Exercises

Since 2010, FS-ISAC has conducted exercises around real-world scenarios that enable you to test your organization's processes, plans and resources against a simulated cyber-attack. These exercises target both the most pervasive threats and different financial segments.

Hands-on participation in simulated attacks and mitigation is by far the most effective way for members of your security team to develop and maintain their identification, analysis, and response skills — a must for any financial institution in today's threat environment. FS-ISAC exercises can help you meet this need.

For more information and to register visit **fsisac.com/exercises** or email **exercises@fsisac.com.**

Cyber-Range Exercises

A one-day, hands-on-keyboard exercise in which participants observe and respond to different types of attacks such as ransomware, cloud leak, or business email compromise. Teams share and review results, identify methods for improving defenses, then re-run the simulated attack to see if the suggested mitigation techniques improve results. These exercises are usually conducted in a single location (remote participation is optional) with 20-30 participants, enabling attendees to readily share insights and arrive at solutions with peers.

These exercises are discounted for FS-ISAC members and conducted both remotely and onsite in multiple locations globally.

Playbook Drills

With help from numerous contributors, FS-ISAC has created the Financial Sector Crisis Response Framework, a structured and standardized approach for the sector to manage cyber-attacks. From this broader Framework (formerly known as the All-Hazards Crisis-Response Playbook), FS-ISAC has created regional playbooks to address specific geographies. Playbook drills focus on coordinated trusted information sharing and crisis response by adhering to the common, structured process defined in the playbooks.

Drills are conducted onsite in various locations and at no cost.

Hamilton Series

FS-ISAC partners with the Financial Services Sector Coordinating Council (FSSCC), US Treasury Department (Treasury) and other US government agencies including law enforcement to develop these one-day exercises aimed at improving the cyberthreat response within the US financial sector. Simulations mimic a variety of attacks. Participants include members of both the public and private sectors, so that results can be folded into improved public/private coordination strategies.

This series is conducted at Treasury and is by invitation only.

Cyber-Attack Against Payments Systems

A table-top team exercise specifically designed for the payments industry. Your incident response team practices overcoming a robust, simulated attack on payment systems and processes. Team members gain experience in mobilizing quickly, evaluating the attack under pressure and quickly identifying the best response. Aggregate, unattributed survey data provides benchmarking. For all members, with versions for banking, insurance, and securities & investments.

Conducted virtually.

Customized Exercises

Custom-designed exercises that are tailored for your organization's environment. Such exercises can target threats that are specific to a particular region, to organizations of a specific size or financial segment and adaptable to your institution's highest priority.

Pricing based on request.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is the only global cyber intelligence sharing community solely focused on financial services. Serving financial institutions and in turn their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate, and respond to cyber threats. Headquartered in the United States, the organization has offices in the United Kingdom and Singapore. Member financial institutions represent $100 trillion in assets, with 16,000 active users in more than 70 countries. To learn more, visit www.fsisac.com. To get clarity and perspective on the future of finance, data, and cybersecurity from top C-level executives around the world, visit FS-ISAC Insights.