TLP:CLEAR

2023 YEAR IN REVIEW

RETAIL & HOSPITALITY ISAC

2023 HIGHLIGHTS

January

Launched partnership with the National Retail Federation

Published CISO Benchmark & Practioner Benchmark Reports

February

Theat Actor Profile Catalog Published in MISP

RH-ISAC Podcast Joins CyberWire Network

Retail & Hospitality Threat Landscape Briefing Webinar Series Begins

April

First-Ever Global Workshop Hosted in Europe

Launched Collaboration with National Corporation of Corporate Directors to Prepare Aspiring Boardroom Leaders

May

In-Person CISO Dinner and Forum Hosted at Target Headquarters in Minneapolis

June

Collaborated with European Council of ISACs to host a booth and networking event at InfoSec Europe

September

Dinner & Dialogue Event Series for CISOs Begins

October

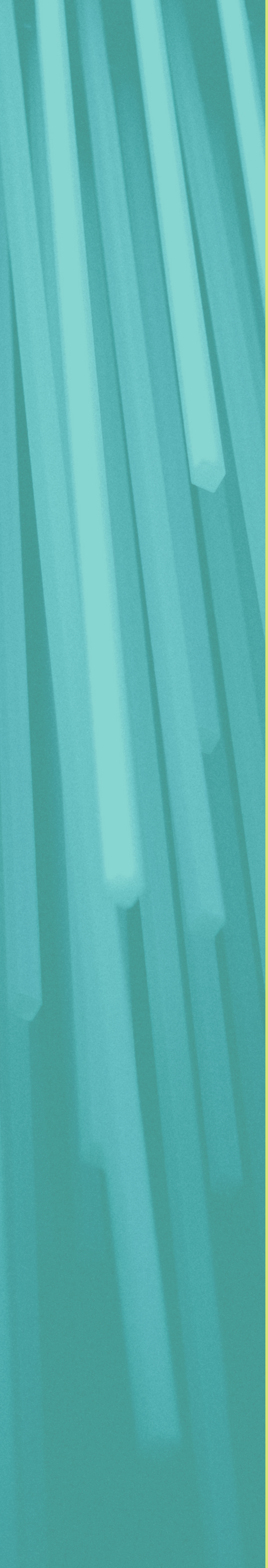
Capture-the-Flag and Tabletop Exercise included at the RH-ISAC Cyber Intelligence Summit

New Awards Introduced During Annual Membership Meeting

November

Fraud Galaxy Published in MISP

RH-ISAC Hosts Workshop for EuroCommerce Cybersecurity Taskforce



2023 SHARING & COLLABORATION OVERVIEW

99%
of members engaged in RH-ISAC

15,535
total shares across all sharing channels

68%
of members shared intelligence

284k
shared IOCs in MISP

13,862
vetted IOCs in MISP

8,029
total participants in calls and webinars

77%
of members attend in-person events

383
RFIs shared

909
Responses to RFIs

INTELLIGENCE & BENCHMARK REPORTS

100+

real-time reports on cyber threats

3

intelligence trend summary reports

7

survey reports

161

Dark Web summary reports

3

benchmark reports

Ad Hoc Reports on Cyber Threats: In 2023, RH-ISAC produced more than 100 real-time reports on developing cyber threats, covering topics like threat actor tactics, major third-party vulnerabilities, and high-profile attacks in the retail, hospitality, and travel industries. These reports provide industry-specific context, allowing members to understand how a threat may impact their environment and take meaningful action to defend themselves.

Intelligence Trend Summaries: RH-ISAC published three Intelligence Trend Summaries this year. These reports provide an analysis of the past four months of member-shared intelligence, supported by relevant content contributed by RH-ISAC Associate Members. This year, with the enhanced capabilities of the RH-ISAC MISP project, the data assembled for trends is more granular and focused on tactics, techniques, and procedures (TTPs).

Daily Dark Web Summary: RH-ISAC improved collection capabilities in 2023 to include dark web threat intelligence. To keep members appraised of threats emerging on dark web forums, the intelligence team started a new product series to provide dark web forum summaries at the end of each business day.

Holiday Season Cyber Threat Trends: RH-ISAC continued publishing the holiday trend report to provide an analysis of past holiday trends combined with threat intelligence indicating which threats are likely to remain a concern, combined with member input on mitigation strategies.

Verizon DBIR Analysis: The RH-ISAC published the second report comparing and contrasting the annual Verizon Data Breach Investigation Report (DBIR) findings for the retail and hospitality sectors against RH-ISAC community sharing data that our analysis and intelligence teams assembled. Like the enhanced Intelligence Trend Summaries, this report is also improved with granular data from member-shared intelligence in MISP.

CISO Benchmark Report: With a 35% increase in participation in 2023, we learned from 126 companies that a typical RH-ISAC member has 6-8% of their IT budget and 15-25 FTEs dedicated to information security operations. Ransomware, data loss, and cloud security were cited as the top three risks organizations faced.

Practitioner Benchmark Report: According to 105 practitioners surveyed, 83% serve more than one job function and have a diverse skillset across security operations, threat intelligence, and risk management duties; with 63% assessing their skills between intermediate and advanced levels.

Tools & Technology Benchmark Report: 100 member companies participated in the second annual Tools & Technology Report highlighting the most common tools used by members, including TIP, SIEM, SOAR, XDR, and other solutions.

Survey Reports: The RH-ISAC published seven survey reports on the following topics: Cyber Insurance Premiums, Phishing Programs, Configuration Management Database, Business Continuity & Disaster Recovery, Bring-Your-Own-Device (BYOD) Security, BYOD Stipend Model for Mobile Users, and Fleet Card Security at Fuel Retail Locations.

EVENTS & SPEAKING ENGAGEMENTS

Intelligence Workshops

5 U.S.-based workshops hosted in Phoenix, Atlanta, New Jersey, Seattle, and Las Vegas

249 registrants and **180** attendees, more than tripling attendance from 2022

Global Events

2 global workshops hosted in Barcelona and London

59 attendees

RH-ISAC Cyber Intelligence Summit

- **333** participants
- **52** speakers
- **5** keynotes
- **4** networking events
- **20** breakout sessions

CISO Events

29 participants attended the annual in-person CISO meeting in Minneapolis

1 virtual CISO Roundtable discussion focused on Cloud Security

6 Dinner & Dialogue events brought together small groups of CISOs in Columbus, Toronto, Chicago, Washington D.C., Boston, and Orlando.

Networking Events

RH-ISAC joined retail and hospitality cybersecurity professionals at various conferences and held networking happy hours at both RSA and InfoSecurity Europe

Participation

77% of Core Member companies participated in an RH-ISAC event in 2023

RH-ISAC Staff Speaking Engagements

19 presentations given or panel discussions moderated by RH-ISAC staff for outside conferences and webinars

WORKING GROUP COLLABORATION

PARTICIPATION

94%
of members attended a group call

31
average indivdual attendees per call

1307
total call attendees in 2023

252
total number of calls in 2023

Analyst Community

More than 300 individuals attended a Weekly Intel Call and 88 individuals participated in two virtual Capture-the-Flag exercises hosted by Nisos. The RH-ISAC also held six Retail & Hospitality Threat Landscape Briefings featuring 16 Associate Members and Palo Alto's Unit 42 team also held an exclusive threat briefing on Muddled Libra in August.

BISO Community

This group covered topics related to the BISO role, including program overviews and job responsibilities, building relationships with internal stakeholders, utilizing tools to managing risk across the business, and data sources useful in the BISO role.

CISO Community

The CISO Community convened for calls once a month that focused on everything from SEC regulations to using the NICE Framework for staff development plans. RH-ISAC also hosted TLP:Red conversations that allowed CISOs to acknowledge, discuss, and to share information on incidents that significantly impacted our sectors.

Dark Web

This group conducted threat discovery marathons and dark web threat hunts on a bi-weekly basis. They also created a dark web roadmap for members to set up an environment for dark web investigations and held a hands-on workshop at the RH-ISAC Summit.

Fraud

The Fraud Working Group shared intelligence on ATO, bots, ransomware, phishing, refund-as-a-service and loyalty fraud, and domain takedowns/imposter sites; as well as best practices on fraud governance, security controls, and detection tools.

Gift Card Fraud

New in February 2023, this group focused on sharing collective intelligence to combat gift card scams and extortion. Members shared prevention and detection controls, how to collect and share relevant data with law enforcement, and discussed fraud team roles and organizational alignment.

Identity & Access Management

This highly active group tackled passwordless authentication, the rollout of FIDO passkeys, PCI 4.0 requirements, the scope of enterprise IAM practices, and PATO-facilitated guest phishing attacks.

WORKING GROUP COLLABORATION

Incident Response

This group discussed incident response plan practices, policies for third-party vendor breaches, forensics automation, advanced incident response trends, threat actor diagnosis, metrics, and held TLP:RED sessions when needed.

Operational Technology

Members of the OT group discussed network segmentation strategies, secure remote access, pros and cons of vendor solutions, value and investment of OT tools, vulnerability management practices, and service-level agreements.

Risk Management

The PCI Security Standards Council shared updates included in PCI DSS v4.0. The group also discussed how to develop key risk indicators, risk quantification, generative AI, the new SEC disclosure rule, and insider threats.

Security Awareness

This highly engaged group discussed security awareness program best practices and lessons learned, including a special session preparing for cybersecurity awareness month and generative AI education for employees. In November, the group completed a phishing programs survey to better understand the challenges, priorities, and functions of members' security awareness programs.

Small-Cyber Teams

New in April 2023, this group discussed how to build an information security program despite budget and resource challenges. Topics included staff prioritization, maturity road-mapping, security operations fundamentals, zero trust frameworks, and how to use OSINT techniques to search the dark web.

Third-Party Risk

This group focused on mitigating and responding to third-party risks, including collaborating with threat response teams and how to handle vendors with high residual risk. Members also shared their automation and scalability journeys across multiple brands and properties.

Tools Users' Group

More than 1,000 users have logged into MISP and more than 20 members have set up integrations into their tool stack to share and consume data with the platform. The SOAR group set up a GitHub repository to share content, playbooks, and training; and the CrowdStrike and Splunk groups met regularly to discuss their experiences with those tools and matured those integrations.

Vulnerability Management

This group regularly reported on the top vulnerabilities and mitigation strategies, and discussed prioritization metrics, vulnerability disclosure and bug bounty programs, updates to CVSS v4, and how to leverage open-source tools like Shodan to search for vulnerabilities in their systems.

Growth Milestones

2023 YEAR END
287 Members
257 Core Members + 30 Associate Members

2022 YEAR END
256 Members
229 Core Members + 27 Associate Members

2021 YEAR END
224 Members
198 Core Members + 26 Associate Members

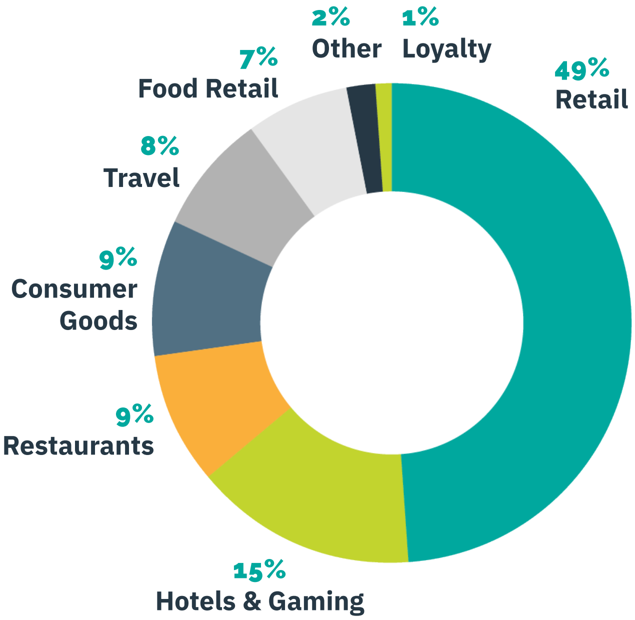
2020 YEAR END
187 Members
161 Core Members + 26 Associate Members

2019 YEAR END
155 Members

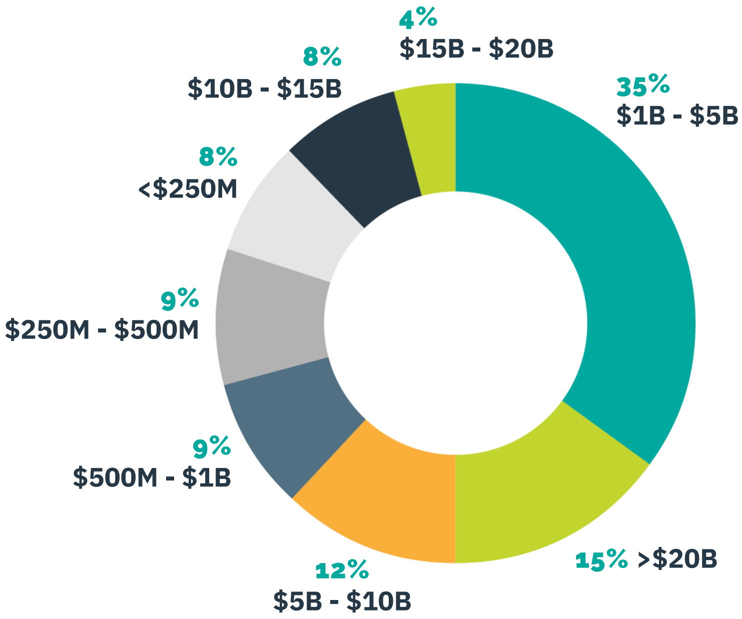
2018 YEAR END
136 Members

MEMBER SNAPSHOT

Industry



Revenue



The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is the trusted community for sharing sector-specific cybersecurity information and intelligence. The RH-ISAC connects information security teams at the strategic, operational, and tactical levels to work together on issues and challenges, share best practices and benchmark among each other – all with the goal of building better security for the retail, hospitality, and travel industries through collaboration. RH-ISAC serves all consumer-facing companies, including retailers, restaurants, hotels, gaming casinos, food retailers, consumer products, travel companies and more.

For more information, visit rhisac.org.

RETAIL & HOSPITALITY
ISAC