TMPG Meeting Minutes
December 2, 2015

TMPG attendees

Zahir Antia (Bank of Canada)	James Hraska (Barclays)	Gerald Pucci (Blackrock)
Julia Coronado (Graham Capital)	Gary Kain (American Capital Agency)	James Slater (BNY Mellon)
James DeMare (BAML)	Steven Meier (State Street Global Advisors)	Mark Tsesarsky (Citigroup)
Michael Garrett (Wellington)	Sandra O'Connor (JPM)	Stuart Wexler (ICAP)
Beth Hammack (Goldman Sachs)	Murray Pozmanter (DTCC)	Thomas Wipf (Morgan Stanley)

FRBNY attendees

Nashrah Ahmed	Frank Keane	Brett Rose
Michelle Ezer	Radhika Mithal	Janine Tramontana
Josh Frost	Simon Potter	Nate Wuerffel

SIFMA attendees

Charles DeSimone	Tom Price

U.S. Department of Treasury attendee
James Clark

- The meeting commenced with the Chair inviting members to submit topics for a future priorities discussion at the January 2016 TMPG meeting. The Chair then introduced representatives from SIFMA.

- The SIFMA representatives updated the TMPG on the organization's recent work on contingency planning for business continuity events. The representatives described the scope and results of the annual SIFMA industry test, which allowed firms to test backup connectivity with a broad range of exchanges, utilities, and services providers. The representatives also described a recent exercise targeted at the equities markets (see appendix) which simulated public and private sector market-wide communications, information sharing, threat monitoring and decision making during a systemic cyber-attack. In the ensuing discussion TMPG members suggested it would be worthwhile for SIFMA to consider conducting a similar exercise for the fixed income market.

  SIFMA representatives also updated the TMPG on the ongoing preparedness work of its Market Response Committees for the fixed income and equity markets. These standing committees determine whether a market disruption would warrant special trading or settlement recommendations, including closure if necessary, and facilitate the dissemination of information to various stakeholders. The TMPG members reiterated prior recommendations that the Market Response Committees should aim to agree a set of criteria to be analyzed in the event of certain pre-identified emergency conditions. It was noted that, for each, SIFMA could then document the expected decision the Committees might make. Members opined that establishing criteria in advance can effectively reduce delays and streamline decision making around market open/close recommendations and provide transparency in advance to market participants of the likely outcomes of certain events and conditions. The TMPG encouraged

SIFMA to prioritize the development of criteria around market open/close recommendation for the fixed income market and invited SIFMA to share progress at a future meeting. Following this discussion, SIFMA representatives left the meeting.

- Next, the TMPG reviewed and agreed to release for consultation a set of proposed best practice recommendations to address the use of financial benchmarks in TMPG covered markets, along with a related document that describes the findings from three case studies on selected reference rates relevant to the TMPG covered markets.[1] It was noted that the TMPG expects to release a final set of best practice recommendations after the consultation period. The TMPG also agreed to establish a working group to continue coordinating with other industry groups that are focused on evaluating potential alternatives to the use of the ICAP Fed Funds Open, one of the three case studies examined by the TMPG.

- The TMPG discussed recent market developments including expectations for the December FOMC, the potential implications of the FOMC meeting for money markets, and expected year-end liquidity conditions. Certain recent regulatory developments related to automated trading were noted, including the Securities and Exchange Commission's proposed amendments to Regulation ATS and the Commodity Futures Trading Commission's proposed Regulation AT.

  The Treasury representative thanked TMPG members for attending the recent Treasury market structure conference and the Roundtable on Treasury Markets and Debt Management. It was noted that the U.S. Treasury is working on a request for information (RFI) related to the changes in the structure and liquidity of the Treasury market, and TMPG members were invited to provide input into the process.

- Finally, the margining working group noted that it had conveyed to FINRA and SEC staff the TMPG's support for the proposed amendments to FINRA Rule 4210 to establish margin requirements for forward settling agency MBS transactions. The working group also noted that it had shared the TMPG's expectation that the best practice for margining will remain a two-way exchange of margin, which better ensures a level playing field and mitigates credit and systemic risk. A fuller discussion of the TMPG's perspectives on the FINRA proposal is available in the November minutes.

- The next TMPG meeting is scheduled to take place on Thursday, January 14th, 2016 from 3:00-5:00 PM.

[1] The TMPG subsequently released, for comment, the proposed best practice guidance to address the use of benchmarks in TMPG covered markets on December 3, 2015.

Deloitte.

sifma
Invested in America

Standing together for financial industry cyber resilience

Quantum Dawn 3 after-action report

November 23, 2015

Table of contents

Background

In November of 2011 and July of 2013, the Securities Industry and Financial Markets Association (SIFMA), in conjunction with Norwich University Applied Research Institutes (NUARI), coordinated two cybersecurity exercises for the financial services sector (Sector) called Quantum Dawn 1 and Quantum Dawn 2, respectively. These wide-scale simulations provided a forum for participants to exercise risk practice responses to a systemic cyberattack. On September 16th 2015, SIFMA hosted Quantum Dawn 3 (QD3), the third cyber simulation in the series. It included over 650 participants from over 80 financial institutions, government agencies and market utilities.

QD3 was designed with a focus to improve the readiness of the Sector to respond to Sector-wide cyberattacks. The exercise allowed firms to rehearse response mechanisms, both internally across departments and externally across the Sector, against a broad range of attacks, as well as to simulate public and private sector market-wide communications, information sharing, threat monitoring, and decision-making during a systemic cyber-attack.

Deloitte Advisory observed the simulation and assisted in the preparation of this after-action report containing recommendations aimed to further protect the nation's critical financial services infrastructure. This report focuses on the industry's overall response to cyber-attacks (e.g., communication and escalation, decision-making, government interactions, financial sector process implications) and provides high-level observations that individual market participants should consider to better respond to cyber incidents.

Exercise objectives

Goals of the exercise, as defined by SIFMA, are as follows:

1. Simulate the degradation of critical infrastructure by effecting the timeliness and /or accuracy (integrity) of the clearance and settlement process for equities, allowing participants to exercise their coordination to remediate or resolve the situation.
2. Rehearse firms' internal response capabilities to a cyber-attack scenario, which requires coordination of business continuity, operations and information security practices in order to maintain equity operations.
3. Exercise the interaction between the firms and the public sector (e.g., government agencies, regulators) with a focus on sharing information or requesting assistance.
4. Facilitate crisis-state information sharing using only real world communication paths [e.g., phone, email, Financial Services Information Sharing and Analysis Center (FS-ISAC) portal].
5. Exercise the Financial Services Sector Coordinating Council (FSSCC)/FS-ISAC All Hazards Playbook and the Financial Sector Cyber Response Coordination Guide (FSCRCG) so that firms understand what coordination will occur at a Sector level during a systemic crisis situation.

QD3 cyber-attack scenario

The scenario, designed by NUARI, was a one-day exercise which featured several different attacks that participants faced over a simulated three-business-day timeline. The scenarios were built on lessons learned from past exercises and with thoughtful input from industry specialists.

Participants first experienced a set of individual firm-level attacks, such as a distributed denial of service (DDoS), a domain name system (DNS) poisoning or breach of personally identifiable information (PII) that prevented them from conducting business normally. These attacks allowed participants to rehearse their response playbooks and plans.

The next set of attacks caused market-wide disruption by affecting equity exchanges, alternative trading systems, and the overnight settlement process. These attacks forced the market participants to work in collaboration with each other and government agencies and regulators to address the incident at hand.

QD3 stands out from previous Quantum Dawn exercises by:

Allowing firms to rehearse their internal response and recovery practices against a diverse set of threats

Highlighting dependencies on critical market utilities and infrastructure

Providing opportunities for firms to engage and interact with law enforcement

Cyber-attack scenario (contd.)

The five cyberattacks the participating organizations worked through are summarized below. No organization received all four of the firm-specific attacks.

Attack Name

Domain Name System (DNS) Attack	Distributed Denial of Service (DDoS)	Insider PII Breach	Loss of Availability	Settlement System Compromise (Malware)
• The firm's website traffic redirected to a bogus website through manipulated router settings. • Customers that attempted to access the affected websites during this time may have had their login credentials compromised and/or may have been targeted with malicious software.	• Attackers threatened to launch a DDoS attack if banks failed to pay a internet Bitcoin ransom within two hours. • After the stated time elapsed, the attacker conducted a small scale and relatively short "demonstration" attack that caused minor disruption to the customer website. • The group asserted that it has the capability to launch more powerful and sustained attacks and demanded that firms pay a larger ransom.	• An insider gained unauthorized access to account information of key clients and posted additional client data in exchange for Bitcoin Internet currency. • FBI reported that this was a data breach and a patch was issued which needed to be applied to repair functionality. • If unaffected firms were informed about the need to patch, they could prevent data breaches at their firm.	• Firms lost availability/ connection to major trade processing provider or custodian. • An insider compromised the exchange router to disrupt order processing between self clearing firms and the exchanges.	• An insider introduced malware into clearing systems leading to transaction failures. • Malware was initiated after close-of-day summary and settlement reports, so that all data will appear correct going into Continuous Net Settlement (CNS) Evening Cycle. • Malware caused major settlement failures (80 – 90%) and increased risk and uncertainty to all parties. • Media released reports to the public, with many errors in the details.

Attack Summary

Firm-Specific Attacks Pervasive Industry-Wide Attack

QD3 benefited the industry

QD3 demonstrated many positive behaviors and continued to raise awareness among industry participants. The Sector should continue to build on these results and successes:

- ✓ Institutions were able to evaluate internal and external capabilities in responding to the market-wide cyberattacks.
- ✓ More than 80 organizations built muscle memory within their crisis response by exercising DDoS mitigation, DNS attack coordination, and data breach assessment and communication. All respondents to the post-simulation survey indicated their organization felt more prepared after the exercise than before.
- ✓ Institutions, along with the FS-ISAC, the FBI, and regulators, enhanced their working relationships and exercised the public/private collaboration that will be required to respond to a large-scale attack.
- ✓ The FS-ISAC and FBI specifically indicated that they were appropriately engaged by organizations and were active participants in information sharing during the exercise.
- ✓ The exercise demonstrated the critical importance of information sharing in responding to a cyberattack and the value of having established and regularly utilized processes prior to a crisis.

Recommendations

While the exercise yielded many positive results, it also identified opportunities to improve response protocols and strengthen coordination among the industry participants.

Theme	Recommendations
Individual Firm Preparedness	**Internal response capabilities during a cyber-attack** • Enhance executive leadership involvement in the response, recovery, and decision making protocols during times of crisis. Firms should create integrated cyber incident response teams consisting of representatives from internal information security, technology, business functions, and required third parties to support a robust response and recovery strategy. • Enhance their internal playbooks to prepare for an expanded array of attacks, including development of additional scenario-based playbooks that account for these various types of attacks or threat vectors.
Sector Preparedness	**Market wide communication, monitoring, and decisions-making** • Enhance the role of market utilities to aid the early detection of, and response to, a systemic crisis. • Develop additional (or augment existing) Sector playbooks to cover Sector-wide events affecting market utilities. **Interactions between firms and the public sector (e.g., government agencies, regulators, law enforcement)** • Strengthen communication with regulators and government agencies, and raise awareness concerning government resources and capabilities available to assist the Sector. • Promote information sharing standards and processes to allow market participants to share various cyberattack data, such as threat actors, common vulnerabilities, and mitigation strategies. • Establish criteria and thresholds jointly between the private sector, government agencies and regulators, that will be used to trigger contact and action between them.

Acknowledgements

- Participating financial institutions and associations
- Federal contributors – US Department of Treasury, US Securities & Exchange Commission (SEC), US Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI)
- Industry groups – Securities Industry and Financial Markets Association (SIFMA); Financial Services – Information Sharing and Analysis Center (FS-ISAC); Financial Services Sector Coordinating Council (FSSCC); Financial and Banking Information Infrastructure Committee (FBIIC)
- QD3 was designed by Norwich University Applied Research Institutes (NUARI) and hosted by SIFMA

Contact Information

Karl Schimmeck
Managing Director
SIFMA
+1 212 313 1183
kschimmeck@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

Edward W. Powers
National Managing Principal
Advisory Cyber Risk Services
Deloitte & Touche LLP
+1 212 436 5599
epowers@deloitte.com

Walter Hoogmoed
Principal
Deloitte & Touche LLP
+1 973 602 5840
whoogmoed@deloitte.com

Vikram Bhat
Principal
Deloitte & Touche LLP
+1 973 602 4270
vbhat@deloitte.com

SIFMA brings together the shared interests of hundreds of securities firms, banks, and asset managers. These companies are engaged in communities across the country to raise capital for businesses, promote job creation, and lead economic growth.

www.sifma.org

Deloitte Advisory's Cyber Risk practice assists many of the world's leading organizations to be Secure.Vigilant.Resilient.™ in the face of cyber threats.

www.deloitte.com/us/cyber-risk

SIFMA is the voice of the U.S. securities industry, representing the broker-dealers, banks and asset managers whose 889,000 employees provide access to the capital markets, raising over $2.4 trillion for businesses and municipalities in the U.S., serving clients with over $16 trillion in assets and managing more than $62 trillion in assets for individual and institutional clients including mutual funds and retirement plans. 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 http://www.sifma.org.

This document contains general information only and Deloitte Advisory is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte Advisory shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, “Deloitte Advisory” means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.