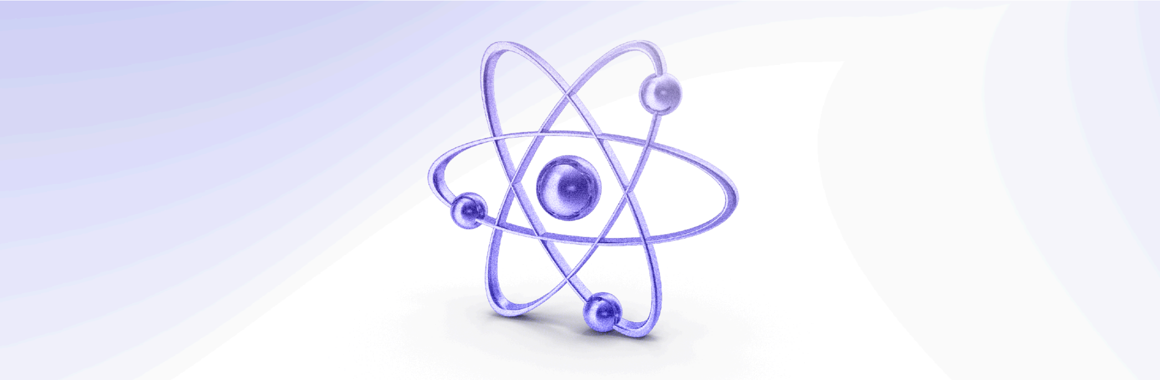
FS-ISAC | Executive Brief

Global Cyber Threat Level 🛡 | Americas: 🛡 EMEA: 🛡 APAC: 🛡 **June 2025**

We encourage you to share this brief with other senior executives of your organization or to incorporate this information in your regular reporting processes.



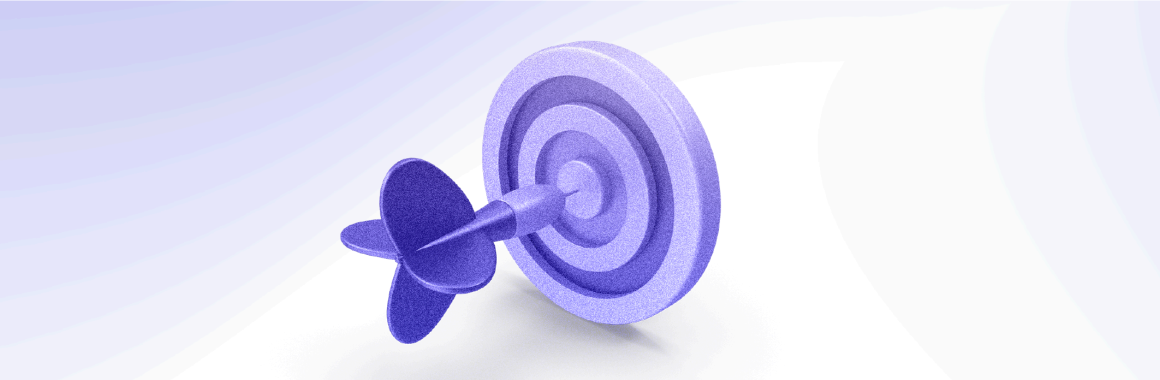
THREAT INTELLIGENCE UPDATE

Message App Archiving Service TeleMessage Breach

TeleMessage, which offers modified end-to-end encrypted message apps to include archiving features – used by some financial sector firms to fulfill regulatory requirements for archiving communications – announced it temporarily suspended its services after a hacker reportedly accessed archived group chats and direct messages on the company's modified version of Signal. TeleMessage modified the source code of Signal to create their version of the app – TM SGNL. The compromised data includes contact information, message content, and TeleMessage back-end login credentials.

On 12 May, the US Cybersecurity and Infrastructure Security Agency (CISA) added a vulnerability in TM SGNL to its Known Exploited Vulnerability catalogue, tracked as CVE-2025-47729. On 19 May, Distributed Denial of Secrets (DDoSecrets), the non-profit whistleblower site, indexed 410 GB of data from the breach. The data exposed reportedly includes metadata like sender and recipient information, timestamps, group names, and plaintext messages. Due to personally identifiable information in the dataset, DDoSecrets limited access to the dataset to journalists and researchers.

FS-ISAC has not been able to verify the contents of this dataset, but Reuters established that the phone numbers in the leaked data were correctly attributed to their owners. Two of the intercepted texts' recipients, including a financial services firm, confirmed to Reuters that the leaked messages were authentic.



WHAT'S NEW AT FS-ISAC

FS-ISAC Publishes Navigating Cyber 2025

FS-ISAC's Navigating Cyber 2025 report is now available. The report highlights the top cyber threats challenging the financial services sector today, including:

- The surge of fraud and scams enabled by generative artificial intelligence (AI)
- Attacks on suppliers that impact critical operations
- Threat actors' exploitation of geopolitical and economic conflict and uncertainty
- The increasing sophistication of long-established attack types, such as DDoS and ransomware

Navigating Cyber 2025 features an incident timeline of 2024, tracks FS-ISAC Cyber Threat Levels throughout the year, and details issues specific to countries and regions. And it provides key predictions for 2025 and beyond – offering firms valuable insights to help strengthen their cybersecurity programs.

A more detailed and technical TLP Amber version is available for members in SHARE.

Google and FS-ISAC Launch Financial Services Priority Flagger Program

Google and FS-ISAC announced a new joint effort, the Financial Services branch of Google's Priority Flagger Program (PFP). The initiative will combine Google's advanced threat detection capabilities with FS-ISAC's extensive network and intelligence sharing capabilities to prevent fraud within the financial sector.

Google's Priority Flagger Program streamlines the process of identifying, reporting, and mitigating fraud threats related to Google platforms. As part of this financial services-specific initiative, FS-ISAC will operate a dedicated CONNECT channel for its members to report fraud and other malicious activity leveraging Google Workspace or Google Ads.

There are more specifics on how members can benefit from this available here, and we held an Ask the Expert session with Google to provide greater insight into the program, the recording is available now.

The program is part of Google's participation in FS-ISAC's Critical Providers Program, which ensures collaboration and ongoing dialogue between the financial sector and Google.

FS-ISAC Publishes Guidance on Roles & Responsibilities of AI Usage

Financial services firms increasingly use AI to manage compliance, detect fraud, automate tasks, assist customers, simplify complex information, and other operations. However, the benefits and risks of AI usage depend on how well AI tools align with business strategies and how clearly the roles and responsibilities of usage are defined.

The FS-ISAC AI Roles and Responsibilities Working Group, made up of global cybersecurity experts, studied this issue and reported their findings in Define the Role, Limit the Risk: The Roles and Responsibilities of AI Usage in Financial Services. The paper describes how clearly defining roles by phase — governance, development, and implementation — and delineating responsibilities in each phase helps firms use AI more effectively and with less risk. This paper details how financial leaders can draft those definitions, determine responsibilities, and integrate AI into their business and risk strategies. Further, the paper offers advice on aligning AI with business goals, designing risk strategies, and developing secure AI technologies.

Read the guidance on FS-ISAC Knowledge

INDUSTRY NEWS

Coinbase Refuses $20 Million Ransom Demand, Offers $20 Million Reward to Help Identify the Extortionists

In mid-May, US cryptocurrency exchange Coinbase suffered a ransomware attack. The attackers bribed overseas staff to steal sensitive data, which was held for a $20 million ransom. Coinbase refused to pay the ransom demand – instead, the company is offering a $20 million reward to anyone with information that helps identify the extortionists.

Coinbase estimates the cost of the incident to range from $180 million to $400 million. That includes reimbursing customers who were tricked into sending funds to the attackers and greater investment in extra safeguards.

Read more in Reuters

New Resource from Global Security Agencies on Securing Data Used to Train & Operate AI Systems

In a recent Cybersecurity Information Sheet (CSI), global security agencies – including CISA, the Australian Cyber Security Centre (ASCS), and the UK's National Cyber Security Centre (NCSC) – released guidance on AI data security for organizations using AI systems in their operations. The CSI, AI Data Security, provides an overview of the AI system lifecycle and best practices for securing data used during the development, testing, and operation of AI-based systems. The CSI emphasizes data security to ensure the accuracy and integrity of AI outcomes, and encourages data encryption, digital signatures, data provenance tracking, secure storage, and trust infrastructure. It also reviews data security risks and provides mitigations for issues such as the data supply chain, maliciously modified data, and data drift.

Read the agencies' guidance

FS-ISAC | Knowledge

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

AI Risk

- Charting the Course of AI
- More Opportunities, Less Risk: 8 Steps to Protect Financial Services Data with GenAI
- Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks
- Building Cryptographic Agility in the Financial Sector

Post Quantum Cryptography

- The Impact of Quantum Computing on the Payment Card Industry
- Building Cryptographic Agility in the Financial Sector

Fraud

- Leveling Up: A Cyber Fraud Prevention Framework Framework for Financial Services

Phishing/Ransomware/Cloud

- Stop the Scams: A Phishing Prevention Framework for Financial Services
- Ransomware Essentials: A Guide for Financial Services Firm Defense
- Principles for Financial Institutions' Security and Resilience in Cloud Service Environments
- Cyber Fundamentals

Resilience

- Risk and Resilience Report: Subsea Cable Infrastructure
- Resilience in Action - Lessons from the Field

See the full list of Knowledge resources

FS-ISAC FinCyber Today

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Season one of 2025 is here!

- Olivier Nautet: Infobesity - How Much Data is Too Much?
- Karl Schimmeck: Data Security in a Demanding Regulatory Environment
- Claus Norup: Governance - What a CISO Needs to Succeed
- Matt Harper: The Convergence of Business and Cyber - Risk Management Through a Bigger Lens

Season two is coming soon, stay tuned at the links below.

See the full FinCyber Today Podcast catalog

Subscribe

TLP GREEN