Cyber Crisis Exercising: The Way Forward

THOUGHT LEADERSHIP PAPER

JULY 2026

Contents

1

Cyber Resilience

In today's operating environment, organizations can no longer rely solely on traditional cybersecurity approaches, focused primarily on prevention and protection. While these controls remain essential, they are no longer sufficient on their own. The modern technology environment is complex, characterized by interconnected systems, legacy infrastructure and evolving cyber threats, which requires organizations to shift from a security-focused approach to a resilience mindset.

Cyber resilience goes far beyond preventing attacks; it reflects the organization's ability to withstand, recover from, and adapt to the external shocks caused by cyber risks. Disruptions will occur despite even the most advanced defenses. As articulated in the literature, cyber resilience is "the ability to continuously deliver the intended outcome despite adverse cyber events."[1]

Cyber resilience matters because it is fundamentally tied to trust.

Cyber resilience matters because it is fundamentally tied to trust, from customers, partners, regulators, and the broader ecosystem. Effective resilience ensures continuity of operations, maintains stakeholder confidence, and minimizes the long-term impact of cyber events. Ultimately, a resilient organization not only survives disruption; it learns, adapts, and emerges stronger.

The Mastercard European Cyber Resilience Centre

Across Europe and around the world, cyber threats have grown more frequent, more automated, and increasingly coordinated. Attackers move faster, target critical infrastructure, and exploit the interconnection of our digital economy. There is broad

consensus across governments, regulators and industry that cyber resilience is a collective responsibility.

It is in this context that **Mastercard established the European Cyber Resilience Centre (ECRC) in 2024. Designed to strengthen our ability to protect Mastercard, our network, our customers, and ultimately consumers,** the ECRC also supports the expectations of governments, policymakers, and regulators across Europe.

Resilience cannot be built in silos.

The ECRC brings together more than 30 teams from across the organization, enabling us to move faster in our response and recovery, while maintaining a strong regional focus in Europe. It also reinforces a critical principle: resilience cannot be built in silos. Cyber threats do not respect borders, and neither can our response. The Centre strengthens public private collaboration, improves situational awareness, and supports collective defense across the payments ecosystem.

At its core, the ECRC is built on the principle of **security through unity**. We work closely with leading financial institutions and senior Mastercard stakeholders, regulators, law enforcement, central banks, and European institutions. We continue to expand this ecosystem, welcoming partners from government, industry, and international organizations as part of a shared commitment to resilience.

The ECRC plays a critical role in responding to incidents, coordinating actions and partnering with stakeholders to ensure an efficient approach. At the same time, the **ECRC looks well beyond the immediate horizon, examining low probability but high impact scenarios** that could affect Mastercard or the broader ecosystem. This forward-looking approach informs activities such as contingency planning, helping the company prepare for best and worst-case scenarios and develop effective mitigation strategies. Similarly, the "Threatcasting" event held in October 2025 brought together experts from industry, academia, governments, regulators, and NGOs to

explore emerging technologies and develop mitigation strategies before future risks materialize (5-10 year horizon).

Crisis Management at Mastercard

Crises are abnormal, unstable and complex situations that pose a serious threat to the reputation and existence of an organization. A crisis occurs when established processes have failed or cannot fully address the scale or urgency of the event. In these moments, normal governance and incident response procedures are not enough. Crisis Management is thus required to mobilize extraordinary resources, apply creative problem-solving, and enable swift decision-making.

As Mastercard we define Crisis Management as the structured process of predicting, preventing, preparing for, responding to, and recovering from events that have the potential to significantly impact an organization. Crisis Management is essential because every organization, regardless of size or maturity, will inevitably face a crisis at some point. No company is too big to fail, and major incidents can escalate rapidly without coordinated leadership. Crisis Management provides the structure needed to coordinate decision-making under pressure and avoid reactive or misinformed responses.

Cyber Crisis Exercising

Cyber crisis exercising is what turns resilience plans into practice.

Cyber crisis exercising is what turns resilience plans into practice. Policies and plans alone are not enough, exercising brings them to life by testing how teams perform under pressure and helping them understand how to respond when disruption occurs. Exercising during peace time allows organizations to identify gaps, better understand challenges, and assess whether current processes are fit for purpose.

A key benefit of crisis exercising is the **development of muscle memory.** Working through realistic scenarios helps teams recall information quickly, act with confidence, and make better decisions under pressure. Ultimately, a plan is only as strong as its rehearsal. Crisis exercising ensures that response teams know not just what is written, but how to apply it when the situation is complex or unexpected.

It is important to balance internal exercises, which allow you to test your own processes, with external or industry-wide exercises, which help build coordination with the wider ecosystem. Exercises can be run virtually or in person, depending on scope, resources, and objectives. Virtual simulations, supported by modern exercise platforms, make it easier to run frequent, realistic scenarios through automation.

There are several types of exercises, each serving a different purpose:

1. **Walkthrough exercises** are discussion-based sessions designed to familiarize teams with plans, roles, and responsibilities. They help uncover high-level gaps and ensure everyone understands the basics of the response process.

2. **Tabletop exercises**, the most common format, take teams through a simulated crisis scenario that unfolds step by step, requiring participants to talk through decisions and actions. They are a practical way to test coordination in a safe environment.

3. **Live exercises**, otherwise known as Cyber Ranges, go a step further by activating real-world procedures, systems, and personnel in real time. These exercises validate operational readiness, test tools and technology, and build deeper confidence across responding teams.

Choosing the right type of exercise depends on the organization's maturity, capacity, and risk profile. A risk-based approach helps determine which scenarios should be prioritized, as no organization can test every possible situation.

It is also important to recognize that crisis response teams have varying levels of experience and confidence. The format, difficulty, and content of exercises should be adapted to the participants involved.

Lessons Learned from Crisis Exercising

Lessons learned turn crisis exercises into actionable change.

Lessons learned turn crisis exercises into actionable change. The objective is to enable all participating teams to reflect on what worked well during the simulated response and where improvements are needed so the same mistakes aren't repeated during a real incident. Lessons learned drive updates to playbooks, clarify roles and responsibilities, refine escalation paths, and streamline processes, ultimately strengthening crisis readiness across the organization.

Avoid a common pitfall: **lessons should be considered holistically**. If a gap surfaced in one region or department, it may exist in others; if a role is unclear in one playbook, similar ambiguity might be present across adjacent processes. It's important that any improvements identified are applied consistently throughout the organization to ensure alignment.

2

Cyber Crisis Exercise Solution

Cyber Crisis Exercise: a data and intelligence-driven tabletop exercise solution.

In a previous whitepaper published by Mastercard, the Cybersecurity Solutions team detailed how today's operating environment and ecosystem reality as explained above, coupled with Mastercard's own expertise and thought leadership, created an opportunity to partner with cybersecurity simulation industry leaders and offer Mastercard customers a solution aimed at encouraging resilience plan testing through regular exercising, and using lessons learned to promote best practices for cyber workforce readiness and increased cyber resilience.[2] The resulting joint approach is Cyber Crisis Exercise: a data and intelligence-driven tabletop exercise solution delivered by Mastercard's Cybersecurity Advisory experts to support decision-making, and powered by Immersive, an industry-leading crisis simulation platform and one of Mastercard's technology partners.

The Cyber Crisis Exercise offering complements Mastercard's integrated cybersecurity solutions portfolio, which focuses on assessing risk exposure at the speed of business, protecting against risks using unique threat intelligence, and **organizing ecosystem trust** through orchestrating continuous improvement of global cybersecurity. It addresses the human element of cyber resilience head-on, highlighting the reality that technology and processes are only as effective against attacks as the skills of the people using them.

Since its launch in 2024, Cyber Crisis Exercise has evolved in tandem with market pain points and needs. While originally designed as a purely consultant-delivered solution, supported by Mastercard's Cybersecurity Advisors, customer engagements quickly made it clear that different organizations have different paces and requirements when it comes to exercising frequency, determined in many cases by company size, complexity and applicable regulatory standards. As a response, Cyber Crisis

Exercise shifted to include a **Self-Exercise offering** in 2025, allowing customers to access the Immersive platform and run cyber simulations at their own pace from a catalog of AI-powered and intelligence-driven crisis scenario templates, curated by Advisors who prompt the system according to the organization's threat landscape and likely attack vectors. Through this new capability, larger and highly-targeted institutions are now able to exercise their resilience plans quarterly, in adherence to Mastercard's best-practice recommendations for its customers.

Training Labs as a method to implement lessons learned post-exercise.

Additionally, the solution has become more actionable through the incorporation of Training Labs as a method to implement lessons learned post-exercise. These hands-on Labs, available on the Immersive platform and tailored by Advisors, align to the attack paths of the crisis scenarios utilized during the original exercise, and serve as an upskilling tool for specific exercise participants (teams and individuals) whose simulation performance uncovered training gaps. Training Labs can now be leveraged by Mastercard's customers for targeted cyber workforce skill development and benchmarking, as part of the **"prove-and-improve" cycle** used to build a continuous exercising program and enhanced resilience over time, i.e. "prove" workforce readiness via exercises, "improve" said readiness via Labs, only to "prove" improved skills in the next exercise, and so on.

The next step for Cyber Crisis Exercise in 2026 will be to build upon Mastercard's Corporate Security and European Cyber Resilience Centre expertise, and crisis management best practices to offer our customers more comprehensive **live cyber exercises or Cyber Drills**, which will include technical cyber ranges in combination with strategic-level tabletop simulations. This new solution tier will adopt a model similar, albeit at a smaller scale, to Mastercard's Cyber Defense Exercises (CDX) as described in the following section. Cyber Drills will empower Mastercard customers to measurably reduce incident duration and cost by validating and optimizing the collective response

efficacy of their teams - tactical, operational and strategic/executive - against realistic attacks, driving a successful outcome-focused crisis management program, ensuring alignment between cyber exercising and broader security initiatives, and future-proofing their organization through improved cyber resilience.

3

What is CDX?

The Mastercard Cyber Defense Exercise (CDX) was established in 2016 to foster industry partnerships and strengthen relationships. This engagement collaborates with public and private organizations to enhance resilience and response plans, **impacting critical infrastructure and national security**. The CDX has evolved over time to put focus on training and exercising the tactical, operational and strategic elements that embody a private organization.

The CDX has evolved over time to put focus on training and exercising the tactical, operational and strategic elements that embody a private organization.

The tactical exercise is hosted on Mastercard's own Cyber Range providing hands-on, simulated technical environments for live testing of defenses and is conjoined with a tabletop exercise that is collaborative, discussion-based sessions that walk through incident response, communication and decision-making processes. Both exercises together aim to identify gaps and build resilience.

One of Mastercard's recent Cyber Defense Exercises was hosted by the ECRC in October 2025, as a European multi-sector initiative bringing together technical teams and senior leaders from the finance and telecommunications sectors for a force-on-force, real-time exercise that mirrored a sophisticated, complex cyber-attack. With cyber threats in Europe intensifying, the ECRC's CDX showcased how the private sector, powered by partnership, can take the lead in strengthening defenses by building scalable, repeatable models for cyber collaboration that can be deployed across industries and geographies. Read the full story here.[3]

What are the CDX Objectives?

The Cyber Defense exercise has three main goals it sets out to achieve:

1. **Strengthen real-world cyber defense readiness**. Enhance the organization's ability to detect, analyze, and respond to complex, multi-vector cyberattacks in a realistic, high-pressure environment.

2. **Improve cross-functional and cross-organizational coordination.** Develop stronger collaboration and communication between internal security teams, business units, executive leadership, and external partners during large-scale cyber incidents.

3. **Validate resilience of critical infrastructure, processes, and technology.** Assess how well critical systems—networks, applications, cloud environments, ICS/OT, or third-party integrations—perform when subjected to sustained, targeted attack scenarios.All of this activity is captured for analysis and reporting to support a structured retrospective—commonly referred to as an After-Action Report (AAR)—which documents the tasks, decisions, challenges, and outcomes associated with achieving these goals.

What is the Organization of the CDX?

The resources required for a successful and dynamic event include red teams, blue teams, incident responders and organizational leadership that comprise a team and play with other teams that are similarly resourced.

The exercise is designed to elevate the cyber incident scenario and allow it to proliferate through additional layers of players with the goal of engaging each layer of the organization from **tactical** (blue team) to **operational** (incident responders) to **strategic** (organizational leadership).

From a technical perspective the CDX is engineered to simulate small to medium sized enterprise networks that simulates a

business productivity workload as well as customer-facing applications with built-in dependencies.

- **Blue teams** are tasked with defending their networks that are riddled with security vulnerabilities, security misconfigurations and insider threats. Blue teams use open-source platforms to perform these functions to remain vendor agnostic and force blue teams to rely on security foundations and fundamentals to protect and respond to attacks against their networks.
- **Red teams** are tasked with performing offensive operations against the blue team networks, attacking applications and network infrastructure to fully compromise the blue team networks, establishing persistence and stealing data during their campaigns.
- **Incident responders** act as the operational or business layer for the organization requiring participants to think about business impact that the blue teams are responding to in the tactical exercise. This portion of the engagement is a tabletop exercise and allows for focused objectives to challenge how different stakeholders such as legal, data privacy, or external communications of an operations team might respond to a cyber crisis.
- **Leadership or strategic players** help respond in the tabletop exercise as incident responder elevate issues that require more strategic responses in a cyber crisis. Material responses, brand/image considerations, board communication, engaging government or public partners are all elements that challenge players during the CDX.
- **Partners and Platforms leveraged**
    - **Partners**:
        - Mastercard selects the participating organizations through current business relationships and customers (such as banks, issuers and acquirers). Additional partners are selected from critical infrastructure, specifically from energy and telecommunications
        - Technology partners – WWT, Dell, Intel, Immersive
    - **Platforms**:
        - The Cyber Range platform used for the competition is provided and supported by Mastercard.
        - Built to resemble a small to medium business network, this dedicated stack is designed for resiliency and performance throughout the event. The attack-and-defend environments are also designed and engineered by Mastercard and are deployed and run on the Mastercard Cyber Range.
        - Immersive Crisis Exercise platform runs the table top portion of the exercise

4

From One-Off Drills to Continuous Resilience

Most organizations have accepted a hard truth about today's threat landscape: strong defenses reduce risk, but they do not eliminate it. When a serious incident happens, outcomes depend on resilience, meaning the ability to keep critical services running, make clear decisions under pressure, recover quickly, and adapt as facts change.

This shift is also reflected in how regulators, auditors, and industry frameworks approach preparedness. Many sectors now expect organizations to run incident simulations on a recurring basis, not only to "prove" readiness but to continuously improve coordination, escalation, and communications.

In practice, the biggest gap is rarely a missing document. It is the human and organizational element: who gathers whom, how quickly decisions are made, which facts matter, how tradeoffs are evaluated, and how technical response aligns with business priorities. That is why the future of crisis exercises is moving away from annual check-the-box tabletop sessions toward ongoing, measurable practice that builds real operating rhythm.

When exercises are designed well, they create usable muscle memory. People learn how to operate under uncertainty, how to escalate at the right time, and how to communicate with clarity. When exercises are too lightweight, too scripted, or too infrequent, they risk producing the opposite: a false sense of confidence and a plan that looks good on paper but does not work under stress.

The next generation of crisis exercising is defined by three traits:

1. Realism that forces teams to react as they would in real life
2. Frequency that prevents skill decay
3. Integration across technical response and executive decision-making

The goal is not theatre. The goal is operational readiness and a culture where practice is routine, lessons are captured, and improvements are actually implemented.

Many organizations are already pairing realistic simulation environments with expert facilitation to create hands-on experiences that feel close to the pressure of a real event.

The goal is not theatre. The goal is operational readiness and a culture where practice is routine, lessons are captured, and improvements are actually implemented.

A Best-Practice Flow for Ongoing Cyber Crisis Exercising

Instead of treating simulations as isolated events, organizations get better results by running a continuous program that creates a loop: test, learn, train, retest, and institutionalize improvements.

Below is a practical four-step cycle.

STEP	DESCRIPTION	RECOMMENDED FREQUENCY	VALUE DELIVERED
1. Baseline Cyber Drill (Advisor-Led)	A comprehensive advisor-led cyber crisis exercise that combines a realistic incident simulation with a leadership crisis management workshop to assess current response capability and establish a baseline.	Annual	Realistic stress-test of people, process, and technology. Establishes baseline readiness indicators and observations. Identifies gaps in incident response plans, technical controls, role clarity, escalation, and executive decision-making.
2. Targeted Training and Labs	Focused upskilling and workshops that address weaknesses found in the baseline drill. Can include hands-on technical labs, crisis communications practice, incident management workshops, and playbook execution exercises.	Ongoing (for example monthly as part of a training program)	Closes specific skill and process gaps. Reinforces best practices and keeps teams current. Builds confidence and competence in tools, workflows, and playbooks under pressure.
3. Quarterly Self-Run Simulations	Regular in-house simulations led by the organization using a platform or prepared scenarios. Typically 60 to 120 minutes. Involves technical responders, business continuity, communications, legal, and executives as appropriate.	Quarterly	Maintains muscle memory through repetition. Validates that improvements are working in realistic conditions. Strengthens a culture of continuous readiness and avoids one-off compliance behavior.
4. BCP and Playbook Updates	Institutionalize lessons learned by updating Business Continuity Plans, incident response plans, escalation paths, and playbooks after major exercises and meaningful changes.	At least annually, and after major exercises or significant change	Converts lessons into documented, repeatable practice. Closes the loop between exercising and operational change. Ensures plans remain aligned with how teams actually respond.

Forward-Looking Considerations

Crisis exercising is becoming more immersive and more adaptive. Scenario design is improving, simulations are easier to run for distributed teams, and digital platforms can help scale repetition without requiring massive facilitation every time.

That said, technology will not replace the core requirement: people must practice together. Tools can make scenarios more realistic and enable remote participation, but resilience still depends on how teams coordinate, decide, communicate, and execute under pressure.

Organizations that build an ongoing exercise rhythm do more than survive incidents. They become faster, calmer, and more consistent, and that reliability translates into trust with customers, partners, and regulators.

See how Mastercard's Enterprise Cybersecurity solutions, including Cyber Crisis Exercise, can strengthen your resilience. Connect with our team to learn more.

References

1. Björk, Fredrik, Henkel, M, Stirna, Janis, and Zdravkovic, J. (2015), "Cyber resilience – Fundamentals for a definition", in Rocha, Alvaro, Correia, Anna Maria, Costanzo, Sandra, and Reis, Luis Paulo (eds.), New contributions in information systems and technologies, Springer, London, pp. 311-316. doi: 10.1007/978-3-319-16486-1_31

2. Fail to Prepare, Prepare to Fail: Cyber Crisis Exercising for Operational Resilience Paper

3. Europe | Mastercard Newsroom

Contributors

Yonatan Israel Garzon
Director, Product Management, Risk & Resilience
Mastercard

Gokhan Demirel
Director, Product Management, Risk & Resilience
Mastercard

Fadwa Rachi
Director, Security Monitoring and Response
Mastercard

Aaron Gomez
Director, Information Security Engineering
Mastercard

Coordinator

Eda Boltürk
Director, Product Development
Mastercard