Deloitte.

sifma
Invested in America

Quantum Dawn 2

A simulation to exercise cyber resilience and crisis management capabilities

October 21, 2013

Table of contents

Background

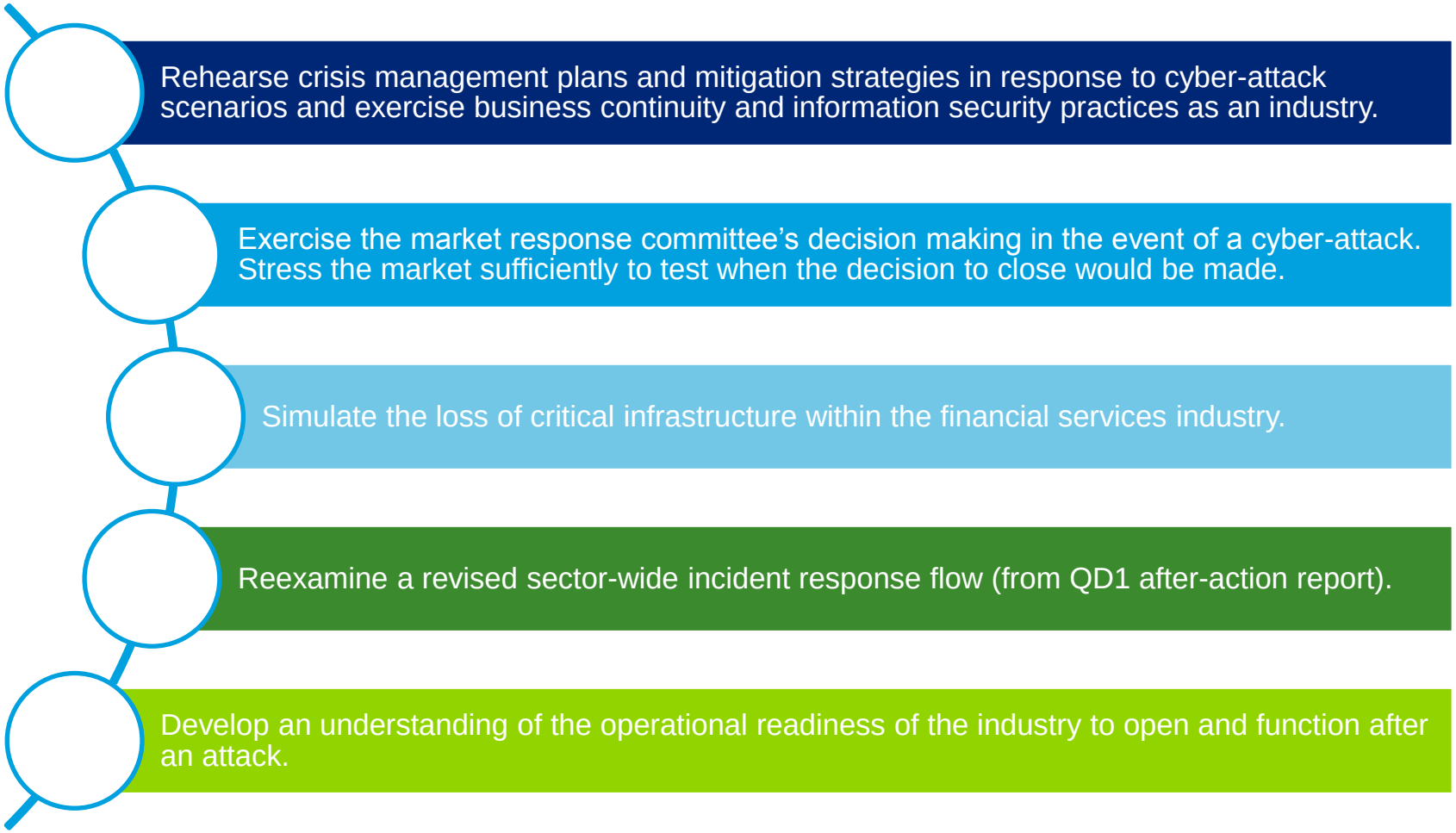
Throughout 2013, a number of high-profile media reports have called attention to the growing threat of cyber-attacks against our country and especially our critical infrastructure. Cyber-attacks often have little forewarning and can happen rapidly or over a period of time, requiring the financial services sector (the "sector") to be vigilant and ready to respond.

On July 18, 2013, the financial services sector set out to exercise its capabilities to respond to a wide-scale cyber-attack. The Quantum Dawn 2 cyber-exercise ("QD2" or "exercise" or "simulation"), hosted by the Securities Industry and Financial Markets Association ("SIFMA"), represented the next step in the continuing effort by the sector to improve its ability to coordinate and respond to a systemic cyber-attack.

Deloitte joined with SIFMA to serve as objective observers of the simulation and to assist in the preparation of this after-action report ("AAR") to identify ways to improve sector-wide responses to cyber events.

Exercise objectives

QD2 was a six-hour exercise simulating multiple trading days. Goals of the exercise, as defined by SIFMA, were as follows:



QD2 cyber-attack scenario

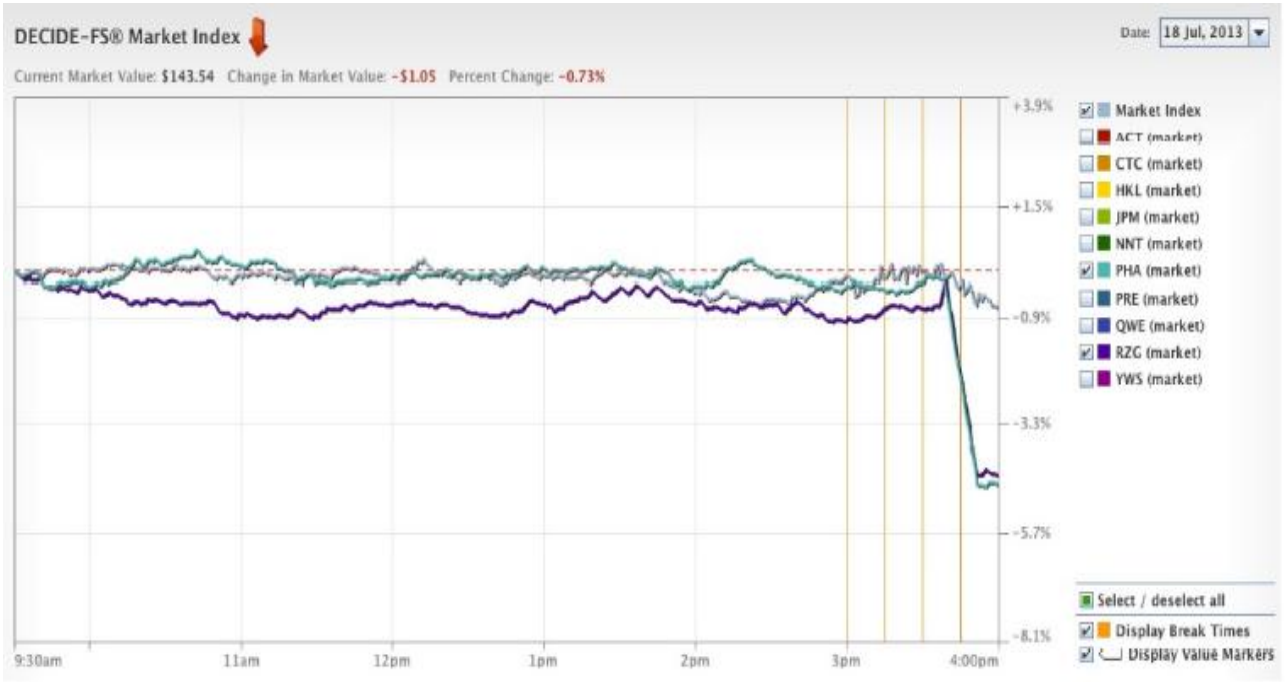
The exercise scenario included multiple attack vectors originating from both external sources and malicious insiders. Motives for the attacks included the desire to steal large amounts of money, disrupt the equities market, and degrade a firm's post-trade processing capability.

1. Creation of an automatic sell-off in target stocks by using stolen administrator accounts
2. Introduction of counterfeit and malicious telecommunication equipment to divert attention and slow the investigation into the automatic sell-off
3. Substantiation of the price drop by issuing fraudulent press releases on target stocks
4. Disruption of governmental websites and services through a distributed denial of service ("DDOS") attack
5. Corruption of the source code of a financial application widely used in the equities market
6. Degradation of the credibility of an industry group by sending a phishing email to harvest user names and passwords and submitting false information on the attack
7. Disruption of technology service by unleashing a custom virus with the goal of degrading post-trade processing

QD2 cyber-attack scenario (continued)

The attack vectors described directly affected market performance and were intentionally designed to force the decision to close the market by the end of the exercise.

The screen capture below from the first day in the simulated environment shows how the introduction of attack vectors impacted the market. A visible drop in the market index shows reaction of the markets and the ensuing crisis that could happen in a real-world scenario.



QD2 yielded many positive results

The simulation brought together key members of business, operations, technology, security, and crisis management teams, allowing them to escalate and respond to cyber-attack scenarios effectively.

The ongoing public-private partnership between the sector and various government and regulatory agencies that play a critical role in protecting the markets and investor confidence was furthered.

As the incident unfolded, the Financial Services Information Sharing and Analysis Center (FS-ISAC), SIFMA, and market participants executed on the core components of the incident command structure as defined in the FS-ISAC crisis management playbook and other relevant protocols, including the formation of various committees and forums to support the sector.

The role of the exchanges and clearinghouses as the hubs of information gathering and sharing was highlighted.

Strong coordination between SIFMA and various FS-ISAC committees was evident.

The Market Response Committee protocol was executed and was able to reach the decision to close the markets.

The QD2 exercise successfully tested many of the processes and protocols that the industry has worked over the years to implement for incident response and crisis management. It raised awareness among industry participants about working together in a coordinated manner to address systemic risk issues.

Recommendations

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

Sector-wide incident command structure and processes:

- Enhance the existing sector response playbook to better account for a securities industry specific incident with the goal of strengthening the integration between industry groups, market participants, and government agencies.
- Improve coordination between business and technology leaders during cyber incident analysis and response.
- Enhance the role of exchanges, clearing firms, and trusted government partners in cyber incident response and crisis management. Increase awareness about government resources available to assist the sector.

Systemic risk assessment and decision process:

- Augment existing guidelines and decision frameworks to determine if cyber incidents are systemic in nature.
- Invest in next-generation capabilities to support systemic risk analytics, information sharing, and crisis management.

Communication and information sharing:

- Institutionalize procedures for the market open/close decisions during times of cyber incident response and crises.
- Enhance protocols to promote increased communication and information sharing among market participants.
- Formalize public awareness and communications strategies with a view to promote trust and confidence in the markets.

Acknowledgements

- Participating financial institutions and associations

- Federal contributors – U.S Department of Treasury, U.S Securities & Exchange Commission (SEC), 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); BITS - Financial Services Roundtable and Chicago First

- QD2 was designed by Norwich University Applied Research Institutes

Contact information

Karl Schimmeck
Vice President
SIFMA
+1 212 313 1183
kschimmeck@sifma.org

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

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.

Edward W. Powers
National Managing Principal
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

Deloitte's Security & Privacy practice assists many of the world's leading organizations to be secure, vigilant, and resilient in the face of cyber threats.

http://www.sifma.org/services/bcp/cyber-exercise---quantum-dawn-2/