Frequently Asked Questions

What is the RH-ISAC?

The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is the trusted community for sharing cybersecurity information and intelligence in the consumer-facing sector. 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 and hospitality industries through collaboration.

Who Can Join the RH-ISAC?

RH-ISAC Core Membership is open to all retail, hospitality, and travel companies, including retailers, restaurants, hotels, gaming casinos, food retailers, consumer products, and other consumer-facing companies.

What are the Benefits of Joining the RH-ISAC?

RH-ISAC members join a confidential sharing community of industry leaders, all working to continually improve the security posture of the retail and hospitality sector. Intelligence shared within RH-ISAC helps members prioritize industry threats, formulate an intelligence-driven strategy, and mitigate cyber risks.

- **Intelligence Sharing:** Get real-time cyber intelligence on incidents, vulnerabilities, threats, and associated threat remediation from nearly 3,000 analysts, threat hunters, and security engineers. Intelligence is shared through the RH-ISAC Member Exchange, MISP, and Slack channels.
- **Automated Access:** Gain access to shared indicators of compromise (IOCs) via API integration, MISP integration, and manual pulls.
- **Threat Research and Analysis:** Save time with vetted intel from reports, threat bulletins, intelligence briefs, and quarterly and yearly threat trend reports.
- **Education, Training, and Networking:** Attend our RH-ISAC Cyber Intelligence Summit, tabletop exercises, regional workshops, and more, for opportunities to learn from, and collaborate with, peers and industry experts.
- **Industry-Specific Benchmarking:** Compare your cybersecurity team's information security practices and processes to your peers in the industry.
- **Working Groups:** Sector- and tool-specific working groups provide platforms for collaboration between peers with shared interests and job responsibilities.
- **Discounts from Associate Members:** RH-ISAC works with Associate Members to provide Core Members discounts to programs and services.

How Much Does it Cost to Join the 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. The table below outlines the membership fee structure.

Annual Corporate Revenue (USD)	Core Membership Dues (USD)
>$20B	$44,000
$15B - $20B	$33,000
$10B - $15B	$26,000
$5B - $10B	$18,500
$1B - $5B	$12,250
$500M - $1B	$6,500
$250M - $500M	$4,150
$100M - $250M	$1,825
<$100M	$550

How Do I Join the RH-ISAC?

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

Information Sharing & Analysis Centers

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

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?

In 2013, ISAOs were created, which are similar to ISACs except they can be for any sector or industry, while ISACs are limited to the 16 critical infrastructure sectors as designated by the U.S. government.

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. They provide a sector specific perspective and allow for anonymization and aggregation of data.

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?

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. 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.

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. Together, as we share information and cyber threat intelligence across the community, we decrease attackers' chances of success.

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.

Find an ISAC for Your Sector

To find the ISAC for your industry, visit the National Council of ISACs website.

https://www.nationalisacs.org/