



2022

Year In Review



Dear
members,

This has been a year of new and evolving cyber exploits, pandemic disruption, war in Eastern Europe with mass migrations, financial sanctions, and economic dislocation. All of this has impacted our sector and the people it serves in unprecedented ways. In response, this community banded together as never before to protect the global financial system and society's financial life. From the latest in phishing lures to nation-state threats, from evolving ransomware tactics to managing supply chain risk, we focused on arming our members with the intelligence and knowledge needed to keep our sector secure. Helping to drive this was a new level of sharing within the community, creating the collective strength that can only come from the sum of all efforts.

FS-ISAC's activities ranged across the subsectors of financial services and around the world, ensuring that members with shared interests had the platforms they need to cooperate and learn from each other, so that every member could tap the vast reservoir of knowledge of their peers, no matter their size or location.

The focus on Russia-Ukraine did not distract us from our global mission to advance the cybersecurity and resilience of the financial system. Our work in convening members with shared interests continued, with communities of interest focused on community institutions, insurance firms, asset managers, and payments becoming more active than ever. We kicked off new working groups focused on key issues for the sector such as the software supply chain and post-quantum cryptography.

With trust being so central to the strength of our community, we were thrilled to be able to resume meeting in person, with excellent attendance and myriad substantive discussions at our physical Summits around the world.

We know that threats constantly evolve, and that we must always test and improve our preparedness for whatever may come next. This year, FS-ISAC expanded our exercise program to help our members build the muscle memory to respond to new cyber threats. From our signature CAPS exercise at the firm level to leading the financial sector's participation in the multi-country, multi-sector NATO Locked Shields exercise, more than 12,000 members of our community participated in exercises.

We look to 2023 with focus and determination to keep FS-ISAC's members armed with actionable information and knowledge they need to protect their firms and customers. We are excited about our new strategic initiatives to both grow and strengthen the fincyber community around the world.

Thank you for everything you do to contribute to our collective mission, both in the work you do for FS-ISAC and as well as your tireless efforts in your own institution, day in and day out, to keep the world's financial system safe and secure. We look forward to continuing this journey together in the new year.

Wishing you happy and restful holidays,

Steven Silberstein

CEO, FS-ISAC

Contents

Intelligence	4
Security	6
Resilience	10
Membership	12
<i>Asia Pacific</i>	13
<i>EMEA</i>	14
<i>Latin America</i>	16
<i>North America</i>	17



The Russia-Ukraine conflict demanded the community's attention for much of the year, but the threat landscape continued to expand and evolve in myriad ways. While working to keep our members informed of potential threats connected with Russia-Ukraine, our Global Intelligence Office also ensured our community is prepared for the many other cyber threats facing the sector on a daily basis.



► Milestones and Developments

Direct Defense

- > Supported Microsoft's disruption operation of Zloader malware

Threat Actor Cards

- > Detailed information about individual threat actors and groups, as well as a DIY template for member use

Threat Landscape Report

- > Expansion to new geographic regions

GIO Internship Program

- > Expansion to all three regions, building the talent pipeline serving the sector

Intelligence Sharing with Critical Providers

- > Establishment of channels and processes for sharing intelligence with Akamai

► New Efforts

Digital Assets

- > Began research that will culminate in a series of reports and webinars
- > Held first of Spotlight Calls on Cybersecurity Concerns with Digital Assets

Fraud & Anti-Money Laundering

- > Expanded fraud channels in Connect
- > Started anti-money laundering specific discussions with members

Russia-Ukraine: Arming the Sector with the Latest Intelligence

The Russia-Ukraine conflict, and its accompanying potential for cyber activities, was a key focal point for the global financial sector in 2022. FS-ISAC's Global Intelligence Office coordinated regional and global intelligence gathering and disseminated it out to members, helping the entire sector stay informed and coordinated and contributing to the global view that the financial sector's cyber defenses are extremely mature.

Below is a summary of our activities supporting the sector during a time of high concern for the potential of concentrated attacks targeting the sector by a highly capable adversary and its allies.

Threat Intelligence Committees and the Global Cyber Threat Level

The Cyber Threat Level (CTL) is an industry barometer of cyber risk set by regional Threat Intelligence Committees (TICs) made up of members. As the conflict ramped up, our three regional TICs convened to discuss what members were experiencing due to the war, what their firms were preparing for, what they thought the CTL for the region should be, and providing guidance for members on what to do in an ELEVATED CTL environment.

The Global CTL remained at ELEVATED (the second highest of 4 levels) from February until May, the longest ever span for it to remain so high.

► Dedicated Communication Channels

- > The **Russia-Ukraine Connect channel** was created to discuss cyber activities facing the sector and geopolitical triggers that may lead to further events – **1330 members**
- > Two all-member **Spotlight Calls** on the potential for cyber action and preparedness – **3000 members each**
- > Frequent **consolidated alerts** via Share, our intelligence sharing platform, with running lists of alerts, articles, and materials

Cross-Sector Coordination

The Russia-Ukraine situation prompted us to recognize the need to collaborate with other critical infrastructure sectors. In Europe, we have extended our sharing between the financial sector and the telecom backbone providers.

Sector Representation to the US Congress

In April 2022, FS-ISAC CEO Steven Silberstein [testified](#) before the US House of Representatives Homeland Security Committee in a session entitled "Mobilizing Our Cyber Defenses: Securing Critical Infrastructure Against Russian Cyber Threats." He joined other senior critical infrastructure representatives from CrowdStrike, Tenable, and the American Water Works. Steven conveyed that the sector was being very diligent regarding the potential for heightened threats and well-situated to navigate the threat environment surrounding the war in Ukraine. He also discussed how strong and effective public-private partnership enhances the resilience of our critical sector not only generally, but also specifically relating to the geopolitical situation in Ukraine.

Representing the Financial Sector's Cyber Preparedness to the Media

Bloomberg

WSJ

The New York Times

FT FINANCIAL
TIMES

CNN

B B C

At the request of members, FS-ISAC activated its Media Response Team (MRT) to coordinate the sector's public messaging via the media. The MRT fielded more than 40 inquiries from global business and trade publications as well as major broadcast networks, resulting in a strong public message that the sector was vigilant, coordinated with relevant stakeholders, and prepared.



Security

As part of FS-ISAC's updated offerings structure, we have added the pillar of security to encompass all of the sharing within our community outside of threat intelligence: knowledge sharing at our events and best practices sharing among our many communities of interest and working groups.

► Events

Summits

Our flagship events returned in full force with our first in-person events in two years. Members were thrilled to be back together to share and discuss all the latest developments in the field, strengthening the trust so critical to our community.

6

Summits

~3000

Attendees

60

Countries represented

150

Member sessions

300

Sponsors

In Our Members' Words

“ The most important aspect was this event was in-person, open to all people, and we could once again **talk face to face** about our current challenges.

“ Great agenda and line up of speakers. **Real life examples** of incident handling, implementation challenges in different domains, and how people have overcome them.

“ Out of all the security conferences I've exhibited at as a vendor, FS-ISAC seems to have the **most cordial atmosphere between vendors and attendees.**

“ As a small bank the very best session was the horror story that is Active Directory. It gave issues and fixes that **I can use immediately.**

FS-ISAC Events Around the World



Re-imagining Resilience

Resilience and Cryptocurrency *Minimum Viable Data*

Collaboration as the Cornerstone of Cybersecurity

Women in Cyber Security **Post-Quantum Era of Cryptography**

Purpose Driven Collective Defense *Future of Money*

Ransomware Control Framework **Life After CISO**

Ranking Actors in the Threat Landscape

Diversity and Inclusion within Information Security Teams

Evolution of Cyber Threats

In Our Members' Words

“FS-ISAC is an excellent source of information that has made my job easier over the years.”

“I am typically on the site at least once daily for: alerts, library, dashboards, insights, member services and collaborations.”

“I use the information in the Risk Summary Report for our board meetings so please don't ever stop creating that content. It is much appreciated.”

“We have been a formal member of FS-ISAC for the past three years and we are clearly benefiting from the information sharing that you foster. Thank you for all you do to keep us informed and for providing us with the tools to collaborate with other members of the financial services community.”

► Communities of Interest & Working Groups

FS-ISAC communities support industries, regions, roles, functions, and relevant topics, ensuring that our members connect with and learn from peers with similar interests. FS-ISAC working groups allow subject matter experts to share ideas, exchange success stories, navigate challenges they face in protecting their firms and customers, and produce guidance for the rest of the membership. In 2022, FS-ISAC formed new working groups on post-quantum cryptography and the software supply chain, among others.

Key Topics of Discussion in 2022

Threat Actor TTPs

Cyber Insurance Coverage & Policy Acquisition

Ransom and Extortion Payment Policies

Breach Simulation Tools & Techniques

NY State DFS Regulation updates

Operationalizing Resilience

Establishing & Maintaining Responsible Disclosure Programs

Post Quantum Computing

Payment Card Industry (PCI) Data Security

Standard (DSS) 4.0 changes and how to operationalize

Community Institution and Association Council (CIAC)

The CIAC, in operation for a decade, is currently the largest community of interest (COI) in FS-ISAC.

Our goal with CIAC is to help distill the vast reservoir of information and knowledge shared throughout the FS-ISAC community into resources that community institutions can practically put to use protecting their firms and customers.

CIAC by the Numbers

~4000
Participants

16
Countries

410
consecutive Risk
Summary Reports

1600
Sample
documents

New in 2022:

- > **Executive Risk Report:** A single topic, high-level threat report for C-suite and board executives that summarizes a particular risk and engages the reader with questions designed to stimulate discussion and assist in increasing control objectives within the firm.
- > **Commercial Services Security Newsletter:** A TLP Green co-branded document designed for members to provide security awareness information to commercial customers.

Coming up in 2023:

- > **State Coordination Pilot (SCP):** A new effort to increase local, state, and regional coordination and information sharing. The pilot, focused on Michigan and Wisconsin, creates regional and state Connect teams to allow secure sharing at the local level. The pilot also offers trial membership to non-members, as well as specialized support and training.

Securities Industry Risk Group (SIRG)

Our securities community continues to grow. Member firms vary widely in size, yet often face many of the same cyber threats and resilience challenges.

~1000 Participants
~30 Countries

To enable the group to share through additional mechanisms, FS-ISAC introduced the ability to obtain logs of electronic communications (Connect chats) for members to meet regulatory obligations.

Our work was highlighted by FINRA in a note to firms they oversee for being a trusted sharing community with intelligence and information specifically tailored to security staff at asset managers.

Insurance Risk Council (IRC)

Over the past several years, insurance has become a bigger

~900 Participants
20 Countries

target, and their regulatory requirements and need for resilience have increased. This year, we hosted a special session on the New York State DFS proposed regulation changes, as well as kicked off a dedicated Insurance Fraud Working Group aimed at understanding and reducing insurance fraud. Next year will bring IRC groups to our insurance members based in EMEA and APAC.

Payments Risk Council (PRC) and the Payment Processor Information Sharing Council (PPISC)

FS-ISAC is dedicated to reducing payment-related cyber risk and fraud. This year, we reinvigorated the PPISC with a four-part series on operationalizing the Payment Card Industry (PCI) Data Security Standard (DSS) v4.0 changes.

In partnership with members, we've constructed a PRC agenda for 2023 aimed at combatting the most common risks and fraud within payment systems.

In 2023, we will grow the breadth and depth of our payments work, broadening our scope to all types of payments processing and members around the

world, increasing dialogue and engagement between both groups, and building out our work with fintech and digital assets-focused members.

560 Participants

30 Countries

Post-Quantum Cryptography

In August 2022, we hosted the first Financial Services Post-Quantum Cryptography Global Congress. The event convened leading researchers and subject matter experts from around the world to align the industry's preparations and priorities for moving to a post-quantum world.

Key issues discussed:

- > Documenting all quantum-safe solutions and architectures currently embedded in systems
- > Identifying and prioritizing what will need to be quantum-safe and when
- > Engaging with critical service providers to understand their paths to quantum resilience, and ensuring alignment on secure solutions and adoption plans

The Congress set the stage for future collaboration and joint work products, which will continue in 2023. On an all-sector call on 23 September, the US's CISA recognized the leadership role FS-ISAC is playing in ensuring the financial sector is coordinated and prepared for the sea change quantum computing will bring to the industry and the world at large.

Software Supply Chain

Given the sector's common reliance on many of the same software packages and suppliers, we formed the Supply Chain Working Group to coordinate efforts around software supply chain management with 20 inaugural participants.

Initial outputs included a Software Supply Chain Primer and the creation of a Software Bill of Materials (SBOM) Working Group.

In September, FS-ISAC became an Associate Member of the Open Source Security Foundation, demonstrating our commitment to enhancing open source software supply chain security and reducing risks. In 2023 we expect this partnership to create opportunities and avenues to identify and remediate open source code vulnerabilities in packages commonly used within the financial sector.

New Resources Created by FS-ISAC Working Groups and Communities of Interest:

FS-ISAC serves as a vast reservoir of knowledge for fincyber professionals to share and learn from each other, avoid re-inventing the wheel, and of course, improve the security of the sector.

Created in 2022:

- > Software Supply Chain Primer White Paper
- > Digital Assets Primer
- > FS-ISAC Responsible Disclosure program: an avenue for researchers to disclose FS-ISAC findings and to connect researchers' disclosures to the appropriate financial services contact
- > Tailored newsletters for Community Institutions, Payments Council, Insurance, SIRG and Mortgage Risk Council, serving 8000 member users.

Up Next in 2023:

- > Software Supply Chain Threat Model
- > Perspectives on Digital Asset Threats Report
- > Vendor Selection Considerations for a Managed SOC
- > Connect-based Live Chats for Securities & Investments



T rue cyber resilience means being prepared for whatever comes. One of the key tools firms have for building resilience is exercises, which enable teams to build the muscle memory for incident response by practicing what to do in a wide variety of scenarios.

In 2022, FS-ISAC significantly expanded its breadth and scope of exercises serving the sector, from coordinating the financial sector's participation in the world's largest live-fire cyber exercise to enabling more than 10,000 cyber practitioners at member firms to practice responding to plausible real-world scenarios.

► CAPS – Cyber Attack Incident Response Virtual Tabletop

October



FS-ISAC continues to support the global financial sector by providing a virtual team exercise for any group or team across organizations of all sizes. For the first time in 2022, CAPS provided three versions of its scenario to accommodate securities and investments, insurance, and banking. This allows a shared scenario to be provided amongst various industry segments to identify the implications of an incident across the entirety of the sector.

CAPS looks to improve the applicability of its scenarios to both insurance and securities and investments for 2023 and will build on the progress it made for regional language promotion and support in 2022.

In Our Members' Words

“ This year was our organisation's first involvement in the CAPS 2022 exercise, and the feedback from participants was overwhelmingly positive. It highlighted the importance of cross functional involvement across the wider business teams and demonstrated it is not just an information security challenge.

Additionally, it reinforced the importance of developing a specific playbook for these types of scenarios to ensure a coordinated and consistent response across the business.

Running the exercise, without any alterations, created an engaging and informative experience for the team which subsequently created a 'buzz' as word spread across the business. In fact, next year we might be struggling to keep the number of participants limited, a good problem to have!!!”

► Locked Shields

April



Held annually in April, NATO's Locked Shields is the world's largest live-fire cyber defense exercise. The exercise simulates a multi-faceted, multi-sector attack by one nation-state on its neighbor.

As a primary planning partner, FS-ISAC worked with member organizations and key sector partners to develop the financial sector elements for all levels of the exercise. Locked Shields is an important opportunity for FS-ISAC to promote information sharing across borders and between sectors, as well as enhance public-private partnerships and collective defense to strengthen the resiliency of the global financial system. FS-ISAC continues to support this initiative and is actively engaged in Locked Shields planning for 2023.

► **Hamilton Series (US): Incident Communications and Messaging Tabletop Exercise**

September


17
Organizations

FS-ISAC supported and participated in this public-private exercise to understand the US financial sector's policies, procedures, and general readiness to

coordinate communications and messaging during a cybersecurity incident.

FS-ISAC's Media Response Team was integral to the discussion on how FS-ISAC engages with its members and partners during an incident to assist with public messaging around sector health.

This discussion highlighted ways in which FS-ISAC and government partners can work together more closely prior to public messaging to increase alignment in communication and anticipate questions from the press.

► **Steel Resolve (US): FS-ISAC Hosts First Functional Exercise**

October


200
Participants


30
Organizations

As part of its continuing support of the sector's broad preparedness and operational resilience

efforts, FS-ISAC provided an environment for participants to act out their policies and procedures in real-time in response to a large-scale attack on a global financial institution.

Steel Resolve is a significant step in the sector's ability to observe and assess incident response capabilities at the firm level, the interaction between firms, and public-private partnership activities.

Through this exercise we were able to identify several opportunities to improve information sharing and sector coordination across FS-ISAC committees. These recommendations will be incorporated into FS-ISAC's playbook to enhance its ability to support the incident management process.

► **International Cyber League Financial Cup**

October


55
Teams


36
Member firms

During Cybersecurity Awareness Month, FS-ISAC and its partner Cyberbit hosted a tournament for cybersecurity teams around the world to respond to live-fire cyber attack simulations replicating attacks they may encounter in real life.

Teams were evaluated based on industry standard incident response KPIs, including investigation, eradication, and remediation goals, as well as their response times. The exercise provided a virtual arena emulating an organizational network and a virtual security operations center (SOC) that simulated the live attacks and automatically scored the teams based on their achievements.

Membership



Member Experience

In 2022, the FS-ISAC Member Experience Team introduced our Member Success program. This new initiative focuses on the practical education of members to help them get the most value out of their benefits. In the first year, the team saw participation from over 3000 users in our Success sessions globally. Looking ahead to 2023, the team will continue our monthly sessions while adding new foreign language sessions in our global regions.



Affiliates

FS-ISAC Affiliates are trusted vendor firms who provide crucial services to our members.

Affiliates share their knowledge with members throughout the year on webinars as well as at in-person events.

19
Expert Webinar
Series

19k
Attendees

New Offerings



Scout

Our solutions directory, launched in January, allows FS-ISAC Sector Advisors and Affiliates to share company information, thought leadership, and discounts with members. Members can upvote and comment to share their experiences with other members.



MISP Send

This feed allows members to automatically share IOCs via MISP. Alpha testing began in November; roll out to the wider membership is planned in 2023.



Critical Providers

The program facilitates a two-way dialogue with members and critical providers about threat intelligence as well as efficient communication should a vulnerability, outage, or breach potentially impact members' operations. FS-ISAC piloted the program this year with Akamai and expects to announce new critical provider participants in 2023.



FS-ISAC Video

In April, we introduced a new streaming platform for members to view intelligence, exercise, summit and membership content on demand, magnifying our sharing across both space and time.

Asia Pacific

Operating from our regional hub in Singapore, FS-ISAC continues to build its presence across the Asia Pacific region. We work closely with partners such as the Monetary Authority of Singapore (MAS), collaborating through the CERES Forum for central banks and regulators.

In November, we signed a Memorandum of Understanding with South Korea's FSI to establish an agreed and transparent approach to sharing and management of global cyber threat intelligence and to strengthen capabilities for understanding and responding to cybersecurity threats through mutual cooperation.

► Australia Subsidiary

Given its role as a key strategic player in the global financial system, FS-ISAC is investing in building the Australian fincyber community through the creation of its Australian subsidiary, with a dedicated Regional Director and Intelligence Officer already on staff and another analyst being added in 2023 specifically to work on public-private partnership.



► Community Expansion in APAC

This year, we expanded two of our standing communities of interest to the APAC region, and created a committee to focus on deepening our presence in India.

APAC Business Resilience Committee

The APAC Business Resilience Committee (BRC) plans and conducts exercises to enhance the operational resilience of the financial sectors' critical functions and technology. It also serves to communicate impact and needs during a sector crisis through the maintenance of the Intelligence Sharing and Incident Response Playbook.

APAC Insurance Risk Council

The APAC IRC is a forum for insurers to collaborate and share best practices to address emerging or existing cyber security issues and raise their security posture.

India Strategy Committee

The India Strategy Committee (ISC) was set up to serve the security needs of the financial services industry in India, grow the member community, and enhance collaboration.

Up ahead in 2023

Initial discussions to form APAC chapters of the Payment Risk Committee (PRC) and Post-Quantum Cryptography (PQC) Working Group have begun. There is also a strong appetite to build a new regional community around regulatory requirements to address challenges encountered by CISOs. The APAC team will continue their deep engagement with members and public partners while strengthening FS-ISAC's brand awareness in Asia's emerging economies.

Global Leader



Jorell Magtibay

National Australia Bank Limited

"NAB has invested a lot in the readiness and resilience of not just our organisation, but the financial sector

as a whole. Cyber threats and malicious actors are constantly evolving, and sharing intelligence and best practices across the industry is crucial to developing solutions to keep our organisation and customers safe."

Europe & UK

► Europe

2022 saw a profound deepening of our European presence, with the establishment of our office in The Hague and the establishment of a European board to help guide and govern our European strategy. Their focus on Europe will help make the work we do here more impactful and meaningful for all our members in the region. It will also give European members and institutions the transparency and control that is necessary to trust FS-ISAC in strengthening and protecting European critical infrastructure.

► Connecting the Local to the Global: Switzerland

FS-ISAC promotes sharing of intelligence and security knowledge as well as resilience-building throughout the global financial system, but also recognizes that the world is not a uniform place. For this reason, we have developed a “global, local” policy where local needs at a regional or sovereign level are also supported.

FS-ISAC has agreed to form the Operational Cybersecurity Cell in the Swiss Financial Sector Cybersecurity Centre (Swiss FS-CSC). This follows a mandate from the National Cybersecurity Centre (NCSC) and regulators to address the need for greater national cybersecurity readiness and sharing of cyber intelligence and best practices, and to better coordinate incident response during a crisis. Swiss FS-CSC was founded in April and went live in September with a suite of early services, including critical alerts, moderated chats, and member meetings with the support of existing FS-ISAC staff. Additional services with exclusive Swiss channels are expected to go live in 2023 as the Centre builds out staff in-market.

► European Financial Services Roundtable

The European Financial Services Roundtable (EFR) brings together Board Chairs and Chief Executives of leading European banks and insurance companies to contribute to the policy debate on issues relating to financial services and financial stability. In 2021, EFR members nominated FS-ISAC as their strategic information sharing partner for cyber security in the region. As well as supporting monthly EFR information sharing calls with intelligence briefings. In 2022 FS-ISAC launched a European-hosted instance of Connect so that information shared can be domiciled in Europe as required.

Global Leader



Derek Pillar
Mastercard

"Mastercard is a proud supporter of the FS-ISAC community in EMEA, as we firmly believe that greater resiliency comes from the active sharing of best practices and actionable cyber threat intelligence."

► United Kingdom

The UK is FS-ISAC's second largest membership base, with more than 230 member firms. It is also our second largest office, with 10 full-time staff as well as the key roles of Global Head of Intelligence, Executive Director for Europe, and our new Third-Party Risk lead based there.

FS-ISAC continues to grow its role in the UK's fincyber ecosystem, with representation on:

- > UK NCSC (National Cyber Security Center) Industry 100
- > Bank of England CMORG CCG (Cross Market Operational Resilience Group Cyber Coordination Group)
- > Financial Services Information Exchange

New in 2022

UK
headquartered
firm
membership:
↑ 15%

In 2022, FS-ISAC was featured in the Bank of England's Sector Response Framework as a local organization with international reach, connecting the UK fincyber community with its global counterparts for sharing of both intelligence and security and resilience best practices.

As part of our work as strategic partner and executive committee member of UK Finance's Financial Services Cyber Collaboration Council (FSCCC), FS-ISAC analysts who are seconded to the NCSC's Industry 100 group sync regularly with FSCCC Fusion Cell members to discuss the tactical threat environment.

May 2023: Our First Fincyber Forum London

Given the strength of our UK community, for the first time in 2023, FS-ISAC will host a [full-day conference in London](#). The event will focus heavily on practical workshops and breakout sessions with immediately actionable takeaways.

Latin America

We continue to build our presence in Latin America and work with our members to build security maturity, both through increased intelligence and knowledge sharing in the region as well as by connecting the region with peers around the world.

New in 2022

Spanish
Language
Threat Calls
& Intelligence
Reports

to both locally-operating threat actors as well as a target for those from overseas.

In 2022, we worked with regulators from Brazil, Bolivia, Guatemala, Costa Rica, and Peru as they develop their national cyber defense strategies to understand the value of and encourage cyber information sharing in their national financial sectors.

This year, we welcomed three new Latin American authorities to CERES, our sharing forum specifically for central banks and regulators. CERES not only serves as a trusted platform for intelligence sharing, but also for knowledge sharing and coordination around evolving approaches to regulation around the world.

In 2022, we also saw growth of locally headquartered members in Chile, Mexico, Argentina, Bolivia, and Ecuador.

In 2023, three new events in Mexico, Brazil, and Costa Rica will connect member firms and public sector authorities to help build maturity and resilience of the industry.

Global Leader



Jaqueline Duarte
Banco do Brasil

"The financial sector only becomes stronger the more institutions across industries and regions cooperate, and this is just as true for the financial institutions in Latin America as it is for the US and the EU. Brazilian institutions have been a key player working with the FS-ISAC community, showing the strength of our market and our eagerness to support our counterparts across the globe."

North America

Given FS-ISAC's founding and two decades of work in the US, it is our largest membership base, and much of our US work is detailed elsewhere in the report. In this section, we highlight the public-private partnerships that exemplify our sector leadership as well as our growing work in Canada.

► Canada

2022 marked the first full year of FS-ISAC Canada's operations. The creation of FS-ISAC Canada in 2021

was prompted by 11 top Canadian member firms who had been sharing cyber intelligence within their respective industry associations such as the Canadian Bankers Association. The CISOs recognized the need to share across the larger financial industry, from banking to insurance, from financial markets infrastructure to asset management, to effectively respond to cyber threats at the national level. FS-ISAC is the global industry body that already does this, and so FS-ISAC Canada was created to enable Canadian firms to share among themselves as well as integrate with the global financial community.

Membership
growth

↑ 50%

Since
establishment of
FS-ISAC Canada,
May 2021

Key Initiatives

Canadian Cybersecurity Event

This year, FS-ISAC took over running the Canadian Cybersecurity Event, previously hosted by the Canadian Bankers Association, to open up participation by all financial sub-sectors.

850

Attendees at
the Canadian
Cybersecurity
Event

Canadian CISO Council (C3)

The leadership council, comprised of major member firms' CISOs, meets monthly and provides strategic leadership and guidance. It also serves to facilitate coordination with other cybersecurity organizations operating in Canada in order to eliminate duplication of effort.

Canadian Intelligence Council (CIC)

Integrated into the larger Americas Threat Intelligence Committee but also operating as its own smaller group, the Canadian Intelligence Council's 42 participants meet every week to discuss the local threat landscape.

During this year's major telecom outage in Canada, the CIC acted as a central hub for information on incident impacts and subsequently lessons learned on the risks and mitigating actions that should be considered from a global perspective.

Incident Response Team (IRT)

There is also a newly formed Incident Response Team (IRT) that meets monthly and as required. This group monitors and responds to defined national cybersecurity incidents and provides structure for appropriate national coordination.

Global Leader



Mark Cooke

Jack Henry and Associates

"Preparation through training and exercises are essential to defending against impending cyber incidents

and some of the most effective ways to strengthen internal defenses. Exercises develop muscle memory and concrete response procedures, and it is vital that all types of financial firms participate to boost the resilience of the sector."

► United States

Financial Services Sector Coordinating Council (FSSCC)

The Financial Services Sector Coordinating Council celebrated its 20th anniversary this year, along with its US government counterpart, the Financial and Banking Information Infrastructure Committee (FBIIIC). Through this official US public-private partnership forum, the FSSCC has provided sector leadership on several important issues, including a first of its kind data protection framework with our FBIIIC partners, CISA's initial Common Cybersecurity Performance Goals, and a variety of domestic and international regulation and policy proposals.

As the operational arm of the council, FS-ISAC is not only one of the FSSCC founding members and serves on its Management Committee but has also provided strategic leadership, with senior FS-ISAC staff serving as the FSSCC Executive Director and Deputy Director for FSSCC continuity as its Chair and Vice Chair change with routine elections. Our role within the FSSCC ensures that our members are privy to the latest policy issues being discussed at the US national level. In addition, in cooperation with the US Treasury, we increased monthly unclassified sector briefing attendance from 200 to 2000.



Thank You

to our members
and our broader community,
including Critical Providers, Sector
Advisors, Affiliates, and Sponsors.

We are grateful for your engagement
and participation, and look forward to
working together in 2023 and beyond.

Contact

www.fsisac.com

communications@fsisac.com