RETAIL & HOSPITALITY ISAC

RH-ISAC FAQ

What is the RH-ISAC?

The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is the trusted cybersecurity community for the retail and hospitality sectors, including retailers, restaurants, hotels, gaming casinos, food retailers, consumer products, and other consumer-facing companies.

The RH-ISAC is dedicated to building and sustaining valuable programs, partnerships, products, and opportunities that enable members to build their trust-based relationships, and mature their strategic knowledge and tactical capabilities.

How did the RH-ISAC form?

The Retail & Hospitality 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 sector. What started with about 30 companies coming together in Pittsburgh, PA, in 2014 has now grown to include more than 130 Core Members (retailers, restaurants, hotels, gaming casinos, food retailers, consumer products, and other consumer-facing companies) sharing not only the threat information that they are seeing but their cybersecurity journey, as well, so others can learn, grow, and continue to mature.

Who can join the RH-ISAC?

Core membership is available to retailers, restaurants, hotels, gaming casinos, food retailers, consumer products, and other consumer-facing companies.

RH-ISAC also accepts Associate Members from industry-leading security service providers committed to adding value within the retail community, understanding industry challenges and supporting our retail members. Although Associate Members do not participate in the Core Member information sharing, our analysts forward important reports and other information provided by these key industry stakeholders.

What are the benefits of joining the RH-ISAC?

RH-ISAC members join a confidential sharing community of industry leaders and experts all working to continually improve the security posture of the retail and hospitality sector. Through the RH-ISAC, members benefit from real-time cyber intelligence on incidents, threats, vulnerabilities, and associated threat remediation from more than 1,200 analysts, threat hunters, and security engineers. Intelligence shared within RH-ISAC provides deeper insights and research into threats and vulnerabilities to help members prioritize industry threats, formulate an intelligence-driven strategy, and mitigate cyber risks with benefits.

Members also benefit from real-time collaboration, industry-specific benchmarking, threat intelligence reports and analysis, industry-relevant committees and working groups, and numerous training and education opportunities. Benefits include:

- **Intelligence Sharing**
  Intelligence is shared through the RH-ISAC email exchange, collaboration portal, real-time chat, virtual discussions, RH-ISAC vetted enclave, and more**.**
- **Committees and Working Groups**
  Sector-specific committees and working groups on industry-relevant topics and deliverables in support of RH-ISAC goals and objectives.
- **Automated Access**
  Gain access to shared indicators of compromise (IOCs) via API integration, MSSP partnerships and manual pulls.
- **Discounts from Associate Members**
  RH-ISAC works with Associate Members to provide Core Members discounts to programs and services, such as Cybrary for Business.
- **Industry-Specific Benchmarking**
  Compare your cybersecurity team's information security practices and processes among your true peers in the industry.
- **Education, Training, and Networking**
  Attend our RH-ISAC Cyber Intelligence Summit, sector-wide cybersecurity tabletops, Regional Workshops, monthly Cyber Thursday webinars, and education opportunities on leading-edge technologies.
- **Threat Research and Analysis**
  Benefit from daily intelligence reports, weekly intelligence reports, threat analysis reports, threat bulletins, threat intelligence briefs, and an annual threats trends report.

How much does it cost to join RH-ISAC?

Membership fees are based on annual corporate revenue. RH-ISAC dues are used to provide and produce products and services to support its members. Below outlines the membership fee structure.

Annual Corporate Revenue (USD)	Core Membership Dues (USD)
>$20B	$38,500
$15B - $20B	$25,000
$10B - $15B	$19,250
$5B - $10B	$14,100
$1B - $5B	$10,000
$500M - $1B	$5,000
$250M - $500M	$2,500
$100M - $250M	$1,000
<$100M	$500

How do we become a member?

If you'd like to become a Core or Associate Member of RH-ISAC, contact membership@rhisac.org or visit the RH-ISAC website at www.rhisac.org.

What is an Information Sharing and Analysis Center (ISAC)?

Sector-specific ISACs are trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats. Typically, global, private, non-profit organizations, ISACs work directly within their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness. ISACs are trusted entities that collect, analyze, and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. Besides sharing threat information with members, ISACs also share information with government and other critical infrastructure ISACs as applicable.

ISACs were created in response to Presidential Decision Directive-63 (PDD-63), signed in 1998, which called for each of the 16 critical infrastructure sectors to voluntarily establish sector-specific organizations to share information about cyber threats and vulnerabilities. After 9/11, the mission of ISACs was expanded to include the sharing of physical threats and vulnerabilities.

What is the difference between an ISAC and ISAO?

ISACs were created in 1998 in response to PDD-63 to advance the security of critical infrastructure/key resources (CIKR) sectors – those sectors deemed vital to the well being of a nation – through the sharing of information within and among the sectors and with government. Information Sharing and Analysis Organizations (ISAOs), formed in 2013 in response to Executive Order 13691, are information sharing organizations for any sector or community. ISAO's do not need to be part of the 16 critical infrastructure like ISACs. Instead, ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities.

ISACs are the original ISAOs for the critical infrastructure sectors. However, ISACs play a much bigger role in critical infrastructure protection and resilience than just sharing information. ISACs are a vital operational component in the national partnership framework. ISACs work through the National Infrastructure Protection Plan (NIPP-13) and collaborate with sector specific agencies and coordinating councils to perform structured collaboration within an established role in incident response across the CIKR. They are recognized as the designated arms for dissemination of information, manage and set the threat levels, and have strong reach and subject matter expertise within their respective sectors. ISACS consider all types of hazards, and look at threats in both the cyber and physical realms. They provide a sector perspective and allow for anonymization and aggregation of data.

What does an ISAC do?

ISACs help critical infrastructure owners and operators protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. ISACs collect, analyze, and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.

ISACs share information, collaborate, and discuss threat, vulnerability, and risk information about cyber and physical security risks through secure forums. ISACs also provide operational services – such as risk mitigation, incident response, and information sharing – that protect critical infrastructures. Other ISAC services include annual meetings, technical exchanges, workshops, webinars, 24/7 threat warning, incident reporting capabilities, setting the threat level for their sectors, and sharing actionable and relevant information more quickly than government partners.

Why is belonging to an ISAC important?

Being a member of an ISAC can extend the scope and capabilities of your organization's security and risk management activities and help bolster threat and risk awareness, preparedness capabilities, and help connect you to organizations and insights that may not be readily available to individual organizations, particularly smaller organizations with limited staff. Our adversaries – extremists of all stripes, cyber criminals, nation states and others – share their tactics, techniques, and procedures to outsmart and out-maneuver us individually. Together, as we share information and cyber threat intelligence across the community, we decrease attackers' chances of success.

What are the benefits of an ISAC?

Joining your sector's ISAC is one of the best ways organizations can protect themselves and their employees against cyber and physical threats and vulnerabilities while taking an active stance in safeguarding our nation's critical infrastructure. ISACs provide trusted sector specific forums for active information sharing and collaborative analysis around cyber and physical threats, vulnerabilities, and incidents. ISACs bring together analysts from companies of all sizes to share information on how to identify and defend against active attacks. In this way, companies with more robust capabilities assist each other and those with less robust programs.

The ability to have a single point of outreach to each critical infrastructure community is an important tool for national cyber incident response. ISACs can quickly and effectively share information from government to their members and can provide an important source of company-neutral analysis as to how a threat or incident affects their particular sector.

How do ISACs work with the government?

Information may be shared from ISACs with government partners and organizations but only with the submitting organization's explicit approval, under the agreed to Traffic Light Protocol designation and with or without member attribution, as desired by the member. ISACs work through the National Infrastructure Protection Plan (NIPP-13) and collaborate with sector specific agencies and coordinating councils to perform structured collaboration within an established role in incident response across the critical infrastructure sectors.