sifma Quantum Dawn V Fact Sheet

PURPOSE:

The primary goal of the Quantum Dawn V exercise was to identify opportunities to improve coordination, communication and information sharing during a globally disruptive event. The exercise simulated a low probability "extreme scenario" with a significant global impact across the financial sector. The scenario emphasized cross-jurisdiction communication & coordination between member firms and regulatory agencies in North America, Europe, and Asia.

Specifically, Quantum Dawn V 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 which impacted market integrity and created cross-border impacts.

Quantum Dawn V built upon previous exercises by adding a robust global component. 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 (U.S.), AFME (Europe) and ASIFMA (Asia) member firms. Protiviti provided consulting support.

SPECIFIC QUANTUM DAWN V OBJECTIVES:

1. Identify key public and private sector participants who would lead their firms, organizations or jurisdiction during a global cyber disruption.
2. Bring the Financial Sector together in a unified exercise to build global response and recovery capabilities and identify participants' roles and responsibilities.
3. Test operational resiliency key concepts across the Financial Sector.
4. Improve coordination and information sharing across the sector around detecting, responding to, and recovering from a global disruption, including between:
   - SIFMA, AFME and ASFIMA member firms
   - Across regions between organizations responsible for crisis management, regulatory bodies and central banks.

INDUSTRY CYBERSECURITY PRIORITIES:

Quantum Dawn V 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;
- 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; and

EXERCISE BACKGROUND:

Quantum Dawn I & II:

In November of 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 across equities trading and clearing processes and market closure protocols 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. In a change from previous exercises, Day 1 of Quantum Dawn IV provided a real-life "hands-on-keyboard" exercise for participating institutions to test their technical cyber response capabilities. Day 2 involved participants engaging in a sector-wide simulation to test their crisis response, communication, and coordination capabilities that revolved around a simulated "bad day" on Wall Street in which a large-scale targeted cyberattack is made against numerous financial institutions and news organizations, with rolling impacts for the sector, markets, and customers.

KEY FACTS:

Quantum Dawn V took place November 7, 2019.

Over 600 participants from over 180 financial institutions and government agencies from Australia, Canada, Europe, Hong Kong, India, Malaysia, Japan, Singapore, and the U.S. participated in the drill.

Participating entities included securities firms, banks, asset managers, FS-ISAC, and financial market infrastructure providers of all sizes. The exercise allowed regulators, central banks and government entities, including U.S. Treasury, the Securities and Exchange Commission, the Bank of England, Bank of Canada, Monetary Authority of Singapore, Honk Kong Monetary Authority, Reserve Bank of India and others to participate or observe.

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 V 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 cyber event.