CISO BENCH MARK

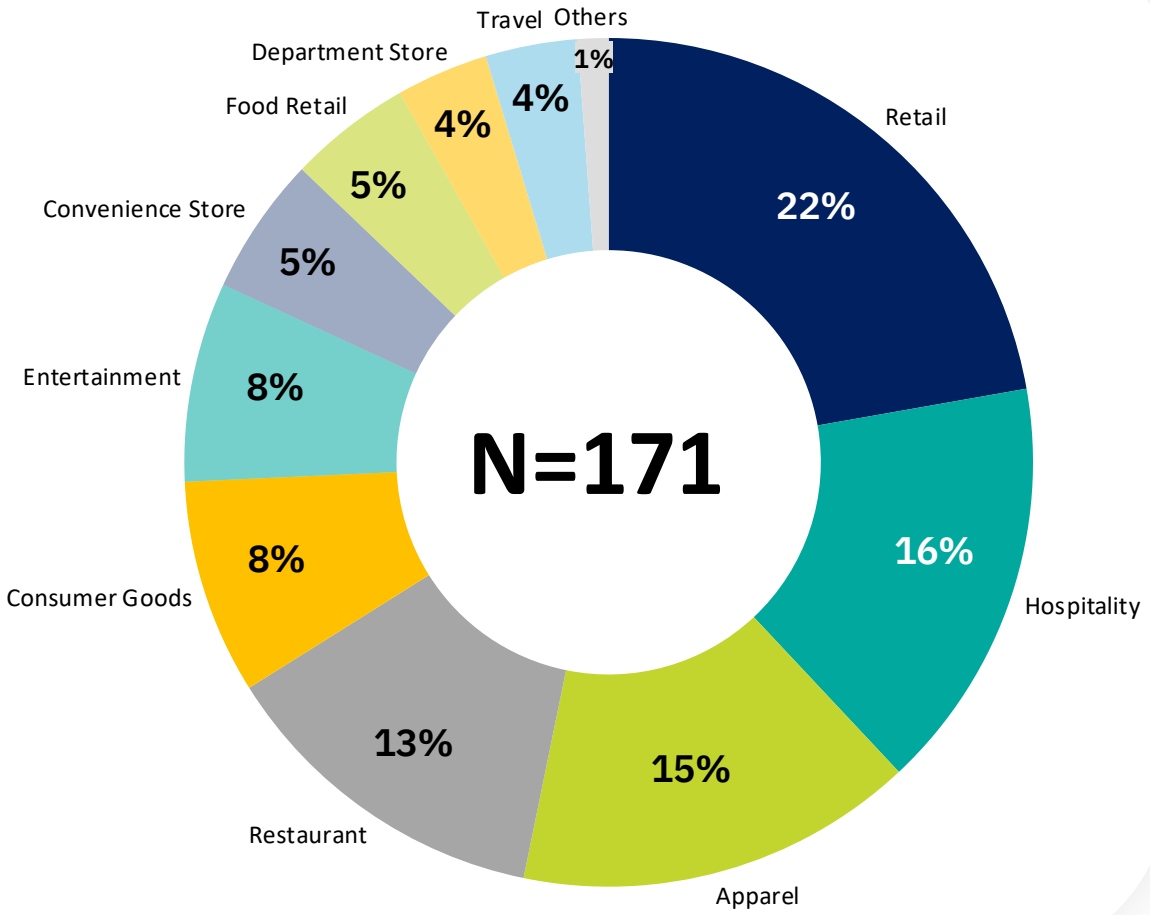
accenture | RETAIL & HOSPITALITY ISAC

TLP: CLEAR

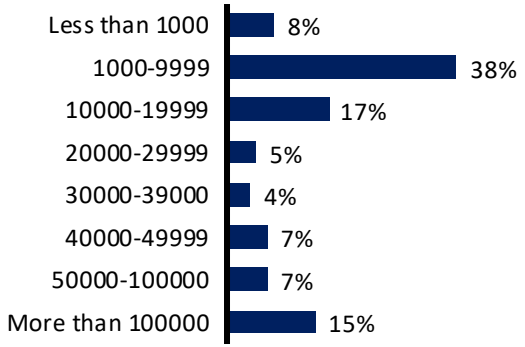
About the Research:

The 2025 RH-ISAC CISO Benchmark Report was developed in collaboration with Accenture and the RH-ISAC Taskforce. For this report we took a multi-method approach, utilizing the CISO survey. Sample size: 171 CISOs (32% increase YoY)

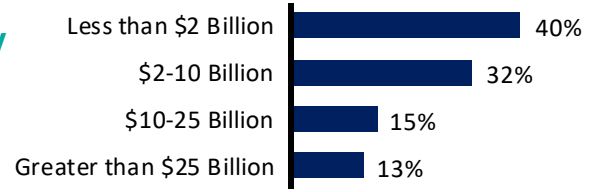
Participants by Industry Sector



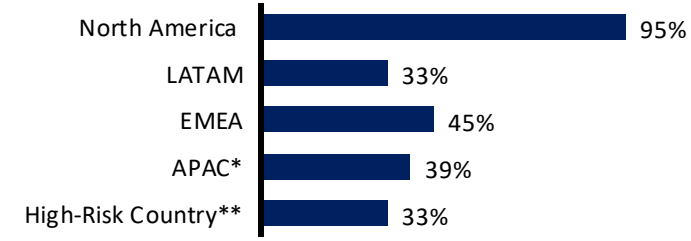
Participants by Total Employees



Participants by Revenue



Participants' Regional Coverage



RH-ISAC CISO Benchmark Survey (n=171); APAC* Non-high-risk countries; **high-risk countries: e.g., China, Hong Kong, Taiwan, Russia, Ukraine

By the Numbers: Key Highlights

Security Spending

Security spend rises with a steady budget outlook— third-party spend grows in priority

44% | **anticipating budget increases** and 43.6% foresee no change in 2026

11% | increase from 2024 on **third-party security services spending**

Security Workforce

Cybersecurity full-time employees expected to grow in 2025

38% | plan to **grow full-time cybersecurity staff** in 2025

44% | of InfoSec FTEs work on **IT, security operations, IAM, security engineering, GRC, or fraud prevention**

CISO Responsibilities

Cybersecurity as a business priority gaining momentum

12% | overall growth in **CISOs reporting to business** executives, rising from 7% in 2024 to 19% in 2025

26pp* | **rise in data management** as a CISO area of responsibility

Challenges & Opportunities

Ransomware & supply chain risks dominate, and business continuity takes priority

Top 3 | **Challenges** cited: **budget** constraints (**71%**), competing IT priorities (**69%**), and business demands (**45%**)

Top 2 | **Risks** cited: ransomware (**70%**) and supply chain attacks **(58%)**

51% | say **business continuity** is their top cybersecurity priority *(**up 4 places** from last year)*

NIST Adoption

NIST CSF dominates adoption, with scores rising steadily

25% | **rise in NIST scores** since 2024 to reach 3.1 on average across functions in 2025

83% | of organizations **adopt the NIST Cybersecurity Framework**

Benchmarking Survey Results

Benchmarking Coverage

1. Challenges & Opportunities
2. CISO Responsibilities
3. Security Spending
4. Security Workforce
5. NIST CSF Adoption

1. Challenges and Opportunities

Ransomware and supply chain risks dominate, while new threats emerge

The top three information security risks that retail & hospitality organizations face are:

#1 Ransomware/malware (70%)

#2 Third party/supply chain attacks (58%)

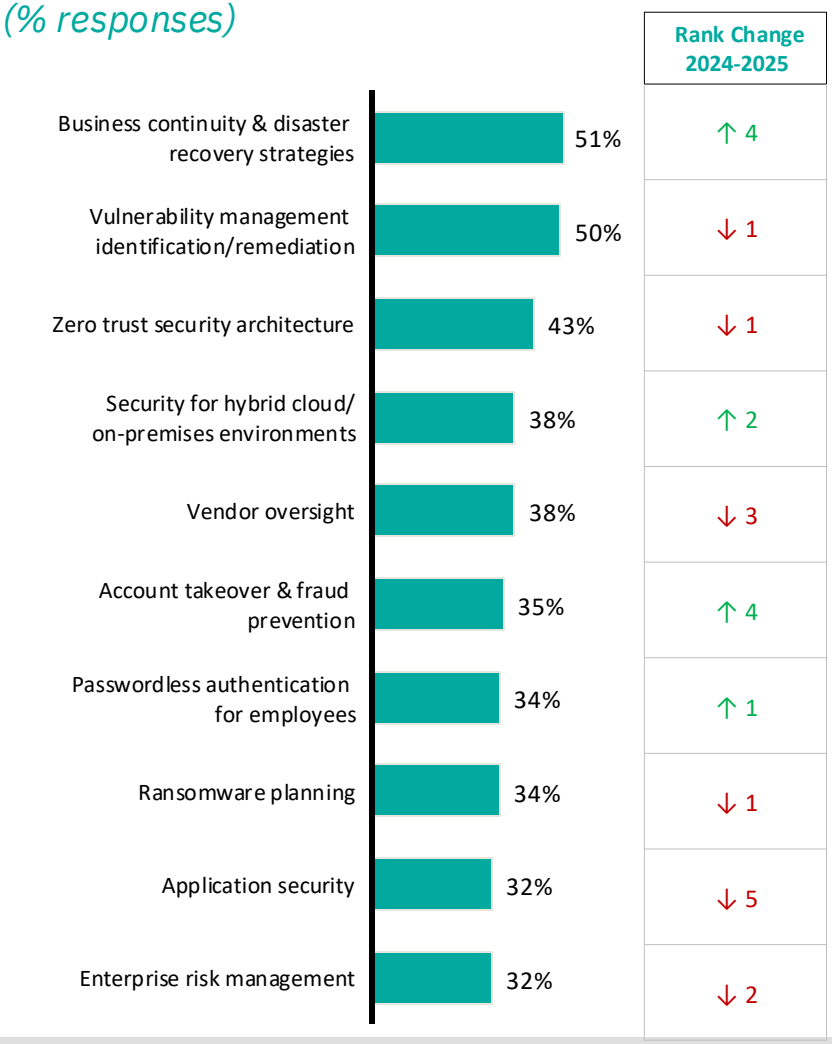
#3 Phishing (47%)

The top 10 cybersecurity initiatives have remained consistent from 2024 to 2025.

Business Continuity & Disaster Recovery now ranks #1 (up from #4 in 2024)

Top 10 key initiatives planned to mitigate risk

(% responses)



2. CISO Responsibilities

Data security gains traction

The top 5 priorities are consistently cited by over 90% of CISOs over the past year.

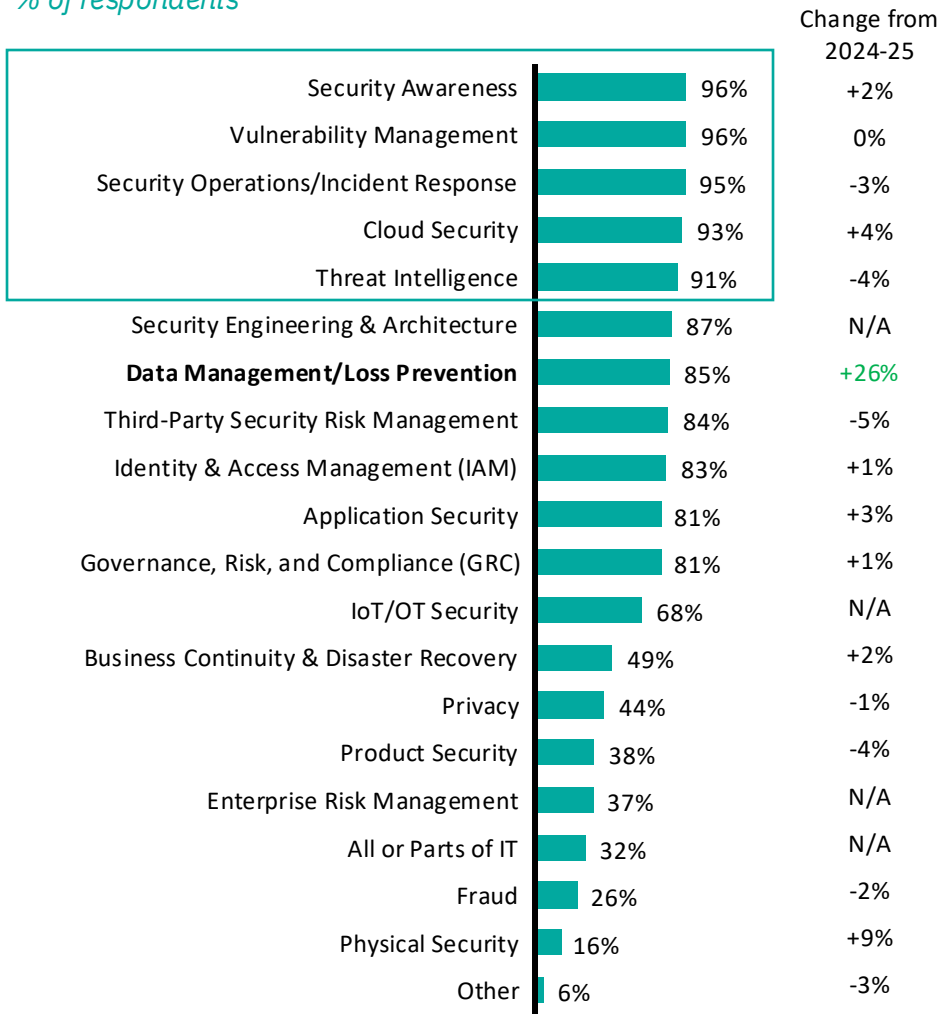
Shifting Focus Areas

- +26% increase in focus on Data Management & Loss Prevention, driven by AI adoption.

Cybersecurity as a business priority gaining momentum

- 12% overall growth in CISOs reporting to business executives, rising from 7% in 2024 to 19% in 2025
- 7% increase in CISOs reporting directly to the CEO and Board

Cybersecurity leadership roles have a wide range of responsibilities:
% of respondents



Other (member written): All parts of TechOps; Change management; CISO Chief of Staff; Consumer Trust & Safety; Cyber Risk Management; data security and DL; Records and Information Management, eDiscovery, Software Licensing Compliance; Red Team; SIEM & Logs

3. Budget & Spending

Security spend rises as resilience takes priority

4.2% Average annual IT spend as a % of revenue in 2025

Security spending remains stable: 42% allocate 4-7% of IT budget to cybersecurity, same as 2024.

Increased investment: 35% now spend 8%+ on security (6% increase from 2024).

Security Spend (% of IT Budget)

	2024	2025
0%-3%	20%	18%
4%-7%	41%	42%
8-10%	21%	22%
Greater than 10%	8%	13%
Don't Know	10%	5%

Budget outlook holds steady

Steady Investment Outlook

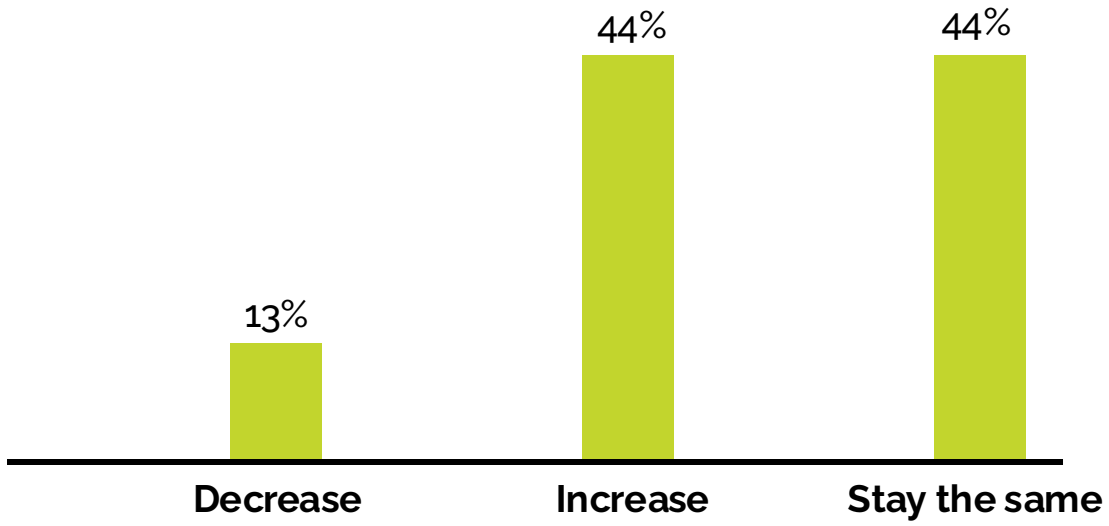
- **Only 13%** of organizations expect budget cuts in 2025.
- **44% expect an increase**, while another **44% foresee no change.**

Key Budget Drivers

- **Company growth, rising costs, and macroeconomic conditions** shape cybersecurity spending.

2026 Security Budget Outlook

*Q: Do you expect the information **security budget to view , decrease, or stay the same** next year?*



Spending Priorities: Workforce & Outsourcing

Cybersecurity spend priorities

Approximate breakdown of annual cybersecurity budget
(% responses)

Staff and compensation, including FTEs and contractors	33%
Software off-premises (e.g., cloud-based)	27%
Outsourcing, including on-going support contracts (e.g., MSSPs)	13%
Projects, including discrete consulting engagements (e.g., penetration testing)	8%
Software on-premises (e.g., in-house)	8%
Hardware (e.g., the portion of hardware attributable to security)	5%
Discretionary, including unexpected events (e.g., breach response)	4%
Training and development	3%

- **Workforce costs dominate** security spending, with **3%** allocated to training
- **Third-party security services** spending increased by **11%** from 2024.
- **Penetration testing & SOC** are the most outsourced services, reflecting reliance on external expertise.

Most common outsourced services	2024	2025
Penetration Testing	82%	83%
Security Operations Center	66%	66%
Managed Detection & Response	57%	57%
Threat Intelligence	41%	43%
Bug Bounty Program	18%	22%
Managed Vulnerability Management	13%	15%

Other outsourced services include: Assessments (NIST, PCI); External vulnerability scans; Firewalls; MSSP; Provisioning; Security tooling operations; IAM operations; SIEM; Third-Party Risk Management; User Access Management; Application Security

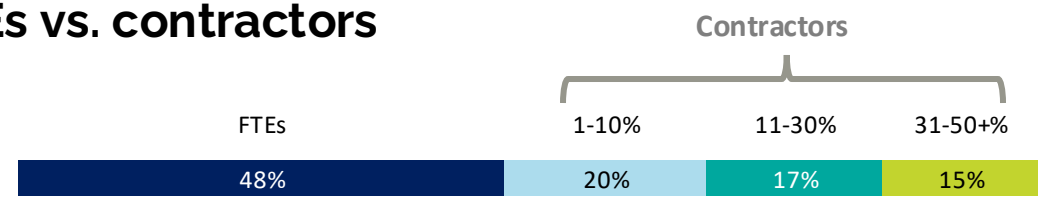
Please note: Totals may not equal exactly 100% due to rounding of decimal places.

4. Security Workforce

Workforce Outlook and Departmental Shifts

- **46% of CISOs foresee no departmental mergers** in the next 1–3 years.
- **38% of organizations plan to expand full-time** cybersecurity staff in 2025.

% of InfoSec team: FTEs vs. contractors



Do you expect the number of information security FTEs, contractors, and offshore employees to increase, decrease, or stay the same in the next budget year? *(% responses)*

Number of Total InfoSec FTEs in 2025	About the Same	58%
	Decrease	4%
	Increase	38%
Number of InfoSec Offshore Employees in 2025	About the Same	80%
	Decrease	3%
	Increase	17%
Number of InfoSec Contractors in 2025	About the Same	70%
	Decrease	11%
	Increase	18%

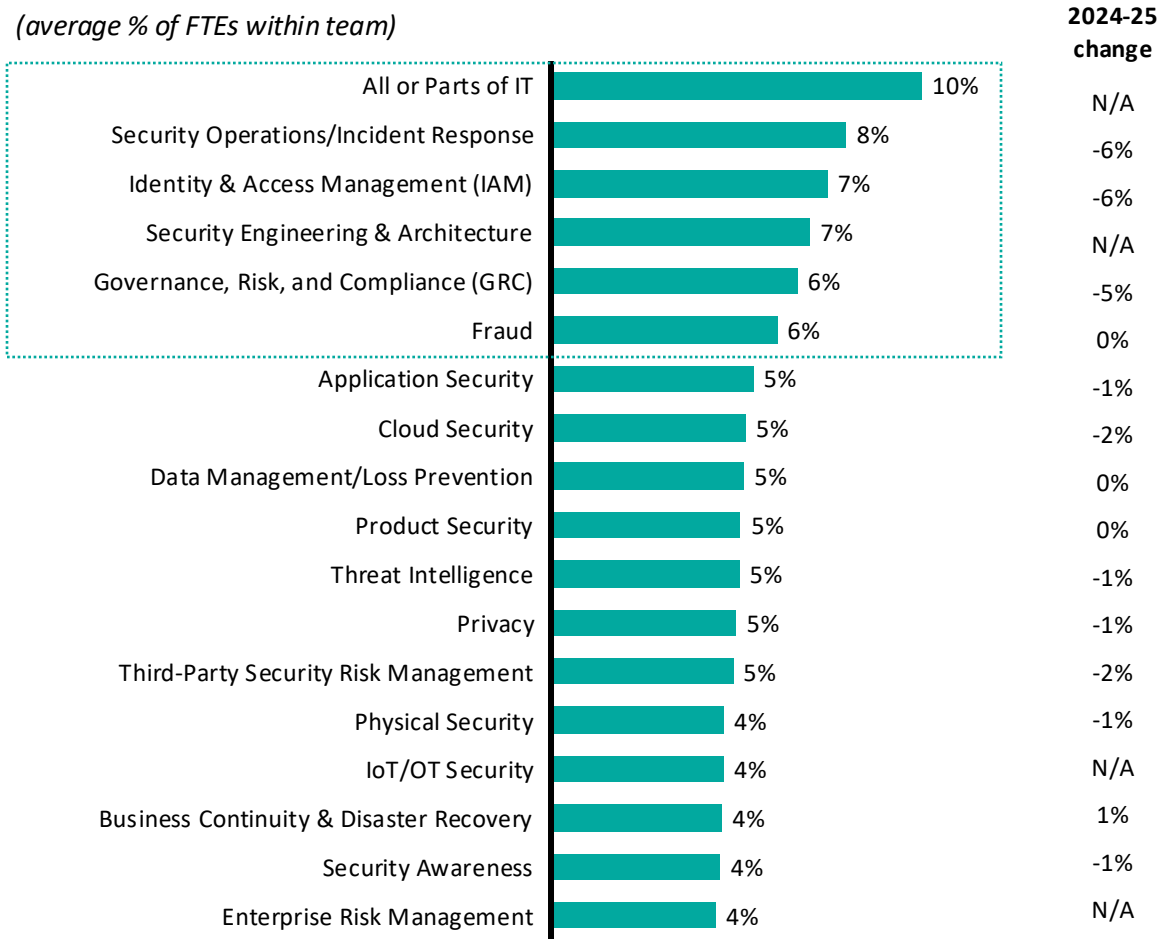
Key roles in security teams

- Largest resource allocation **(44%)** to IT, security operations, IAM, security engineering, GRC, and fraud prevention.

- **Third-party & supply chain** attacks rank as the **#2 cybersecurity risk**, yet **FTE allocations** to this area **dropped** by 2 percentage points from 2024.

InfoSec FTEs are dedicated to the following roles:

(average % of FTEs within team)



2024-25 change
N/A
-6%
-6%
N/A
-5%
0%
-1%
-2%
0%
0%
-1%
-1%
-2%
-1%
N/A
1%
-1%
N/A

5. NIST CSF Adoption

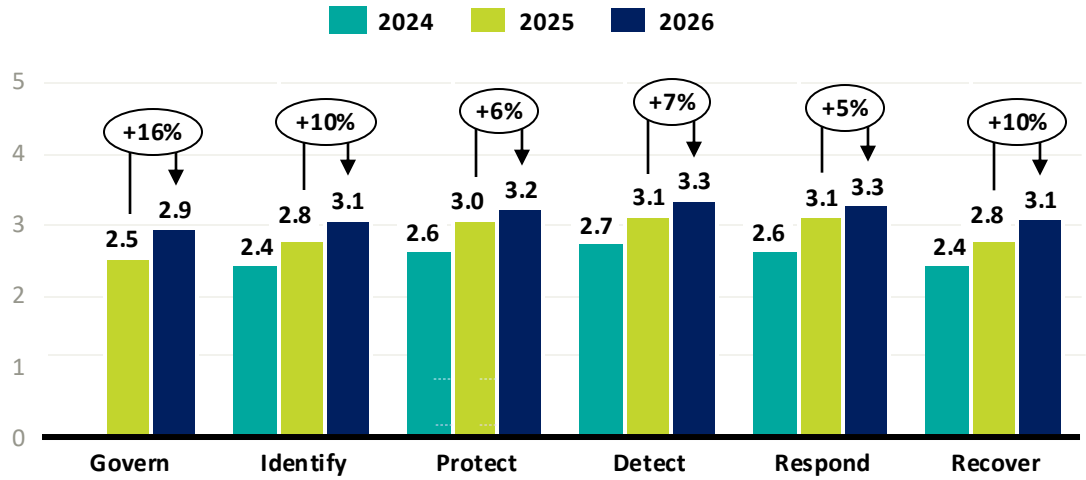
NIST CSF dominates adoption, with scores rising steadily

83% of organizations adopt the **NIST Cybersecurity Framework (CSF), thus it remains the dominant standard** for assessing cybersecurity maturity.

25% **rise in NIST CSF scores** (2024-2026), with 8% growth from 2025.

NIST Maturity scores trend

(average response)



Key Takeaways

Influence Cybersecurity as a Strategic Business Priority

Champion cybersecurity as a core business driver to strengthen resilience and business impact.

- **Strengthen C-suite accountability** by aligning cybersecurity with broader business goals, ensuring executives—including CEOs, CFOs, and COOs—**share responsibility for risk management.**
- **Enhance collaboration** across technology, security, and business teams to position security as a driver for **competitive differentiation.**
- **Drive measurable impact** by advocating for shared performance metrics that track security integration from design to deployment.

Secure and Scale AI and Cybersecurity-as-a-Service

CISOs must leverage AI-driven automation and managed security services to enhance efficiency, resilience, and scalability.

- **Deploy AI-powered defenses to strengthen security postures**, using automated threat testing (e.g., red teaming, penetration testing) as AI-driven attacks grow more sophisticated.
- **Augment security with generative AI**, automating and augmenting security tasks to **boost efficiency and effectiveness.**
- **Adopt Cybersecurity-as-a-Service (CSaaS) to scale security operations, reduce complexity**, and shift focus from security management to **innovation.**