TLP: CLEAR

RETAIL & HOSPITALITY ISAC

BENCH MARK

CISO

JANUARY 2023

TABLE OF CONTENTS

INTRODUCTION

Information security teams have always had to do more with less, but 2023 might be the year when they are able to do more with more. Riding a three-year trend, 70% of CISOs expect their budgets to increase again next year, while 60% also expect more FTEs. It's possible that, in some cases, security has moved beyond its risk-mitigator role and can now expand as a critical part of business operations.

The time is ripe. This year, business disruption emerged as a top 10 (No. 7!) risk that organizations currently face, up seven spots from No. 14 in 2021. Similarly, 50% of CISOs now have business continuity/disaster recovery as part of their core responsibilities, an increase of 11 percentage points since last year, and typically 1-2 FTEs are dedicated to this area.

Many CISOs were concerned about the loss of operational systems, third-party compromises that impact the supply chain, and the inability to conduct eCommerce transactions, which generate an average of 21-30% of annual revenue for companies. It's no surprise ransomware reigns as the top risk this year, and vulnerability management is the No. 1 priority CISOs are focused on in 2023.

As you read this report, we hope you find ways to connect with peers in this community — whether that is by revenue or industry sector — that you share common concerns and interests.The knowledge shared by fellow CISOs can help guide your decision-making when it comes to budget allocation across personnel, tools, and technology, and third-party services. Both the large ($10-25 billion) and enterprise (greater than $25 billion) companies illustrate a maturity model you can follow, especially as to how they've grown their teams and prioritized identity and access management, application security, and DevSecOps.

You may even find a few insights surprising. For example, we all know that fraud in its many forms greatly impacts the bottom line, and it continues to be a top risk for organizations. However, very few CISOs have fraud as part of their core responsibilities, with even fewer FTEs dedicated to this area. We all know how complex organizational cultures can be, but even here, information security can play a leading role in protecting the business.

We look forward to continuing the conversation with you all, whether it is on our sharing platforms, at both virtual and in-person events, or participation in our working groups. We're excited to see the RH-ISAC CISO Benchmark Report has become a staple within the retail and hospitality communities. Thank you to everyone who completed the survey to make this happen.

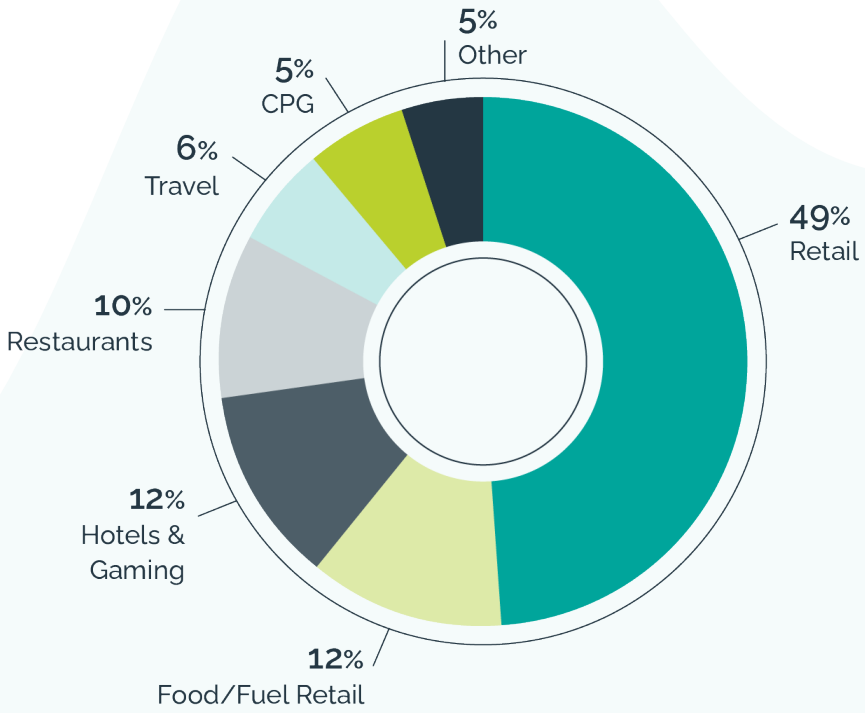
— The CISO Benchmark Task Force | RH-ISAC

SURVEY DEMOGRAPHICS

The RH-ISAC completed its fourth annual CISO Benchmark Survey in October 2022. It was fielded in September and October 2022 and generated 126 unique responses, a 35% increase in participation compared to the previous year.

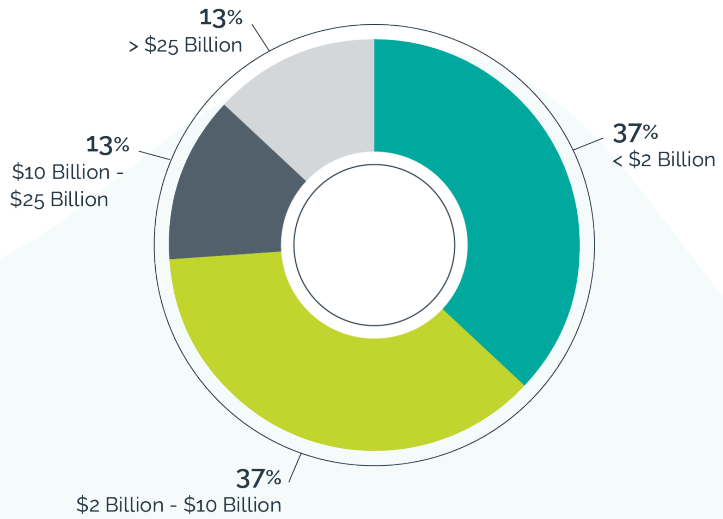
Participants by Industry Sector

The classes of trade represented in the 2022 survey are similar to the 2021 report, although this year, we combined food and fuel retail into one class. We also saw a slight decrease in participants from hotels and gaming.



Participants by Annual Revenue

The majority (74%) of participants generate up to $10 billion in annual revenue.



The companies represented in this survey reflect:

- 718,000 locations
- 3.4 million corporate employees
- $2.3 trillion in annual sales
- 6.6 million people connected to networks
- 95% have an eCommerce presence
- Average 21-30% of revenue generated from online sales

SUMMARY OF FINDINGS

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

BUDGET OVERVIEW

A typical RH-ISAC member has **6-8% of the IT budget dedicated** to information security operations and is allocated in the following ways:

- Personnel – 31-40%
- Tools & Technology – 41-50%
- Third-Party Services – 11-20%

Most Common Out-Sourced Services

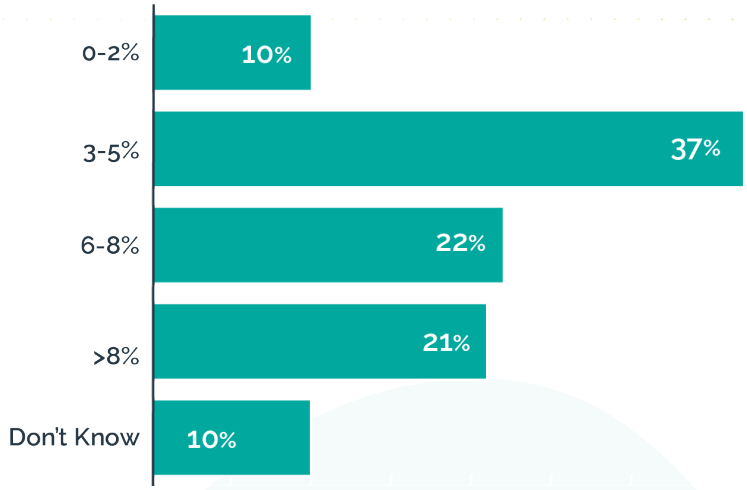
Pen Testing – 88%

Security Operations Center – 56%

Threat Intelligence – 38%

Budget Range

The chart below shows the range of budgets in the RH-ISAC community.



Budget Trends

- For the second year in a row, 70% of CISOs expect their information security budget to increase in 2023.
- Only 4% expect budget cuts.

PERSONNEL OVERVIEW

The **average size of an information security team is 15-25 FTEs**, including fewer than 5% offshore employees and 5-10% contractors. Interestingly, 64% do not have offshore employees, and 48% do not work with contractors.

Personnel Trends

InfoSec Team Sizes are Increasing

- Similar to last year, 60% of CISOs expect their FTE count to grow in 2023. Only 3% expect a staff reduction.

InfoSec Staff Roles are Changing

- Since last year, we've seen a rise in FTEs dedicated to tools and integrations and a decrease in FTEs dedicated to fraud and e-discovery.

Personnel Allocation

InfoSec Department FTEs are dedicated to the following roles:

3 – 5 FTEs

- Governance, Risk & Compliance (GRC)
- Identity & Access Management (IAM)
- Security Operations/Incident Response
- Tools & Integrations

1 – 2 FTEs

- Application Security
- Business Continuity & Disaster Recovery
- Cloud Security
- Data Management/Data Loss Prevention
- DevSecOps
- Infrastructure
- Network Security
- Privacy
- Product Security
- Security Awareness
- Third-Party Risk Management
- Threat Intelligence
- Vulnerability Management

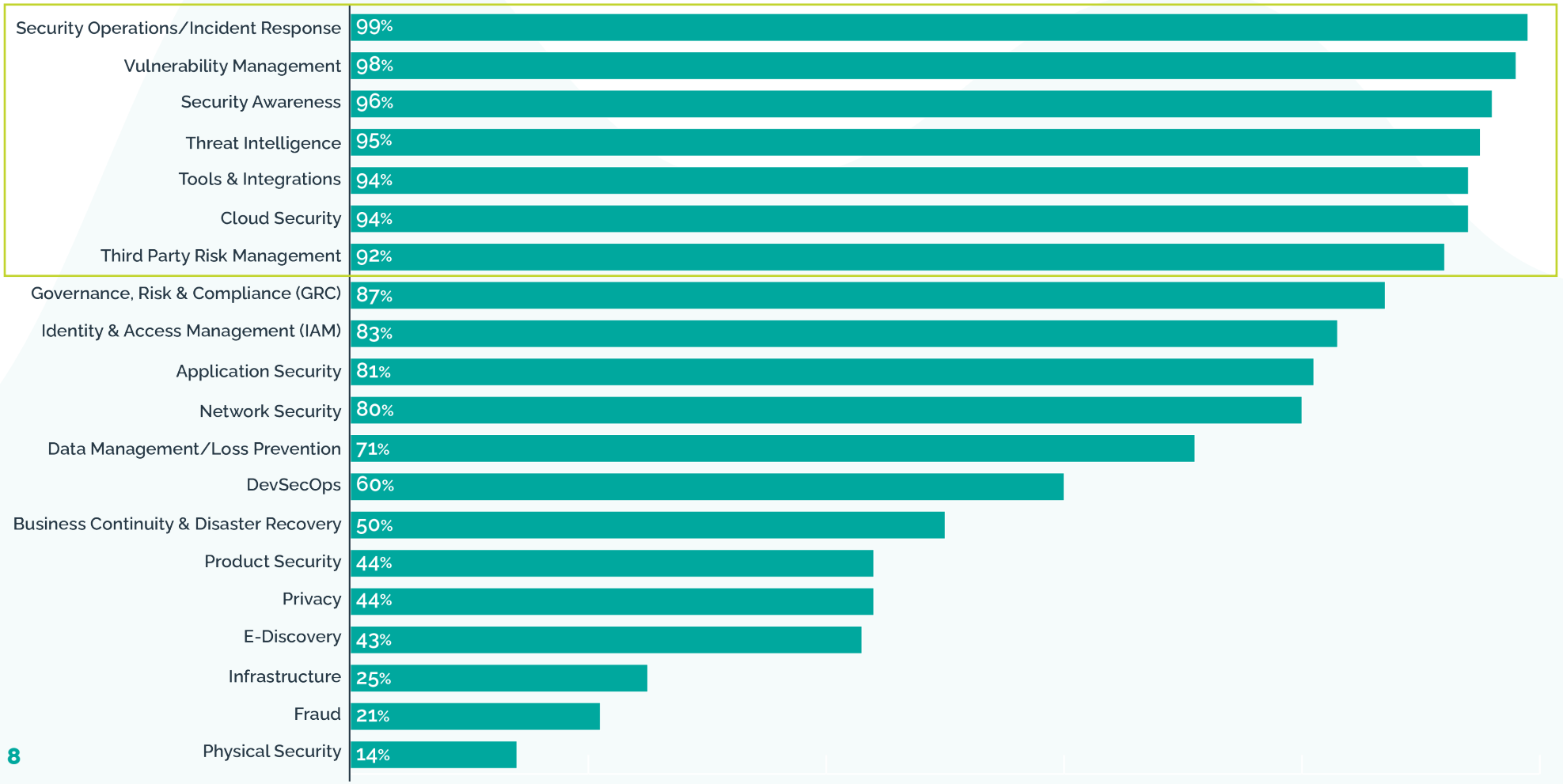
< 1 FTE

- e-Discovery
- Fraud
- Physical Security

RESPONSIBILITIES OF CISOS

Cybersecurity leaders have a wide range of responsibilities, but the top seven remain the same as last year, all of which 92% of CISOs have as part of their key responsibilities. Application security (81%), DevSecOps (60%), and infrastructure (25%) were new categories added this year, with some minor changes in existing responsibilities:

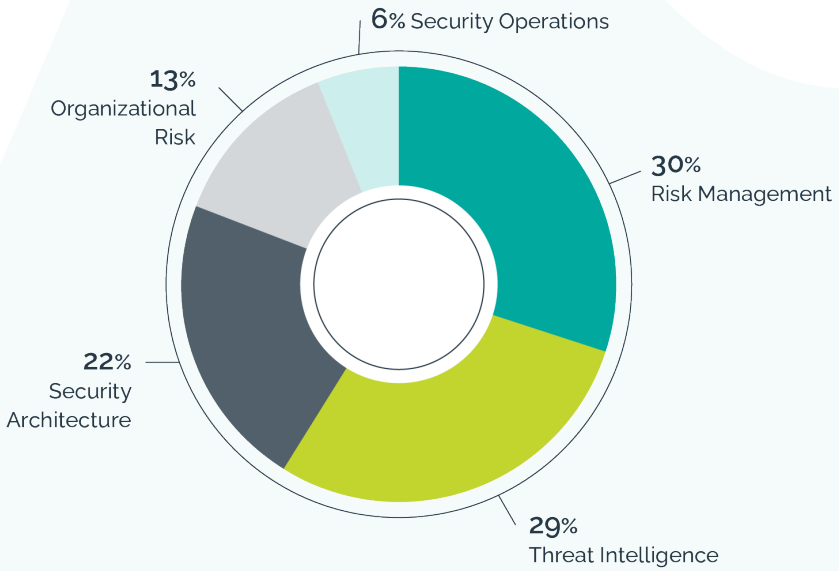
- Business continuity/disaster recovery increased by 11 percentage points, up to 50%
- Fraud decreased by 10 percentage points, down to 21%
- E-discovery decreased by 9 percentage points, down to 43%



ORGANIZATIONAL RISKS

Top Risks by Category

CISOs cited more than 400 organizational risks, but **most are concerned about risks related to risk management** (30%) and **threat intelligence** (29%), specifically ransomware, data loss prevention, third-party risk management, and phishing. For a breakdown of risks by domain, see Figure 1 in the Appendix.



Top 10 Risks

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

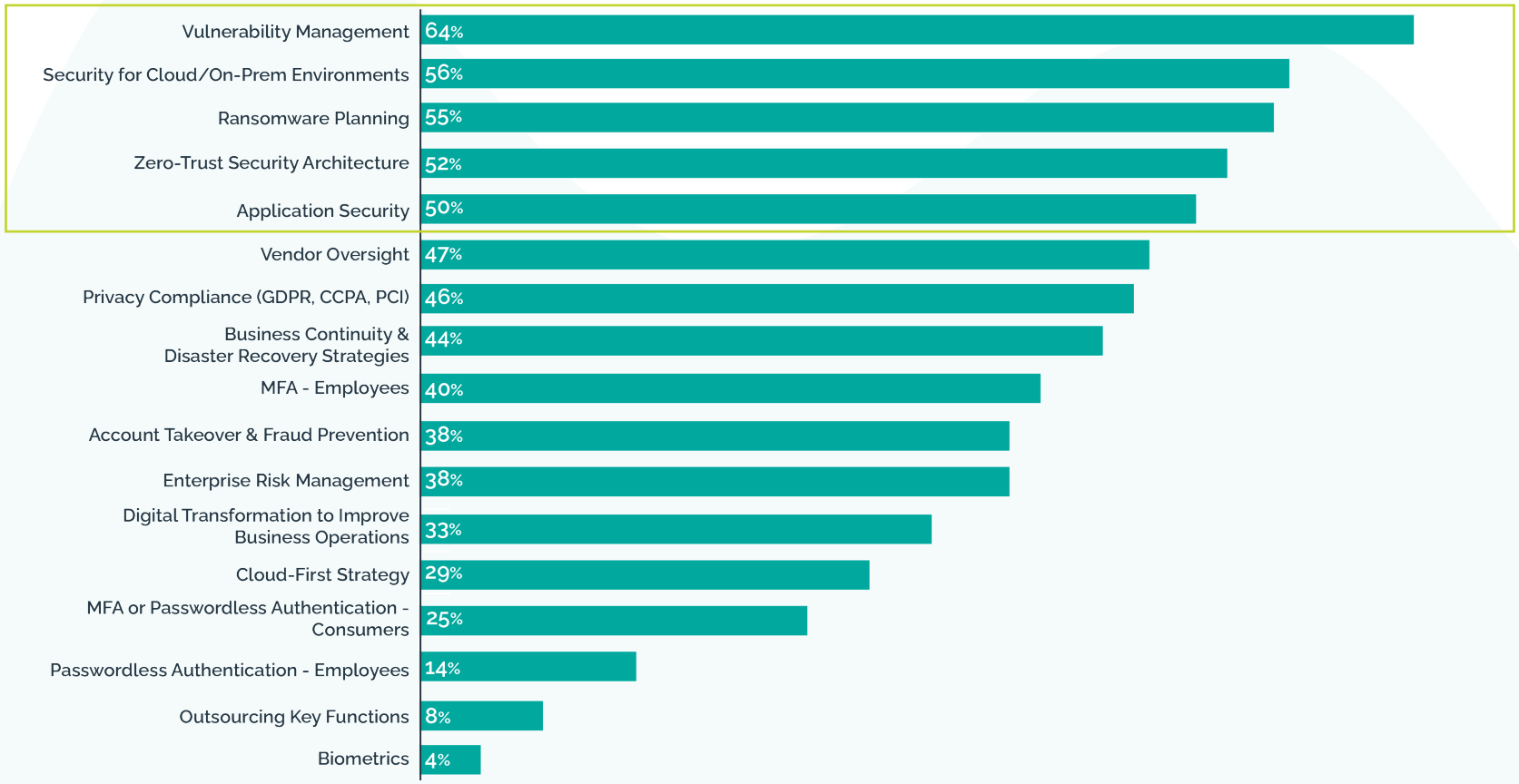
1. Ransomware
2. Data Loss Prevention
3. Digital Transformation & Cloud Security
4. Third-Party Risk Management
5. Identity & Access Management
6. Phishing
7. Business Disruption
8. Vulnerability Management
9. Fraud
10. Governance, Risk & Compliance

INITIATIVES PLANNED TO MITIGATE RISK

Vulnerability management is the top initiative CISOs are prioritizing in 2023, and at least 50% are focusing on securing hybrid cloud/on-premises environments, ransomware planning, zero trust security architecture, and application security. This is similar to last year's priorities, with two exceptions:

- Cloud-first strategy dropped 10 percentage points to 29%
- Privacy Compliance with GDPR, CCPA, PCI, etc., increased by 9 percentage points to 46%

Key Initiatives Planned for 2023



There are, however, challenges to achieving these initiatives. CISOs cited limited talent and resources, competing business priorities, and budget constraints 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