FS-ISAC

Strengthening the Banking Sector: Collaborative Approaches to Cybersecurity Threats

California Banking Association, January 2025

Mike Silverman, Chief Strategy & Innovation Officer, FS-ISAC

Introductions and FS-ISAC Overview

Mission

FS-ISAC advances cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve.

FS-ISAC is the **member-driven, not-for-profit organization** that advances cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve.

Founded in 1999, the organization’s **real-time information sharing network** amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defense. Member financial firms represent more than $100 trillion in assets in 75 countries.

Overview

Strengthening the Banking Sector: Collaborative Approaches to Cybersecurity Threats

FS-ISAC Insights on the Current Threat Landscape

The Importance of Intelligence Sharing

Building a Cyber Resilience Playbook

Cyber Hygiene Best Practices

TLP GREEN

Cyber Threat Landscape

In addition to long-standing threat vectors, new threats are continuing to emerge that have disruptive implications on the financial services sector.

- Changing geopolitics and regulations
- Advancements in quantum computing challenge established cryptography
- The malicious use of AI by threat actors to automate and elevate cyberattacks
- Zero-Day vulnerabilities in the supply chain

TLP GREEN

The Importance of Sharing Intelligence

No institution can foresee all cyber threats. Sharing intelligence helps reinforce organizations' security and resilience, which in turn improves the overall resilience of the global financial system.

- Sharing intelligence benefits organizations on a tactical, operational, and strategic level.
  - Provides an early warning of attacks on peer firms
  - Enables potential victims to learn mitigation strategies from impacted firms
  - Increases industry-wide resilience and strengthens the world's financial system

Building Resilience Through Coordinated Exercises

Regular participation in cyber exercises ensures organizations have concrete procedures in place to respond to cyberattacks.

1 Uncovers vulnerabilities

2 Builds muscle memory

3 Fosters continuous improvement

TLP GREEN

Building a Cyber Resilience Playbook

Regular participation in cybersecurity exercises helps organizations build muscle memory that ensure an effective response in the face of disruption.

A playbook for cyber resilience enables organizations to determine procedures and protocols, ensuring continued operations. Key features include:

- Roles and responsibilities
- Decision-making hierarchy
- Procedures by attack scenario
- Playbook maintenance

Cyber Hygiene Best Practices

Organizations must shift from reactive to resilient by developing effective countermeasures, staying apprised of new threats, and building a culture from the top-down that actively champions cybersecurity initiatives.

Robust cyber hygiene is the bedrock of cyber defense and resilience.

- Staff training
- Regular updates
- Zero-Trust policy
- Password policies
- VPN usage

Additional Industry Tools

FS-ISAC

Cyber Fundamentals

Critical baseline security practices for today's threat landscape

FS-ISAC's Cyber Fundamentals, a comprehensive tool designed to help organizations bolster their baseline cybersecurity practices, offers 15 recommendations applicable to organizations at all levels of cyber maturity.

Data encryption

Employee training

Password management

Software patching

TLP GREEN

fsisac.com