sifma

protiviti®
Global Business Consulting

SIFMA QDVIII After-Action Report

Table of Contents

TLP: White

Executive Summary

From November 4 to 6, 2025, some 1,000 participants from both the public and private sectors—including over 100 financial institutions, critical market utilities and financial market infrastructure (FMIs), public agencies, and cross-sector partners—participated in the Securities Industry and Financial Markets Association (SIFMA) global Quantum Dawn VIII exercise. The three-day event combined a tabletop exercise, intra-firm dialogue, and expert panel discussions to test the sector's readiness for polycrisis incidents—compound operational shocks that arrive in parallel, cascade across sectors, and intensify through real-world interdependencies.

The scenario sequence stressed the ecosystem with a Category 5 hurricane, a transatlantic cable cut, an FMI outage, and a zero-day cybersecurity attack attributed to a state actor. The overarching goal was to simulate end-to-end response and recovery for severe, concurrent disruptions and to strengthen cross-border coordination and information-sharing mechanisms under duress. Quantum Dawn VIII focused on decisioning, governance, and public-private interplay, including:

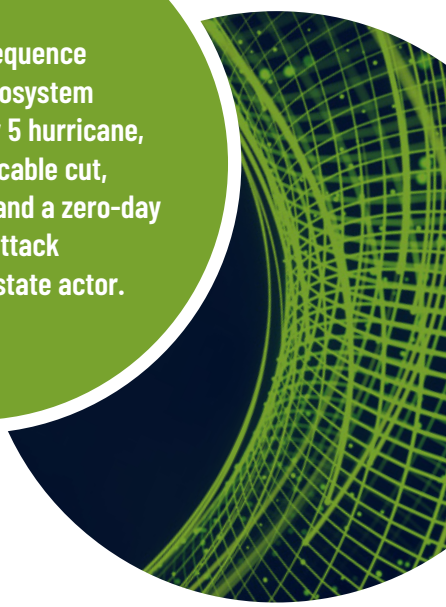
- Crisis command structures and escalation;
- Sector and cross-sector communications;
- Operational resilience across telecom, cloud, and physical infrastructure;
- Third-/fourth-party disconnection and reconnection protocols; and
- The evolving role of artificial intelligence (AI) as both adversary tradecraft and defender capability.

Overall, Quantum Dawn VIII revealed a sector that is confident in its operational resilience capabilities while still having room for improvement in individual members' understanding of and resilience to some systemic risks.

Nearly two-thirds of participants expressed high confidence in their organization's ability to respond to a polycrisis, with significant comfort in handling a major storm, reflecting sector maturity in emergency response activation, employee communications, and remote work enablement. Participants felt incidents impacting telecommunications or other third-party infrastructure relied on by the organization, such as an undersea cable cut or FMI outage, could be more challenging due to under-mapped dependencies, concentration risk, and limited cross-firm testing.

Quantum Dawn VIII identified access credentialing for essential staff, adoption of disconnect/reconnect frameworks, and consistent execution of evidence-based reconnection with critical third and fourth parties as areas where additional focus could further strengthen industry resilience. The exercise also underscored the growing influence of AI as both a defensive tool and an accelerant.

The scenario sequence stressed the ecosystem with a Category 5 hurricane, a transatlantic cable cut, an FMI outage, and a zero-day cybersecurity attack attributed to a state actor.



Quantum Dawn History and Approach

SIFMA's Quantum Dawn exercises, conducted biannually since 2011, provide a structured venue to test sector-wide coordination for cyber, physical, and operational disruptions.

These exercises provide a forum for financial firms, regulatory bodies, central banks, law enforcement, government agencies, trade associations, and information-sharing organizations to respond to simulated cyber and/or physical attacks. They are designed to evaluate the industry's ability to share information in a timely manner during events that could impact market integrity or cause widespread disruptions to the financial ecosystem.

Over the last 15 years, the Quantum Dawn series of exercises has served as a critical biannual event for the financial services industry.

15 Years of Testing and Resilience

QDI NOVEMBER 2011 **QDII** JULY 2013	QUANTUM DAWN I AND II	In November 2011 and July 2013, the financial services sector, in conjunction with service provider Norwich University Applied Research Institutes, organized two market-wide cybersecurity exercises called Quantum Dawn I and Quantum Dawn II, respectively. Those events provided a forum for participants to exercise risk practices to manage a disruption in equity trading and clearing processes caused by a systemic attack on market infrastructure.
QDIII SEPTEMBER 2015	QUANTUM DAWN III	Quantum Dawn III, held in September 2015, focused on exercising procedures to maintain market operations in the event of a systemic attack. Participants first experienced firm-specific attacks, followed by rolling attacks on equity exchanges and alternative trading systems that disrupted equity trading without forcing a close. The concluding attack centered on a failure of the overnight settlement process at a clearinghouse.
QDIV OCTOBER 2017	QUANTUM DAWN IV	In November 2017, SIFMA introduced the concept of integrating cyber range capabilities into industry exercises and engaged the SimSpace Corporation's Cyber Range software for the simulation. Day 1 of Quantum Dawn IV provided a real-life "hands-on keyboard" experience for participating institutions to test their technical cyber response capabilities, while Day 2 involved participants engaging in a sector-wide simulation to test their crisis response communication.
QDV NOVEMBER 2019	QUANTUM DAWN V	SIFMA's first global cyber exercise, held in November 2019, enabled key public and private bodies around the globe to practice coordination and exercise incident response protocols, both internally and externally, to maintain smooth functioning of the financial markets when faced with a series of sector-wide global cyberattacks. The exercise helped identify the roles and responsibilities of key participants in managing global crises with cross-border impacts.
QDVI NOVEMBER 2021	QUANTUM DAWN VI	The industry-wide exercise simulated a large-scale ransomware attack by a state actor against several major global financial institutions servicing the custody markets. The exercise provided an opportunity for financial firms to assess their existing response playbooks, identify leading strategies and processes, and examine internal and external communications plans for responding to a ransomware attack.
QDVII NOVEMBER 2023	QUANTUM DAWN VII	In November 2023, SIFMA launched an exercise aimed to simulate operational impacts to financial firms, critical third parties, and the global financial ecosystem, and improve crisis and incident management response and recovery. The scenario involved an outage caused by a data disruption event at a fictional critical third party hosted in the cloud and used by the global financial sector to trade in the U.S. Treasury and repo markets.

Scenarios and Objectives

The exercise unfolded over three days, combining a central sector "command" rhythm with in-firm discussions and polling. The scenario layered severe weather, telecom infrastructure failure, an FMI outage, and adversarial cyber elements:

1. **Category 5 hurricane**

   A Category 5 hurricane has made landfall near New Jersey and Long Island. Impacts include widespread power outages and infrastructure damage. A state of emergency has been declared, major data centers in New Jersey are flooded, and critical staff cannot get into offices.

2. **Transatlantic cable cut**

   A major transatlantic communications cable has been severed, resulting in widespread disruptions in telecommunications between the U.S. and Europe. Critical data traffic into and out of financial centers in New York is impacted.

3. **FMI outage**

   ACME Clearing, a global central counterparty clearinghouse FMI, is hit with a zero-day ransomware attack causing ACME Clearing (a fictitious entity) to disconnect itself to minimize risk of contagion. The Depository Trust and Clearing Corporation (DTCC) disconnects ACME Clearing from the clearance and settlement infrastructure.

4. **State actor involvement**

   A state actor claims responsibility on social media for both the cable cut and the FMI ransomware attack. A zero-day novel malware surfaces amid the chaos, raising attribution ambiguity and accelerating defender workload, disinformation risk, and attestation complexity. National security concerns are raised.

The scenario's polycrisis elements meant resource collisions.

The scenario's polycrisis elements meant resource collisions, testing prioritization strategies in various realms such as physical access (people, fuel, generators), cyber response (forensics, patching, endpoint isolation), telecom failover priorities, and cloud egress patterns.

This deliberate overlap surfaced dependencies and governance friction that single-vector drills often fail to capture, encouraging the discussion of several themes where compound risk often concentrates: physical access to people and sites; network pathways and cloud service planes; third- and fourth-party trust boundaries; decision rights and attestation; and the people/communications layer that binds technical response to enterprise judgment. All of this worked to support achievement of Quantum Dawn VIII's primary objectives.

Quantum Dawn VIII's primary objectives

Strengthen incident/crisis management

Strengthen incident/crisis management and end-to-end recovery workflows for polycrisis conditions.

Exercise sector coordination

Exercise sector coordination across firms, associations, FMIs, law enforcement, and regulators—emphasizing global information sharing.

Validate playbooks and roles

Validate playbooks and roles within firms and at public-private intersections—leveraging live polling to assess preparedness.

Engage business stakeholders

Engage business stakeholders deeply, ensuring front-to-back alignment from technology and resilience teams to legal, communications, and business leadership.

Panels: Additional Insights, Real-World Recommendations

For the first time, Quantum Dawn included panel discussions comprised of a cross-section of industry and sector experts. Their real-world experiences and practical observations on the exercise helped deepen the overall findings and forward-looking recommendations.

Panel 1: Superstorm Sandy—from lessons to playbooks

Over the past decade, the financial services industry has made notable progress in strengthening operational resilience, driven largely by lessons learned from Superstorm Sandy and other major disruptions. Significant infrastructure investments—including enhanced backup power, hardened and diversified data centers, and more robust emergency protocols—have improved firms' ability to sustain critical operations under extreme conditions. **Public-private partnerships have also become a cornerstone of resilience**, enabling faster coordination, clearer information sharing, and more effective collective response.

Panel 2: Critical infrastructure and ISACs—interdependence by design

Cross-sector collaboration has emerged as a foundational requirement for operational resilience, particularly among communications, energy, and financial services. Because these sectors are deeply interdependent, failures in one can cascade rapidly into others. **Joint planning, shared exercises, and coordinated response mechanisms are therefore essential** to identifying hidden dependencies and strengthening collective preparedness. Information Sharing and Analysis Centers (ISACs) play a central role in this ecosystem by enabling timely, trusted, and often anonymous sharing of threat intelligence and incident data.

Panel 3: Cyber, AI, and resilience—convergence and control

AI is becoming a powerful enabler of resilience, accelerating scenario planning, threat detection, and alert triage. At the same time, organizations recognize the need for strong governance to avoid overreliance, misinterpretation, or hallucinated outputs. Looking ahead, **AI-empowered emerging threats such as deepfakes, quantum-enabled attacks, and ransomware reinforce the need for continuous testing**, adaptable defenses, and investment in both advanced technology and human judgment.

Panel 4: Disconnect/reconnect protocols and third parties—trust at speed

Effective disconnect and reconnect protocols are increasingly recognized as critical to managing third-party risk during operational disruptions. **Clearly defined and well-tested procedures enable firms to isolate affected vendors quickly** while minimizing unnecessary disconnections and enabling orderly reintegration once risks are mitigated.

AI is becoming a powerful enabler of resilience, accelerating scenario planning, threat detection, and alert triage.

Resiliency Considerations

In Quantum Dawn VIII, multi-vector conditions added a layer of complexity. These resiliency considerations reflect the realities of managing compound crises—where physical, cyber, and geopolitical shocks converge—and underscore the need for clear governance, deep cross-sector coordination, and disciplined execution.

I. Firms should continue to take steps to understand and address risks stemming from their use of third-party infrastructure.

Given the criticality of third-party services to most financial institutions, it remains important for firms to take steps to ensure they have a clear picture of the third parties they rely on, the potential risks associated with those third parties, and what the third party and the financial institution are doing independently and jointly to reduce those risks. Potential actions identified during the exercise that can help ameliorate risks associated with reliance on third parties include the following:

- **Plan systemically**

  Map third- and fourth-party dependencies and coordinate through industry frameworks and exercises.

- **Harden vendor relationships**

  Update contracts to define crisis roles, data access, and recovery support.

- **Adopt dynamic vendor monitoring**

  Move beyond static assessments to real-time risk ranking and automation.

- **Strengthen trust and transparency**

  Require clear attestations, forensic evidence, and explicit contract clauses on resilience.

- **Strengthen cross-sector coordination**

  No single sector can manage systemic risk alone.

- **Exercise together, regularly**

  Joint simulations reveal hidden interdependencies before crises occur.

- **Standardize to move faster**

  Common frameworks, language, and templates reduce friction in emergencies.

II. Access credentialing for essential staff needs further improvement.

Despite a decade of investment in remote-first resilience, Quantum Dawn VIII surfaced a still yet unresolved bottleneck: getting the right people to the right places during a regional emergency. With only 35% reporting essential staff credentialing and the Corporate Emergency Access System (CEAS) sunsetting, firms flagged post-CEAS modernization as a priority. The gap is most acutely felt when remote work is degraded by power or telecom disruption and when facilities require physical intervention (e.g., controlled shutdowns, failover, hardware swaps, evidence-preserving forensics).

III. Firms should integrate and practice disconnection/reconnection protocols.

Effective disconnect and reconnect protocols are increasingly recognized as critical to managing third-party risk during operational disruptions. Clearly defined and well-tested procedures enable firms to isolate affected vendors quickly while minimizing unnecessary disconnections and enabling orderly reintegration once risks are mitigated.

IV. Geographic dispersion (both of people and infrastructure) can aid resilience.

Certain events—such as natural disasters, electric grid outages, and civil unrest—cause disproportionate impacts to a single geographic area. Strengthening regional and infrastructural diversity by, for instance, diversifying data center locations, geographically separating operations, and having a dispersed personnel footprint can reduce systemic risk and enhance organizational resilience.

V. Firms should plan beyond the last crisis.

Resiliency requires organizations to plan beyond the last crisis. Risk models should anticipate future, more severe disruptions—not just repeat past scenarios.

Firms also benefit from questioning some of their planning assumptions. For instance, a firm should ask itself what it will do if its incident management plan relies on remote work but the incident in question impacts the ability of the workforce to work from home.

Conclusions

Quantum Dawn VIII validates that the industry has embraced polycrisis planning and the public-private collaboration imperative. The exercise's most challenging element—the undersea cable cut—spotlights how telecom and technical concentration risks can dominate sector resilience, especially when paired with FMI outages and adversary tradecraft. The sector shows healthy self-confidence in response capability, but the data reveal areas for improvement.

The financial services sector should prioritize practical, interoperable measures to strengthen systemic resilience. Developing a successor to the CEAS program, with robust verification and integration into emergency response protocols, would improve coordination during connectivity disruptions. Firms should also evaluate satellite-backup options, audit cloud dependencies, and maintain up-to-date inventories of third- and fourth-party connections to reduce concentration risk.

Expanding the use of AI for threat detection and continuity planning, alongside promoting employee personal preparedness and geographic dispersion, will further enhance resilience. Finally, broader adoption of DTCC and SIFMA reconnection protocols—supported by strong ISAC partnerships, clear vendor communications, realistic exercises, and shared resilience metrics—will be critical to improving sector-wide readiness and coordination.

At the sector level, calls for global directories and formal crisis structures point to the next stage of maturity. By integrating infrastructure status, FMI posture, anonymized firm signals, and coordinated communications, a joint operating picture can reduce response variance and accelerate consensus on the ground without diminishing firm autonomy.

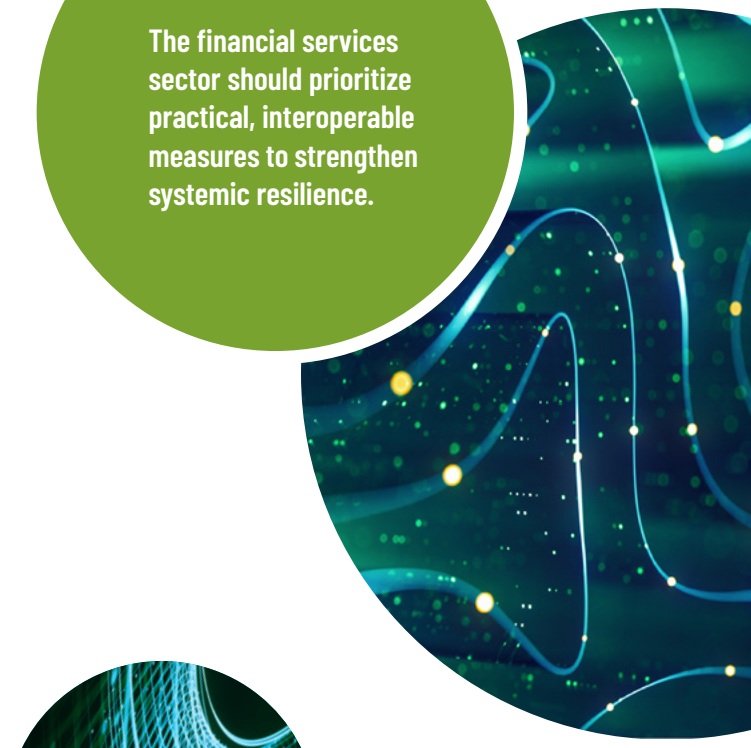
Finally, participating in more regular, realistic exercises can help close the gap between planning and execution. Compound crisis drills, reconnection sprints, cross-sector simulations, and broader war room participation can build the verification discipline and coordination muscle needed for rapid, confident recovery.

Next Steps

SIFMA will work to support members in these areas by:

1. Supporting efforts to better understand telecommunications, cloud, and other third- and fourth-party interdependencies
2. Socializing and encouraging adoption of reconnection protocols
3. Facilitating good AI governance practices for financial institutions
4. Exploring post-CEAS credentialing options
5. Building/maintaining a global directory and/or emergency notification capability
6. Sponsoring exercises

The financial services sector should prioritize practical, interoperable measures to strengthen systemic resilience.



SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

Protiviti is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit—enabling organizations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the Fortune 100 Best Companies to Work For® list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

sifma.org

protiviti.com

Contacts

Stephen Byron
Managing Director
SIFMA
+1.212.313.1254 | sbyron@sifma.org

Charles DeSimone
Managing Director
SIFMA
+1.212.313.1262 | cdesimone@sifma.org

Todd Klessman
Managing Director
SIFMA
+1.202.962.7322 | tklessman@sifma.org

Thomas Wagner
Managing Director
SIFMA
+1.212.313.1161 | twagner@sifma.org

Kim Bozzella
Managing Director
Protiviti
+1.212.603.5429 | kim.bozzella@protiviti.com

Andrew Retrum
Managing Director
Protiviti
+1.312.476.6353 | andrew.retrum@protiviti.com

Dugan Krwawicz
Director
Protiviti
+1.760.802.2882 | dugan.krwawicz@protiviti.com