eBook

How Realistic Cyber Exercises Build Real-World Resilience

IMMERSIVELABS

FORRESTER
WAVE
LEADER 2023
Cybersecurity Skills
And Training Platforms

Welcome!

Organizations need to be ready to absorb the shocks from a cyber attack.

Organizations that do not effectively prepare for and respond to a cyber attack risk untold reputational and financial damage. Preparation builds resilience, or the ability to recover quickly from disruptions.

Preventing every breach is not a realistic goal, so resilience matters more than ever and requires more than a dusty crisis management plan and shiny tech. Technology can identify and detect many threats and facilitate recovery from a cyber attack, but it alone cannot effectively respond to every issue. Only an organization's people – upskilled with the right capabilities – can successfully adapt, respond, and recover from the inevitable operational disruption caused by a cyber attack.

Resilience depends on the collective responsibility of the entire organization, not solely on security operations or business continuity teams. Resilience also depends on the ability to measure strengths and weaknesses across teams and in individuals to drive continual improvement.

Does your current program efficiently allow all teams to practice and demonstrate cyber capabilities across your workforce? Is your team adaptable and able to respond to any situation that arises? Can you prove it?

Dan Potter

Director of Operational Resilience, Immersive Labs

US Federal Reserve[1]:

> "While advances in technology have improved firms' ability to identify and recover from various types of disruptions, increasingly sophisticated cyber threats and growing reliance on third parties continue to expose firms to a range of operational risk."

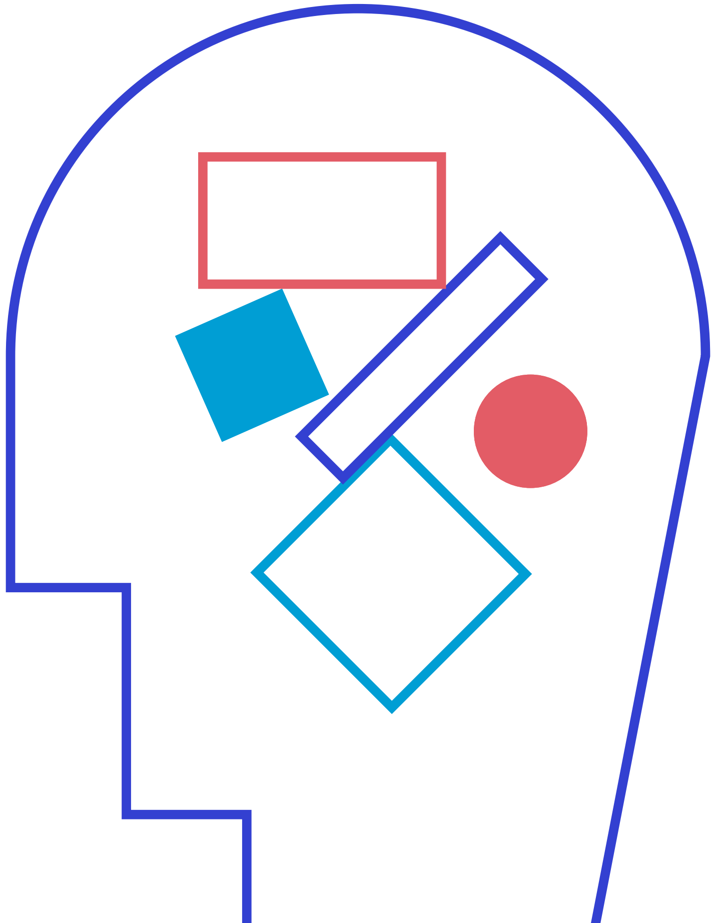
[1] https://www.federalreserve.gov/supervisionreg/topics/operational-resilience.htm

Table of Contents

Successfully Exercising the Business is Hard

Whether you're running a desktop scenario or a complex war game, the logistics are difficult, the scenario takes longer than expected, and participant engagement wanes over time. Implementing cybersecurity training exercises at scale also represents a major challenge for leaders.

While these challenges can make exercising feel futile, there is no doubt that preparing workforces with cyber capabilities is essential for a strong defense.



In fact, the US Government[2] states that exercises are important for achieving the following objectives:

- Evaluate the preparedness program
- Identify planning and procedural deficiencies
- Test or validate recently changed procedures or plans
- Clarify roles and responsibilities
- Obtain participant feedback and recommendations for program improvement
- Measure improvement compared to performance objectives
- Improve coordination between internal and external teams, organizations, and entities
- Validate training and education
- Increase awareness and understanding of hazards and the potential impacts of hazards
- Assess the capabilities of existing resources and identify needed resources

[2] ready.gov

Challenges with Traditional Exercising: Who is Actually Engaged?

The most trying challenge associated with traditional tabletop exercises is delivering engaging learning experiences within a reasonable timeframe.

An innovative, problem-solving mindset can be hard to achieve in a tabletop exercise given the range of views. When engaging with the C-Suite, you often encounter a strategic mindset, although a highly technical subject matter expert (SME) can dominate and derail the conversation. The SME can impact the overall theme of the exercise, resulting in a tactical, technical discussion that impedes exploring the secondary impacts across your organization.

Additionally, lack of attention can occur due to scenario design, as well as the mistaken assumption that the chief information security officer (CISO) is responsible for solving all cyber issues. This perspective on individual responsibility is damaging, as team mentality and culture are critical for success.

The Value of Crisis Simulation Platforms

To build team collaboration and avoid an individualistic mindset, it is essential to engage everyone in the exercise and facilitate a team discussion. Crisis simulation platforms support necessary cultural transformation, while simultaneously engaging each individual. Team members receive prompts and a range of options and their decisions influence subsequent actions from the team in real-time. This hands-on approach can be very powerful, as it allows a facilitator to engage everyone in the exercise while providing an instant, visual representation regarding agreement or disagreement within the team.

Measurement Is Critical for Better Outcomes

If you can't measure progress and performance, how do you know if you are improving in the right areas to increase resilience? How can you prove to your boards and stakeholders that your investment is worthwhile?

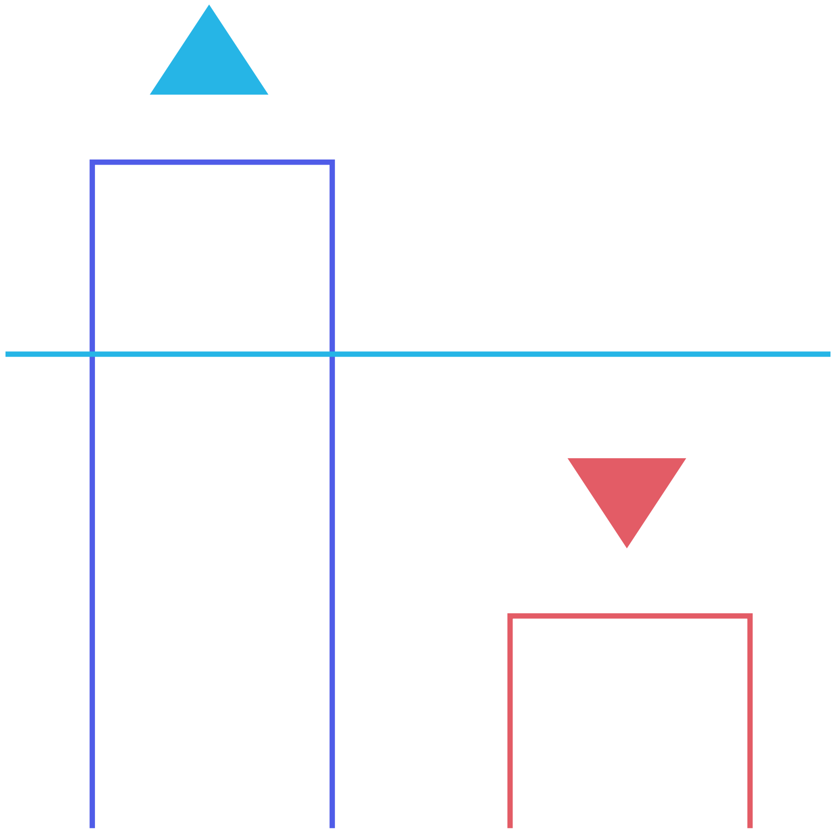
With modern crisis simulation platforms, your organization can move from legacy training and tabletop exercises to measurably improving — and proving — your cyber capabilities and readiness, using a repeatable, four-step process:

Exercise:
Use real-world simulations to evaluate and baseline team capabilities and decision-making

Benchmark:
Evaluate cyber readiness compared to industry benchmarks

Upskill:
Build cybersecurity capabilities to enable teams at all levels to defend against the latest threats

Prove:
Demonstrate risk reduction and resilience to your board, regulators, and customers



This ongoing, holistic approach enables organizations to report on and prove current levels of cyber capability across the organization.

Spotlight:

Fight, Flight, or Freeze?

Do you know how members of the crisis management team will react during a crisis?

A cyber attack requires agile decision-making and resolve across your organization; it is not the time for anyone to freeze or take flight. Driving resilient outcomes requires teams and individuals with skills, knowledge, and judgment to respond effectively under pressure.

Resilient outcomes also depend on a creative, problem-solving mindset with consideration of wider stakeholders and different viewpoints. People across the organization need to think of the big picture without losing sight of the details.

The decisions business leaders face during cyber attacks are not binary; they are complicated and multi-faceted. During a rapidly unfolding cyber incident, many leaders fall into the trap of embracing a better-safe-than-sorry mindset, which can lead to the kind of groupthink that prevents swift

action on various issues. Despite this natural inclination toward hesitancy, exactly the opposite behavior is necessary if an organization is to successfully react, adapt, respond, and recover from an attack.

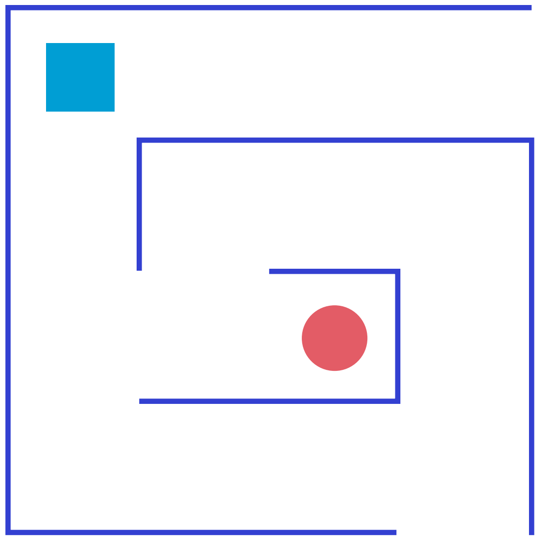
Regular exercising combined with the ability to measure confident decision-making can help organizations — particularly the CISO and Head of Crisis Management — identify potentially conflicting mindsets within your crisis management team.

Exercising is a key strategy for encouraging business leaders to explore issues, enabling them to visualize how their decision could impact the business in a real-life scenario. It's good to explore different perspectives, experiences, and aptitudes across the crisis management team, especially before a real incident occurs.

For example, facilitators can ask the Head of Technology to roleplay as Head of Communications and vice versa during a simulation exercise to understand each thought process. This exchanged perspective helps the team appreciate the different views, needs, and drivers of different functional teams. The exercise facilitator can also help teams identify opportunities for further training with crisis management teams. By comparing results across different teams, functions, and seniority levels within the organization, teams can better understand behavioral tendencies in the organization and increase resilience.

What You Need From a Crisis Management Team:	The Natural Tendency of a Team Facing a Crisis:
Innovative problem solving mindset	A better-safe-than-sorry mindset drives group think
Consideration of wider stakeholders, different viewpoints, and ability to see the bigger picture	Fixated on a specific issue; unable to see wider context

While business leaders may be skilled at managing warring priorities, can they think strategically and operate tactically during a cyber attack?



How to Evolve Exercising:

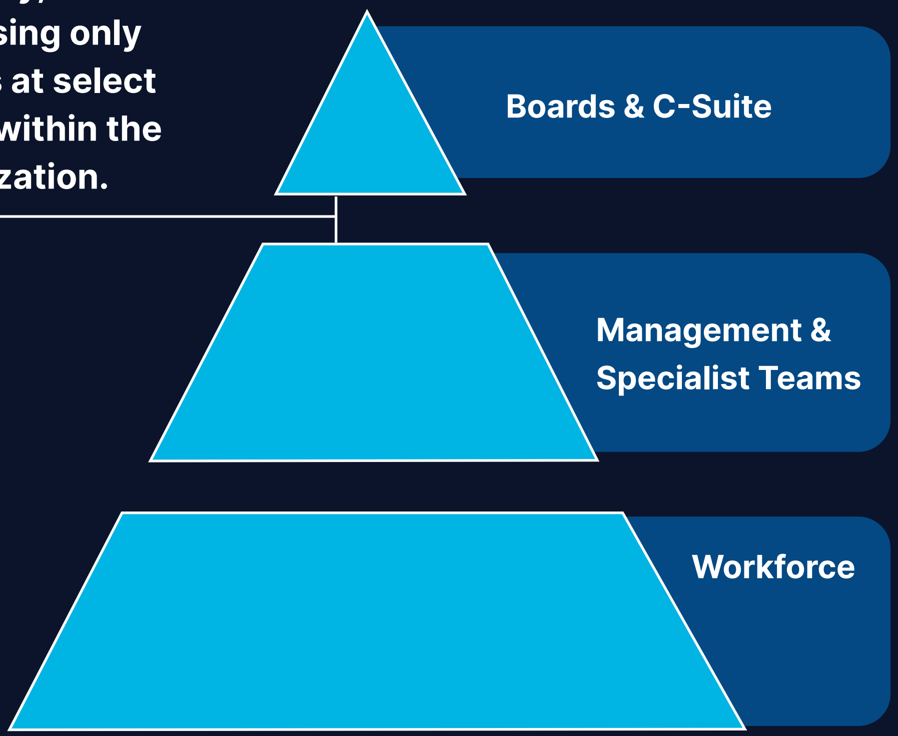
Both individuals and teams improve by doing, not watching. Through exposure to realistic scenarios, teams can prepare for real-world crises. Teamwork doesn’t happen naturally; it requires deliberate practice.

Just like in a real-life crisis, exercises need to be dynamic, with different decisions resulting in different outcomes and leading participants down different paths. The more teams practice, the better their ability to predict the next issue. Through ongoing exercising, your team’s collective ability to make decisions and respond will improve, ultimately building the people-centric resilience your organization needs.

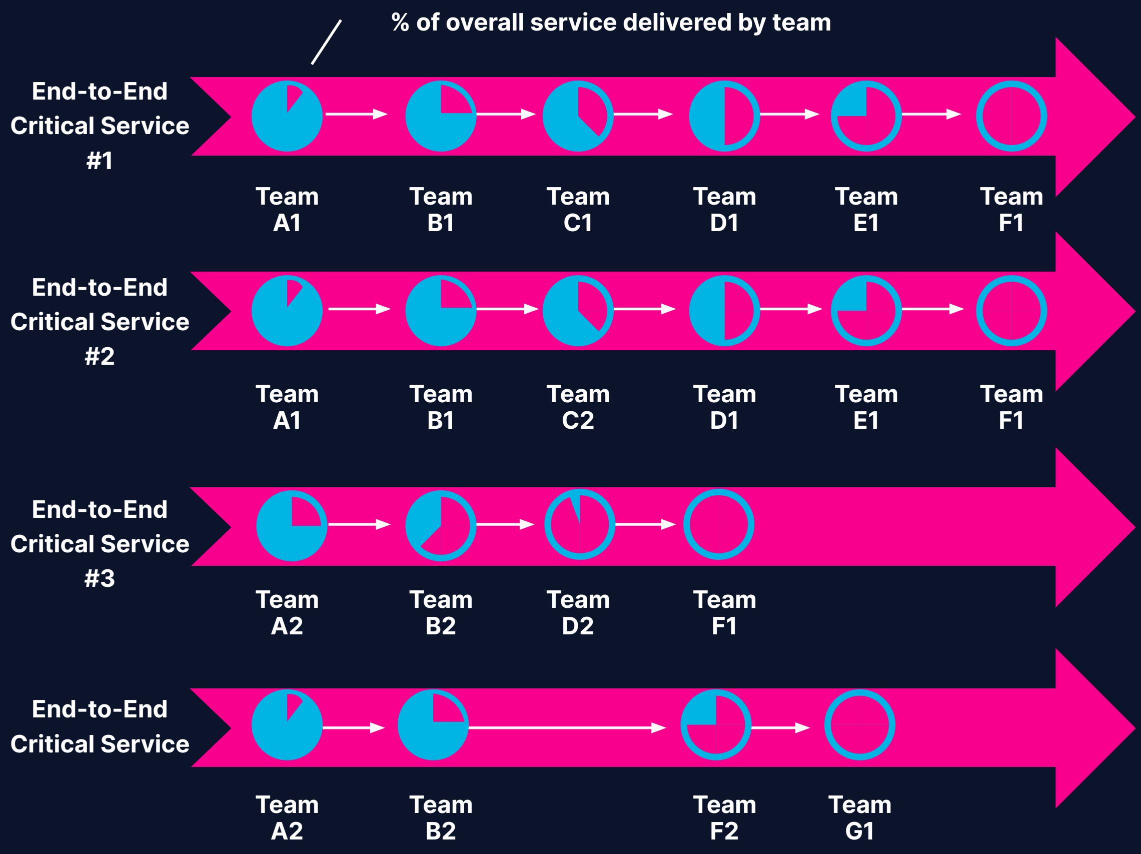
Exercising the Wider Workforce, Not Just the Technology and Business Continuity Teams

Given the challenges associated with scaling the traditional approach to tabletop exercises, inevitably organizations tend to only test 5-10% of the workforce. Considering the cost and resource-intensive needs of traditional exercising formats, the inclination to test a smaller group makes sense. However, this small percentage also limits the overall benefit, as this approach leads to skills gaps throughout the organization and a lack of awareness.

Typically, exercising only occurs at select levels within the organization.



Exercising needs to evolve to concurrently assess the different teams involved in the delivery of a service to a client.



% of overall service delivered by team
End-to-End Critical Service #1
Team A1
Team B1
Team C1
Team D1
Team E1
Team F1
End-to-End Critical Service #2
Team A1
Team B1
Team C2
Team D1
Team E1
Team F1
End-to-End Critical Service #3
Team A2
Team B2
Team D2
Team F1
End-to-End Critical Service
Team A2
Team B2
Team F2
Team G1

Current State

Exercises focuesd on select teams limit penetration across the organization and are highly manual.

Immersive Labs Crisis Sim

Crisis Sim provides a scalable and engaging solution to deliver simulation exercises from the boardroom down.

Today, there are more engaging methods to involve the wider organization in asynchronous exercising or micro-exercises.

Cyber simulations allow individuals to test their responses against mock attacks, either from the perspective of their current roles or by roleplaying other job functions. By allowing the wider workforce to operate in an asynchronous mode, your organization exposes others to the types of difficult decisions teams or individuals might face during a real cyber attack, as well as the consequences of those decisions. Taking on different roles during a mock ransomware cyber attack can enable employees to adopt the lessons learned during training.

These engaging methods provide a holistic view of your organizational resilience. For example, a junior employee may only be responsible for a small process step that delivers business services to clients. That employee is never directly involved in exercising but is your first line of defense in a cyber attack. Their initial decisions are critical to your organization's resilience. Allowing that employee to run cyber crisis simulation as CEO can contextualize the importance of their role.

In addition to this perspective, you can better understand team and individual prioritization during a crisis and assess decision-making across the organization, all while testing crisis management protocols in a safe and engaging environment.

To be resilient, you must invest in your people and expose them to plausible scenarios that build understanding of the types of decisions faced during a disruption. By engaging the wider workforce in realistic scenarios, you will strengthen the collective muscle memory required to withstand the shock of inevitable disruption.

Immersive Labs' comprehensive exercising solution, Crisis Sim, will engage your entire workforce in plausible scenarios based on emerging threats to various industries, even in geographically dispersed locations. The simplicity and versatility of the solution means multiple exercises can be performed on an annual basis.

Immersive Labs is the leader in people-centric cyber resilience. We help organizations continuously assess, build, and prove their cyber workforce resilience for teams across the entire organization, from front-line cybersecurity and development teams to Board-level executives. We provide realistic simulations and hands-on cybersecurity labs to evaluate individual and team capabilities and decision-making against the latest threats. Organizations can now prove their cyber resilience by measuring their readiness compared to industry benchmarks, building team capabilities, and demonstrating risk reduction and compliance with data-backed evidence.

Immersive Labs is trusted by the world's largest organizations and governments, including Citi, Pfizer, Daimler, Humana, T. Rowe Price, and the UK National Health Service. We are backed by Goldman Sachs Asset Management, Summit Partners, Insight Partners, Citi Ventures, and Menlo Ventures.

IMMERSIVELABS