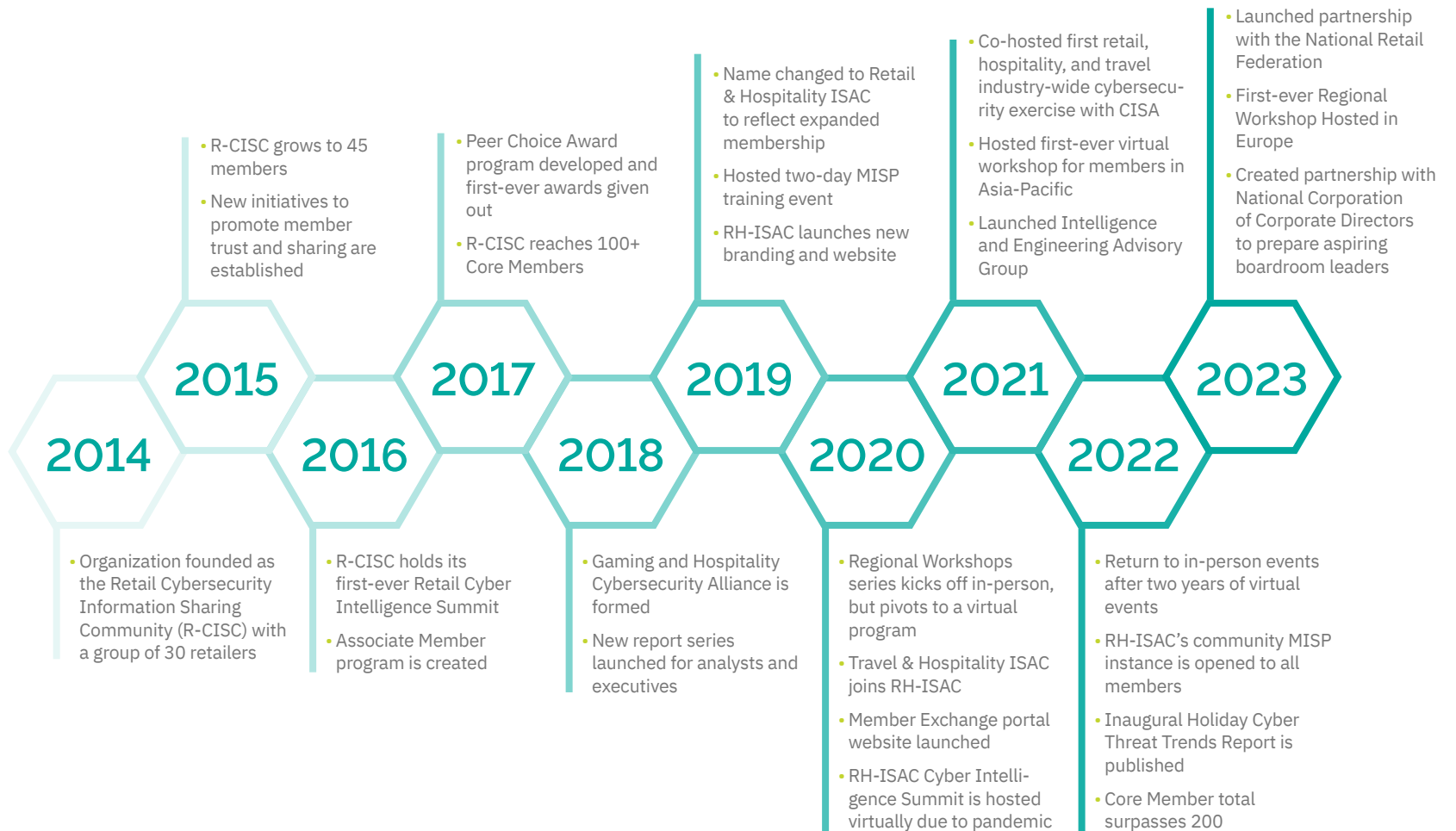# 2024 YEAR IN REVIEW

10 YEAR LOOKBACK TIMELINE

The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) was built to create a secure place for retailers to share cybersecurity information and intelligence to not only better protect their own companies, but to also strengthen the entire industry. Following a series of high-profile cybersecurity incidents in the retail sector, the organization was founded in 2014 with about 30 retail companies. After a decade of growth, RH-ISAC now has nearly 300 Core Members, including retailers, restaurants, hotels, casinos, food retailers, consumer products, and other consumer-facing companies. The types of threats facing the industry are different now than in 2014, but sharing cyber threat intelligence continues to be a critical piece of the puzzle that drives greater security.

2014
- Organization founded as the Retail Cybersecurity Information Sharing Community (R-CISC) with a group of 30 retailers

2015
- R-CISC grows to 45 members
- New initiatives to promote member trust and sharing are established

2016
- R-CISC holds its first-ever Retail Cyber Intelligence Summit
- Associate Member program is created

2017
- Peer Choice Award program developed and first-ever awards given out
- R-CISC reaches 100+ Core Members

2018
- Gaming and Hospitality Cybersecurity Alliance is formed
- New report series launched for analysts and executives

2019
- Name changed to Retail & Hospitality ISAC to reflect expanded membership
- Hosted two-day MISP training event
- RH-ISAC launches new branding and website

2020
- Regional Workshops series kicks off in-person, but pivots to a virtual program
- Travel & Hospitality ISAC joins RH-ISAC
- Member Exchange portal website launched
- RH-ISAC Cyber Intelligence Summit is hosted virtually due to pandemic

2021
- Co-hosted first retail, hospitality, and travel industry-wide cybersecurity exercise with CISA
- Hosted first-ever virtual workshop for members in Asia-Pacific
- Launched Intelligence and Engineering Advisory Group

2022
- Return to in-person events after two years of virtual events
- RH-ISAC's community MISP instance is opened to all members
- Inaugural Holiday Cyber Threat Trends Report is published
- Core Member total surpasses 200

2023
- Launched partnership with the National Retail Federation
- First-ever Regional Workshop Hosted in Europe
- Created partnership with National Corporation of Corporate Directors to prepare aspiring boardroom leaders

2024 HIGHLIGHTS & KEY INITIATIVES

Hospitality Standards & Best Practices document released to outline critical cybersecurity controls for the sector

RH-ISAC collaborates with the Aspen Institute Financial Security Program to join the **National Task Force for Fraud & Scam Prevention**

MISP integration documentation released as member **usage of MISP expands** with 71 members automatically consuming RH-ISAC MISP threat intel and 5 members automatically sharing threat intel into RH-ISAC MISP

Partnership established with SANS Institute and ICF International to provide a **free upskilling program for RH-ISAC members** to take the GFACT certification exam

Conducted member satisfaction survey and received positive results. Members rated RH-ISAC with an **"Excellent" Net Promoter Score** of 73, which is higher than the industry average of 44.

Celebrated **RH-ISAC's 10th anniversary** with a special event, Member Exchange LIVE, held in Minneapolis

Associate Member program expands to 3 tiers: Critical Provider, Intelligence Partners, and Community Services

Launched LinkSECURE, a new program for small- to mid-sized vendors and service providers to help mature their cybersecurity operations

Partnered with NRF's Fraud Working Group to **develop a fraud taxonomy**

Established new working groups for Consumer Goods, Restaurants, Hospitality & Travel, and Mergers, Acquisitions & Divestitures
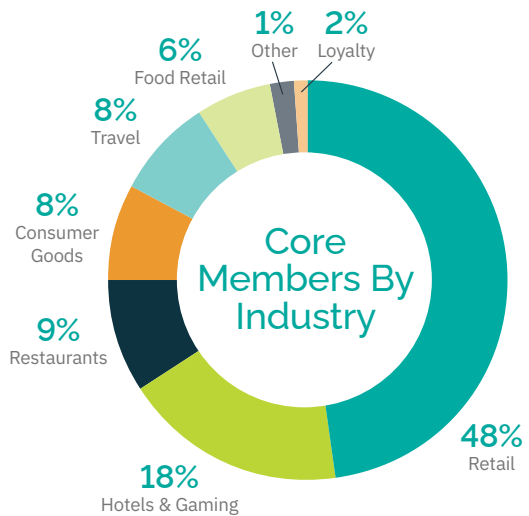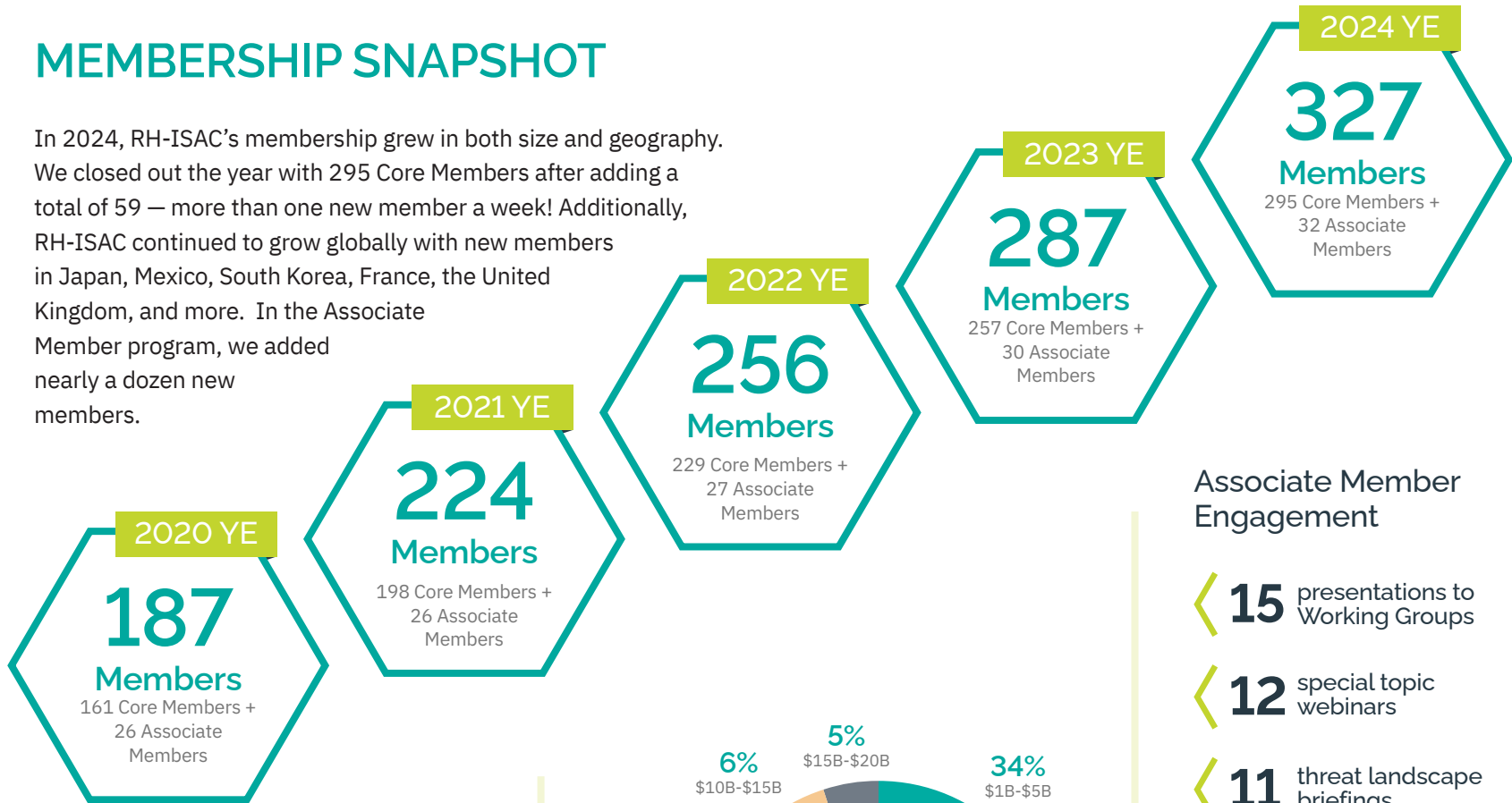
Significant **growth in EMEA and APAC** region-focused programs, including monthly regional intelligence calls, regional workshops, speaking engagements, and an advisory committee

Created the CTI Roundtable, a monthly webinar series focused on solving challenges CTI teams face from framework, processes and tools, talent development, and cross team collaboration.

> The RH-ISAC is the most well-run community organization I've been a part of and I know it's due to the passionate leadership and many long hours of hard work from all the staff."

MEMBERSHIP SNAPSHOT

In 2024, RH-ISAC's membership grew in both size and geography. We closed out the year with 295 Core Members after adding a total of 59 — more than one new member a week! Additionally, RH-ISAC continued to grow globally with new members in Japan, Mexico, South Korea, France, the United Kingdom, and more. In the Associate Member program, we added nearly a dozen new members.

2024 YE
327 Members
295 Core Members + 32 Associate Members

2023 YE
287 Members
257 Core Members + 30 Associate Members

2022 YE
256 Members
229 Core Members + 27 Associate Members

2021 YE
224 Members
198 Core Members + 26 Associate Members

2020 YE
187 Members
161 Core Members + 26 Associate Members
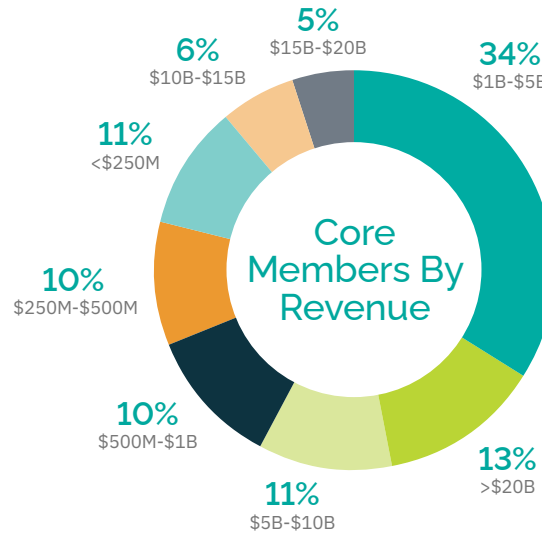
Associate Member Engagement

15 presentations to Working Groups

12 special topic webinars

11 threat landscape briefings

35 reports submitted

12 blog posts published

Core Members By Industry

- 48% Retail
- 18% Hotels & Gaming
- 9% Restaurants
- 8% Consumer Goods
- 8% Travel
- 6% Food Retail
- 1% Other
- 2% Loyalty

Core Members By Revenue

- 34% $1B-$5B
- 13% >$20B
- 11% $5B-$10B
- 10% $500M-$1B
- 10% $250M-$500M
- 11% <$250M
- 6% $10B-$15B
- 5% $15B-$20B

Global Growth

In 2024, RH-ISAC continued to grow globally adding a record-number of new members in Europe and the Asia-Pacific region.

Global Core Member Growth in 2024

30% of new members from outside U.S.

11 different countries

23 events and calls for EMEA or APAC-based members

> I'm a big fan of this membership. The best part is the community. Members are always willing to help and share. The RH-ISAC team is phenomenal to work with."

2024 SHARING & COLLABORATION OVERVIEW

941 members attended in-person events

700 RFIs shared

60% of members shared intelligence

51,094 IOCs shared in MISP

94% of members engaged in RH-ISAC

1,934 responses to RFIs

13,039 vetted IOCs in MISP

116 real-time alerts & incident reports sent to specific companies

24,021 total instances of member engagement

10,680 total attendance in calls and webinars

4,395 individuals credentialed to sharing platforms

14,025 total shares across all sharing channels

" "The community is bar none the best in the industry, I've learned and grown a lot from my interactions with the community at large and that includes RH-ISAC staff themselves."

INTELLIGENCE & BENCHMARK REPORTS

RH-ISAC continued to develop both the quality and quantity of reports issued in 2024. Several new intelligence reports were created, including a monthly leadership briefing and a monthly practitioner briefing. Additionally, the research team revamped publishing custom surveys and RFI summary reports based on member feedback.

Intelligence Reports

246 Daily Intelligence Reports
Daily recap of need-to-know intel including reports, RFIs, summary of prior day's community discussions

246 Daily Dark Web Summary Reports
End-of-day summary of major updates from cybercriminal activity on dark web forums

9 Leadership Briefing Reports
Monthly review of major threat trends and community discussions to inform senior-level decision makers

5 Practitioner Briefing Reports
Monthly review of major threat trends and community discussions to inform hands-on cyber operators

120 Ad Hoc Intelligence Reports
Intelligence reports on incidents and issues of interest to the wider Core Member community

52 Weekly CISA Alert Summary Reports
Major alerts shared by CISA, including Industrial Control System Advisory Project Alerts

4 Intelligence Summary Reports
Quarterly analysis of member-shared intelligence, RFI trends, and intelligence reports and surveys

1 Holiday Season Cyber Threat Trend Report
Analysis of past holiday trends combined with threat intelligence and member input on mitigation strategies

1 Industry Insights Verizon DBIR Analysis Report
Comparison of the annual Verizon Data Breach Investigation Report (DBIR) findings for the retail and hospitality sectors against RH-ISAC data

702 total reports

684 intelligence reports

6 benchmark reports

6 survey reports

6 RFI summary reports

Report Highlights

Annual RH-ISAC CISO Benchmark Report
The RH-ISAC CISO Benchmark Task Force partnered with Booz Allen Hamilton to conduct the survey and analysis for this year's report. In 2024, 56% of CISOs expected budget increases, and 60% anticipated more full-time employees, continuing a three-year trend of growth.

2024 RH-ISAC Tools & Technology Report
RH-ISAC conducted its third annual Tools & Technology Benchmark, collecting insights from 71 member companies. This report highlights the most commonly used tools, including TIP, SIEM, SOAR, EDR, and other key solutions.

Data Loss Prevention (DLP) Survey Report
RH-ISAC conducted a Data Loss Prevention (DLP) survey, gathering insights from 26 unique member companies. This report provides an in-depth analysis of maturity levels, key performance indicators (KPIs), tools, challenges, and solutions related to DLP.

Gift Card Fraud Survey Report
RH-ISAC conducted a Gift Card Fraud survey, collecting insights from nine member companies. The report analyzes tampering trends, collaborations with internal teams, gift card providers, and law enforcement, along with strategies for packaging, in-store security, and improving the customer experience.

Best Practice Summary Report–Bulk User Account Impact on Return Fraud
This summary outlines best practices for managing the impact of bulk user accounts on return fraud, focusing on the retail industry. It covers key IoCs and effective mitigation tactics to counteract TTPs commonly associated with bulk account fraud.

Best Practice Guide Report–Implementing DLP To Mitigate Security Risks
This report provides a comprehensive overview of how DLP can be used to reduce risks both for customers and internally. It includes a list of IoCs as well as recommended best practices and mitigation strategies.

RFI Summary Highlights

Firewall Management Responsibilities
This RFI sought to clarify whether the Information Security department or the Networking department is responsible for managing and overseeing the firewall.

Vulnerability Management (VM) Board Reporting
The RFI aims to gain insights into best practices for communicating vulnerabilities and related security issues to board members.

Assessment of Brand Protection and Digital Risk Management Responsibilities
This RFI seeks to identify who within organizations is responsible for managing Brand Protection and Digital Risk Management. Its goal is to explore various management options related to these critical areas.

Assessing Personal Email Access on Company Devices
This RFI aims to assess whether organizations block employees from accessing personal email on company devices. It seeks to explore the benefits and drawbacks of allowing employees to access personal emails on their workstations.

Justifying Financial Costs of PAM Solutions
This RFI is seeking advice on options like CyberArk, BeyondTrust, and Okta to meet a cyber insurance requirement but is concerned about the high implementation costs, which could be three to five times higher than the licensing fees.

Level 1 PCI Compliance QSA Services
This RFI is seeking advice on achieving or maintaining Level 1 PCI compliance for large payment card transaction volumes and finding Qualified Security Assessor (QSA) services.

EVENTS

In line with the growth in membership, RH-ISAC grew the event offerings to provide more in-person and virtual events than ever before – more than 43 events and webinars throughout the year. The footprint of event locations also expanded to serve our continued growth in members located in the EMEA and APAC regions.

43 events

19 in-person events

24 virtual events

2,040 total attendees

Regional Workshops

The 2024 Regional Workshop series fanned out across the globe with 6 workshops coast-to-coast in the U.S. and 4 workshops serving members in Europe, Canada, and the Asia-Pacific region.

Workshop Presentation Highlights

Report Curation and Threat Library: How to Organize Your Knowledge

Using Subject & Deductive Reasoning When Managing Third-Party Risk

Implementing Lessons Learned from eCommerce Incidents: Theory, Reality, and GDPR

Workforce Automation for Small Team Security

- 10 workshops
- Locations: London, Amsterdam, Toronto, Washington, D.C., Atlanta, Los Angeles, Seattle, Chicago, Las Vegas, APAC (virtual)
- 376 attendees
- 84 speakers
- 3 training sessions

" The community is second to none that I've been a part of. I know if we are facing challenges within our organization, we can rely on the RH-ISAC community to help guide us."

RH-ISAC Cyber Intelligence Summit

RH-ISAC's biggest event of the year was bigger than ever in 2024 with nearly 400 attendees and more than 50 presentations. Summit was hosted in downtown Denver over three days and received high marks from attendees.

Summit Presentation Highlights

A Decade in Cybersecurity: The RH-ISAC Eras Tour

Beyond Chat: GPTs & Security Awareness in the Workplace

Catphish: Infiltrating an International Refund Fraud Operation

Cyber Resiliency: Preparing the Business for Incident Response

- 390 attendees
- 52 speakers
- 5 keynote presentations
- 26 breakout presentations
- 5 networking events
- 1 training session
- 4.75 out of 5 rating in attendee satisfaction

Member Exchange LIVE!

In September, RH-ISAC hosted a special event in Minneapolis to celebrate the organization's 10th anniversary. Dubbed Member Exchange LIVE, the event featured workshops, the CISO Forum, and the member awards ceremony dinner.

- 121 attendees
- 26 presentations
- 6 breakout sessions
- 1 CISO Forum
- 39 RH-ISAC Member Awards
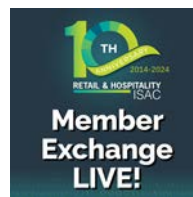
Member Exchange LIVE! Agenda Highlights

Malware Analysis Workshop

MISP Training Session

Cyber Threat Intelligence Workshop

Advanced OSINT Workshop

CISO Events

This year's CISO-focused events included a mix of in-person and virtual opportunities for networking and professional development.

2 CISO Roundtables > Discussion topics focused on threats related to IoT and OT, and also securing APIs

2 CISO Forums > In-person events held in conjunction with Summit and Member Exchange LIVE!

2 Dinner & Dialogue > Small groups of CISOs in Columbus and Atlanta

2 Industry Conference Events > Networking events held during RSA and BlackHat

Webinars

RH-ISAC's virtual programming expanded in 2024 with three distinct webinar series that were all supported by Associate Members and leading solutions providers.
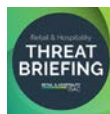
11 Retail & Hospitality Threat Briefings > Intelligence and research about threats facing the industry

6 Solutions Showcase Presentations > Product demos showcasing new technology

6 Topic-Specific Webinars > Presentations about a specific topic of interest
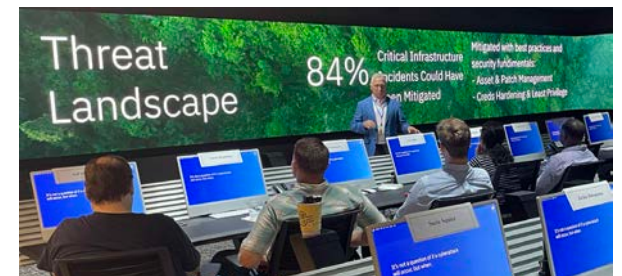
GROUP COLLABORATION

RH-ISAC's group collaboration opportunities continued to grow in 2024. A new EMEA-focused monthly intelligence call was added, along with three new working groups: Consumer Goods, Hospitality & Travel, and Mergers, Acquisitions & Divestitures. A new call series focused on Cyber Threat Intelligence was also created.

23 total groups

311 total calls in 2024

1,404 total call attendees in 2024

9,581 total attendances in 2024

89% of members attended a call

31 average individual attendees per call
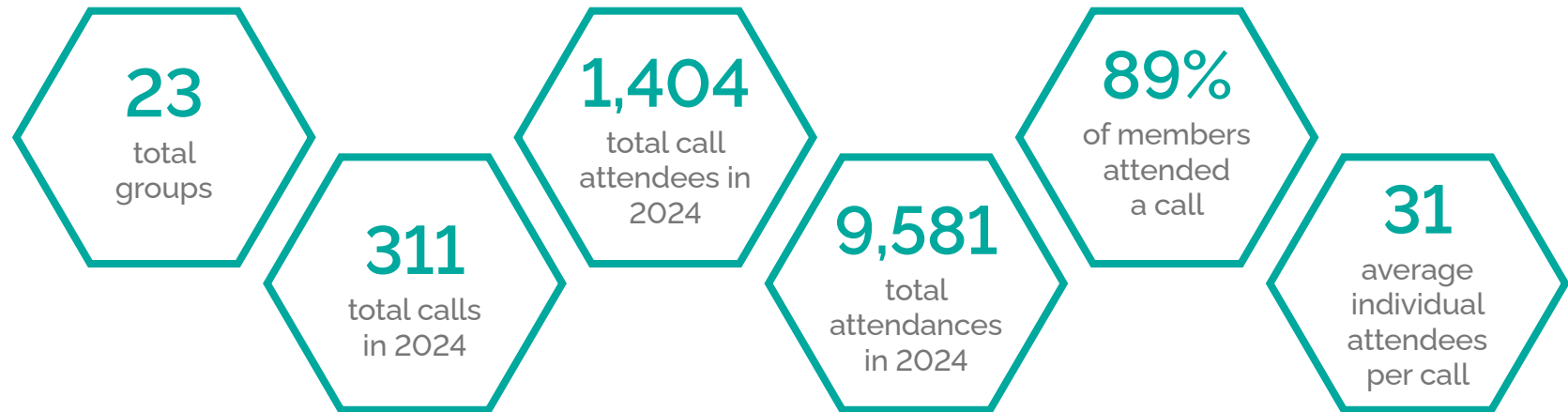
Analyst Community
The Analyst Community takes part in the Weekly Intelligence call series and is instrumental in responding to RFIs from throughout the community.

APAC Community
The monthly APAC intelligence call series continued to grow in attendance and member engagement, reflecting the overall growth in Core Members in this region. Additionally, a virtual APAC regional workshop was hosted in February.

BISO Community
Group discussions focused on leadership tools and techniques, PCI 4.0 updates, assessment methodologies, work prioritization, best practices for effective security guidelines, and risk management. In addition, the FS-ISAC presented their first iteration of a BISO whitepaper and invited our members to contribute to the second iteration.

CISO Community
More than 350 CISOs/CISO equivalents and deputies met monthly throughout 2024 to discuss everything from dealing with the CrowdStrike and Blue Yonder

issues to perspectives on also owning infrastructure. The monthly calls are also an open forum for members to bring questions to their peers for discussion.

Consumer Goods
Focusing on the unique business risks of manufacturing within retail and consumer goods, the Consumer Goods Sector Interest Group discussed topics ranging from doing business in China to how to secure IOT/OT devices. The call always includes a briefing focused on the particular threats facing manufacturing and a round-robin forum.

CTI Roundtable

New this year, RH-ISAC launched a Cyber Threat Intelligence (CTI) Roundtable group. This meeting series is focused on the strategies and challenges of building and managing a CTI program.

Dark Web Working Group

This group conducted threat discovery marathons and dark web threat hunts. They also supported members in setting up an environment for dark web investigations. The group also hosted a hands-on workshop at the RH-ISAC Summit.

EMEA Community

A monthly EMEA intelligence call was launched in the spring to serve the growing number of members in this region. Additionally, regional workshops were held in London and Amsterdam.

Fraud Working Group

Discussion topics included refund fraud, loyalty account fraud, click fraud, account takeovers, reseller fraud, trends in airline/hospitality fraud, takedown strategies for fraudulent domains and malicious ads, and return fraud scams. This group also collaborated on developing two resources, the fraud taxonomy framework and the fraud sharing guide.

Gift Card Fraud

This group had presentations and discussions on the collaboration between law enforcement and retailers, gift card tampering, Storm 0539, and organized retail crime. Additionally, DHS HSI representatives gave presentations about Operation Bad Bot and Project Red Hook.

Hospitality & Travel

This group helps coordinate and foster closer collaboration between hospitality members, and shares intel, countermeasures, strategies, and best practices for the hospitality and travel sector.

Identity & Access Management

Topics covered by this group included consumer passkeys, maturity assessments, building an IAM program from scratch, and upcoming identity standards. Additionally, an IAM vendor gave a TLP: RED presentation about a recent high-profile incident they experienced.

Incident Response

This group held a TLP: RED discussion on lessons from recent cyberattacks. They also discussed a vendor's cybersecurity incident from an incident response perspective, maturing incident response plans, utilizing MITRE ATT&CK Flow, and moving away from third-party tabletop exercises. DHS CISA presented to the group on how to prepare for cybersecurity and physical security exercises.

Mergers, Acquisitions & Divestitures

Formed in June 2024, this group focuses on cyber diligence and integration planning for acquisitions and divestitures. Topics covered this year include different approaches to due diligence threat intelligence and benefits of buying vs. DIYing these services.

MISP

The MISP group met monthly to showcase new MISP features, share member use cases for vetted intelligence, and provide support for integrating with and troubleshooting MISP instances. The group also delivered hands-on MISP training during the Member Exchange Live event, which fostered deeper engagement with community intelligence.

Operational Technology

This group met quarterly to discuss OT-specific challenges, such as evaluating OT access, cyber threat hunting in an OT environment, implementing tools and technology, network segmentation, visibility over OT attack surface, and securing both managed and unmanaged devices without disruption.

Restaurants

A regular schedule of calls for restaurant members was established, along with a Slack channel to discuss issues unique to their sector. This group includes pure-play restaurants—both QSR and full service—as well as hotels and retailers that also operate restaurants on their properties.

Risk Management/Third-Party Risk Management

This group discussed risk-based decisions and metrics, cyber risk management, third-party risk management innovations, cyber risk quantifications, insider threat, impacts from third-party breaches, data loss prevention, and cyber resilience.

Security Architecture

Formed in March 2024, this group meets monthly to discuss security architecture topics and infrastructure, such as selecting the right framework for security architecture, security architecture roadmaps, zero-trust, and identity proofing.

Security Awareness

This group focused on educating employees about scams and leveraging AI for awareness functions. Discussions included AI threats, training at-risk roles, building security champions, and deepfake scams. The group also held a special meeting to plan Cybersecurity Awareness Month, sharing best practices, lessons, content, and event ideas.

Small Cyber Teams

The group explored best practices for growing cyber teams, including staff prioritization, budgeting, and resources. They also discussed leveraging AI for rapid CTI enrichment and addressed social media security concerns, such as access management, account ownership, and third-party risks.

Tool User Groups

Discussed how to identify the right tool for your environment, shared playbook use cases and tool automation scripts, crowdsourced upvoting of tool ideas, highlighted member experiences with new tool features, and provided members with community insight on issues they encountered.

Vulnerability Management

This group covered overwhelming scope, emerging vulnerability response, advanced threat hunting, prioritization myths, strategies for protecting e-commerce data, and 2024's top 5 CVEs. Additionally, two TLP: RED discussions focused on vulnerability discovery to mitigation and IoT security

> **Well worth the investment in order to gain and share experiences from CISO peers in the same industry. I value outputs from RH-ISAC more than any conferences I attend."**

RAISING OUR PROFILE

As RH-ISAC grows as an organization, our public presence as industry leaders also continues to grow. This year, RH-ISAC was featured as a subject matter expert in dozens of media outlets. Additionally, RH-ISAC staff took part in nearly 20 presentations to provide industry insights at conferences and events across the globe.

25 Earned Media Placements
> Top outlets include Wall Street Journal, CNBC, and Axios

18 Thought Leadership Articles
> Showcasing RH-ISAC staff in trade and niche media outlets

63 Blog Posts Published
> Promoting RH-ISAC intelligence reports and industry insights

17 Staff Speaking Engagements & Presentations
> RH-ISAC staff was featured at industry conferences and panel discussions

2,830 Comments, Reposts, and Reactions on RH-ISAC Social Media
> Total impression count is more than 100,000

> " I truly appreciate the welcoming environment and the eagerness of members to share information for the common good of the industry and the cybersecurity community overall."

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