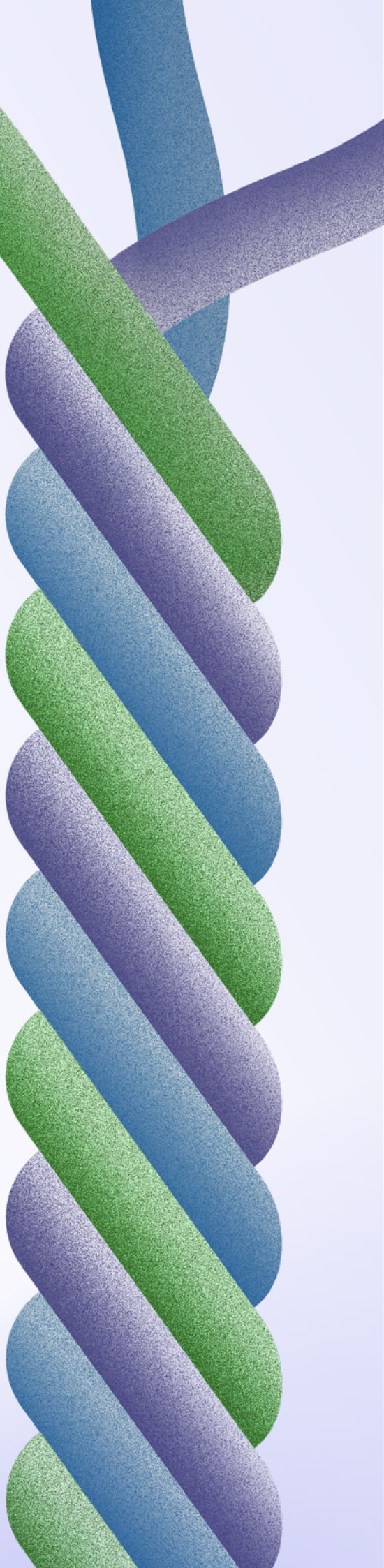
FS-ISAC

2023

Year In Review



Dear members,

In 2023, the many dimensions of FS-ISAC's work took on new urgency in response to the complex security and resilience challenges faced by the sector. Third-party incidents reached an all-time high, raising concerns of systemic impacts. Geopolitical tensions threatened to spill into the cyber arena at any time. Threats previously considered largely "solved problems," such as DDoS, roared back with sophisticated new tactics. New regulations changed the calculus for managing security programs. And emerging technologies like artificial intelligence and quantum computing amped up both the unpredictability and the velocity of the constantly changing landscape.

To help our members navigate this complexity, our incident response approach has matured to include private communication channels for those directly impacted as well as sector-level intelligence sharing and mitigation guidance. In addition to our ongoing analysis work at the strategic, operational, and tactical levels, we curated our members' expertise and insights to help the entire sector manage emerging risks, such as artificial intelligence and quantum computing. We coordinated with the public sector, other critical infrastructure sectors, and our critical providers, and exercised together to continuously improve our agility and effectiveness across a wide range of crisis scenarios.

While cyber threats know no borders, many challenges have local dimensions, and so we have expanded our staff around the world. Given varying levels of complexity, cybersecurity maturity, and regulatory obligations, our local leaders ensure that our work is valuable and relevant in every context in which we operate.

Looking forward to 2024, I see no end to the challenges facing us as a sector. However, I am confident that we will continue to rise to these challenges together. As a community of communities, we are investing in strengthening our many smaller groups based on geography, sub-sector, topic, and role to deepen the trust amongst members as well as maximize the relevance and value of their engagement. For example, as cyber and fraud converge, we are building up our fraud community within our membership and working across the sector on a holistic approach to reducing fraud. And of course, we will keep deepening and broadening our intelligence, security, and resilience work around the world.

We could not do any of this without the tireless dedication of our members. Thank you for everything you do to defend not only your firms and your customers every day, but also for sharing your knowledge and expertise to protect the entire global financial system. We look forward to continuing to deepen our work together in 2024 and beyond.

Happy holidays,

Steven Silberstein

CEO, FS-ISAC

Contents

Intelligence

In 2023, FS-ISAC played a sector leadership role in a record number of incidents, many of which involved key third-party providers to the sector. FS-ISAC's playbook for incidents, which was activated 28 times in 2023, includes:

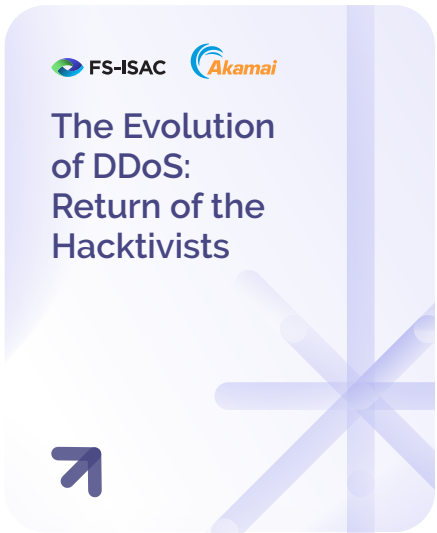
- Direct coordination with victim entity and impacted parties
- Dedicated information sharing channels for the wider membership
- Engagement of relevant communities
- Spotlight Calls prepared for members on the issue to disseminate information from experts, including from impacted firms
- Coordination and collaboration with public sector partners and other stakeholders
- Coordination of media response across the sector
- Published TLP White mitigation guidance for the sector

2023
Key Incidents Impacting the Financial Sector

- Ion
- LastPass
- Anonymous Sudan
- MOVEit
- HTTP/2 Rapid Reset
- Lockbit 3.0 & Citrix Bleed
- Scattered Spider
- Okta

We also hired a dedicated Third-Party Risk Lead to support the move from a reactive approach to third-party incidents to a more proactive approach. Using FS-ISAC's existing Affiliate program and our Critical Providers Program, we have built intelligence-level relationships with key suppliers to the sector to enhance communications and sharing, both on an ongoing basis and during incidents. We are also jointly leading the UK's NCSC Third-Party Supply Chain Working Group.

This work is alongside our daily activities of alerts, analysis, and reports on the full gamut of cyber threats facing the sector, from DDoS to ransomware to nation-state threats.



A joint report with Critical Provider Akamai to educate our community on the evolution of DDoS and mitigation best practices.

73k Indicators of Compromise	**13.7k** Member Alerts	**33** Technical Analysis Reports	Threat Calls (2 per region per month) **>17k** attendees **885** firms **67** countries
7k Product Vulnerabilities Reported	6 Spotlight Calls **>9.7k** attendees	**13** Intelligence Spotlight Reports	Member Feeds Activated **149** STIX/TAXII **60** MISP

Milestones and Developments

▸ Fraud Intelligence

As cyber and fraud converge, we have increasingly integrated fraud into our work, including enhanced alerting, tagging, analytical capabilities, and hiring a new Director of Fraud. In 2024, we will augment network defense capabilities with additional fraud analysis expertise, increase emphasis on fraud-related topics in our priority intelligence requirements, and support anti-fraud campaigns and task forces.

▸ MISP Submit

MISP, the open-source threat intelligence sharing platform developed by European CERTs, provides a format for machine-to-machine collection and communication of cyber threat intelligence. FS-ISAC trialed accepting automated intelligence submissions via MISP, which allows potentially much larger volumes of intel sharing. In 2024, we plan to introduce some of the automated MISP sharing into our feeds.

▸ Threat Actor Cards

Our Global Intelligence Office (GIO) expanded its use of Threat Actor Cards by printing them out in a friendly, accessible card game format and providing them to members at our events. The unique methodology used for the GIO assessments that form the basis of the cards is also available for member use as a standalone assessment tool, or to plug into their own threat modelling systems.

In Our Members' Words

"The value it's added to our reporting has been tremendous ... it really emphasises why we place so much value on our membership." - *T5 UK Bank*

"This ransomware incident affected a common provider to a lot of banks and financial services and there was a real need to communicate with the other big banks, not only in Australia, but globally. We often had more reliable information coming from the updates from FS-ISAC's analysts than we did from the victim of the incident." - *T2 Australian Bank*

"Those were excellent reports on stealer malware with great details." - *Tier 1 US bank*

"Although we are based in the US, a lot of times information that has come through via APAC or EMEA feeds is just as relevant and has allowed us to be ahead of the pack in regards to threats." - *Tier 4 US Bank*

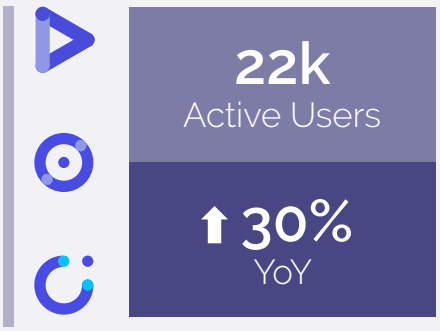
"We really liked the (specific incident) channel because it operated 24/7 with the latest updates as they came through, so we could use that to brief our Exec around the clock." - *APAC Threat Intel Committee member*

"I would like to take the opportunity to say how valuable FS-ISAC has been to me in my position as a cyber threat intel analyst. Thanks for providing a forum that allows for sharing of information that is highly relevant for the financial sector!" - *Tier 3 EMEA bank*

Based on GIO analysis and sourced from thousands of member firms in 75 countries, this annual report covers key cyber threats and trends.

Navigating Cyber 2023

▶ Intelligence Exchange



"Connect is brilliant, particularly direct 1-to-1 messaging with GIO and peers. Share is an outstanding piece of work. Threat calls – top class content."
- T5 European bank

Security

Through our security pillar, FS-ISAC curates our members' expertise on mitigating key risks through a wide range of communities, working groups, events, podcasts, reports, white papers, and more. In 2023, we concentrated on key issues facing the sector, from emerging technologies such as AI and quantum computing, to security issues around cloud computing, to the convergence of cyber and fraud.

Post-Quantum Cryptography (PQC)

- PQC white papers
- Named by US Cybersecurity & Infrastructure Security Agency (CISA) as the first industry to respond to PQC
- Co-led US Treasury Hamilton exercise on a cryptographic algorithm compromise
- Invited by US Treasury's Office of the Comptroller of the Currency (OCC) to educate examiners on PQC

Fraud

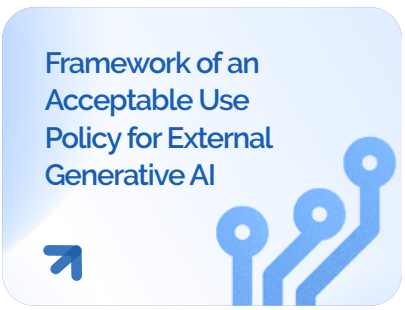
- Sector-wide fraud effort with BPI
- Triangulation Fraud Working Group formed. Published Holiday Shopping Threats white paper in November
- New Fraud Director hired
- Participated in US Federal Reserve's Scams Information Sharing Working Group

Cloud Security

- Google Cloud joined Critical Providers Program
- Cloud Security Working Group established
- FSSCC Cloud Security initiative with UST/Cloud Providers

Artificial Intelligence (AI)

- AI Risk Working Group established
- Framework for Acceptable Use Policy on External Generative AI published
- Adversarial AI exercise
- White paper series on managing AI risks: coming Q1 2024



Knowledge Page

FS-ISAC's Most Popular Communities

Topical

- Cyber Intel
- Fraud
- Cloud

Role-Based

- Threat Hunting
- Insider Threat
- Training & Awareness

Industry

- Community Institutions
- Securities & Investment
- Insurance Risk Council

↑ 30%

Community participation growth YoY

Active members participate in an average of

3

communities

In 2023 we launched our **FinCyber Today podcast,** featuring interviews with some of the top leaders in our field on the topics top of mind for our membership – from AI to PQC to TPRM to DORA and more.

Insights Page

Community Institutions

- State Coordination Pilot allowed for regional sharing and collaboration
- Third-party risk management tool: 1500 downloads

Top 3 topics of discussion

- Policy document requests
- Risk assessment templates
- Service provider feedback/outages

Securities

- Close coordination during cyber incidents impacting financial markets infrastructure

Top 3 topics of discussion

- Managed phishing detection and response
- Mobile monitoring and archiving
- Software agents

Insurance

- 8 surveys helped members learn from and benchmark against their peers
- APAC Insurance Risk Council launched

Top 3 topics of discussion

- Website attacks
- Regulatory changes
- Insurance fraud

Securities

- White paper on triangulation fraud
- Cyber Fraud Kill Chain Working Group launched

Top 3 topics of discussion

- Triangulation fraud
- Tracebacks
- PCI DSS V4.0 readiness

FS-ISAC

Events in 2023

▸ North America

> Denver
> Montreal
> New York
> Orlando
> San Francisco
> Toronto

▸ Latin America

> Mexico City
> Sao Paulo

▸ Europe, UK, Middle East, & Africa

> Amsterdam
> Cape Town
> Edinburgh
> Frankfurt
> London
> Zurich

▸ Asia Pacific

> Bangkok
> Bengaluru
> Hong Kong
> Melbourne
> Mumbai
> Singapore
> Sydney
> Tokyo

At FS-ISAC events, we gather to share knowledge and build the trust so vital to our community. Our regional summits continue to grow in scale and scope, with record attendance of both members and sponsoring providers to the sector.

Summit attendance
20% ⬆
YoY

Sponsor growth
25% ⬆
YoY

15
Expert Webinar Series

14k
Attendees

The most popular Expert Webinar Series this year:

- Threat Intelligence for Better Cyber Resilience
  Palo Alto
- How to Prepare for Mandatory Board Reporting
  Safe Security
- Identity and Access Management Roadmap
  Security Compliance Corp

In Our Members' Words

"It was a pleasure and privilege to present and be in the company of the breadth of our industry peers and experts. We thoroughly enjoyed the setup, pace, and variety at the conference and look forward to many more!"
- Tier 1 US Bank

"The richness of the programme means that there's something for everyone. As technical staff we've enjoyed hearing from speakers with hands-on experience of challenges we face daily. That's where the real value lies."
- Tier 2 EMEA Bank

"It's nice to see that I'm not on an island and face the same challenges as others. Also, the sharing of ideas is fantastic. I've found my people!"
- Tier 8 US Bank

FS-ISAC Women in Cyber Scholarships

Scholarship winners at EMEA Summit in Amsterdam

In 2023, we awarded 30 scholarships to students around the world, the largest class so far. These outstanding young women entering cybersecurity are sponsored by member firms. In addition to monetary awards, winners are paired with mentors at sponsoring firms and are invited to an FS-ISAC Summit to build their networks and get insight on the range of opportunities within cyber as they begin their careers.

Scholarship winners at FinCyber Today Summit in Orlando

Learn more about the program and sponsoring diverse young talent

Resilience

True resilience means being prepared for whatever comes. In 2023, we expanded the breadth and depth of our resilience work, including ~30 exercises around the world with thousands of participants across the financial sector, public sector, and other critical infrastructure sectors. We tested a wide range of scenarios and brought in an array of business functions as participants. And we incorporated our findings into playbooks and other key resilience plans.

Key Activities

> Establishment of the EMEA and APAC Exercise Committees

> Sector playbook enhancement drawn from exercise after-action recommendations

> Strengthened strategic partnerships (e.g. NATO Locked Shields, Tri-Sector Tabletop, GridEx)

> Explored emerging risks in exercise scenarios (e.g. post-quantum cryptography, AI)

> Improved firm and sector responses to severe but plausible threats such as third-party risk scenarios

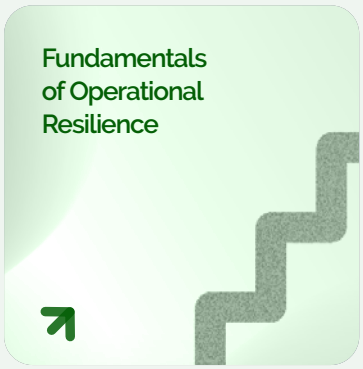
Exercise Highlights

> **NATO Locked Shields:** Strengthened the relationship between the financial sector and NATO in the world's largest live-fire cyber exercise with more than 3000 participants from 38 countries

> **Steel Resolve:** FS-ISAC-run functional exercise for improving coordination between public and private sectors during a significant third-party incident

> **Tri-Sector:** Led to the tri-sector playbook update for information sharing between Finance, Energy, and Telecommunications

> **US Treasury Hamilton Exercise on Cryptographic Algorithm Compromise:** Tackled complex PQC issues in a collaborative environment with law enforcement



Provides high-level guidance on establishing a resilience program

2023 CAPS

Signature firm-level exercise

1300
firms participated, reaching
>10k
participants

Scenarios customized for banking, insurance, and securities

83%
identified opportunities for improvement after on completing the exercise

In Our Members' Words

"As an employee that leads our cyber exercising, I found it extremely valuable to witness an operations-based test as we want to continue our exposure to this style of testing internally and externally." – *anonymous participant survey*

"Being the bank's IT officer, I struggle to keep up with testing and most of the time lack the ability to come up with good scenarios. I registered for this exercise thinking, why not – could be beneficial. Holy cow, I loved it!" – *anonymous participant survey*

"Interesting as ever to see where other jurisdictions are on some of these issues." – *Tier 5 EMEA Central Bank*

▸ International Cyber League Financial Cup

The second annual **International Cyber League (ICL) Financial Cup**, a hyper-realistic technical cyber exercise tournament, featured 75 teams competing from all over the world with top teams based in the APAC, EMEA, and North America regions.

FS-ISAC Around the World

2023 APAC Global Leader

David Gee
Global Head of Cyber, Technology, and Data Risk at Macquarie Group Limited

"At Macquarie Group Limited, we've collaborated to build a regional community, including working through the CERES Forum around regulatory harmonization to ensure industry-wide security progression through information sharing."

Asia Pacific

▸ Key Milestones

- Established an Australian subsidiary with dedicated Regional Director, Intelligence Officer, and Intelligence Analyst
- Signed intelligence sharing MOU with Singapore Cybersecurity Agency (CSA) and South Korea Financial Security Institute (building on existing intel sharing arrangements with Japan F-ISAC and Australia Cyber Security Centre)
- APAC Business Resilience Committee launched
- APAC Insurance Risk Council launched
- APAC Payment and Fraud Risk Council launched
- APAC CISO Congress attendance doubled
- Inaugural analyst workshop held in Sydney to increase understanding of basic intelligence analysis tradecraft

2023 EMEA Global Leader

Marina Nogales
Global Head Cyber External Engagement & Governance, Santander, accepting her Global Leaders award at our EMEA Summit in Amsterdam.

Europe, UK, Middle East & Africa

▸ Key Milestones

> Launch of European Board of Directors to ensure local governance and focus on Europe-specific issues, such as the unique regulatory environment

> Launch of UK Strategic Subsidiary Board to address specific needs of UK members and public-private partnerships:

- Bank of England Sector Response Framework
- FSCCC Executive Committee and Fusion Cell

> Largest EMEA Summit attendance ever

> Operation of Swiss FS-CSC Operational Cybersecurity Cell (OCS) to support domestic Swiss financial sector

> Formation of DORA Working Group (130 participants) and partnership with ENISA for input on DORA standards

> First FinCyber Forum London event, with new format of interactive sessions and workshops to promote community building

> Expansion of EMEA staff to support our growth across the region

Latin America

Key Milestones

- 50% YOY increase in attendance at bi-monthly LATAM threat calls conducted in Spanish
- LATAM Exchange Forum established to provide representatives from financial institutions based in the region an opportunity to connect once a month and share relevant information
- Two original Intelligence Spotlight Reports in Spanish using intelligence from members in the region and a monthly one-page intelligence report in Spanish *(Informe mensual de inteligencia)*
- More than 100 active member firms in the region
- First in-person Member Forum in Mexico and first in Brazil post-pandemic
- All systemically important financial firms in Chile are FS-ISAC members
- Two largest pension funds in Peru are members

2023 LATAM Global Leader

Alejandro Nuñez
Head of Cyber Threat Intelligence at Banco Mercantil del Norte

"Financial institutions across Latin America have been working to connect members and public sector authorities with the goal of building security maturity and resilience of the industry through increased intelligence and knowledge sharing. This award highlights our ongoing efforts to strengthen our cross-border collaboration in the region."

In Our Members' Words

"Thank you very much for bringing this type of event to our country. We lack live networking with our colleagues in the market. The rich content presented encourages us to collaborate even more with the local community." – Tier 2 Latam Payments Company

North America

Key Milestones

- Launched Canadian Incident Response Team to provide centralized coordination of systemic incidents
- Canadian companies started and co-chaired the Fusion Council (CIBC and BMO)

2023 North America Global Leaders

David Broad
Cyber Security Partnerships at CIBC

Samuel Strohm
Senior Vice President and Director, Global Security Fusion Center at PNC

- Launched Regional Meetings in Montreal
- Added new Regional Director to Canadian team

Thank You

to all of our members who have participated in the FS-ISAC community in countless ways.

And a special thank you to our sponsors and affiliates who make it possible to provide top quality events for our members

Contact

www.fsisac.com
communications@fsisac.com

FS-ISAC Affiliates

Accenture
Akamai
Allure Security
Anomali
Anvilogic
AppOmni
Arctic Wolf
Bancsec
Binalyze
Black Kite
Booz Allen
CECyber
Cerby
Cipher Tech
Cisco
Crowe
Cyborg Security
CyCognito
Cyware
Darktrace
Datex DataStealth
DefenseStorm
Doppel
EclecticIQ
Eclypsium
Enzoic
EY
ExtraHop
F5
Flare
Flashpoint
Fortinet
Fortra
Google
Group-IB
GuidePoint Security
HackerOne
HiddenLayer
HYPR
IBM
Illumio
Imperva
Inspira Enterprise
Intel 471
Island
KELA
KPMG
Mandiant, now part of Google Cloud
Mattermost
MazeBolt
Microsoft
Netcraft
NetSPI
LRQA Nettitude
Noname Security
Optiv
Palo Alto Networks
Prodaft
Proofpoint
Protiviti
PwC
Qohash
QOMPLX
Reflectiz
Resecurity
ReversingLabs
SafeBreach
SafeGuard Cyber
Safe Security
SailPoint
SCYTHE
Searchlight Cyber
SecurityScorecard
Securonix
SEI
ServiceNow
SessionGuardian
Silent Push
Silobreaker
SnapAttack
Splunk
Symphony Communications
Synack
Talon Cyber Security
Tanium
Team Cymru
ThreatBlockr
ThreatConnect
ThreatFabric
ThreatQuotient
Traceable
TrojAI
Trustwave
Vaultree
VMRay
Votiro
YouMail
Yubico
ZeroFOX
Zero Networks
Zscaler