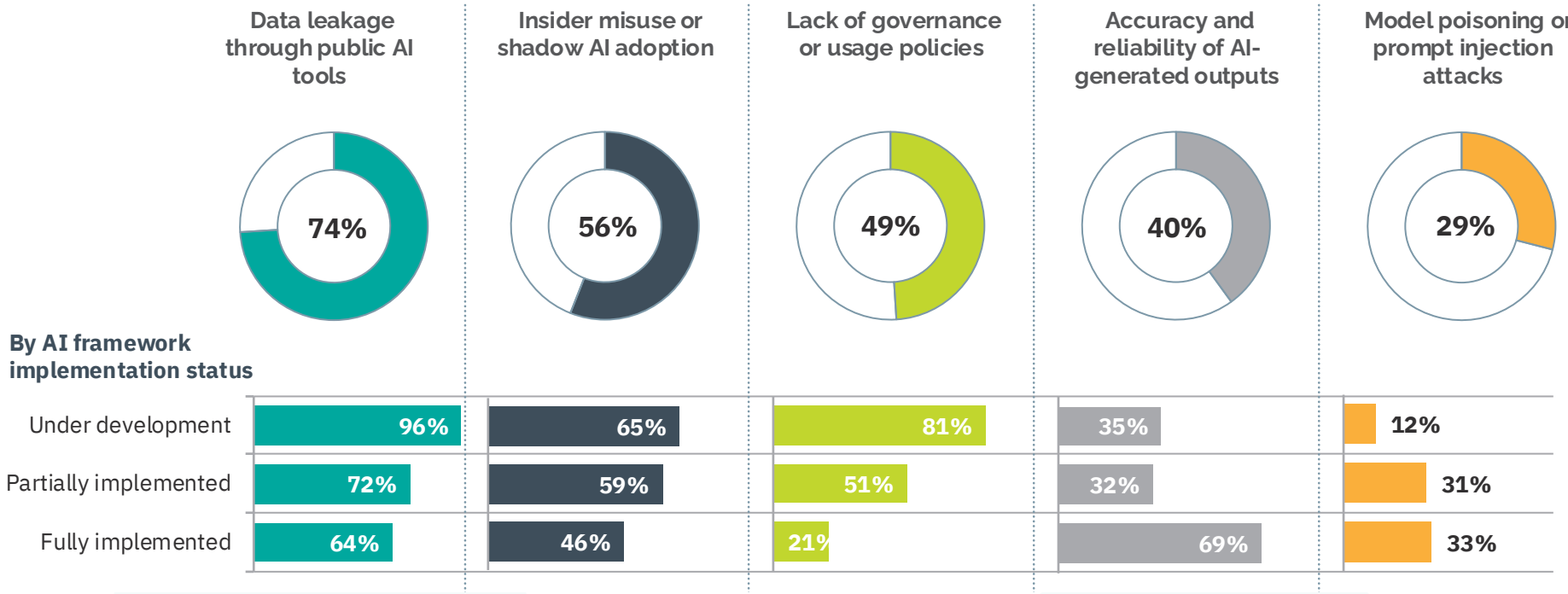
AI Policy Implementation Status

Does your organization have a formal governance framework or policy for AI usage and security oversight?



CISOs' Key Concerns Regarding AI Security

What are your biggest concerns related to AI use in cybersecurity operations or across the enterprise? Up to three answers possible.

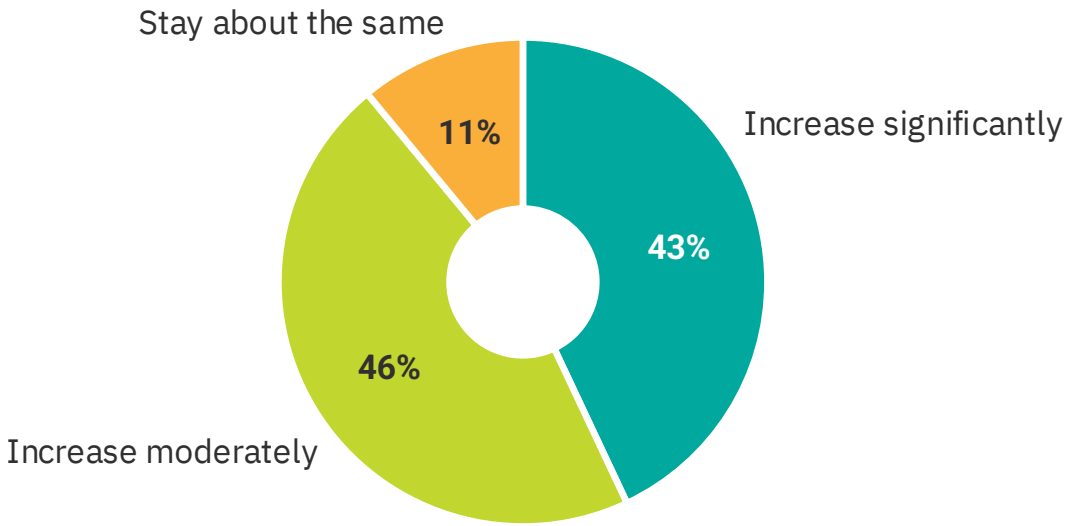


AI investments accelerate, despite limited budget expansion

AI-security investment is set to rise sharply over the next 12–18 months, with nearly 90% of CISOs expecting increase and 43% anticipating significant growth. However, this momentum is not translating into dramatic overall security budget expansion: 42% report no meaningful budget impact and 28% are allocating existing funds rather than adding new dollars. This implies AI is becoming a priority line item, but often within constrained or reshuffled security budgets rather than through net-new funding.

Investment Expectations for AI-Security Initiatives

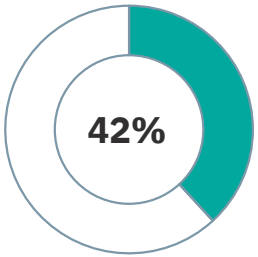
Over the next 12–18 months, how do you expect your organization's investment in AI-related security initiatives to change?



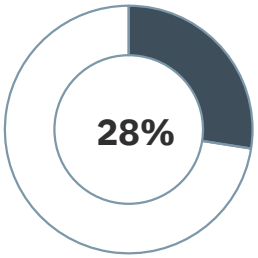
The Impact of AI-Related Security Initiatives on the Security Budget

How are AI-related security initiatives impacting your organization's overall security budget?

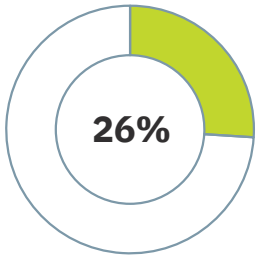
No meaningful impact on the security budget



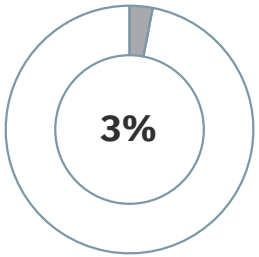
Causing a reallocation of existing funds without increasing total budget



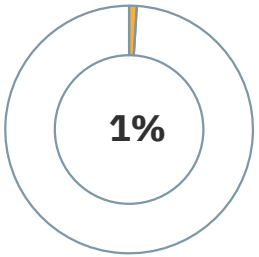
Increasing the security budget moderately



Causing a reduction in other security investments



Increasing the security budget significantly

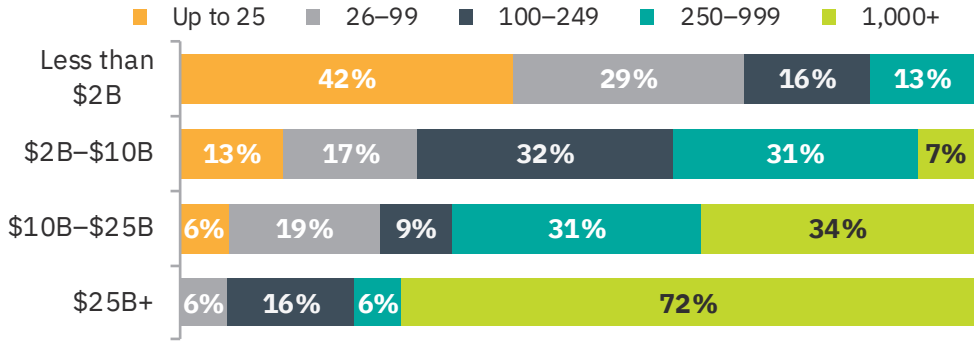


Staffing

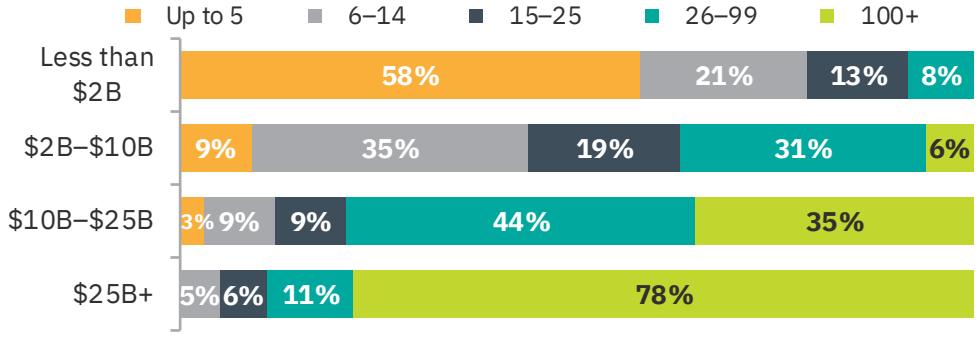
The Size of IT and Security Teams: FTE and Contractors, by Revenue

How many full-time equivalents (FTE) and contractors do you have on your IT and security teams?

IT staff count: FTE and contractors



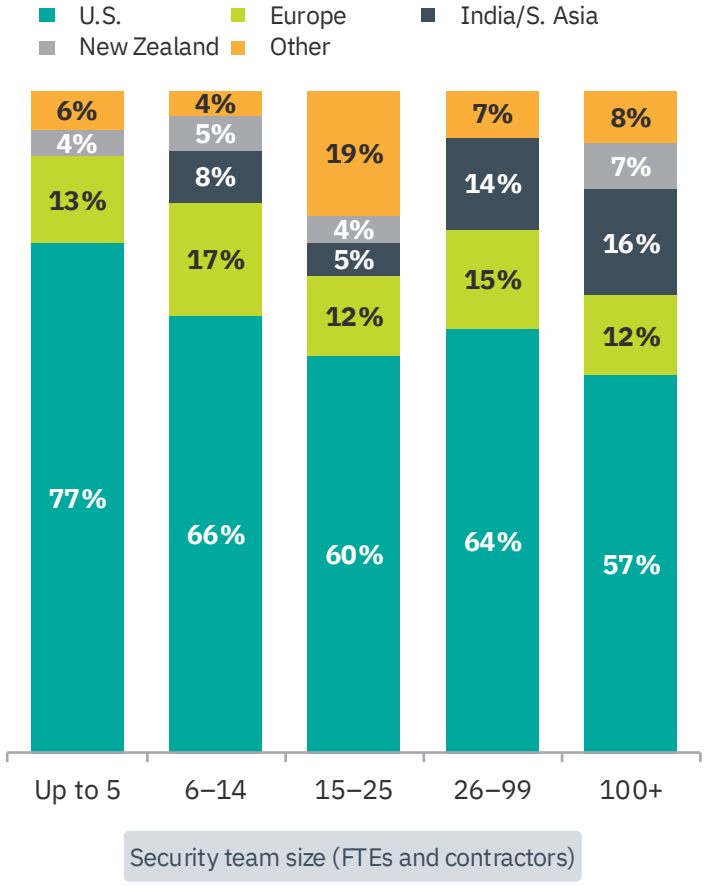
Security staff count: FTE and contractors



Totals may not sum to 100% due to rounding.

Security Staff Breakdown Across Geographies

What is the breakdown of your information security team (i.e., employees and contractors) by region?

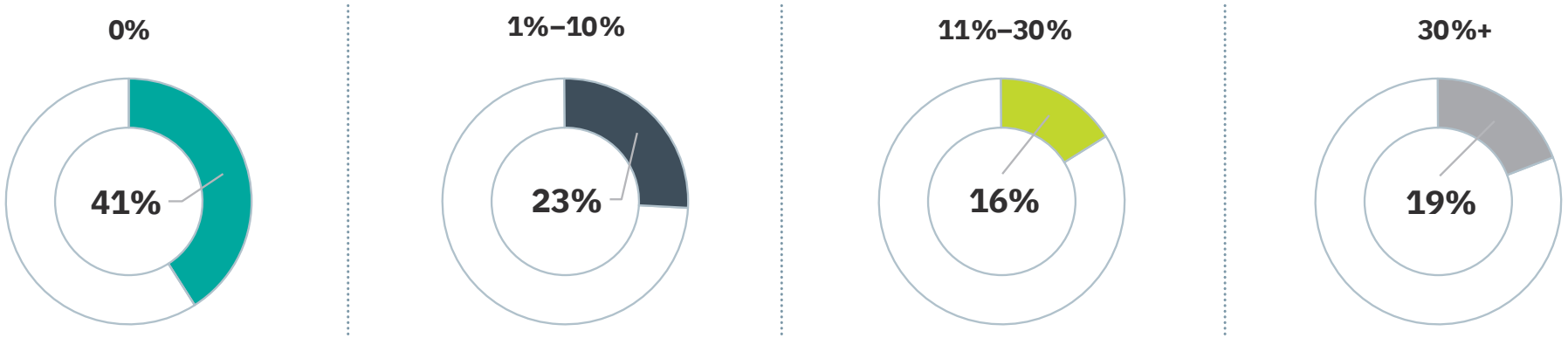


"Other" includes broader Asia and Latin America

Totals may not sum to 100% due to rounding.

The Share of Security Staff Who Are Contractors

What percentage of your information security team is made up of contractors?



CISOs prioritize stability and efficiency over headcount growth

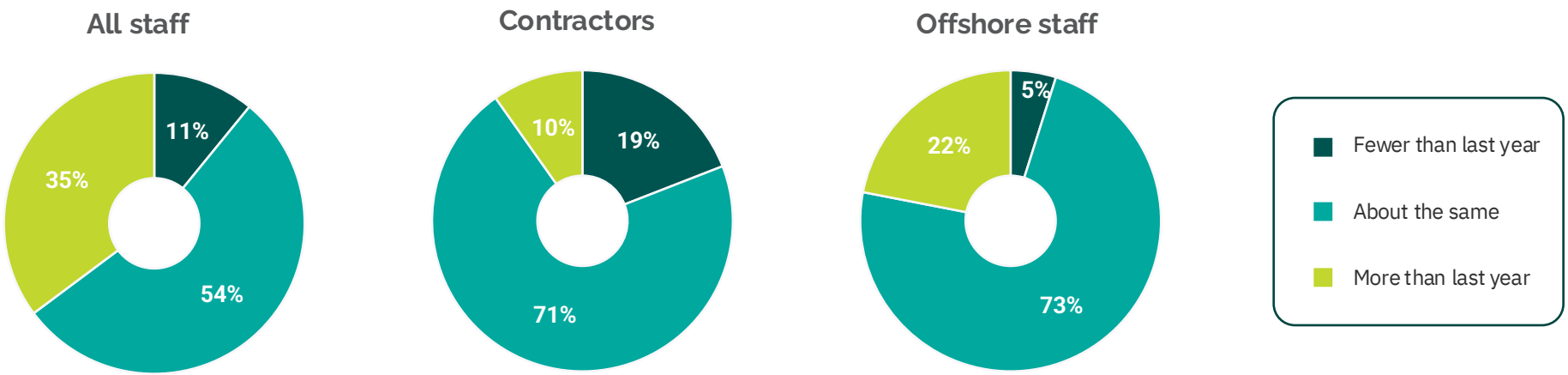
Staffing levels are expected to remain largely stable in 2026, with most organizations focused on maintaining current headcount while seeking efficiencies. Approximately 36% of respondents anticipate incremental staff increases, but large-scale hiring overhauls are uncommon. Significant layoffs or cuts at scale are unlikely. The impact is more pronounced for contractors, with 20% of CISOs projecting cuts to contractor staff, particularly at firms with more than $10 billion in revenue.

AI is increasingly viewed as a tool to extract more value from existing teams rather than a reason to reduce them.

> *"Parts of our program will be very mature, and there we're trying to find those incremental savings through efficiency. And then there are new emerging threats like AI that are going to drive new costs."*
>
> **— CISO, Retail & Apparel, $2B–$10B revenue**

Expected Staff Changes in 2026

How do you expect the number of information security FTEs, contractors, and offshore employees to change in the 2026 budget year?

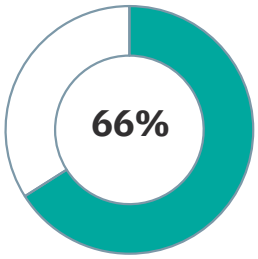


Security Program Maturity

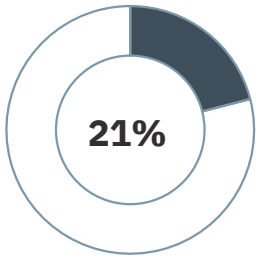
Maturity Frameworks Used

What frameworks do you use to measure program maturity? Multiple answers possible.

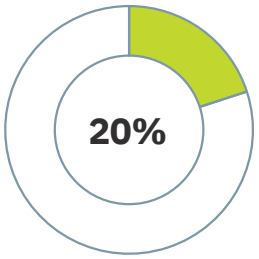
NIST CSF



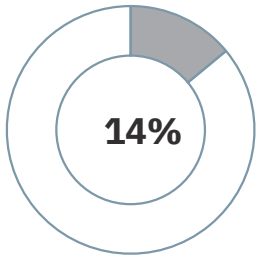
CIS 18



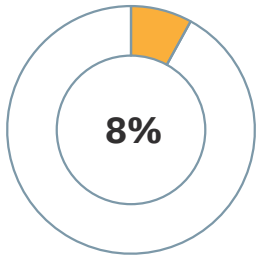
MITRE ATT&CK



ISO 27001



Other



CISOs project higher NIST maturity scores for 2026

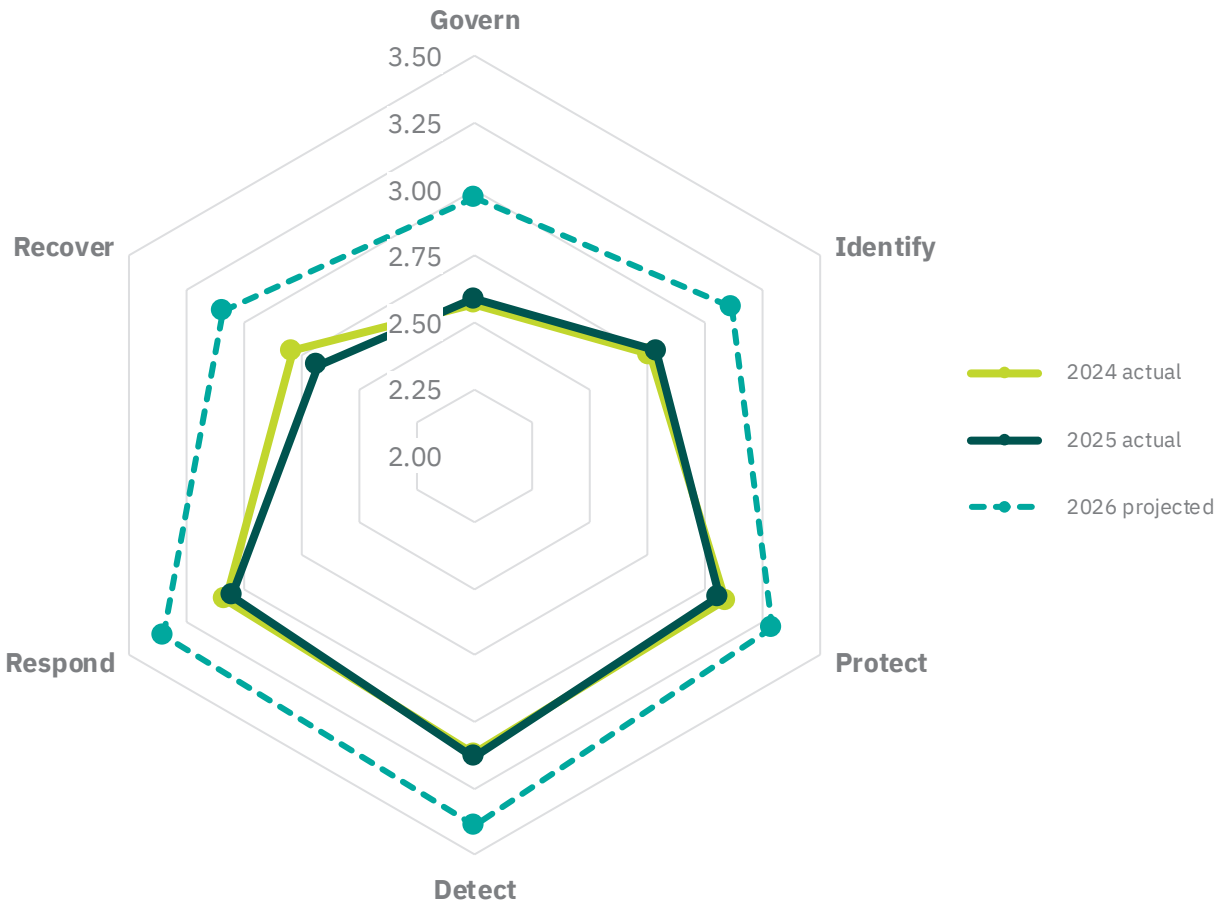
The data shows that organizations are seeking upward movement in the Govern function (which is new to NIST CSF 2.0), while there is less appetite for advancement in the Identify function. The areas seeing the most emphasis and investment are Detect and Protect, with incremental upward movement also noted in Respond and Recover.

"The focus on governance and identification may reflect the uncertainty that AI introduces, and because we can't yet fully build out protection controls, we're leaning more heavily into detection and recovery instead."

— CISO, Restaurant/Quick Service Restaurant, $2B–$10B revenue

Average NIST Maturity Scores: 2024 and 2025 Actual, 2026 Projected

Using the NIST Cybersecurity Framework, what is the relative maturity score (on a scale of 1.0-5.0) for your current security program and your projected security program in each of the following areas?



Methodology

This research is based on data from our proprietary annual CISO Benchmark Survey, launched in mid-December 2025. Of the 300 non-members were invited to participate in the survey, only 8 responded, resulting in a response rate of just 0.026%. On the members side, 193 out of 335 took the survey, giving us a completion rate of 57.6%.

A task force comprising RH-ISAC members and data scientists from RH-ISAC and IANS supported the research process, including survey design, respondent recruitment, and data hygiene and analysis. This report includes quotes and insights shared by members during a preliminary results webinar.

Sector Groups

Sector classifications reflect respondents' self-reported industry.

Retail & Commerce

Retail; e-commerce; third-party marketplaces; convenience stores; fuel retail; food retail; drug stores, pharmacies & health

Dining

Full-service restaurant; quick-service restaurant

Hospitality, Travel & Entertainment

Hotels; travel; entertainment, sports and media; casinos and gaming

Consumer Products & Services

Consumer packaged goods; consumer durables; consumer services; apparel

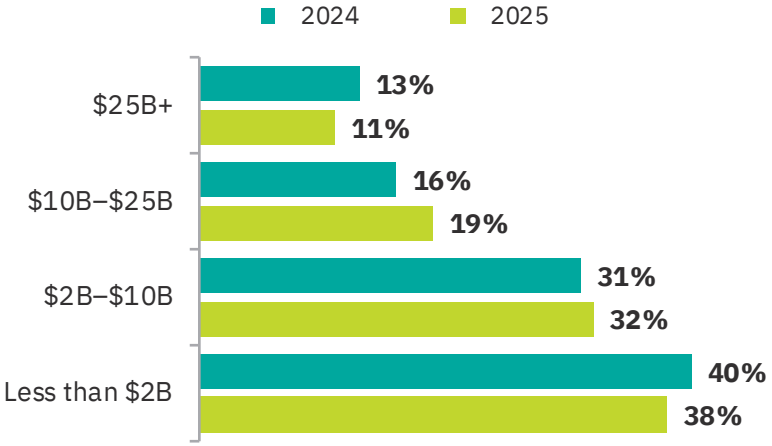
Specialty & Other

Customer loyalty and gift card programs; and other, including niche retail (jewelry, pets, luxury goods), food & beverage manufacturing/ wholesale, hospitality & entertainment (golf, ski resorts, spas), and real estate and fintech

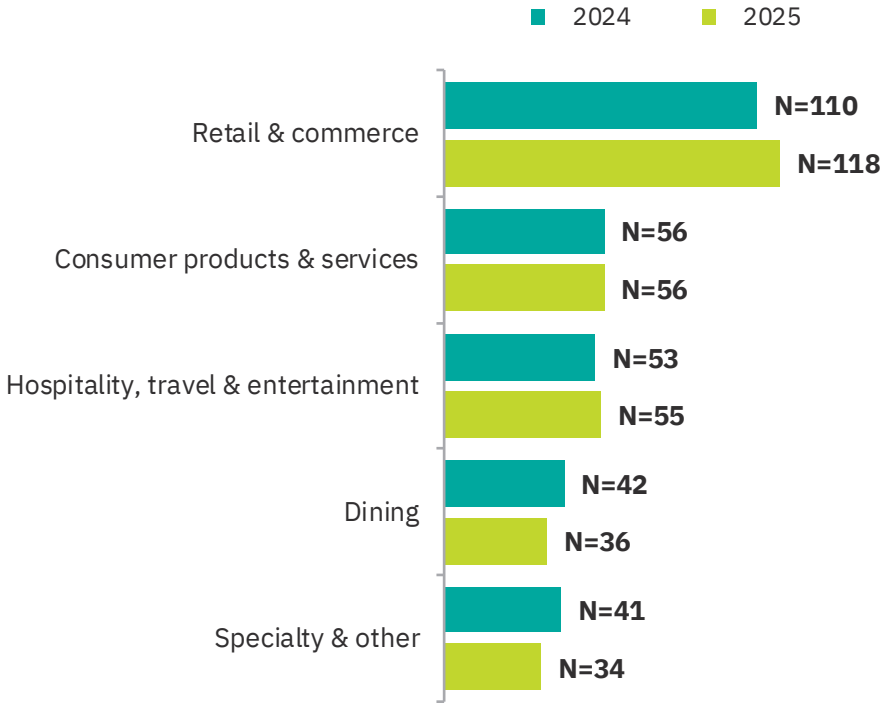
Sample Breakdown

Unique respondent organizations, by year

Breakdown by annual revenue



Respondent count by sector (multiple selections possible)



About Us

This publication is created in partnership among RH-ISAC and IANS.

IANS

For the security practitioner caught between rapidly evolving threats and demanding executives, IANS is a trusted resource to help CISOs and their teams make decisions and articulate risk. IANS provides experience-based insights from a network of seasoned practitioners through Ask-an-Expert inquiries, a peer community, deployment-focused reports, tools and templates, and executive development and consulting.
iansresearch.com

RH-ISAC

The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is the trusted community for sharing cybersecurity information and intelligence among retailers, restaurants, hotels, casinos, food retailers, consumer goods manufacturers, and other consumer-facing companies. RH-ISAC connects information security teams at the strategic, operational, and tactical levels to work together on issues and challenges, share timely and actionable threat intelligence, best practices, and benchmarks among each other – all with the goal of building better security for the retail and hospitality industries through collaboration.
rhisac.org