Fact Sheet: Quantum Dawn 3

PURPOSE:

A large scale cyber attack that broadly impacts the financial services sector and the US economy is a low probability, high impact event that the industry prepares for along with other possible crisis events. Quantum Dawn 3 is designed to enable financial institutions and the sector as a whole to practice and improve coordination with key industry and government partners such as the US Treasury, federal law enforcement, federal regulators, the Department of Homeland Security and the Financial Services Information Sharing and Analysis Center (FS-ISAC), to maintain equity market operations in the event of a systemic attack.

Quantum Dawn 3 is one component of how SIFMA is working with its members on a variety of cybersecurity initiatives including:

- Promoting information sharing and membership in the FS-ISAC;
- Principles for effective regulatory guidance and voluntary standards;
- Best practices for managing insider threats and third party risk;
- Guidance for small firms;
- Exercises and industry tests designed to improve protocols for incident preparedness, response and recovery;
- And specific protocols for coordination regarding market open and closing in the event of a major crisis.

SPECIFIC QUANTUM DAWN 3 OBJECTIVES:

1. Simulate the degradation of critical infrastructure by effecting the availability and accuracy of the clearance and settlement process for equities, allowing participants to coordinate to remediate or resolve the situation.
2. Rehearse firms' internal response capabilities to a cyber attack scenario which requires coordination of business continuity, equity operations and information security practices in order to maintain equity operations.
3. Exercise the interaction between firms and the public sector with a focus on sharing information or requesting assistance. Simulate the experience of crisis-state information sharing.

EXERCISE BACKGROUND:

In November of 2011 and July of 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 1 and Quantum Dawn 2, respectively. Those events provided a forum for participants to exercise risk practices across equities trading and clearing processes in response to a systemic attack on market infrastructure.

Quantum Dawn 3 built upon lessons learned from the previous exercises and utilized the newest version of the simulation software DECIDE-FS created by NUARI under a grant from the US Dept. of Homeland Security. Whereas Quantum Dawn 2 focused on exercising procedures for closing the equity markets, Quantum Dawn 3 focused on exercising procedures to maintain market operations in the event of a systemic attack.

This one-day exercise simulated three business days within the markets. Participants first experienced firm specific attacks, such as a distributed denial of service (DDoS), a domain name system (DNS) poisoning or breach of personally identifiable information (PII). These attacks were 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.

KEY FACTS:

Quantum Dawn 3 took place on September 16, 2015 and was coordinated by SIFMA, utilizing service provider NUARI (Norwich University Applied Research Institutes) for the planning and execution of the exercise. The simulation utilized NUARI's latest version of the DECIDE-FS software.

Over 650 participants from over 80 financial institutions and government agencies took part in the exercise. Participating entities included key industry and government partners such as the U.S. Department of the Treasury, Department of Homeland Security, Federal Bureau of Investigation, federal regulators and the Financial Services Information Sharing and Analysis Center (FS-ISAC).

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 3 was not a pass/fail test but rather an opportunity for participants to interact across functions internally and with partners externally and exercise their crisis response and communications plans. Participation in Quantum Dawn 3 increased to over 80 entities as compared to 50 entities in Quantum Dawn 2.

RESULTS AND NEXT STEPS:

The exercise was completed successfully and demonstrated the critical importance of information sharing in responding to a cyber attack and the value of having established and regularly utilized processes for information sharing prior to a crisis. Over the next several weeks we will work with Deloitte Cyber Risk Services, which served as an independent observer of the exercise, to analyze participant feedback and produce a public after-action report with key takeaways and recommendations for enhancing the sector's ability to respond.