2025 YEAR IN REVIEW

RETAIL & HOSPITALITY ISAC

2025 HIGHLIGHTS & KEY INITIATIVES

- Appointed Board of Directors **Regional Vice Chairs** for three global regions: Americas, Asia Pacific, and Europe Middle East Africa
- Hosted inaugural **CISO Forum EMEA** and gave out Sharing & Collaboration Awards for EMEA-based members
- Published first-ever **interactive CISO Benchmark dashboard** to allow benchmark data to be filtered by sector and revenue
- **Continued to grow usage of MISP** with 142 Core Members consuming MISP data, 9 Core Members automatically sharing to MISP, and 177 distinct integrations across 44 different tools
- Joined Meta's Threat Exchange Platform, a fraud intelligence sharing program used to **report fraud signals** collected from members
- **Revamped Associate Member** program to prioritize quality over quantity, ensuring stronger alignment with our mission
- Established new collaboration **groups for Gaming, Privacy, Infrastructure, and Doing Business in China**
- Integrated Feedly into centralized threat intelligence collections infrastructure to enhance collection, correlation, and production, while also streamlining the use of DataMinr and improving Jira automation for **higher-fidelity alerts**
- Established a **Working Group Champions** program to create more member ownership of groups and proactively identify relevant discussion topics
- Developed **multi-faceted fraud defense resources** that leveraged in-person events, presentations, strategic partnerships, detailed reports, and more
- In collaboration with stakeholders from across the organization, created a **strategic plan to guide RH-ISAC's priorities and goals** through 2029

> *"RH-ISAC has been essential in helping protect our organization from modern cyber threats. There is no other place we get the quality of intelligence at the pace we need to action on it before adversaries take advantage of us."*

FIGHTING FRAUD

As fraud continues to impact the industry, RH-ISAC launched several new initiatives in 2025 to address the threat and reaffirm our role in advancing collaboration and sharing in order to bolster fraud defense.

Reports & Playbook

- **Monthly Fraud Reports:** This report series provides an overview of notable fraud affecting the industry, along with analysis and predicted activity.
- **Ad Hoc Fraud Reports:** This report series details research findings from RH-ISAC fraud investigations.
- **Fraud Sharing Playbook:** In collaboration with Fraud Defense Forum attendees, RH-ISAC developed a playbook to guide members on fraud intelligence sharing. The playbook includes information about fraud indicators and offers templates for sharing with the community.

Fraud Defense Forum

- RH-ISAC hosted **two full-day in-person events** to convene cybersecurity professionals and strengthen collective efforts to combat fraud. Attendees learned about the end-to-end process of fraud intelligence sharing, focusing on breaking down organizational silos to ensure the timely dissemination of actionable insights.

Working Groups & Collaboration

- **Working Groups:** The Fraud Working Group and the Gift Card Fraud Working Group continued to meet monthly and saw increased attendance in 2025.
- **Fraud Investigations:** RH-ISAC hosted regular calls with members to enable collaborative fraud investigations.

Fraud Resources in MISP

- **Fraud Intel:** Utilizing the MISP platform's bookmark functionality, RH-ISAC established a unified bookmark for all threat intelligence tagged with the "fraud" attribute. This mechanism provides members with a streamlined, one-click method for filtering and reviewing exclusively fraud-related data.

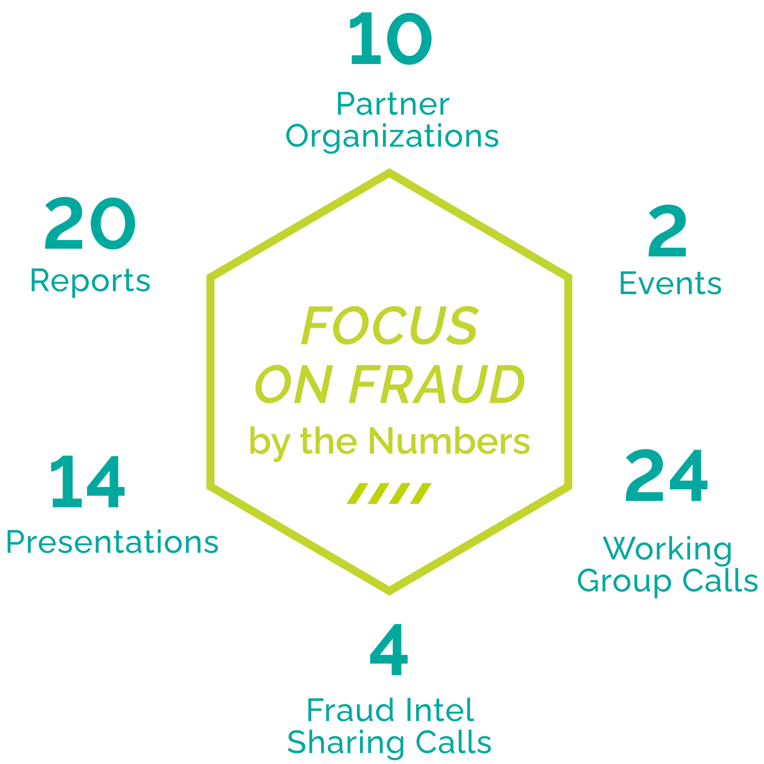
RETAIL & HOSPITALITY ISAC
Receipt Generated Fraud
Micky Haflund,
Associate Consultant, Threat Intelligence, Best Buy
Steve Diamond,
Sr. CTI Analyst, RH-ISAC
Lowe's
Information Security Group

Presentations

- **Fighting Fraud at Scale:** RH-ISAC staff gave this presentation at 13 workshops to reach members across the globe. The presentation included a threat briefing, an overview of fraud, information about fraud indicators and scenarios, and a deep dive into RH-ISAC fraud resources and how members can get involved to fight fraud.
- **Tackling Fraud—Current Trends and Strategies:** This was presented at Summit as a roundtable discussion led by industry experts to address current fraud trends along with mitigation strategies. The presentation fostered an open, collaborative environment that encouraged working together to fight fraudsters.

Partnerships

- RH-ISAC continues to deepen strategic alliances with industry organizations in order to enhance information sharing and resource efficiency by combining expertise and tools. RH-ISAC has 10 fraud-focused partnerships that seek to improve stakeholder coordination, streamline response efforts, and broaden the overall impact of anti-fraud initiatives across the entire community.



FOCUS ON FRAUD by the Numbers

10 Partner Organizations

2 Events

24 Working Group Calls

4 Fraud Intel Sharing Calls

14 Presentations

20 Reports

> *"It is amazing to be part of a group that feels as close-knit as we all are despite our companies ranging from being global companies to small 'mom and pop' shops. Even if our companies are competitors, we are still able to help each other for the greater good."*

MEMBERSHIP SNAPSHOT

In 2025, RH-ISAC's membership continued to grow in both size and geography. We finished the year with 333 Core Members after adding a total of 52 new members. Additionally, RH-ISAC continued to grow globally with new Core Members in countries across Europe and Asia. In the Associate Member program, we refined the partnerships to focus on value provided to the community.

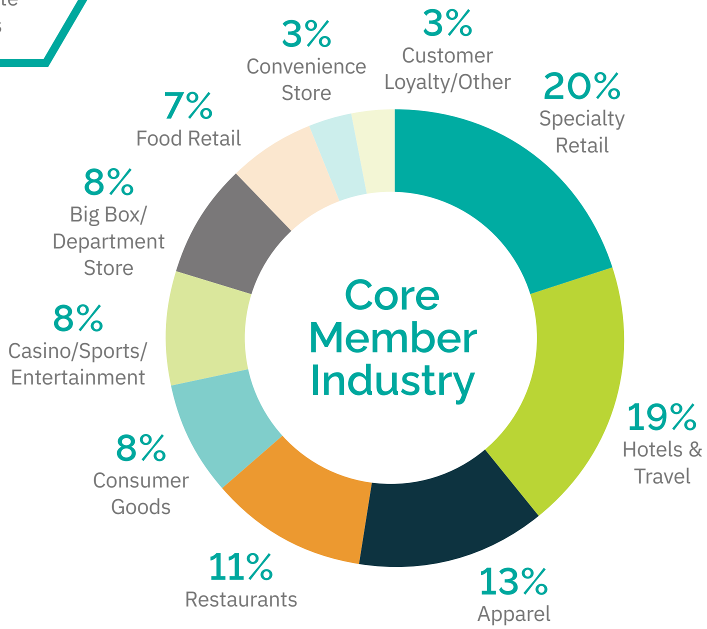
2021
224
Members
198 Core Members + 26 Associate Members

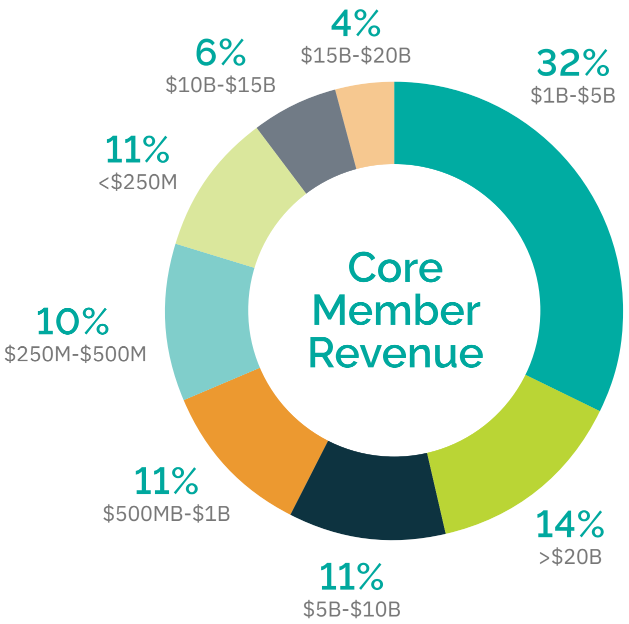
2022
256
Members
229 Core Members + 27 Associate Members

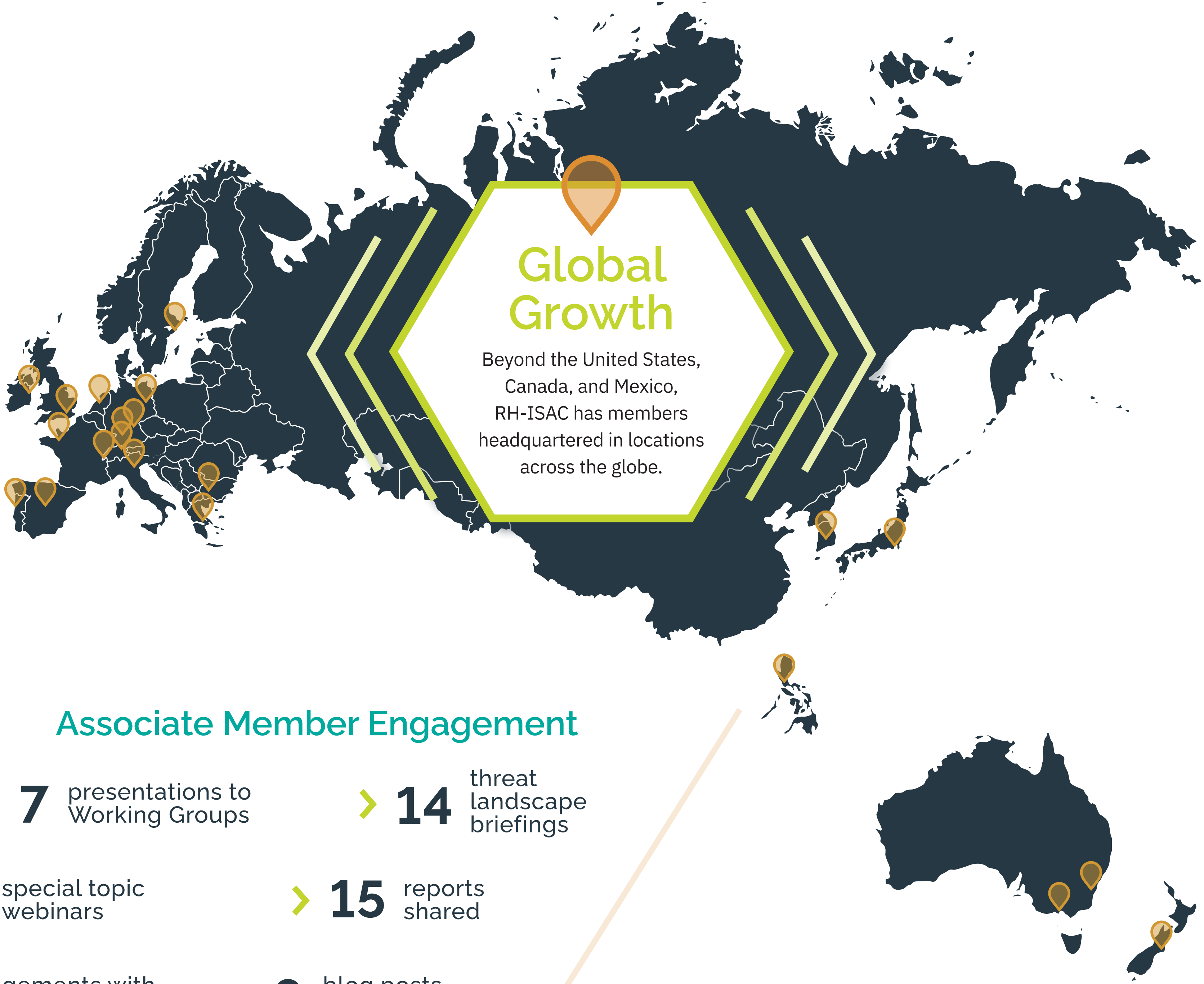
2023
287
Members
257 Core Members + 30 Associate Members

2024
327
Members
295 Core Members + 32 Associate Members

2025
363
Members
333 Core Members + 30 Associate Members







Global Growth

Beyond the United States, Canada, and Mexico, RH-ISAC has members headquartered in locations across the globe.

Associate Member Engagement

- **7** presentations to Working Groups
- **14** threat landscape briefings
- **7** special topic webinars
- **15** reports shared
- **9** engagements with RH-ISAC intel team
- **6** blog posts published

2025 SHARING & COLLABORATION OVERVIEW

96%
of members engaged in RH-ISAC

19,597
total shares across all sharing channels

5,015
individuals credentialed to sharing platforms

59%
of members shared intelligence

35,516
IOCs shared in MISP

17,158
vetted IOCs in MISP

12,302
total attendance in calls and webinars

1,011
attendees at in-person events

1,176
RFIs shared

2,967
responses to RFIs

183
real-time alerts & incident reports sent to specific companies

> *"We were able to leverage the ISAC to anonymously share information regarding a potential breach of a third-party service provider. Our sharing allowed other ISAC members to make better decisions at a time when public information was scarce and fear, uncertainty and doubt were circulating everywhere."*

INTELLIGENCE & BENCHMARK REPORTS

RH-ISAC continued to develop both the quality and quantity of reports issued in 2025. Several new intelligence reports were created, including a recurring fraud briefing report series and ad hoc fraud reports.

Intelligence Reports

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

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

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

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

17 Ad Hoc Fraud Intelligence Reports
Intelligence reports focused on fraud issues and indicators relevant to the Core Member community

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

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

4 Fraud Briefing Reports
Monthly briefing reports with intelligence about fraud

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

› **959** total reports

› **944** intelligence reports

› **8** survey reports

› **7** RFI summary reports

Survey Report Highlights

Annual RH-ISAC CISO Benchmark Report

The RH-ISAC CISO Benchmark Task Force partnered with Accenture to conduct the survey and analysis for this year's report. For the first time, this report included an interactive dashboard to enable data filtering by industry, revenue, and other criteria.

SOC Performance Benchmark

RH-ISAC surveyed member organizations on Security Operations Center (SOC) performance metrics (MTTD, MTTR, MTTC) to develop a first-of-its-kind benchmark report for the retail, travel, and hospitality sectors. Based on insights from member companies, the report analyzes trends in automation, incident volume, false positive/negative rates, and custom detection rules.

Security Awareness Survey Report

This survey focused on key areas like phishing simulations, content development, communication, vendor usage, and employee engagement, seeking to understand how efforts adapt to evolving threats. The resulting report analyzes practices, providing insights into human risk measurement, program maturity, challenges, and opportunities for improvement.

Cyber Risk Quantification Survey Report

RH-ISAC surveyed members on Cyber Risk Quantification (CRQ) implementation, focusing on maturity, integration with business risk management, and strategic prioritization. The report provides a comprehensive analysis of key practices, challenges, and opportunities based on insights from member companies, offering valuable guidance to strengthen CRQ efforts.

Generative AI (GenAI) Survey Report

This survey sought to understand how member organizations manage Generative AI (GenAI) governance. The survey explored governance structures, legal/security considerations, risk management practices, and GenAI solution usage maturity. The report provides analysis of key trends, challenges, and emerging practices from member companies, guiding organizations on oversight and implementation.

RFI Summary Highlights

SEC Materiality Determinations

This RFI sought insight into how organizations structure materiality determinations for cyber incidents under SEC expectations. The compiled summary highlighted common approaches and weighed both quantitative and qualitative factors.

Password Complexity and Rotations

This RFI aimed for guidance on extending the non-privileged user password rotation period from 90 days to annual, citing MFA and SSO as compensating controls. The summary highlighted key trends: widespread MFA use, increased character requirements, and movement toward longer or conditional password lifecycles.

Incident Response Retainers

This RFI asked if organizations rely on third-party forensics firms, utilize their cyber insurance provider's services, or have no formal retainer. Responses offered current approaches, preferred vendor models, and lessons learned.

Email Quarantine

This RFI sought information about how organizations manage employee access to quarantined emails. The request focused on permissions, specifically whether employees can view-only, release emails themselves, or require case-by-case approval.

AI Use in The Boardroom

This RFI asked about using AI tools for recording and producing meeting minutes, especially for board meetings. The member expressed concerns about security, confidentiality, and legal compliance with sensitive information and sought recommendations for tools that ensure data protection.

EVENTS

Reflecting our growing membership, RH-ISAC expanded its event offerings, delivering nearly 50 in-person and virtual events throughout the year—more than ever before. We also broadened the geographic reach of our events to better serve members across the EMEA and APAC regions.

46 events

25 in-person events

21 virtual events

1,732 total attendees

RETAIL & HOSPITALITY ISAC
Defending Retail & Hospitality: Navigating New AI-Powered Attacks and Invisible Threats

Regional Workshops

The 2025 Regional Workshop series expanded its global reach, delivering nine workshops across the U.S. and five workshops for members in Europe, Canada, Australia, and the Asia-Pacific region.

Workshop Presentation Highlights

The Human Element of Security: Using Emotional Intelligence to Build a Stronger Defense

Building a Purple Team Program

Evolving Incident Response Techniques to meet the AI Adversary

Bridging the Gap: Third-Party Cyber Risk Meets SOC & IR

- 14 workshops
- Locations: Portugal, Sydney, San Francisco, Toronto, Seattle, Denver, New York City, Las Vegas, Washington, D.C., Columbus, Charlotte, London, Dallas, Asia-Pacific (virtual)
- 480 attendees
- 100 speakers

RH-ISAC Cyber Intelligence Summit

In 2025, RH-ISAC's premier event grew even larger, bringing together almost 400 attendees and over 70 speakers. Hosted over three days in St. Louis, the Summit received excellent feedback.

FANDUEL SPORTS NETWORK Live!
2024 Sharing Stats
4,395
MEMBER MEETING & AWARDS CELEBRATION
Google Cloud Security

Summit Presentation Highlights

- *The 5% Revolution: How to Stop Being Busy and Start Being Brilliant*
- *Digital Deception: Deepfakes – The New Face of Cybercrime (2.0)*
- *Cyber Risk Quantification: Putting a Price Tag on the Apocalypse*
- *Home Depot's SOC Transformation Story*

- 398 attendees
- 73 speakers
- 5 keynote presentations
- 32 breakout presentations
- 7 networking events
- 4.73 out of 5 rating in attendee satisfaction

Fraud Defense Forum

In 2025, RH-ISAC launched the Fraud Defense Forum event series to provide a focused, one-day gathering for RH-ISAC members involved in fraud prevention and threat intelligence.

- 2 Fraud Defense Forums
- In-person, small group gathering for fraud practitioners

CISO Events

This year's CISO programming prioritized in-person gatherings that fostered networking and professional development.

2 CISO Forums › Full-day in-person events held in Chicago and Amsterdam

4 CISO Dinners › Small groups of CISOs in Dallas, St. Louis, Amsterdam, and Chicago

2 Industry Conference Events › Informal networking events held during RSA and BlackHat

Webinars

RH-ISAC's virtual programming included two distinct webinar series that were supported by Associate Members and leading solutions providers.

14 Retail & Hospitality Threat Briefings › Intelligence and research about threats facing the industry

7 Topic-Specific Webinars › Presentations about a specific topic of interest

> *"As a member of the RH-ISAC, I can confidently state that our participation has been transformative for our security posture. Prior to joining the RH-ISAC, our company experienced a credit card breach. Based on the intelligence sharing and collaborative security resources we've accessed through RH-ISAC membership since then, I am 100% certain that had we been members beforehand, we would have prevented that breach entirely."*

GROUP COLLABORATION

RH-ISAC's group collaboration opportunities continue to grow in 2025 with 25 total groups that hosted regular calls. A sector-interest group for Gaming was added, along with special interest groups for Privacy, Infrastructure, and Doing Business in China.

25
total groups

126
total calls in 2025

743
individual attendees

3,102
total attendances

62%
of members attended a call

25
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.

Artificial Intelligence
New this year, the RH-ISAC launched the AI Working Group. This group is for organizations leveraging AI technologies to enhance operations, customer experiences, and security capabilities. Discussions focused on AI tools for the SOC, the transformative role of AI in retail cybersecurity, and productivity gains in software development through the use of AI.

BISO Community
Group discussions explored the BISO career path, roles and responsibilities, the use of AI to enhance GRC capabilities, and cyber risk quantification. Additionally, RH-ISAC BISO Community members contributed to the second iteration of the BISO Whitepaper, led by FS-ISAC.

CISO Community
CISOs/CISO equivalents met monthly throughout the year to discuss key topics, including generative AI risks, MFA and identity security challenges, social engineering threats, legal liability concerns, and merging IT with security functions. The monthly calls are also an open forum for members to bring questions to their peers for discussion.

CTI Roundtable

This meeting series is focused on the strategies and challenges of building and managing a CTI program. In 2025, key topics discussed included physical security, fraud, phases of the intelligence cycle, and holiday season preparations.

Dark Web Working Group

Discussion topics included IT worker scams and dark web alert sources and management stack. The group supported members in conducting investigations and reporting assessments to leadership and hosted a hands-on workshop at the RH-ISAC Summit.

EMEA Community

Reflecting a broader expansion in the region, the EMEA intelligence call series reached new highs in member engagement and attendance. Key topics discussed include the Scattered Spider attacks against retailers and supply chain/third-party SaaS vulnerabilities.

Fraud Working Group

The Fraud Working Group continues to serve as a forum for members to exchange insights on emerging threats, detection strategies, and threat actors. In 2025, discussion topics included loyalty account fraud, cargo theft, nation-state cyber threats, credential stuffing, check fraud, brand impersonation, and the bot ecosystem.

Gaming Sector Interest Group

New this year, RH-ISAC launched the Gaming Sector Interest Group to strengthen coordination and collaboration among members, enabling the sharing of intelligence, countermeasures, strategies, and best practices specific to the gaming industry, including casinos, online gaming and betting platforms, and industry suppliers. Discussions centered on regulatory requirements and emerging cyber threat intelligence (CTI) trends and updates. These efforts progressed simultaneously, with the Interest Group and the gaming-specific workshop in Las Vegas building off one another.

Gift Card Fraud

This group had presentations and discussions on gift card security strategies, gift card tampering, new gift card fraud deterring technology, and the techniques and tactics used by threat actors committing gift card fraud.

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. Topics discussed included triangulation fraud, on-going sector specific fraud campaigns, and threat actor profiling.

Identity & Access Management

Topics covered by this group included changes in PCI 4.0, zero-trust architecture, Identiverse takeaways, domain consolidation and agentic AI. Additionally, a group member gave a TLP: RED presentation regarding identity verification. Identity & Access Management members collaborated and presented on a panel presentation at Identiverse on Transforming Retail and Hospitality Cloud with IAM: Enhancing Security, Operational Efficiency, and Customer Experience.

Incident Response

This group held a TLP: RED discussion on incident response for critical incidents and incident response playbooks. They also discussed red teaming/blue teaming, automated detections, mitigation assessments, and how to approach tabletop exercises.

Mergers, Acquisitions & Divestitures

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 effective cyber risk management during the M&A process.

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. In addition, there was an Advancing MISP for Better Intelligence: Updates, Enhancements, and Community Impact presentation held at the RH-ISAC annual summit.

Operational Technology

This group met quarterly to discuss OT specific challenges, such as asset inventory, secure remote connection for third-party/vendor, device visibility, and OT access architecture.

Additionally, an Associate Member gave a TLP: RED presentation on an OT-oriented malware.

Restaurants

This group includes pure-play restaurants, both QSR and full service, as well as hotels and retailers that also operate restaurants on their properties. The RH-ISAC Intel team briefed members on sector specific actors and campaigns at every meeting and also had an opportunity for round table discussion.

Risk Management/Third-Party Risk Management

The group explored risk-based decision-making and metrics, cyber risk management and quantification, AI-driven vendor questionnaires, risk registers, and the tools and platforms that support varying levels of maturity across risk management domains. The group also held an interactive Risk Management: Choose Your Own Adventure meeting, which highlighted a strong opportunity for an in-person session at Summit 2026.

Security Architecture

This group meets monthly to discuss security architecture topics and infrastructure, such as post-exploitation on active directory, prescriptive guidance documentation, OT Architecture, secure-by-design, modern defense in depth, and model context protocol (MCP).

Security Awareness

This group focused on educating employees about scams and leveraging AI for awareness functions. Discussions included AI threats and usage, combatting fatigue, repeat clickers, and planning for Cybersecurity Awareness Month (CSAM). The group also held a special meeting to discuss real-world tactics behind an effective CSAM.

Small Cyber Teams

The group explored best practices for growing cyber teams, leveraging automation, AI, and low-cost trainings and exercises. A DHS CISA Cybersecurity Advisor presented free to low-cost cybersecurity services and tools.

Security Tools and Technology

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

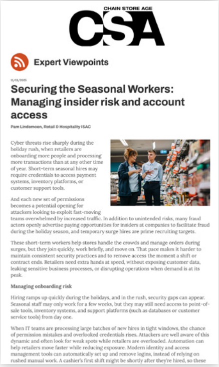
Vulnerability Management

This group covered metrics, bug bounty programs, trends in SaaS delivery, vulnerability scanners, AI usage, attack surface management, and 2025's top CVEs.

RAISING OUR PROFILE

As RH-ISAC continues to expand, so does our visibility as industry leaders. In 2025, RH-ISAC was showcased as a subject matter expert in nearly 50 media outlets, and our staff delivered a dozen presentations sharing industry insights at conferences and events worldwide.

26	Earned Media Placements	›	Top outlets include Wall Street Journal, Cybersecurity Dive, and Reuters
4	Podcast Interviews	›	Featured in retail, hospitality, and cybersecurity industry podcasts
25	Thought Leadership Articles	›	Showcasing RH-ISAC staff in trade and niche media outlets
43	Blog Posts Published	›	Promoting RH-ISAC intelligence reports and industry insight
12	Staff Speaking Engagements & Presentations	›	RH-ISAC staff was featured at industry conferences and panel discussions
3,205	Comments, Reposts, and Reactions on RH-ISAC Social Media	›	Total impression count is more than 180,000



CHAIN STORE AGE CSA

Expert Viewpoints

11/13/2025

Securing the Seasonal Workers: Managing insider risk and account access

Pam Lindemoen, Retail & Hospitality ISAC

Cyber threats rise sharply during the holiday rush, when retailers are onboarding more people and processing more transactions than at any other time of year. Short-term seasonal hires may require credentials to access payment systems, inventory platforms, or customer support tools.

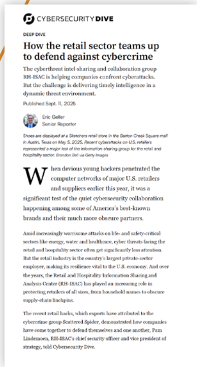
And each new set of permissions becomes a potential opening for attackers looking to exploit fast-moving teams overwhelmed by increased traffic. In addition to unintended risks, many fraud actors openly advertise paying opportunities for insiders at companies to facilitate fraud during the holiday season, and temporary surge hires are prime recruiting targets.

These short-term workers help stores handle the crowds and manage orders during surges, but they join quickly, work briefly, and move on. That pace makes it harder to maintain consistent security practices and to remove access the moment a shift or contract ends. Retailers need extra hands at speed, without exposing customer data, leaking sensitive business processes, or disrupting operations when demand is at its peak.

Managing onboarding risk

Hiring ramps up quickly during the holidays, and in the rush, security gaps can appear. Seasonal staff may only work for a few weeks, but they may still need access to point-of-sale tools, inventory systems, and support platforms (such as databases or customer service tools) from day one.

When IT teams are processing large batches of new hires in tight windows, the chance of permission mistakes and overlooked credentials rises. Attackers are well aware of this dynamic and often look for weak spots while retailers are overloaded. Automation can help retailers move faster while reducing exposure. Modern identity and access management tools can automatically set up and remove logins, instead of relying on rushed manual work. A cashier's first shift might be shortly after they're hired, so these



CYBERSECURITY DIVE

DEEP DIVE

How the retail sector teams up to defend against cybercrime

The cyberthreat intel-sharing and collaboration group RH-ISAC is helping companies confront cyberattacks. But the challenge is delivering timely intelligence in a dynamic threat environment.

Published Sept. 11, 2025

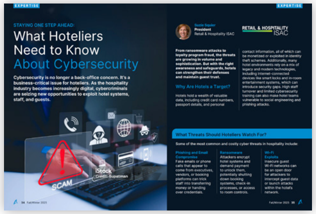
Eric Geller
Senior Reporter

Shoes are displayed at a Sketchers retail store in the Barton Creek Square mall in Austin, Texas on May 5, 2025. Recent cyberattacks on U.S. retailers represented a major test of the information-sharing group for the retail and hospitality sector. Brandon Bell via Getty Images

When devious young hackers penetrated the computer networks of major U.S. retailers and suppliers earlier this year, it was a significant test of the quiet cybersecurity collaboration happening among some of America's best-known brands and their much more obscure partners.

Amid increasingly worrisome attacks on life- and safety-critical sectors like energy, water and healthcare, cyber threats facing the retail and hospitality sector often get significantly less attention. But the retail industry is the country's largest private-sector employer, making its resilience vital to the U.S. economy. And over the years, the Retail and Hospitality Information Sharing and Analysis Center (RH-ISAC) has played an increasing role in protecting retailers of all sizes, from household names to obscure supply-chain linchpins.

The recent retail hacks, which experts have attributed to the cybercrime group Scattered Spider, demonstrated how companies have come together to defend themselves and one another, Pam Lindemoen, RH-ISAC's chief security officer and vice president of strategy, told Cybersecurity Dive.



EXPERTISE

STAYING ONE STEP AHEAD:

What Hoteliers Need to Know About Cybersecurity

Cybersecurity is no longer a back-office concern. It's a business-critical issue for hoteliers. As the hospitality industry becomes increasingly digital, cybercriminals are seizing new opportunities to exploit hotel systems, staff, and guests.

iStock
Credit: Supatman

34 Fall/Winter 2025

EXPERTISE

Suzie Squier
President
Retail & Hospitality ISAC

RETAIL & HOSPITALITY ISAC

From ransomware attacks to loyalty program fraud, the threats are growing in volume and sophistication. But with the right awareness and safeguards, hotels can strengthen their defenses and maintain guest trust.

Why Are Hotels a Target?

Hotels hold a wealth of valuable data, including credit card numbers, passport details, and personal contact information, all of which can be monetized or exploited in identity theft schemes. Additionally, many hotel environments rely on a mix of legacy and modern technologies, including internet-connected devices like smart locks and in-room entertainment systems, which can introduce security gaps. High staff turnover and limited cybersecurity training can also make hotel teams vulnerable to social engineering and phishing attacks.

What Threats Should Hoteliers Watch For?

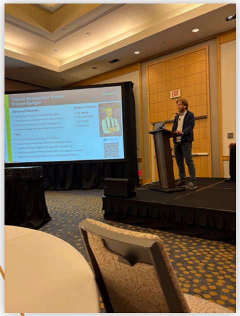
Some of the most common and costly cyber threats in hospitality include:

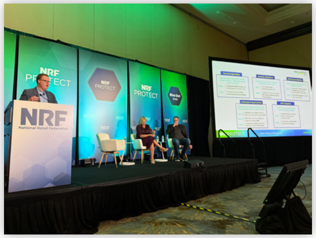
Phishing and Email Compromise
Fake emails or phone calls that appear to come from executives, vendors, or booking platforms can trick staff into transferring money or handing over credentials.

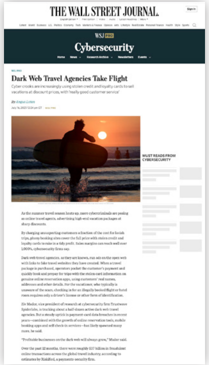
Ransomware
Attackers encrypt hotel systems and demand payment to unlock them, potentially shutting down booking systems, check-in processes, or access to room controls.

Wi-Fi Exploits
Insecure guest Wi-Fi networks can be an open door for attackers to intercept guest data or launch attacks within the hotel's network.

Fall/Winter 2025 35







THE WALL STREET JOURNAL.

Sign In

WSJ PRO

Cybersecurity

Home News Research Archive Newsletters Events

WSJ PRO

Dark Web Travel Agencies Take Flight

Cyber crooks are increasingly using stolen credit and loyalty cards to sell vacations at discount prices, with 'really good customer service'

By Angus Loten

July 16, 2025 12:24 pm ET WSJ PRO

MUST READS FROM CYBERSECURITY

As the summer travel season heats up, more cybercriminals are posing as online travel agents, advertising high-end vacation packages at sharp discounts.

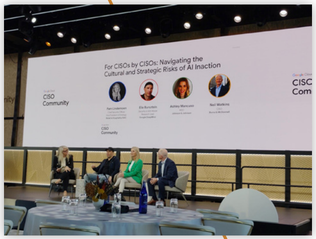
By charging unsuspecting customers a fraction of the cost for lavish trips, phony booking sites cover the full price with stolen credit and loyalty cards to rake in a tidy profit. Sales margins can reach well over 1,000%, cybersecurity firms say.

Dark web travel agencies, as they are known, run ads on the open web with links to fake travel websites they have created. When a travel package is purchased, operators pocket the customer's payment and quickly book and prepay for trips with the stolen card information on genuine online reservation apps, using customers' real names, addresses and other details. For the vacationer, who typically is unaware of the scam, checking in for an illegally booked flight or hotel room requires only a driver's license or other form of identification.

Ziv Mador, vice president of research at cybersecurity firm Trustwave SpiderLabs, is tracking about a half-dozen active dark web travel agencies. But a steady uptick in payment-card data breaches in recent years—combined with the growth of online reservation tools, mobile booking apps and self check-in services—has likely spawned many more, he said.

"Profitable businesses on the dark web will always grow," Mador said.

Over the past 12 months, there were roughly $37 billion in fraudulent online transactions across the global travel industry, according to estimates by Riskified, a payments-security firm.


For CISOs by CISOs: Navigating the Cultural and Strategic Risks of AI Inaction
CISO Community

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