sifma

protiviti
Face the Future with Confidence

Quantum Dawn V After-Action Report

Exercising Industry Coordination in Response to a Global Cyber Disruption

TABLE OF CONTENTS

HISTORY OF QUANTUM DAWN EXERCISES

Since November 2011, SIFMA has coordinated a series of industry-wide resiliency exercises called Quantum Dawn. These exercises provide a forum for financial firms, regulatory bodies, government agencies and trade associations to respond to simulated cyber and/or physical attacks. The key driver for the exercises is to test the industry's ability to recover in a timely manner from events that could impact market integrity or cause widespread harm to the financial ecosystem.

Organized by the U.S. Department of Homeland Security and hosted by the Depository Trust & Clearing Corporation, the **first Quantum Dawn** exercise was held in November 2011. SIFMA then organized subsequent exercises, starting with **Quantum Dawn II** in July 2013. Those seminal events provided a forum for participants to test incident response playbooks and protocols across equities trading, clearing processes and market closure procedures in response to an ecosystem-wide attack on market infrastructure. Quantum Dawn II also focused on testing procedures that would inform the decision to close equity markets.

Quantum Dawn III, conducted in September 2015, simulated a large-scale cyberattack lasting three business days and focused on exercising procedures to maintain market operations through firm-specific and rolling attacks on equity exchanges and alternative trading systems. These attacks disrupted trading but did not result in market closures. The concluding attack centered on a failure of the overnight settlement process at a major clearinghouse.

Held in November 2017, **Quantum Dawn IV** (QDIV) provided firms with a real-life "hands on keyboard" exercise to test their technical cyber response capabilities using cyber range technologies. QDIV also engaged participants in a sector-wide exercise to test their crisis response, communication and coordination capabilities. The exercise simulated a "bad day" on Wall Street during which a large-scale cyberattack targeted financial institution payment infrastructures, with rolling impacts on the sector and markets. The events caused widespread consumer panic and market contagion after a major news outlet was hacked and "fake news" stories were presented.

EXERCISE OBJECTIVES

Quantum Dawn V (QDV), conducted in November 2019, tested the financial services industry's response to extreme cross-border cyberattacks, with a focus on evaluating the information-sharing and communication protocols of individual firms and the sector.

The Key Objectives of QDV:

1. Identify critical public and private sector participants that would likely be involved in a coordinated response to a global cyber disruption and educate all participants on their current roles and responsibilities.

2. Understand existing information-sharing capabilities and response protocols by testing them in a unified global exercise.

3. Identify gaps in the industry's response to a global disruption and document ways to improve coordination and strengthen information sharing across the sector.

QDV: SCENARIO OVERVIEW

During QDV, exercise designers and participants presented a fictitious scenario involving a rolling ransomware attack that targeted global systemically important financial institutions (G-SIFIs) in the United States, Asia-Pacific and the United Kingdom, as well as a U.S.-based financial markets utility (FMU).

The attack was orchestrated by a criminal insider and the sequencing of the scenario highlighted the sector's interconnectedness as well as the need to share information across regions to coordinate an effective response.

A GLOBAL EVENT FOR THE FINANCIAL SECTOR

QDV brought together key participants from the global financial community, attracting public and private sector institutions from many jurisdictions and professionals representing a broad range of roles and responsibilities.

More than 800 representatives from over 150 financial firms as well as more than 50 regulatory authorities, central banks, government agencies and trade associations across 19 countries participated in the event. The financial institutions included securities firms, banks, investment banks, asset managers and financial market infrastructure providers of all sizes.

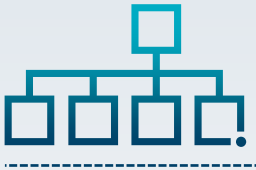
Regulatory organizations, central banks, government agencies and trade associations highlighted their response activities during the exercise. Several organizations discussed their roles in crisis response and what they would do in the presented scenario. These included SIFMA, the Association for Financial Markets in Europe (AFME), Asia Securities Industry and Financial Markets Association (ASIFMA), Securities and Exchange Commission (SEC), U.S. Treasury, Financial Services Information Sharing and Analysis Center (FS-ISAC), Bank of England, Financial Conduct Authority, HM Treasury, UK Finance Sector Cyber Collaboration Centre (FSCCC), the Bank of Canada, and Canadian provincial regulators.

QDV gave firms the opportunity to share their incident response processes, communications protocols and information-sharing practices with industry participants through real-time polling responses.

The exercise helped identify areas for both public and private sector institutions to improve global crisis coordination, information sharing and communication protocols during a sector-wide cyber incident.

RECOMMENDATIONS

The industry should consider implementing the following recommendations to improve information-sharing and incident-response capabilities.



1 Create a Directory of Critical Stakeholders and Key Contacts

Creating a directory of financial services firms and trade associations, regulatory bodies, central banks and government agencies that would respond to a global cyber or physical event is a good first step for the industry. The directory will define the roles and responsibilities of all the key players that will facilitate cross-border information sharing, incident response and recovery.

2 Conduct Periodic Exercises

The industry should schedule regular touchpoints and exercises. These exercises could be catalysts for developing global information-sharing capabilities and incident response and recovery protocols for critical public and private sector organizations and contacts. Additionally, periodic exercises will emphasize the need for all organizations to keep incident response playbooks and contact information up-to-date to ensure a rapid and coordinated global response to major events impacting the financial ecosystem.

3 Expand Information Sharing and Communications Capabilities

Our findings show many formal and informal communication channels exist today among financial firms, trade associations, regulatory bodies, government agencies and central banks mostly centered within each country or jurisdiction. Linking together existing information-sharing networks with organizations that currently manage crises in their respective jurisdictions, prior to an event, will strengthen cross-border information-sharing and communication capabilities among the public and private sector.

CONCLUSION AND ACKNOWLEDGEMENTS

The changing threat landscape requires financial institutions to be diligent about how they assess and manage their exposure to major disruptive events, such as large-scale cross-border cyberattacks.

The QDV exercise highlighted the industry's collective incident response and information sharing capabilities. As participating firms take the lessons learned and recommendations from QDV and apply them within their respective institutions, SIFMA and its partner organizations will continue to collaborate with the industry to enhance information-sharing and incident response practices on a global scale.

SIFMA would like to acknowledge the hundreds of organizations and individuals who helped design and execute the Quantum Dawn V exercise. Global consulting firm Protiviti helped analyze participant feedback and prepare this after-action report.

Finally, SIFMA would like to thank all the participants who engaged in the exercise and provided valuable insights, ensuring its success.

Visit SIFMA.org to learn about SIFMA's Quantum Dawn exercises, our annual industry business continuity tests and ongoing efforts to improve the industry's cyber and operational resilience.

CONTACT INFORMATION

SIFMA

Thomas Wagner
Managing Director
SIFMA
+1 212 313 1161
twagner@sifma.org

Tom Price
Managing Director
SIFMA
+1 212 313 1260
tprice@sifma.org

Charles DeSimone
Vice President
SIFMA
+1 212 313 1262
cdesimone@sifma.org

www.sifma.org

Protiviti

Ron Lefferts
Managing Director
Global Leader of Technology Consulting
Protiviti
+1 212 603 8317
ron.lefferts@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

www.protiviti.com

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). For more information, visit www.sifma.org.

sifma
Invested in America

Protiviti (www.protiviti.com) 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 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 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®