sifma Quantum Dawn VI Fact Sheet

PURPOSE:

The primary goal of the Quantum Dawn VI exercise was to allow financial firms, central banks, regulatory authorities, trade associations, law enforcement and information sharing organizations around the world to rehearse response mechanisms, both internally and across the sector, against a broad range of ransomware attacks.

The intent was to assess public and private sector-wide communications and information sharing mechanisms, crisis management protocols, and decision-making engaging SIFMA's Global Directory Members brought together during QDV, while identifying potential gaps.

SIFMA, in its crisis coordination role, led the exercise with regional support from sister trades AFME in Europe and ASIFMA in Asia. The exercise included participants from SIFMA, AFME and ASIFMA member firms as well as public sector crisis teams across globe. Protiviti provided consulting support.

SPECIFIC QUANTUM DAWN VI OBJECTIVES:

Quantum Dawn VI Objectives:

The objective of the exercise was to simulate an extreme disruption scenario with a significant global impact across the financial sector. The scenario emphasized global cross-jurisdiction information sharing between financial firms, central banks, regulatory authorities, trade associations and information sharing organizations.

1. Incorporate after actions and lessons learned from Quantum Dawn V, as well as recent disruptions including the SolarWinds and other breaches, third-party outages and ransomware attacks.
2. Exercise the industry's ability to respond to and recover from a ransomware attack affecting financial firms and the sector at large.
3. Exercise the interaction and information sharing amongst Global Directory Members with a focus on managing global ransomware attacks and potential impacts to the sector and financial markets.
4. Provide a forum for financial firms to exercise internal incident response playbooks and share best practices for managing a ransomware attack.

INDUSTRY CYBERSECURITY PRIORITIES:

Quantum Dawn VI is just one component of how SIFMA is working with its members on a variety of cybersecurity initiatives including:

- Promoting enhanced regulatory harmonization to encourage a more effective allocation of cyber resources;
- Promoting a robust industry-government partnership grounded in information sharing;
- Conducting exercises and industry tests designed to improve protocols for incident preparedness, response and recovery;
- Leveraging lessons learned to refine industry best practices, including for managing insider threats, third party risk, penetration testing and data security, including secure data storage and recovery.

EXERCISE BACKGROUND:

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 market-wide 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.

Quantum Dawn III:

Whereas Quantum Dawn II focused on exercising procedures for informing decision making for closing the equity markets, Quantum Dawn III, held 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 upon 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.

Quantum Dawn IV:

Quantum Dawn IV, held in November 2017, used service providers NUARI (Norwich University Applied Research Institutes), and its latest version of the DECIDE FS, and the SimSpace Corporation's Cyber Range software for the simulation and execution of the exercise. Day 1 of Quantum Dawn IV provided a real-life "hands-on-keyboard" exercise 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, and coordination capabilities around a large-scale targeted cyberattack made against numerous financial institutions and news organizations.

Quantum Dawn V:

Quantum Dawn V, held in November 2019, was a global exercise which 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. The exercise scenario emphasized cross-jurisdiction communication and coordination between member firms and regulatory agencies in North America, Europe, and Asia.

KEY FACTS:

Over 900 participants from 240 public and private sector institutions, including financial firms, central banks, regulators, and law enforcement entities, across more than 20 countries around the world participated in QDVI to help combat the rising number of ransomware attacks.

This was a "closed loop" simulation – no real-world systems were utilized or impacted.

This was a distributed exercise, meaning that organizations participated from their own locations to further enhance the realism of the simulation and make use of real-world communication systems like email and phone.

Quantum Dawn VI was not a pass/fail test but rather an opportunity for participants to interact across functions internally and with partners externally, both locally and globally, and to exercise their crisis response and communications plans.

RESULTS AND NEXT STEPS:

A clear takeaway from the exercise is the importance of a robust partnership between the industry and government grounded in information sharing. No single actor – not the federal government, nor any individual firm – has the resources to protect markets from cyber threats on their own.

SIFMA will work with Protiviti, who served as consultant on the exercise, to analyze participant feedback and produce a public after-action report with key observations and recommendations for enhancing the financial services sector's ability to respond to a global ransomware event.