TLP: CLEAR

RETAIL & HOSPITALITY ISAC

Booz | Allen | Hamilton®

BENCH MARK

CISO

JANUARY 2024

TABLE OF CONTENTS

INTRODUCTION

The RH-ISAC CISO Benchmark Task Force partnered with Booz Allen Hamilton to facilitate the survey and analysis of this year's report. Information security teams have always had to do more with less, but 2024 looks to be the year where they get more and can hopefully do more. Riding a three-year trend, 56% of CISOs expect their budgets to increase again this year, while 60% also expect more FTEs. This isn't the case for all though, as roughly 10% are expecting budget cuts.

The continued rise in spending during challenging budgetary pressures signals a greater business understanding of the risks and is reflected in the projected improvements in program maturity. This year, CISOs are prioritizing vulnerability management as one of the top focus areas that can reduce Ransomware/Malware threats.

Zero trust architecture emerged as the second top initiative that CISOs are focused on in 2024, accounting for an uptick in headcount aligned to Infrastructure and Fraud. Conversely, there was a reduction in staff dedicated to Security Operations/Incident Response, which remained a top outsourced service due to the rising need for security analytics and fraud detection capabilities.

We hope you use this data to bolster your own security programs and connect with peers who share similar concerns and interests based on common revenue or sectors served.

Specifically, this report can guide your decision making when it comes to justifying budget allocation across personnel (up from last year), tools (same as last year), technology (up from last year), and third-party services. You can also check out the NIST maturity analysis, where across all revenue segments, CISOs expect to improve their programs, most notably in the Recover category.

Our two special topics this year – Generative AI and the new SEC requirements – did not appear to be a major concern for security leaders. Of the two, Generative AI presented a higher concern and is quickly gaining steam as a business enabler; however, security teams can play a leading role in informing the business of the risks involved in adoption. Conversely, the SEC requirements are of lesser concern as members are consulting with executive leaders to review existing plans.

Thank you to everyone who completed the survey - the most participation we've ever had! With your help, this report provides a significant snapshot of security programs and priorities for the sectors this community serves.

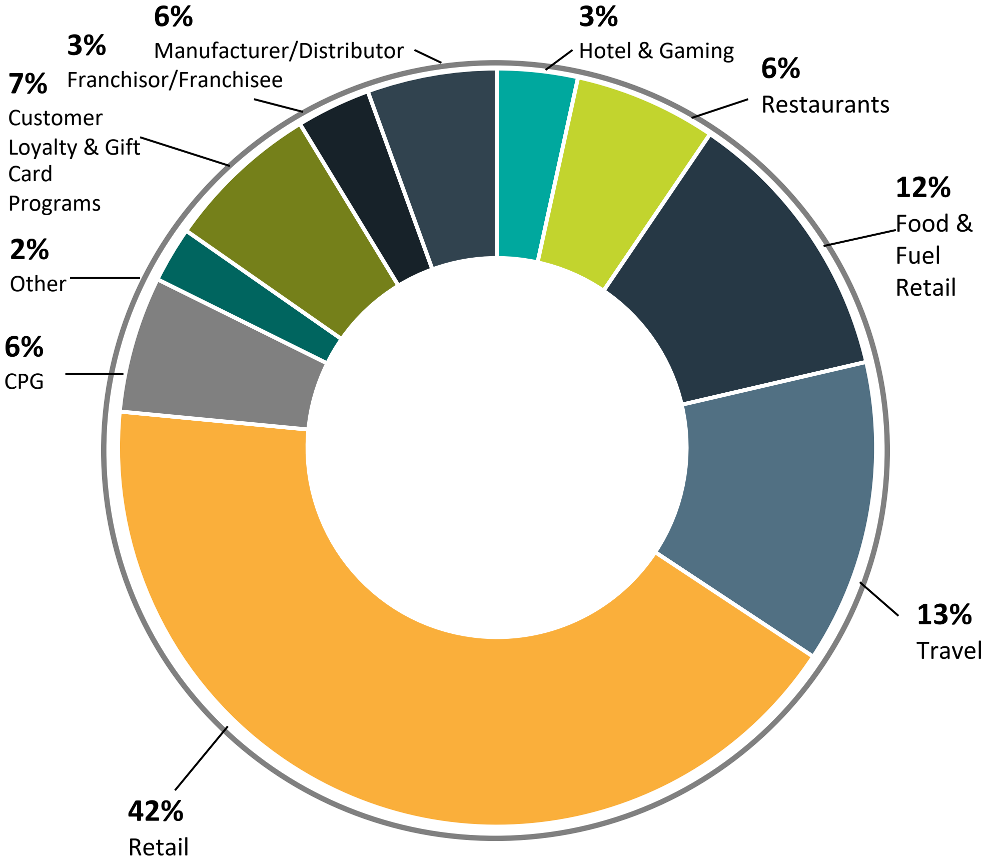
—The RH-ISAC CISO Benchmark Task Force & Booz Allen Hamilton

SURVEY DEMOGRAPHICS

The RH-ISAC completed its fifth annual CISO Benchmark Survey in October 2023. It was fielded in September and October 2023 and generated 133 unique responses; a 6% increase in participation compared to the previous year.

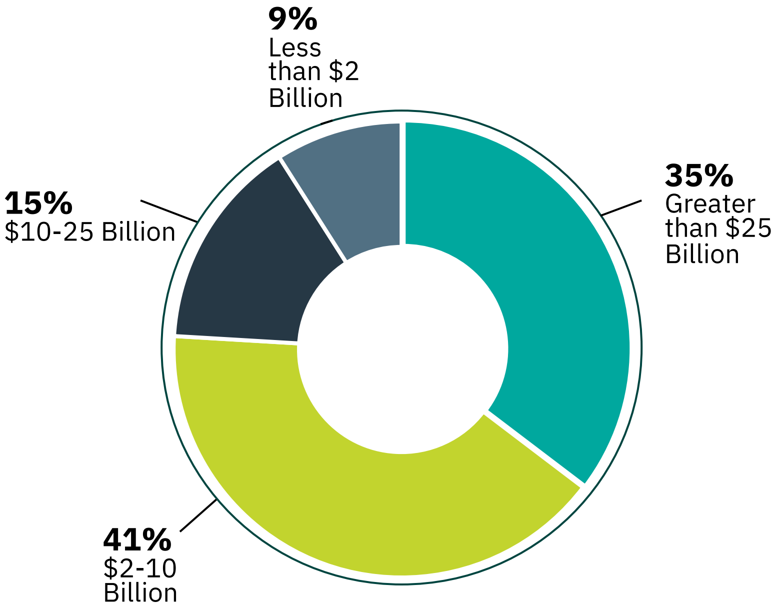
Participants by Industry Sector

The classes of trade represented in the 2023 survey have been expanded from the 2022 report, with more than one selection allowed. The complex nature of member businesses was reflected by 61% selecting more than one class of trade.



Participants by Annual Revenue

There was an even split in revenue representation, with 50% of participants generating more than $10 billion in annual revenue and 50% generating less.



The companies represented in this survey reflect:

- 91% have an eCommerce presence
- 28-33% of annual revenue from eCommerce
- eCommerce revenue is expected to increase in 2024
- 2.3 million corporate employees
- 3.7 million people connected to networks
- 718,000 locations

SUMMARY OF INDUSTRY FINDINGS

High-level observations on budget and staffing, operational metrics, NIST maturity, and special topics

Spend

- Average IT budget dedicated to Information Security increased **to 8-10%** this year.
- FTEs dedicated to Infrastructure and Fraud have seen an **uptick with the rise** of AI.

Operational

- CISOs predominantly concerned with risks related to **risk management** and **threat intelligence.**
- CISOs are prioritizing **vulnerability management** to mitigate some of the potential operational risk.

NIST Organizational Maturity

- Retail & Hospitality is **overall below-average maturity** in NIST CSF scoring compared to other industry verticals such as Financial Services, Energy, Consumer Goods, and Healthcare/Pharma.
- NIST maturity for Retail & Hospitality is **projected to improve to 3.0 in 2024** compared to 2.5 in 2023.

Special Topics

- CISOs are **moderately concerned about AI** as primary uses are in customer/business analytics or customer engagement .
- CISOs are only **slightly concerned with SEC requirements**, with many already working with senior leadership to review/update existing plans.

SUMMARY OF FINDINGS

This report helps cybersecurity leaders understand how RH-ISAC peers are allocating their budget and resources.

BUDGET OVERVIEW

Up from last year, a typical RH-ISAC member has **8-10% of the IT budget dedicated** to information security and is allocated in the following ways:

- Personnel – 21-30%
- Tools & Technology – 41-50%
- Third-Party Services – 10% or Less

Most Common Out-Sourced Services

Pen Testing – 83%

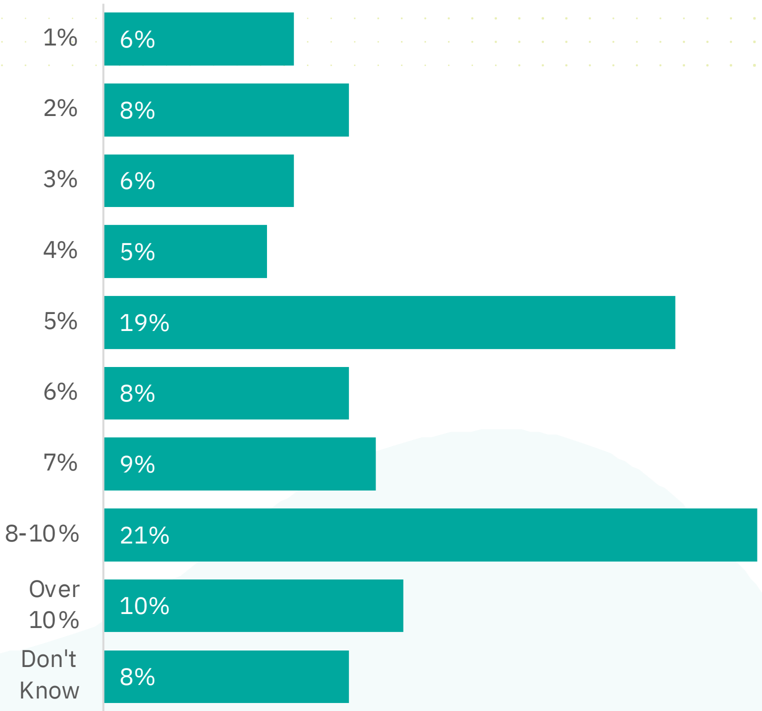
Managed Detection & Response– 53%

Security Operations Center – 50%

Threat Intelligence – 37%

Budget Range

The more detailed analysis this year in the chart below shows the range of budgets in the RH- ISAC community.



Budget Trends

- **56%** of of CISOs (down from 70% last year) expect their information security budget to **increase** in 2024.
- Almost **10%** of CISOs (up from 4% last year) **expect budget cuts** in 2024.

PERSONNEL OVERVIEW

The **average size of an information security team has grown to 26-99 FTEs this year**, including fewer than 5% offshore employees and 5-10% contractors. Interestingly, 70% do not have offshore employees, and 54% do not work with contractors.

Personnel Trends

InfoSec Team Sizes are Increasing

- Like last year, **60%** of CISOs expect their **FTE count to grow in 2024**. Only 3% expect a staff reduction.

InfoSec Staff Roles are Changing

- Increase in FTEs dedicated to Infrastructure and Fraud due to rise in AI.
- Increase in Physical Security FTEs
- Decrease in staff dedicated to Security Operations/Incident Response due to improvements in security analytics.

Personnel Allocation

Information Security FTEs are dedicated to the following roles:

3 – 5 FTEs

- **Fraud (up from last year)**
- Governance, Risk & Compliance (GRC)
- Identity & Access Management (IAM)
- **Infrastructure (up from last year)**
- **Physical Security (up from last year)**
- Security Operations/Incident Response
- Tools & Integrations (e.g., TIP, EDR, SIEM, SOAR, etc.)

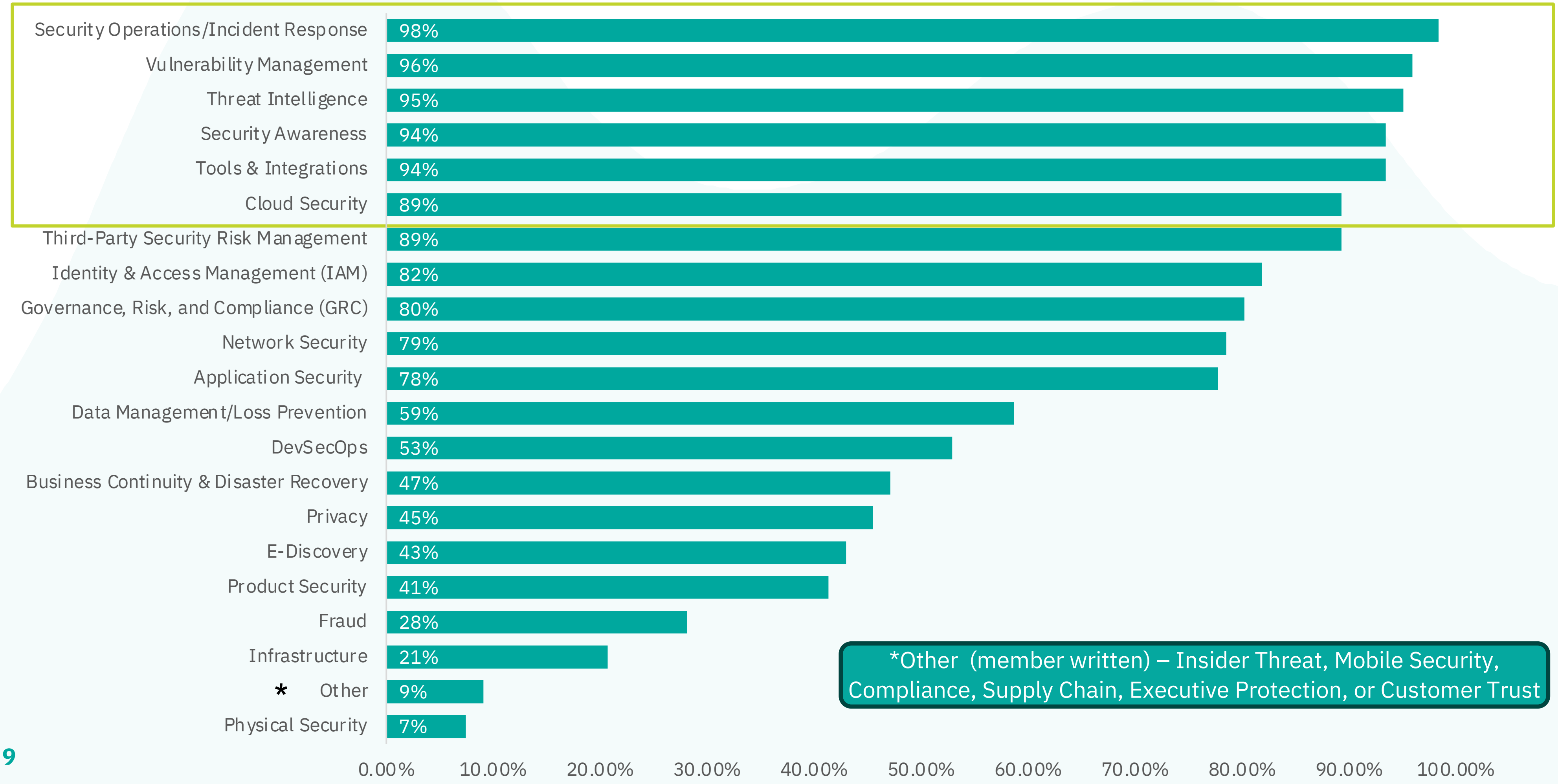
1 – 2 FTEs

- Application Security
- Business Continuity & Disaster Recovery
- Cloud Security
- Data Management/Data Loss Prevention
- DevSecOps
- **E-Discovery (up from last year)**
- Network Security
- Privacy
- Product Security
- Security Awareness
- Third-Party Risk Management
- Threat Intelligence
- Vulnerability Management

RESPONSIBILITIES OF CISOS

Cybersecurity leaders have a wide range of responsibilities, but the top seven remain the same as the past two years – all of which 89% of CISOs have as part of their key responsibilities. Some minor changes have happened in the past year in existing responsibilities:

- » Fraud increased by 7 percentage points, up to 28%
- » Data Management/Loss Prevention decreased by 12 percentage points, down to 59%
- » Physical Security decreased by 7 percentage points, down to 7%

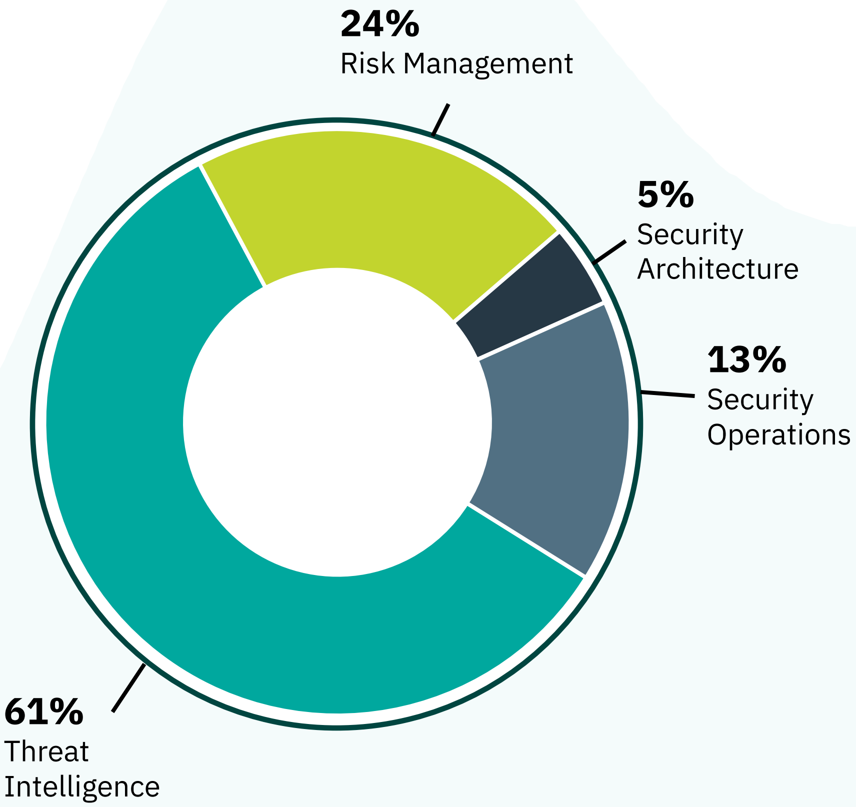


*Other (member written) – Insider Threat, Mobile Security, Compliance, Supply Chain, Executive Protection, or Customer Trust

ORGANIZATIONAL RISKS

Top Risks by Category

This year CISOs cited more than 350 organizational risks, **but most are concerned about risks related to threat intelligence (61%),** specifically ransomware and phishing; and **risk management (24%)**, specifically third-party/supply chain attacks.



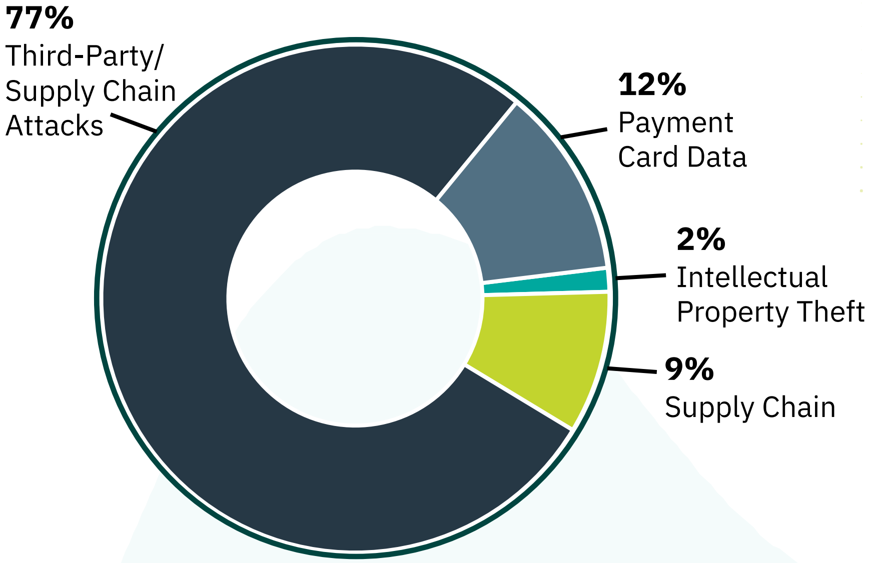
Top 10 Risks

Regardless of category, here are the top 10 risks CISOs said their organizations currently face:

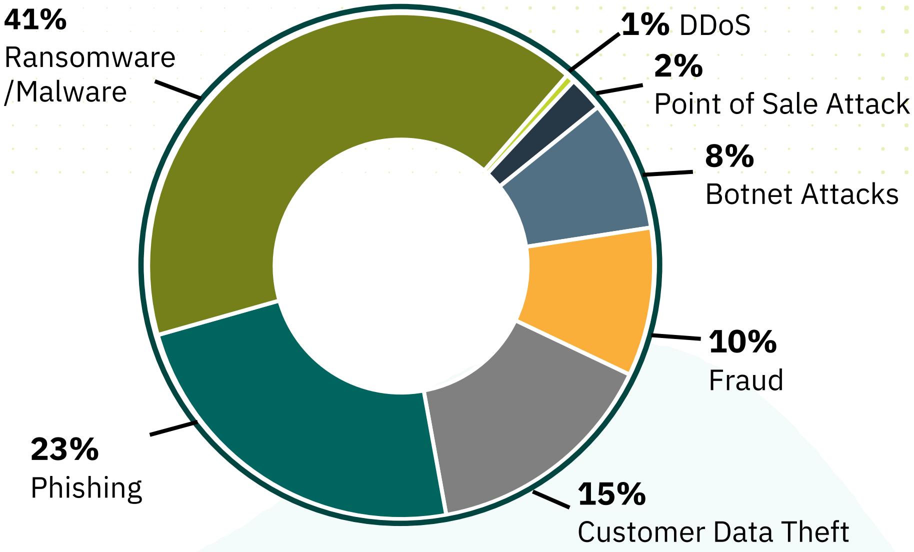
1. Ransomware/Malware
2. Third-Party/Supply Chain Attacks
3. Phishing
4. Customer Data Theft
5. Vulnerability Identification & Remediation
6. Fraud
7. Enterprise Visibility/Monitoring
8. Botnet Attacks
9. Payment Card Data
10. Event/Incident Response Timelines

ORGANIZATIONAL RISKS BY DOMAIN

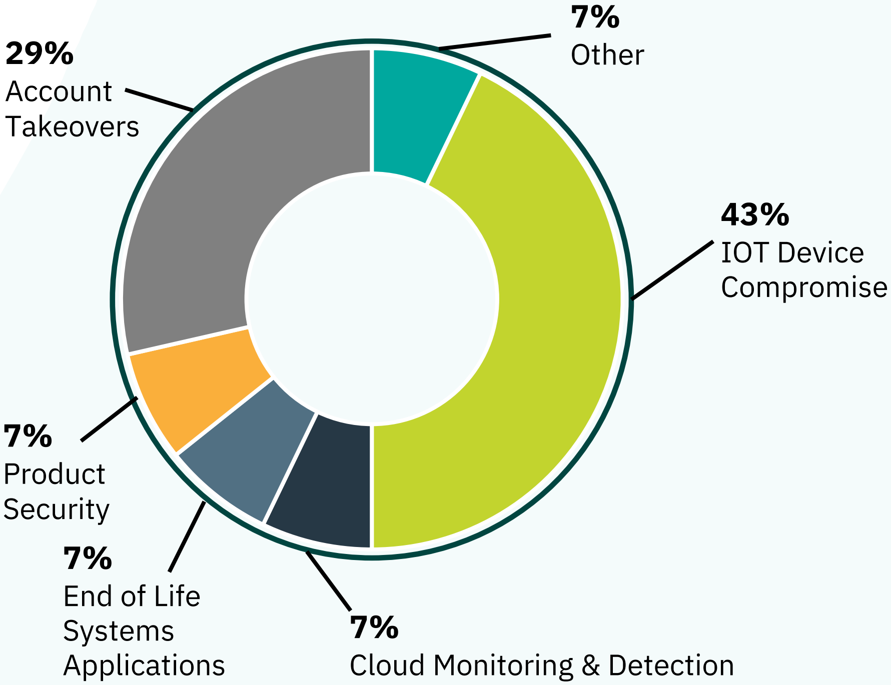
Risk Management Risks (22%)



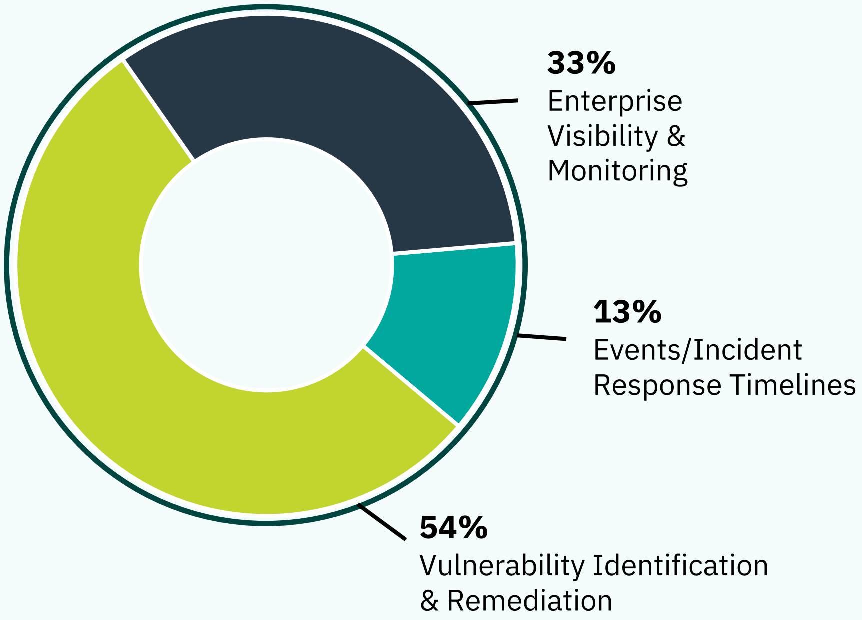
Threat Intelligence Risks (58%)



Security Architecture Risks (5%)



Security Operations Risks (15%)

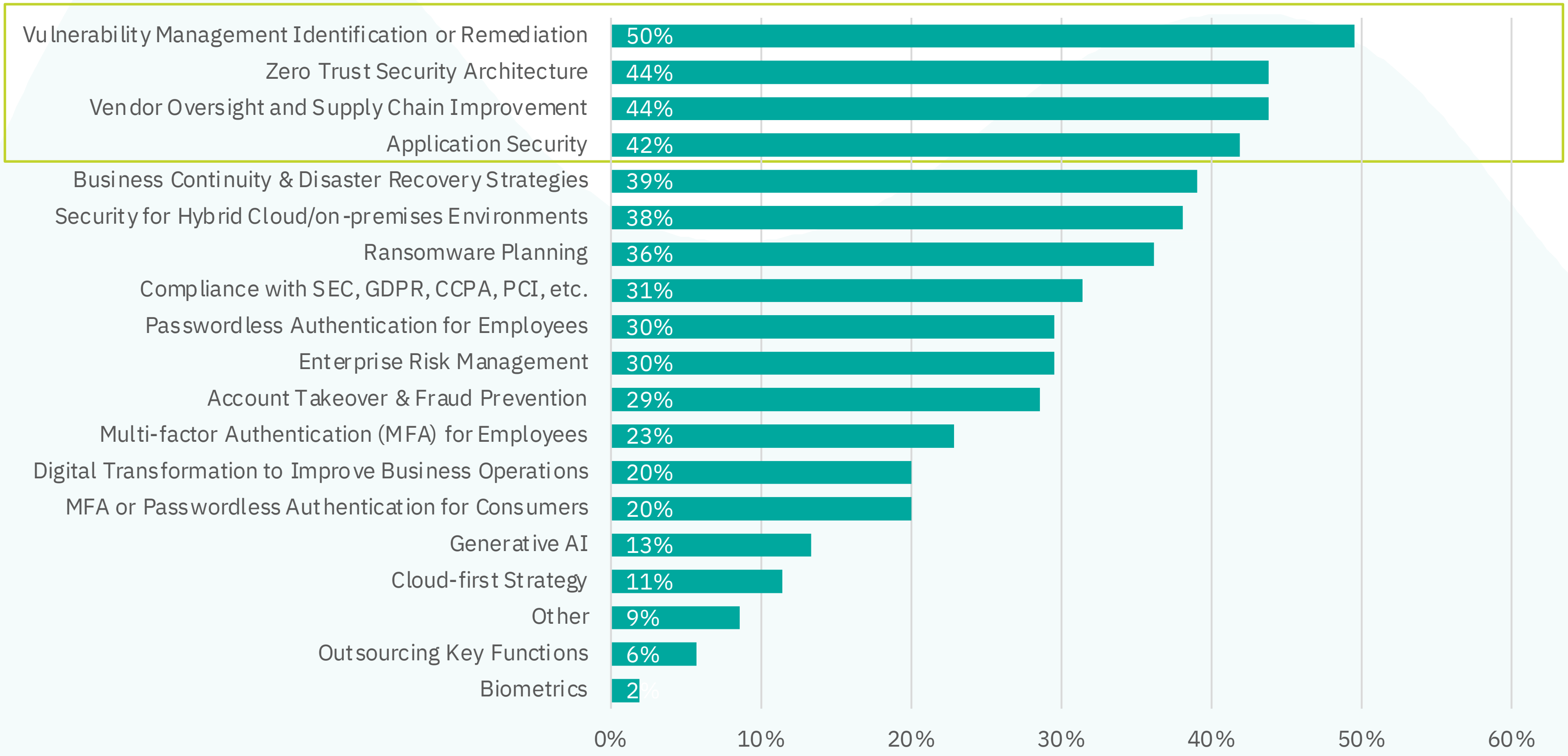


INITIATIVES PLANNED TO MITIGATE RISK

Vulnerability management is the top initiative CISOs are prioritizing in 2024, and at least **40% are focusing on zero trust security architecture, vendor oversight, and application security**. This is similar to last year's priorities, with exceptions:

- » Security for Hybrid Cloud/On-premises Environments dropped 18 points to 38%
- » Ransomware planning dropped 19 points to 36%

Key Initiatives Planned for 2024



There are, however, challenges to achieving these initiatives. CISOs cited Cyber vs IT prioritization challenges, budget constraints, and speed of business requirements as the top three barriers to success.

FULL REPORT AVAILABLE TO RH-ISAC CORE MEMBERS

RH-ISAC members can download the entire report in Member Exchange.
Not a member? Learn more about how to join at rhis.ac/Join