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

Exercise Objectives

**Phase 1: Cloud Storage Investigation**
Participants will be introduced to the environment and the potential threat posed by the adversary. They will work to capture and preserve artifacts from an attack on a cloud storage service. This information will be used to determine the origin and extent of the attack.

- Identify methods(s) used to compromise the cloud storage service.
- Extract tools and files left by the attacker.
- Identify the types and locations of data potentially compromised in the attack.

**Phase 2: Network Compromise Investigation**
Participants will use tools to capture, preserve and recover network and host-based artifacts from the attack to determine if/how the enterprise network was compromised as a part of this attack. The information obtained during this phase should provide a clear picture of how the adversary attempted/successfully pivoted from the cloud storage site to the enterprise network.

- Identify all systems compromised in the attack, as well as the methods and tools used to compromise each system.
- Extract samples of tools or malware left on the network.
- Find any persistent adversary activity on the network.

**Phase 3: Briefing of Findings**
Participants will be given time to integrate the evidence gathered in Phase 1 and Phase 2 and compose a detailed report of the attack, which will then be briefed to the larger group. This report should address the objectives below.

- Provide a description of how the attacker was able to gain access to the cloud storage site.
- Identify the types of data compromised in the attack.
- Provide specific instructions to recover from the compromise.
- Offer recommendations for changes that will limit the impact of future cloud storage compromises.

**Phase 4: Hot Wash**
A Red Team member provides the “Attacker Point of View” detailing the different methods used in the attack to encourage discussion about what might have been missed and what can be learned and improved upon.

- Discuss ways to better identify and protect against this type of attack.
- Relate the lessons learned to what can be implemented within the institution's own environments.

**Ideal Candidates**
Beginner, intermediate and expert cybersecurity analyst wishing to update their hands-on skills.

**Prerequisites**
An understanding of the basics of incident reporting and evidence gathering. Hands-on experience with IDS tools and firewalls is preferred; however, they are not necessary as instructional guides are available for all open source tools used in the exercise.

**Scenario**
In this scenario, a major news organization has contacted your institution's, bank.com, media relations department asking for a statement about the discovery of consumer information for thousands of your institution's customers. The information has been breached on a cloud storage service, although you don't yet know anything about a breach. The CEO has requested an immediate investigation.

Participants will determine how the cloud storage site was compromised and the extent of the intrusion, including the types of data exposed and any further infiltration of bank.com's network. Participants will learn how to:

- Identify techniques used to compromise cloud and other network services;
- Determine the extent of a network intrusion campaign;
- Capture, preserve and recover network and host-based artifacts from an attack on cloud storage;
- Identify the steps needed to secure a cloud storage site and the enterprise network following intrusion; and
- Document and report the source and extent of a compromise along with recommendations for hardening the network against attack and better data hygiene practices.