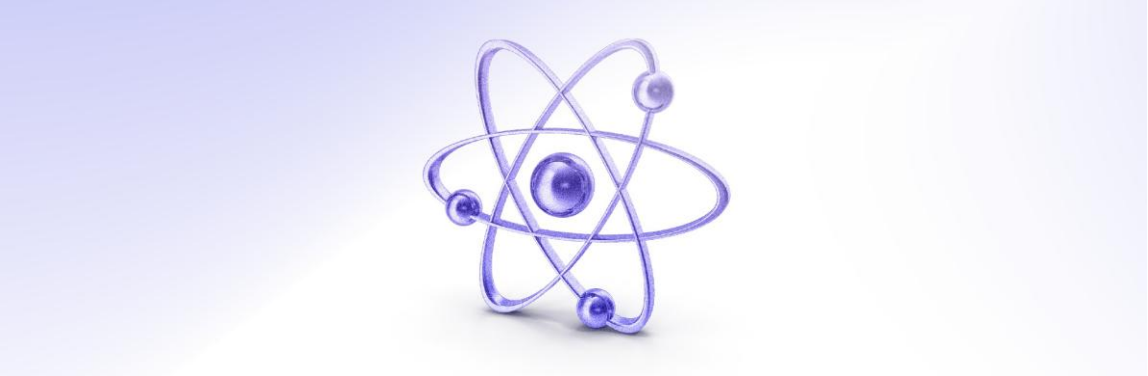
FS-ISAC | Executive Brief

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

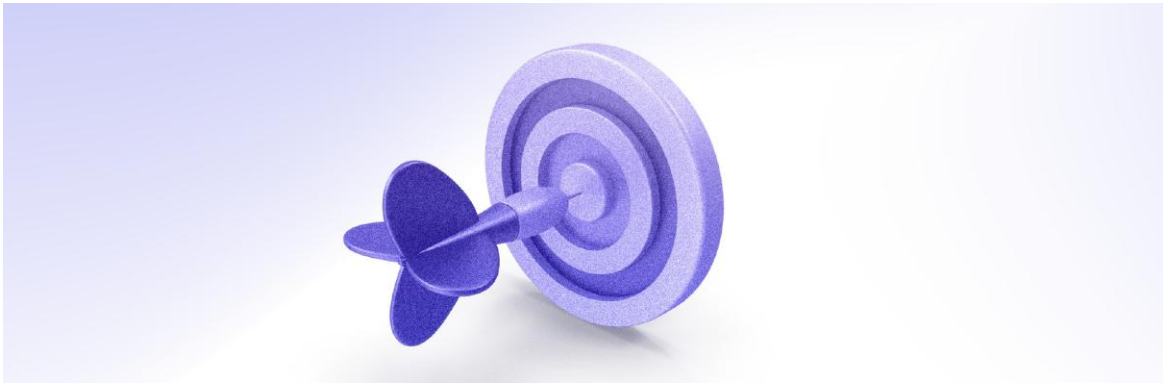
SharePoint Vulnerability

On 19 July, Microsoft published an advisory for two critical vulnerabilities affecting on-premises SharePoint servers:

- Remote Code Execution (RCE) vulnerability (CVE-2025-53770), which allows a threat actor to run malicious code on a system without physical access to it
- Spoofing vulnerability (CVE-2025-53771), which enables an adversary to create a request mimicking a legitimate SharePoint workflow, exploit a vulnerability in SharePoint's request handling, and bypass authentication mechanisms

These vulnerabilities have reportedly been chained and exploited as a zero-day vulnerability – i.e., a previously unknown or unaddressed security flaw – observed in widespread campaigns since at least 18 July. These attacks have enabled threat actors to achieve RCE, establish persistence, and extract cryptographic keys to allow the forgery of valid authentication tokens.

On 22 July, Microsoft reported observing two named Chinese state-sponsored adversaries exploiting the vulnerabilities against internet-facing SharePoint servers as early as 7 July. On 24 July, FS-ISAC members reported ongoing exploitation attempts observed since 21 July and have reported continuing indicators of compromise (IOCs). FS-ISAC assesses with moderate confidence that the exploit chain will be adopted by a wide range of adversaries in the near term. FS-ISAC recommends members review and implement Microsoft's mitigation guidance immediately.



WHAT'S NEW AT FS-ISAC

10 ISACs Collaborate on Scattered Spider Guidance

Scattered Spider is a financially motivated group known for extensive reconnaissance and highly effective social engineering techniques. To help organizations strengthen their defenses, FS-ISAC, the National Council of ISACs, and eight other ISACs jointly published Cross-Sector Mitigations: Scattered Spider, Guidance for Proactive Defense on 30 July.

The ISACs' analysis details Scattered Spider's activity based on its observed tradecraft across sectors as of May 2025 and provides:

- Background on Scattered Spider so that firms can better scope their threat surface
- Technical procedures and cultural practices to thwart Scattered Spider attacks
- ISAC, Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) intelligence
- MITRE ATT&CK® and other mitigations that have proven effective against Scattered Spider and similar threat actors

The ISACs assess with high confidence that Scattered Spider presents a real threat, and that its ability to exploit human vulnerabilities through social engineering makes the group a significant risk to organizations.

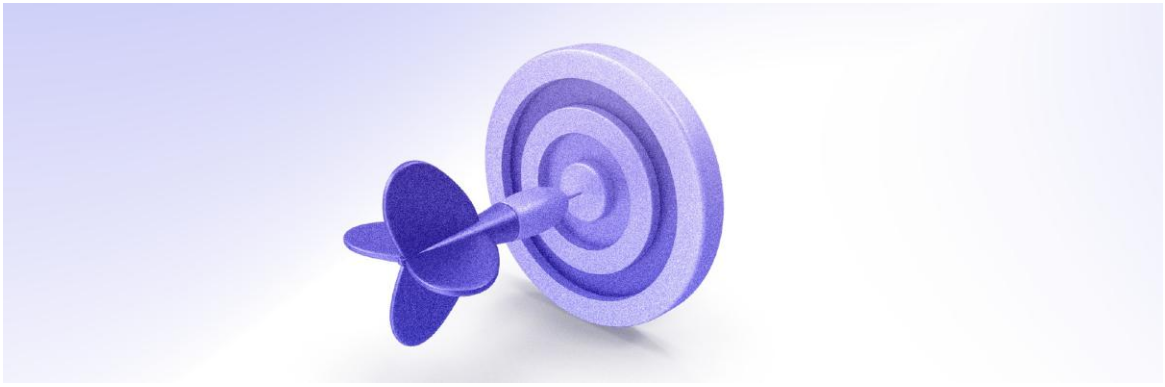
Multi-Sector Analysis of the Business Information Security Officer Role

Many companies have implemented the Business Information Security Officer (BISO) role to accelerate the security capabilities of – and create close partnerships between – business and technology teams.

To help businesses build an effective BISO program, members of the Financial Services, Health, and Retail and Hospitality ISACs developed a series of three white papers on the BISO role:

- *The Business Information Security Officer: An Overview; Actionable Advice from Practitioners in Four Industrie*s, which outlines the role, its responsibilities, its service catalog, and concludes with a step-by-step outline for building a BISO program
- *Structuring a BISO Role for Success: Responsibilities, Organizational Approaches, and Performance Indicators in the Business Information Security Officer Role*, covering BISO duties, organizational structures, and performance indicators
- *Mapping the BISO Career: The Development of an Effective Business Information Security Officer*, which details the skillsets, development approaches, and career paths typical of the role

The collaboration of three ISACs – representing over a dozen companies in four industries – offers a broad perspective on the BISO function and a comprehensive examination of organizational structures, tactical advice, and lessons learned from real-world experience.



INDUSTRY NEWS

Ransomware Payments Drop by Over a Third

Though 79% of IT and security professionals in finance surveyed for the 2025 Semperis Ransomware Risk Report said their organization had been targeted by a ransomware attack in the past 12 months (and 77% paid the ransom), a recent Chainalysis study finds that the total volume of ransom payments decreased year-over-year by ~35%. Chainalysis says the reduction is "driven by increased law enforcement actions, improved international collaboration, and a growing refusal by victims to pay."

Decisions regarding extortion payments are complicated business matters, but payment doesn't guarantee results – Semperis researchers found that 55% of ransomware victim organizations paid the ransom multiple times. Further, ransom payments fund threat groups and may violate Office of Foreign Assets Control (OFAC) sanctions.

Cybersecurity Budget Growth Falls, Amplifying Value of Intel Sharing

Researchers at IANS and Artico report that in most sectors, cybersecurity budget growth is half what it was last year (4%, vs. 8% in 2024) and a quarter of what it was in 2021 (16%). However, financial services cybersecurity budget growth remained above 5% and over half the surveyed financial services sector CISOs said their cybersecurity teams expanded.

The financial services sector's investments in cybersecurity enable an exceptionally robust security profile. Nonetheless, the financial sector is connected to others via payment and data transmission tools, among other mechanisms – and threat actors such as Scattered Spider prey on multiple sectors. In a threat landscape that spans industries, sharing threat information within and between sectors is a necessary aspect of resilience and security.

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

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Season two of 2025 is here!

- Meg Anderson: Lessons in Cyber Leadership From a Trailblazing CISO
- Jochen Friedemann: The Fun Side of Financial Services Cybersecurity
- Debbie Janeczek: How to Prepare for the Quantum Revolution
- Susan Koski: Managing the Move to the Post-Password Cyber Landscape
- Ariel Weintraub: Ensure Your Supply Chain Continuity – Even Under Pressure

See the full FinCyber Today Podcast catalog

Subscribe