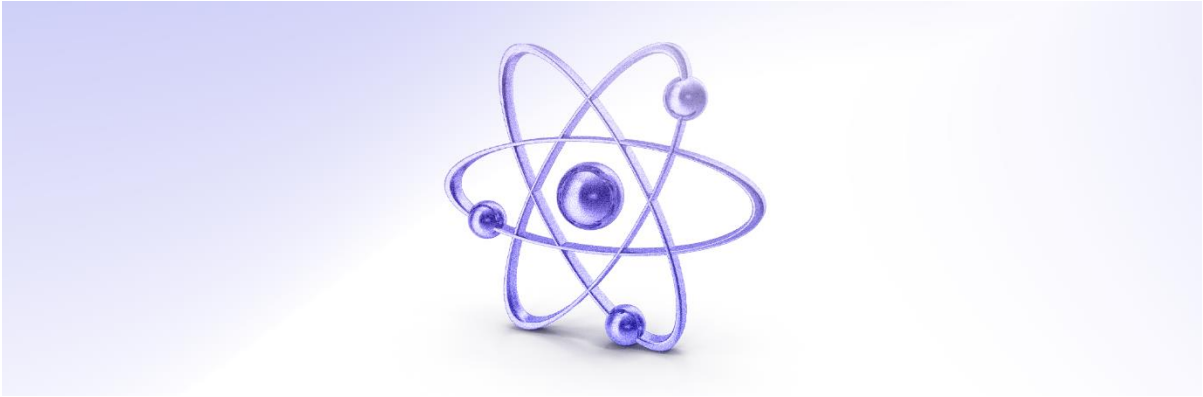
FS-ISAC | Executive Brief

Global Cyber Threat Level | Americas: EMEA: APAC: **March 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

North Korean Remote IT Worker Scheme

Between November 2024 and February 2025, FS-ISAC members reported receiving many suspicious applications from job seekers believed to be part of the North Korean remote information technology (IT) worker scheme. Several FS-ISAC members reported discovering cases of suspicious contractors they believed to be remote North Korean IT workers.

In this scheme, the North Korean government sends workers to locations around the world outside of reach from US authorities including Russia, China, Africa, and Southeast Asia so they can access the internet and steal identities of US citizens to obtain work in IT fields. Once hired, the threat actors have pivotal access within technology departments to conduct cyber attacks, intrusions, and data exfiltration and extortion.

To prevent this scheme, members can educate their HR staff and hiring managers on commonly used tactics and work with staffing partners on safer hiring processes and practices. Mitigations include conducting in-person interviews with candidates, verifying identification details with biometric and background checks, and reviewing applicants' contact information against known IOCs associated with these actors. FS-ISAC will be publishing a spotlight report on this topic soon.

RESILIENCE UPDATE

Findings from FS-ISAC's Third Annual Cybex Paladin Functional Exercise

On 25-26 February, FS-ISAC's Business Resilience team conducted its third annual Cybex Paladin functional exercise. The event included 435 participants from over 220 small- and mid-sized organizations in both the private and public sectors. In this remote simulation, FS-ISAC members tested their incident coordination and communication mechanisms in response to a fraudulent account takeover campaign.

By examining how the firms' employees would handle such an attack, the exercise

highlighted how individual organizations approach fraud campaigns internally and at a sector level. As a result, the exercise helped strengthen the resilience of the participants and the overall financial sector. The key takeaways from this exercise will become recommendations that small- and mid-sized FS-ISAC members can use to reduce fraud within their institutions and the sector.

Key observations from the exercise include:

- In an ever-evolving cyber insurance market, firms need a clearer understanding of the implications of their policies, especially as insurers require firms to have an increasing number of security and protection protocols to qualify for coverage.
- Given the widespread incidence of fraud, organizations should consider incorporating pervasive fraud activity and fraud campaigns into their incident response frameworks, together with fraud thresholds to trigger the activation of such a firmwide incident response.

WHAT'S NEW AT FS-ISAC

New Cyber Fraud Prevention Framework for Financial Services

A major challenge of fraud prevention is that the intel necessary for mitigation is often siloed in various teams, such as cybersecurity, fraud, financial crimes/anti-money laundering, and others.

To help these teams coordinate and direct their fraud prevention efforts, the FS-ISAC Cyber Fraud Prevention Working Group has published *Leveling Up: A Cyber Fraud Prevention Framework for Financial Services*. The Framework's impact can be dramatic at the institutional level - one bank saved hundreds of thousands of dollars a day, as a case study in the report details. Importantly, the Cyber Fraud Prevention Framework is also a mechanism for sharing cyber fraud information across the sector, making fraud prevention less challenging for everyone.

Read more on FS-ISAC Knowledge

New Paper on the Future State of GenAI

Artificial intelligence (AI) and particularly generative AI (GenAI) bring the financial sector to a new inflection point. However, while GenAI clearly facilitates opportunities for organizations, the sector has just begun charting its course into the future of AI. FS-ISAC's Artificial Intelligence Risk Working Group recently published *Charting the Course of AI* to help financial institutions:

- Predict the problems and identify the uncertainties involved in the phases of AI solution implementations
- Define the challenges and understand the nuances of AI in financial services
- Predict the short-, medium-, and long-term impacts of GenAI tools in realistic scenarios

Read more on FS-ISAC Knowledge

INDUSTRY NEWS

India to Give Banks Exclusive Internet Domain Name to Help Prevent Fraud

On 7 February, the Reserve Bank of India announced the decision to implement the ‘bank.in’ domain exclusively for Indian banks with registrations. The change will go into effect in April and is meant to help prevent scams and maintain trust with customers. After the rollout to banks, the domain ‘.fin.in’ will be unveiled for non-banking financial institutions. The US unveiled a similar initiative in 2015 with the ‘.bank’ top-level domain. Run by fTLD Registry Services on behalf of the American Bankers Association and the Bank Policy Institute, there

is considerable due diligence to ensure that only certified banks can register '.bank'.

Read more from the Reserve Bank of India

FS-ISAC | Knowledge

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- The Impact of Quantum Computing on the Payment Card Industry
- More Opportunity, Less Risk: 8 Steps to Protecting Financial Services Data with GenAI
- Risk and Resilience Report: Subsea Cable Infrastructure
- Stop the Scams: A Phishing Prevention Framework for Financial Services
- Ransomware Essentials: A Guide for Financial Services Firm Defense
- Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks
- Building Cryptographic Agility in the Financial Sector
- 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 Quantified?
- 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