View Online

FS-ISAC | Executive Brief

Global Cyber Threat Level | Americas: EMEA: APAC: **November 2024**

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

WHAT'S NEW AT FS-ISAC

Fraud Prevention Coverage in the FS-ISAC Community

Fraud prevention has emerged as a major focus for FS-ISAC with the 2024 Americas Fall Summit serving as a hub of fraud prevention coverage:

- 14 sessions featured members sharing how they were advancing fraud prevention.
- A Summit-first three-hour Fraud Prevention Workshop brought partners from telecommunications, social media, and members together to advance fraud prevention.
- Three CISO Congress members shared their fraud prevention expertise. Focus areas included fraud/cyber partnerships, fraud technology, check fraud, advancing fraud/cyber analytics, and effective social media monitoring.
- A presentation of the member-created Cyber Fraud Prevention Framework to help financial institutions recognize where they are in the fraud lifecycle, identify and disrupt fraud earlier, and communicate across the FS-ISAC community more effectively in a common language. The Framework covers recon, initial access, positioning, execution, and monetization.

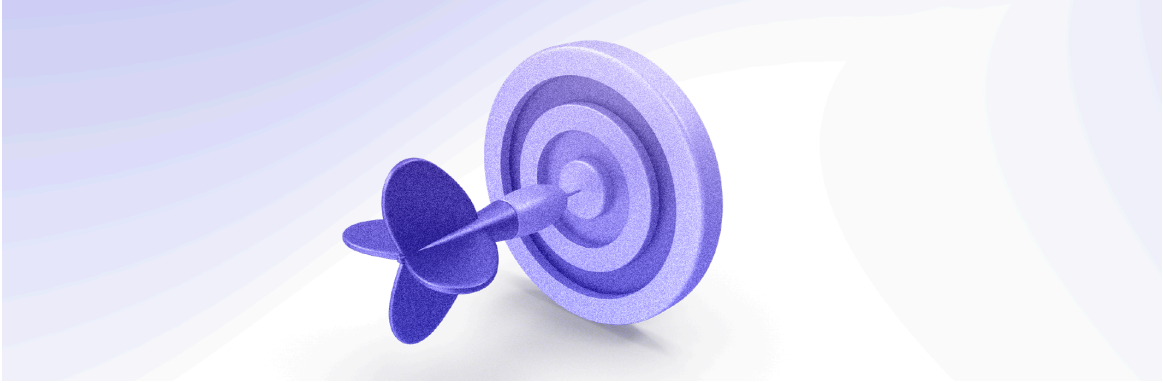
New White Papers on Deepfakes and Cryptographic Agility in the Financial Sector

FS-ISAC's Artificial Intelligence (AI) Risk Working Group produced a new white paper called *Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks*, which contains the first-ever Taxonomy of Deepfake Threats specifically for the financial service sector. Deepfakes are false but highly convincing video, images, and audio that threat actors use to infiltrate and steal from financial institutions. Written for both business and technical audiences, the Deepfake Taxonomy is categorized by threat – from CEO impersonations to attacks on deepfake detection models – and details the controls and mitigations appropriate to each threat. That approach enables firms to identify their greatest vulnerabilities and build bespoke defenses against this costly and growing threat. The paper contains:

- How financial services institutions are likely to be attacked by deepfakes
- The assets threatened by deepfakes
- The primary recipients of deepfakes
- A summary of controls available to financial firms

The latest publication from FS-ISAC's Post-Quantum Cryptography Working Group called *Building Cryptographic Agility in the Financial Sector* focuses on cryptographic (crypto) agility. The Working Group defines crypto agility as a design principle that makes adapting cryptographic solutions or algorithms faster and more efficient in response to developments in cryptanalysis, emerging threats, technological advances, and/or vulnerabilities. The goal of crypto agility is to improve business continuity when existing cryptography is compromised. Quantum computing is likely to make today's commonly used cryptography insecure in the next few years, so transitioning to crypto agility is critical for financial firms. Building Cryptographic Agility in the Financial Sector offers guidance for that migration, including:

- A framework for implementing crypto agility
- Challenges and how to overcome them
- Insights on transition governance and architecture



INDUSTRY NEWS

Cross-Reference Tool for Existing US Supervisory Cybersecurity Guidance

The US Office of the Comptroller of the Currency (OCC) has a tool called the Cybersecurity Supervision Work Program (CSW) that facilitates comparing high-level examination procedures across resources from OCC, Federal Financial Institutions Examination Council (FFIEC), industry frameworks like Center for Internet Security's (CIS) Critical Cybersecurity Controls, Cyber Risk Institute's (CRI) Profile, and National Institute of Standards and Technology (NIST) 800-53.

Learn more about the OCC tool

APAC Central Banks Demonstrate That Regulatory Compliance can be Embedded in Cross-Border Transaction Protocols

Cross-border transactions can create compliance challenges, and disparate jurisdictional regimes may slow transaction speed and increase costs. The Bank for International Settlements (BIS) Innovation Hub Singapore Centre, the Reserve Bank of Australia, the Bank of Korea, Bank Negara Malaysia, and the Monetary Authority of Singapore have demonstrated the ability to embed regulatory compliance in cross-border transaction protocols to reduce these challenges.

Read more from BIS

FS-ISAC | Knowledge

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- Ransomware Essentials: A Guide for Financial Services Firm Defense
- Protecting Financial Data with Encryption Controls
- DORA Information Sharing Requirements and FS-ISAC Membership
- Principles for Financial Institutions' Security and Resilience in Cloud Service Environments
- Business Information Security Officer (BISO) Program and Role
- Resilience in Action - Lessons from the Field
- Navigating Cyber 2024: Annual Threat Review and Predictions

See the full list of Knowledge resources

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Recent Episodes

- Carsten Fischer: The Need for Speed in Threat Mitigation
- Stephen Sparkes: The Evolution of the CISO Role
- Lindsey Bateman: Keep Your Eyes On The Horizon For Emerging Threats – And New Solutions
- Burim Bivolaku: Financial Sector Collaboration Is Key To Third-Party Risk Management
- Beate Zwijnenberg: Can Cyber Risk be Quantifed?
- Josh Magri: The CRI Profile – A Simplified Approach To Better Assessment
- Phil Venables: AI in Cybersecurity - Threats, Toil, and Talent

See the full FinCyber Today Podcast catalog

Subscribe

FSISAC
12120 Sunset Hills Rd
Suite 500
Reston, VA 20190

32 Threadneedle Street
London EC2R 8AY
UK

Hong Leong Building
16 Raffles Quay
Singapore 048581