

E-Book

The Benefits of Cyber Drills for Financial Services CISOs

Version: 01 | Published: Feb 2025

The Importance and Benefits of Cyber Drills

Financial services CISOs face mounting threats, regulatory pressures, and the constant need to prove their organization's cyber readiness to the board and other stakeholders. One effective way to prove and improve cyber capabilities across executive and technical teams is through Cyber Drills, which are dynamic exercises that pressure-test executive and technical teams against a simulated attack.

Teams can exercise together to build trust and confidence in their knowledge, skills, and judgment in responding to actual incidents—creating more coordination between technical and management teams. Most importantly, Cyber Drills offer data to indicate where teams are strong and where they are weak and in need of further upskilling.

Over the past 20 years, nearly one fifth of all global cyber attacks targeted financial services organizations, resulting in \$12 B in losses.* Most attacks involve the human element

*International Monetary Fund (IMF) Global Financial Stability Report, April 2024

**Verizon 2024 Data Breach Investigations Report, 2024

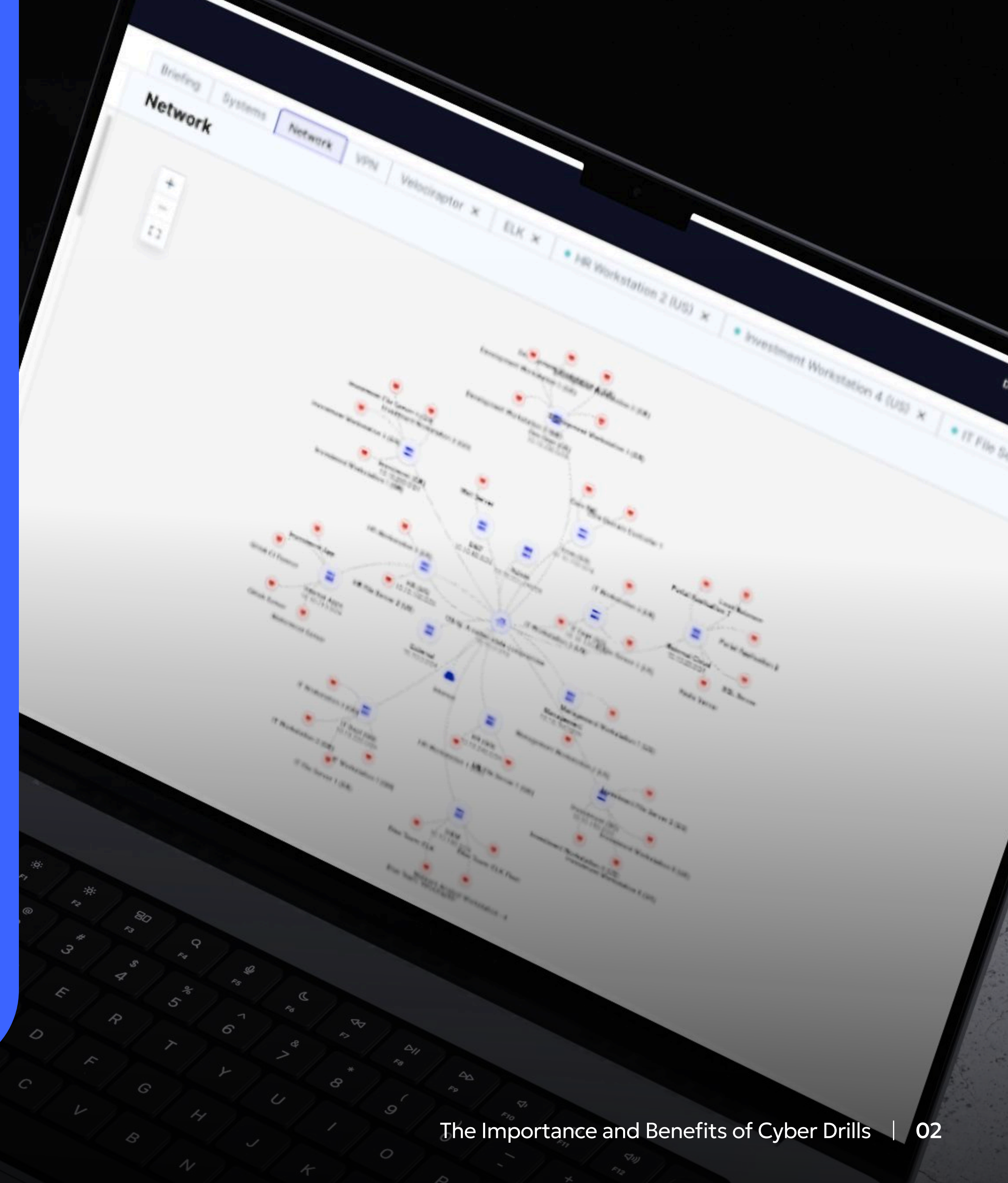
What are Cyber Drills?

Cyber Drills are dynamic experiences that test every aspect of an organization's ability to detect, manage, and recover from high-impact cyber threats.

A Cyber Drill is a strategic blend of in-person training, skill development, and targeted cyber exercises. Immersive's approach ensures your team is equipped with the necessary skills and knowledge to anticipate, withstand, recover from, and adapt to cyber threats or attacks.

Considering the unique challenges of securing a Financial Services business, the greater complex your environment gets, the more the need to identify skill and knowledge gaps.

Immersive can help you implement an effective cyber drills program, which seamlessly blends multiple solutions, including [Immersive Labs](#), [Cyber Range Exercises](#), and [Cyber Crisis Simulations \(Crisis Sim\)](#). Together, these solutions create a holistic and engaging cyber exercising program that ensures teams are ready for threats. Plus, available hands-on labs can be used to help prep teams before taking a Cyber Drill or upskill and fill knowledge gaps after an event.



Benefits

Cyber Drills allow individuals to learn through hands on experiences, realistic Cyber Range Exercises, and directed upskilling with Immersive Labs.

They blend technical and business cyber challenges in one immersive exercise, helping identify and address weaknesses in an organization's incident response plan from a technical and strategic viewpoint.



01 Real-time Collaboration

Cyber Drills run Cyber Range Exercises and Crisis Simulations concurrently, allowing for real-time between technical and non-technical teams, mimicking the dynamic nature of an actual cyber attack response.

02 Information Sharing

Information gathered by the technical team is shared with the crisis management team. This information informs the strategic decisions made by the crisis management team and helps them understand the technical aspects of the attack.

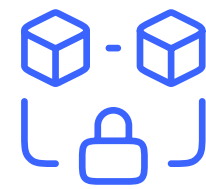
03 Decision Making

The decisions made by the crisis management team can impact the actions taken by the technical team. For example, a decision to shut down a compromised system may affect the technical team's ability to collect forensic evidence.

About Cyber Crisis Simulations (Crisis Sim)

Unlike traditional slide-deck-led tabletop exercises, this method simulates a crisis scenario that executive and crisis management teams must manage strategically and communicate effectively to mitigate organizational risk.

Crisis



Scenario

Participants are presented with a cyber crisis scenario. They are tasked with making high-level decisions, communicating with stakeholders, and managing the overall response to the incident.



Activities:

Participants may develop and execute a crisis communication plan, coordinate with legal and regulatory bodies, and make strategic decisions, such as whether to pay a ransom or notify customers of a data breach.



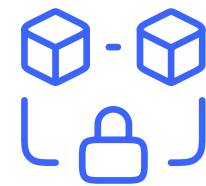
Objectives

The primary objective of Crisis Sim is to test the organization's overall incident response plan, including its ability to communicate effectively, make timely decisions, and manage the incident's impact on the business.

About Cyber Range Exercises

This Cyber Range Exercise is aligned with the Crisis Sim, and specifically focuses on the technical execution of a cyber attack response. It uses pre-configured cyber range scenarios that simulate a cyber threat, allowing technical teams, such as defensive teams, penetration testers, and SOC teams, to practice the steps needed to detect, analyze, and mitigate those threats

Team



Scenario

Participants are presented with a simulated cyber attack scenario, such as a ransomware infection or a data breach. They are tasked with investigating the incident, identifying the source of the attack, and choosing measures to contain and mitigate its impact.



Activities:

Participants may use advanced cybersecurity tools and techniques to analyze the simulated attack, such as examining log files, conducting forensics analysis, and implementing security patches or updates



Objectives

The primary objective is to test a technical team's ability to respond effectively and efficiently to a cyber attack.

Responding to a Cyber Incident is a Team Effort

Cyber Drills, by leveraging several solutions within the Immersive One Platform, are crucial in enhancing an organization's cybersecurity posture and resilience. They promote and establish better communication channels between and across diverse teams.

By bringing technical and management teams together to identify vulnerabilities, test response procedures, and exercise employees, organizations can better protect themselves against cyber threats. Investing in Cyber Drills is an investment in your organization's security and future success - and the ability to prove you're ready.

To find out how Immersive can help you build an effective cyber drilling program, please [visit us here →](#)



Be Ready



Continuously Assess, Build,
and Prove Your Cyber Resilience

To find out how Immersive can help you
build an effective cyber drilling program,
please [visit us here](#).

