SIFMA QDVII After-Action Report

Table of Contents

Executive Summary

From November 14 to 16, 2023, more than 1,000 participants from both the public and private sectors, representing over 170 financial institutions across more than 20 countries, participated in the Securities Industry and Financial Markets Association (SIFMA)'s global Quantum Dawn VII exercise. The goal of the exercise was to simulate operational impacts to financial firms, critical third parties and the global financial ecosystem, improve crisis and incident management response and recovery plans, and strengthen global coordination and information sharing mechanisms necessitated during significant operational outages such as a cyber incident.

The simulation included an outage taking the form of a data disruption event at a fictional critical third party ("CTP") hosted in the cloud and used by the global financial sector to trade in the U.S. Treasury and repo markets.

During the simulation, participants were polled on a series of questions, which provided significant insight into the industry's capabilities for addressing major third-party disruptions. These key findings form the basis of this after-action report:

- A majority of participants (75%) reported having experienced the loss of a critical third party, demonstrating that these outages are not unusual. Ninety-eight percent of firms have developed and maintain response and recovery plans for their critical third parties, and 80% of firms state their plans can account for outages lasting 24 hours or more.
- Information sharing is widespread and involves senior leadership and the board level. Participants demonstrated well-developed and diverse communication plans both internally and externally with stakeholders and industry peers.

History of Quantum Dawn Exercises

Over the past 13 years, SIFMA has coordinated a series of industry-wide resilience exercises known as Quantum Dawn. 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. Since 2011, the Quantum Dawn exercises have served as an important bi-annual event for assessing the financial services industry's capacity to coordinate an effective response to a sector wide outage caused by cyber, physical, or operational events.

Furthermore, the exercises are designed to illustrate 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 A DECADE OF TESTING AND RESILIENCE

QDI 2011 November	QUANTUM DAWN I & II	In November 2011 and July 2013, the financial services sector, in conjunction with service provider Norwich University Applied Research Institutes (NUARI), organized two marketwide cybersecurity exercises called Quantum Dawn I and Quantum Dawn II, respectively. Those events provided a forum for participants to exercise risk practices due to a disruption in equity trading and clearing processes in response to a systemic attack on market infrastructure.
QDII 2013 July		
QDIII 2015 September	QUANTUM DAWN III	Whereas Quantum Dawn II focused on decision making for closing the equity markets, 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 2017 October	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 sectorwide simulation to test their crisis response, communication, and coordination capabilities around a large-scale targeted cyberattack against numerous financial institutions and news organizations.
QDV 2019 November	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 sectorwide global cyberattacks. The exercise helped identify the roles and responsibilities of key participants in managing global crises with cross-border impacts and began development of its Global Directory of key crisis management contacts across the public and private sectors.
QDVI 2021 November	QUANTUM DAWN VI	The industrywide 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. The latest learnings on coordinating a response at a country, regional and global levels were shared, along with communication channels and strategies to liaise with relevant stakeholders, including the media.

Quantum Dawn VII Objectives

The intent of the exercise was to strengthen public and private sector-wide communications and information-sharing mechanisms, crisis management protocols, and decision-making, as well as legal and regulatory considerations, as exercise participants responded to and recovered from the outage of a critical third party used by the financial sector to trade in the U.S. Treasury and repo markets.

Additionally, Quantum Dawn VII achieved the following key objectives:

- Incorporated after actions and lessons learned from Quantum Dawn VI (2021), as well as recent disruptions including third-party outages and ransomware attacks.
- Provided a platform for member firms to assess their ability to respond to and recover from an outage of a critical third party hosted in the cloud that is widely used by the financial sector to trade, clear and settle in the U.S. Treasury and repo markets.
- Allowed financial firm participants to think through their preparations for a long-term outage of a critical third party.
- Reviewed with Global Directory members SIFMA's role to share information on management of cybersecurity attacks and critical third-party outages.
- Provided a forum for financial firms to strengthen internal incident response and crisis management playbooks.

In addition to the registered participants, many organizations gathered their internal crisis and incident management teams in "war rooms" to take part in the discussions. Most participants surveyed (about 62%) were individuals aligned with the first line of defense (information security/business resilience/crisis management) within their respective organizations, while approximately 22% were associated with the second line of defense (operational resilience/legal/compliance/operations/risk management). Almost half (~44%) had management job titles.

Scenario Overview

Exercise designers developed a scenario involving the multi-day outage of a fictional firm (Mammoth CTP), a critical third-party used widely by the financial sector to trade in the U.S. Treasury and repo markets hosted in the cloud. As the scenario progressed, it is discovered that the cause of the outage was due to an issue with the third party and not cloud related. The outage demonstrated the importance of cross-jurisdictional information sharing and coordination between financial firms, central banks, regulatory authorities, trade associations and information-sharing organizations.

The sequence of events for the simulated exercise were as follows:

- **Day 1**

  Mammoth CTP goes off-line. SIFMA stands up its Crisis Management Command Center and Crisis Management Team (CMT) call to engage with the sector, gather ground truth and assess impact to firms, the sector, and global markets.
- **Day 2**

  Participants engaged with SIFMA's crisis command center to assess firm impact and plans, communications, and response, recovery, and reconciliation.
- **Day 3**

  SIFMA reconvenes the CMT call to:
  - Continue recovery conversations with Mammoth CTP's CEO and legal counsel
  - Discuss data resilience status and recoverability
  - Allow the sector to confirm recovery status
  - Begin the reconnection protocol and attestation processes

As part of the exercise, participants had the opportunity to respond anonymously to polling questions such as:

- Has your firm experienced the long-term loss of a critical third-party service provider?
- Does your firm have a response and recovery plan for such an event?
- What actions do you take after confirming the loss of a critical third party?
- What is your information-sharing strategy?
- How long of an outage can you tolerate without facing business interruptions?
- What are your initial points of contact internally and externally once an outage is confirmed?
- What levels of leadership do you expect to engage?

Resiliency Considerations

Financial institutions increasingly rely on third parties for a variety of functions. If a critical third party is suddenly taken offline – whether by an operational disruption, security breach, or other event – it can interrupt a firm's business and potentially lead to larger scale problems.

Following the exercise, SIFMA and Protiviti reviewed the data member firms provided and developed several firm-level and sector-wide resiliency considerations.

The following are resiliency suggestions for firms to consider when evaluating and uplifting their incident and crisis plans and business resilience strategies:

I. Firms should continue to consider the impact of longer-term outages of their critical third parties.

While firms plan for third-party outages, an extended failure due to ransomware attacks may pose unforeseen challenges to interim workarounds and the ability of incident response teams to recover back-up data sources. Based on the firm's risk tolerance for re-connecting to a provider that may have experienced a cyber-attack, it could be much longer than anticipated before a third-party can meet the established reconnection criteria. Recent events show recovery from a ransomware event may be measured in days to weeks. Firms should continue preparing to manage their business through alternative means for a time frame that is aligned to more realistic recovery time objectives, considering recent ransomware events. Firms should evaluate whether their regular risk assessments appropriately reflect the increased volume and severity of critical third-party disruptions.

Firms should continue to enhance their enterprise risk assessment process to deepen understanding of how important third parties are to the delivery of their critical operations. Third-party risk management has increasingly become a focus of resilience guidelines and regulations, such as the Federal Financial Institutions Examination Council (FFIEC)'s Operational Resiliency Guidelines[1] in the U.S. and the Digital Operational Resilience Act (DORA)[2] in Europe, to ensure firms understand, manage, oversee, monitor and establish risk tolerances with critical third parties.

II. Firms should continue to improve their response and recovery processes around the long-term loss of a critical third party.

In evaluating their plans, respondents should consider the following:

- Is the incident isolated or more widespread?
- Are there alternatives, redundancies, and substitutability?
- Is there a plan for manual processing?
- Are the upstream and downstream impacts from a regulatory, liquidity, communications, and investor impact perspective understood?
- How long will the service be disrupted?
- How do counterparties reconnect?
- Has additional validation or testing, once reconnection is reestablished, been considered?

These questions will need to be addressed and understood in all their ramifications. Firms should establish risk-based criteria for disconnection from and reconnection to third parties that are experiencing cyber-attacks to ensure the safety and security of their own firm. In parallel, firms need to evaluate and exercise their plans to ensure there are viable recovery options that limit damage, amidst a disruption to their services.

III. Firms are encouraged to seek industry coordination and collaboration during major outages.

Once a critical third party's services are disrupted, coordination and communication plans are set in motion. Firms should proactively create and validate/evaluate these protocols prior to an incident to enable smoother coordination when an event does occur. Ideally, communication and coordination will not just be underway internally but should also be managed strategically across the industry, with customers, regulators, and the media, if necessary. It is recommended that firms be prepared with escalation protocols, necessary decision-making actions and crisis management templates that can be readily executed. Additionally, firms should incorporate measures for reassuring their market partners of their recovery process as a part of their industry coordination to help ensure the safety and soundness of the sector post-incident.

Conclusion

Quantum Dawn VII demonstrated the industry's preparations for an incident effecting a critical third party, a scenario which is timely given recent sector events that resulted in the loss of several critical third parties impacting the financial sector.

Survey results from the exercise highlight the integration of this scenario in firms' current crisis response plans and demonstrate opportunities for continued evolution. Key observations include:

- Nearly all respondents have response and recovery plans for critical third parties. These plans are documented and include clear reference for third parties deemed critical.
- More than 80% of participants are prepared for outages lasting 24 hours or more, showing a high level of resiliency for longer-term outages.
- Participants report their response and recovery plans for the loss of critical third-party services meet well-established industry standards and follow recognized regulatory guidelines. Their plans include, but are not limited to:
  - Integration with information sharing and crisis response organizations.
  - Plans for resiliency and substitutability amongst third-party providers.
  - Engagement with the C-Suite executives, Boards of Directors, and industry coordination bodies.
- The exercise also found communications plans for outages to be in place, with many firms providing cybersecurity and risk management direct lines to executive management and board members.
- Information-sharing protocols are well-established, with respondents possessing relationships with peer firms that often serve as an initial point of contact in the case of an emergency.

1. *The Fed – Supervisory Policy and Guidance Topics – Operational Resilience*, Federal Reserve, February 4, 2022.
2. *Digital Operational Resilience Act*, September 24, 2020.

Next Steps

SIFMA will continue supporting members in the following ways:

- Seeking improvement and enhancement of the industry's capabilities regarding long-term outages of critical third parties;
- Keeping members apprised of emerging regulations and guidance; and
- Maintaining a directory of organizations and points of contact globally to facilitate communication.

Finally, SIFMA will begin planning for Quantum Dawn VIII which will take place in late 2025 and collaborate with our partners to expand and develop this critical industry exercise.

Acknowledgements

SIFMA would like to acknowledge the 50 plus individuals who helped design and execute the Quantum Dawn VII exercise, as well as the hundreds of private and public sector participants from around the world who engaged and provided valuable insights.

SIFMA also extends a sincere thank you and appreciation to global consulting firm Protiviti for their assistance in coordination of the exercise, analysis of participant feedback, and preparation of this after-action report.

Key Resources

- SIFMA: Principles for Data Recovery From a Severe Cyber Scenario
- SIFMA: Cybersecurity Resources

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).

sifma.org

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Through our network of more than 85 offices in over 25 countries, Protiviti and its independent and locally owned Member Firms provide clients with consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit.

Named to the 2024 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti.com

Contacts

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

Tom Price
Managing Director, SIFMA
+1.212.313.1260 | tprice@sifma.org

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

Kim Bozzella
Managing Director, Global Leader of Technology Consulting, Protiviti
+1.212.603.5429 | kim.bozzella@protiviti.com

Andrew Retrum
Managing Director, Technology Consulting Security and Privacy, Protiviti
+1.312.476.6353 | andrew.retrum@protiviti.com

Douglas Wilbert
Managing Director, Risk & Compliance, Protiviti
+1.212.708.6399 | douglas.wilbert@protiviti.com