accenture | RETAIL & HOSPITALITY ISAC

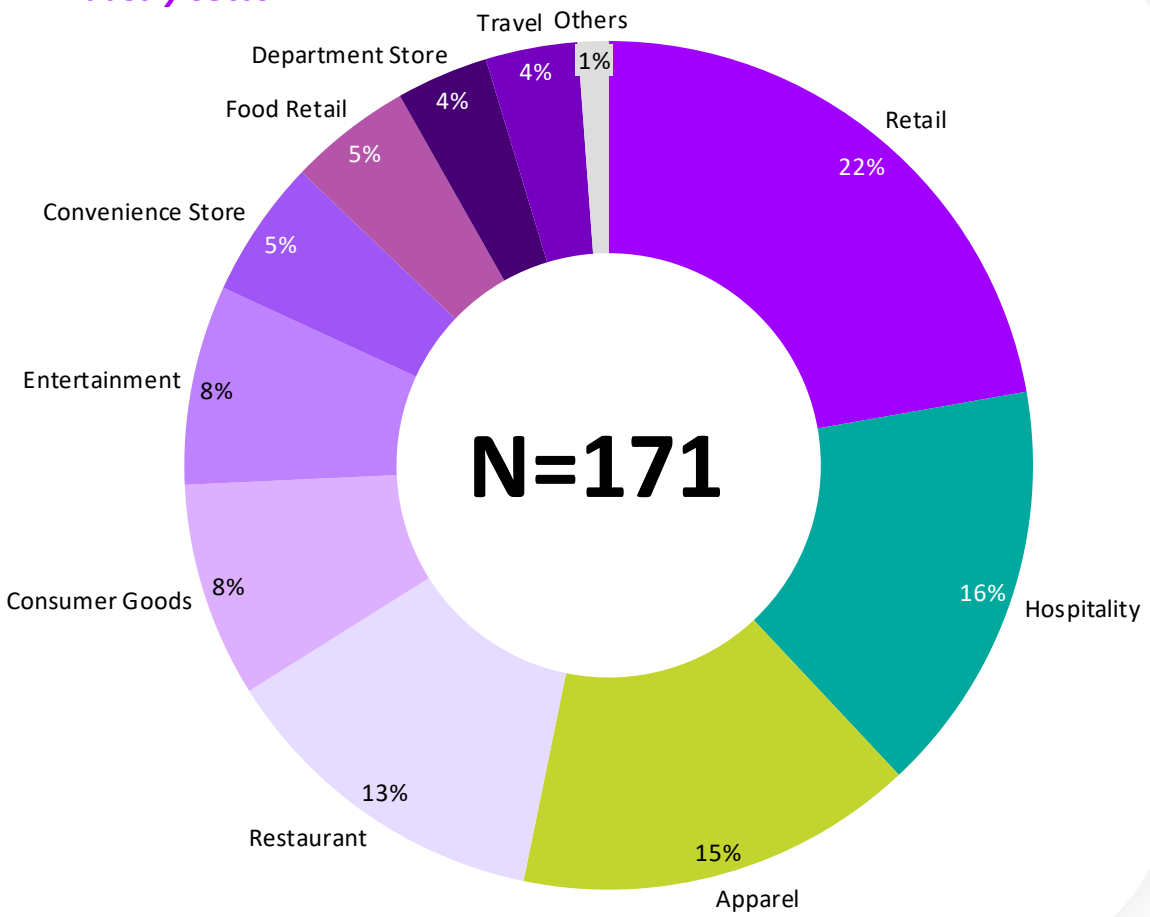
2025 CISO Benchmark Report

Securing the Digital Foundation for Reinvention

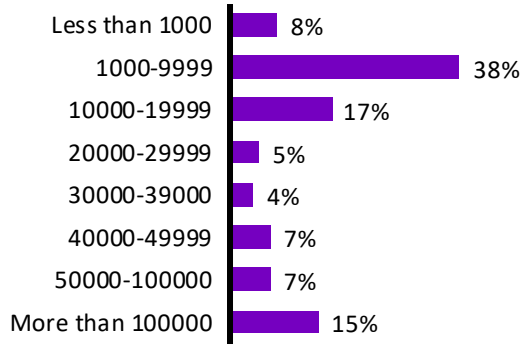
About the Research:

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, economic modelling and insights drawn from additional sources with Reinventing with a Digital Core as a key tenet. **Sample size: 171 CISOs (32% increase YoY)**

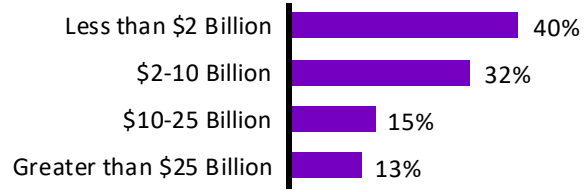
Participants by Industry Sector



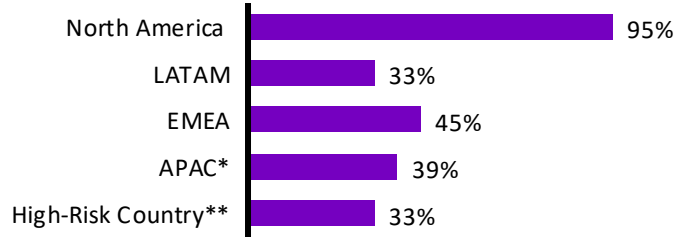
Participants by Total Employees



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

Digital Core Security Maturity

Security maturity gaps persist leaving businesses exposed, while Frontrunners improve tech debt

82% | of companies lack strong **security maturity of their digital core**

2.5X | greater **reduction in technical debt** for Frontrunners over peers, plus **60:40 revenue and profit growth**

30% | average **NIST scores improvement** for those with a secure digital core

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 as Frontrunners set the pace

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

12% | higher— In 2024, **Frontrunners outperformed** the rest across all NIST functions scoring 3.2, a trend set to continue in 2025 to reach an average of 3.5

*pp = percentage point

We've entered an era of radical disruption and unprecedented technological reinvention

75% of retail & hospitality companies are speeding up their reinvention efforts[1]

91% of retail and hospitality companies acknowledge that the accessibility of new technologies like generative AI is amplifying cyber threats.[3]

223% increase seen in the trade of deepfake-related tools on dark web forums between Q1 2023 and Q1 2025.[5]

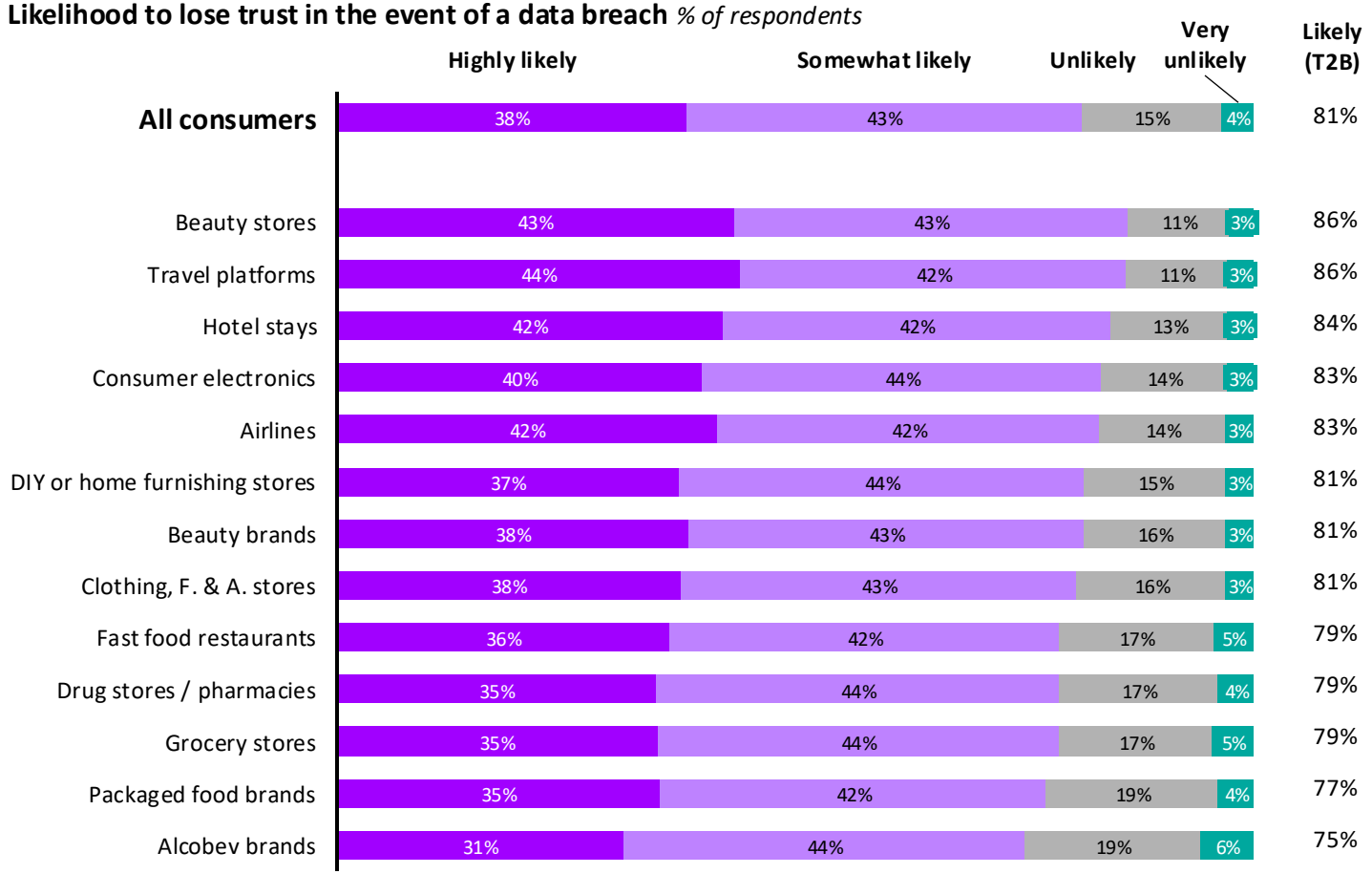
However, while technology fuels reinvention, it also introduces new vulnerabilities, expanding the attack surface for opportunistic actors

The high cost of security failures–financial losses, damaged reputations, and trust erosion

Billions in financial loses, damage to brand reputation, and a deep erosion of customer trust

81% of consumers would lose trust in a brand if a data breach compromised their personal information

Likelihood to lose trust in the event of a data breach *% of respondents*



A security maturity gap exists, amplifying risks and limiting resilience

A **Digital Core** is a foundation that integrates advanced platforms, AI-driven cybersecurity, and zero-trust architectures. We developed an **index** (scored 0–100) to assess **digital core security maturity**.

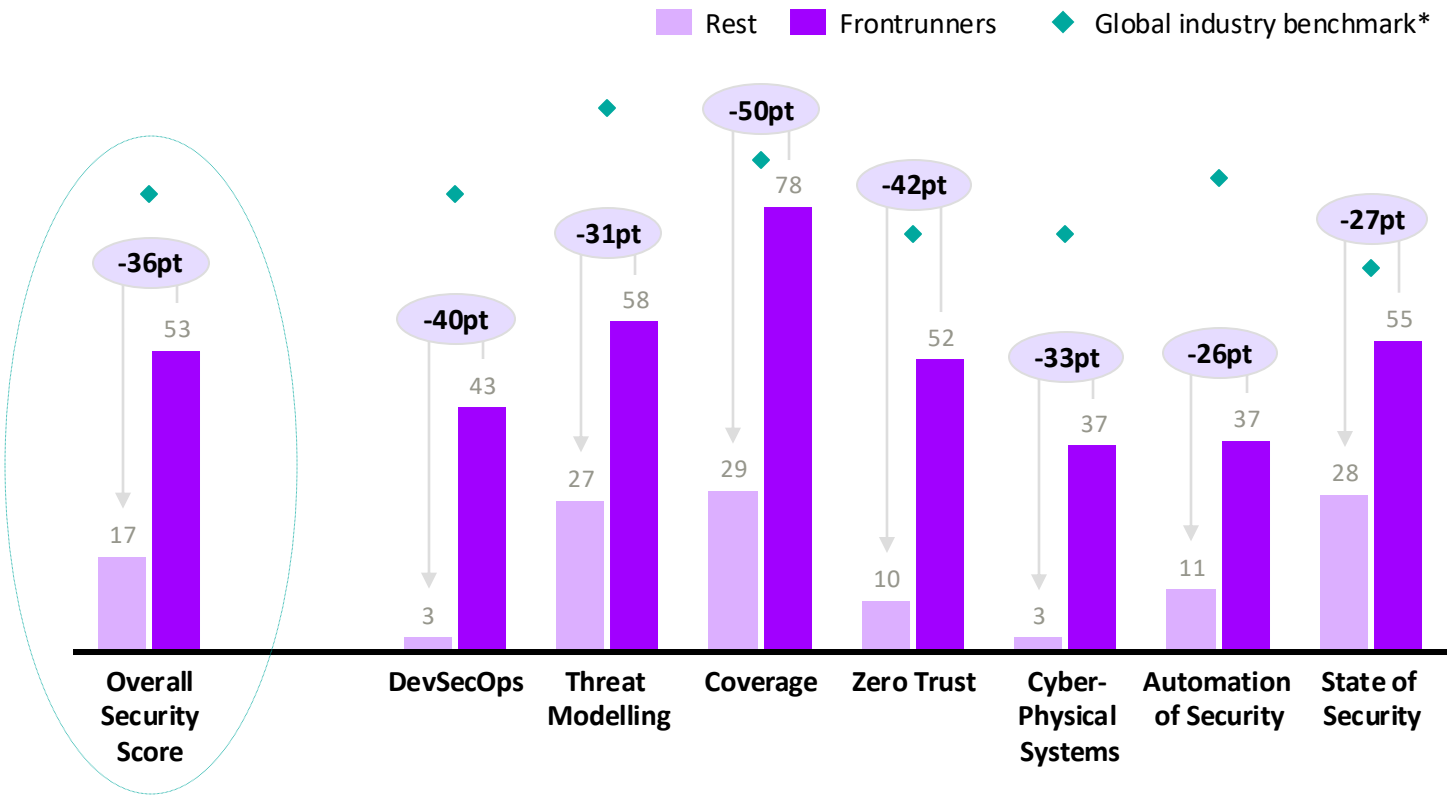
18% of companies emerged as **Frontrunners**, and **outperform** the Rest (82%) of the sample by **36 index points**.

The secure digital core advantage

Organizations with strong digital core capabilities experience:

- **60%** higher revenue growth & **40%** higher profitability ("60:40 Effect")
- **2.5x** greater reduction in technical debt
- **30%** improvement in NIST scores

Digital Core Security Maturity Scores



RH-ISAC CISO Benchmark Survey (n=171); Frontrunners (n=30 (18%))

Frontrunners breakdown: retail (20%); hospitality (16.7%); restaurant (16.7%); consumer goods (13.3%); food retail (10%); apparel (6.7%); entertainment (6.7%); department stores (3.3%); travel (3.3%); others (3.3%)

*Grouping includes retail, hospitality, as well as airlines, travel & transportation industries (industry leaders n=32 (16%); industry sample n=195)[8,9]

However, many struggle to secure the digital core by design

The top three barriers cited by cybersecurity leaders include:		
71%	**69%**	**45%**
Budget Constraints	Cyber vs IT prioritization challenges	Speed of business requirements

Benchmarking Excellence

Benchmark comparison against **industry Frontrunners and year-over-year trends**.

Benchmarking Coverage

1. Challenges & Opportunities
2. CISO Responsibilities
3. 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%)

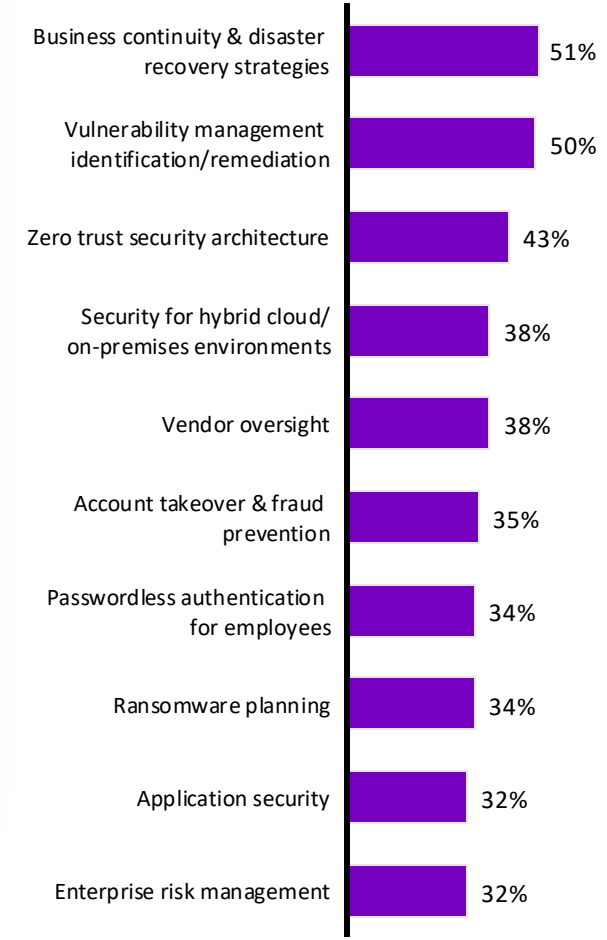
#3 Phishing (47%)

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

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

2025: Top 10 key initiatives planned to mitigate risk

(% responses)



	Rank change 2024-25	Frontrunner rank	Rest Rank
Business continuity & disaster recovery strategies	↑ 4	2	1
Vulnerability management identification/remediation	↓ 1	1	2
Zero trust security architecture	↓ 1	3	3
Security for hybrid cloud/ on-premises environments	↑ 2	9	4
Vendor oversight	↓ 3	6	5
Account takeover & fraud prevention	↑ 4	4	6
Passwordless authentication for employees	↑ 1	5	9
Ransomware planning	↓ 1	6	8
Application security	↓ 5	11	7
Enterprise risk management	↓ 2	7	10

2. CISO responsibilities

Data security gains traction and Frontrunners lead in product security

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

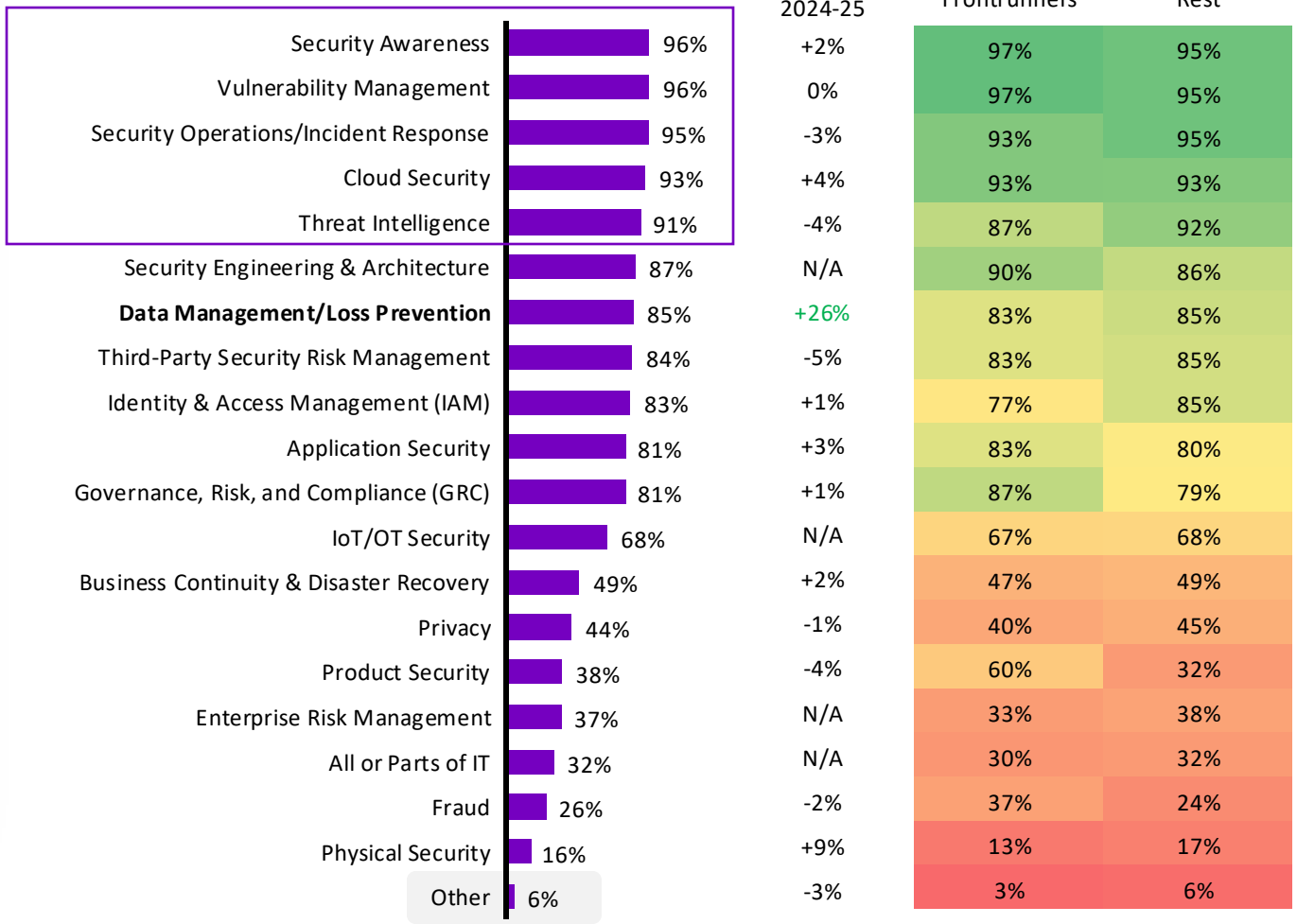
Shifting Focus Areas

- **+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. NIST CSF Adoption

NIST CSF dominates adoption, with scores rising steadily as Frontrunners set the pace

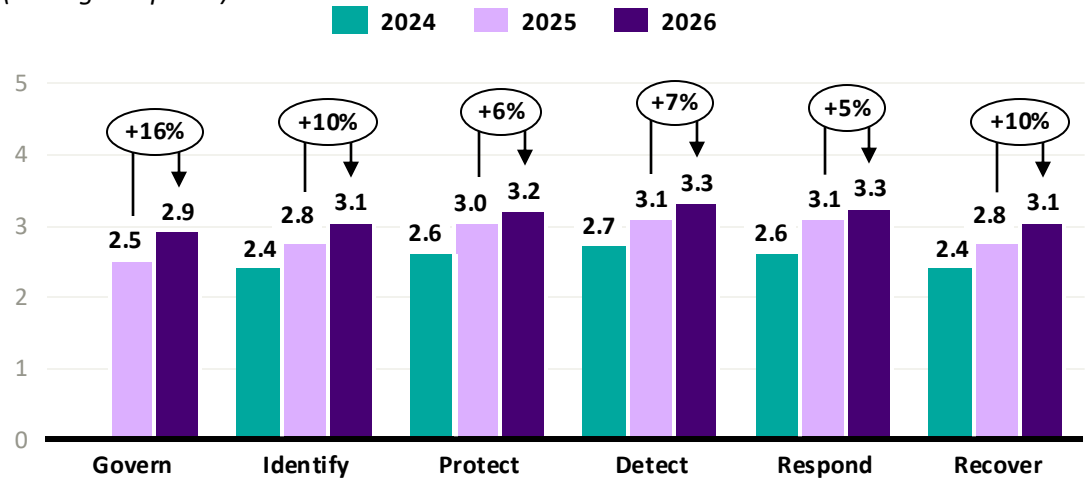
83% of organization adopt the **NIST Cybersecurity Framework (CSF), thus it remains the dominant standard** for assessing cybersecurity maturity.

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

12% higher — In 2025, **Frontrunners outperformed** the rest across all NIST functions scoring 3.2, a trend set to continue in 2026 to reach an average of 3.5

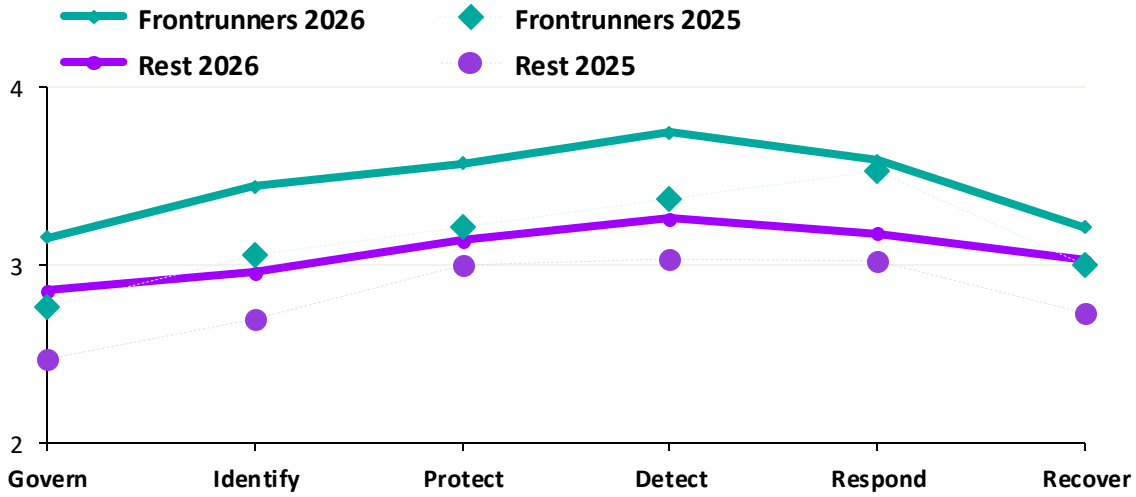
NIST Maturity scores trend

(average response)



Current & projected NIST Maturity scores: Frontrunners vs Rest

(average response)



Key takeaways

Secure the Digital Core

A secure digital core is more than protection—it enables business growth, trust and long-term success. To enable continuous reinvention and resilience, fortify the digital core with security at the foundation.

- **Close the security maturity gap** by securing data, AI, and cyber-physical systems, and adopting zero-trust principles.
- **Strengthen cloud security** by integrating security across the entire Cloud-Native Application Protection (CNAPP) ecosystem.
- **Reduce technical debt** by modernizing outdated systems, retiring legacy tools, and investing in best-in-class solutions and automation to enhance security and agility.

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.**

Access the full interactive version of this report to customize insights by company size and industry

The full interactive benchmark is only available to RH-ISAC core members.

RH-ISAC members can access this in Member Exchange.

Not a member? Learn more about how to join at rhis.ac/Join

Copyright © 2025 Accenture. All rights reserved.