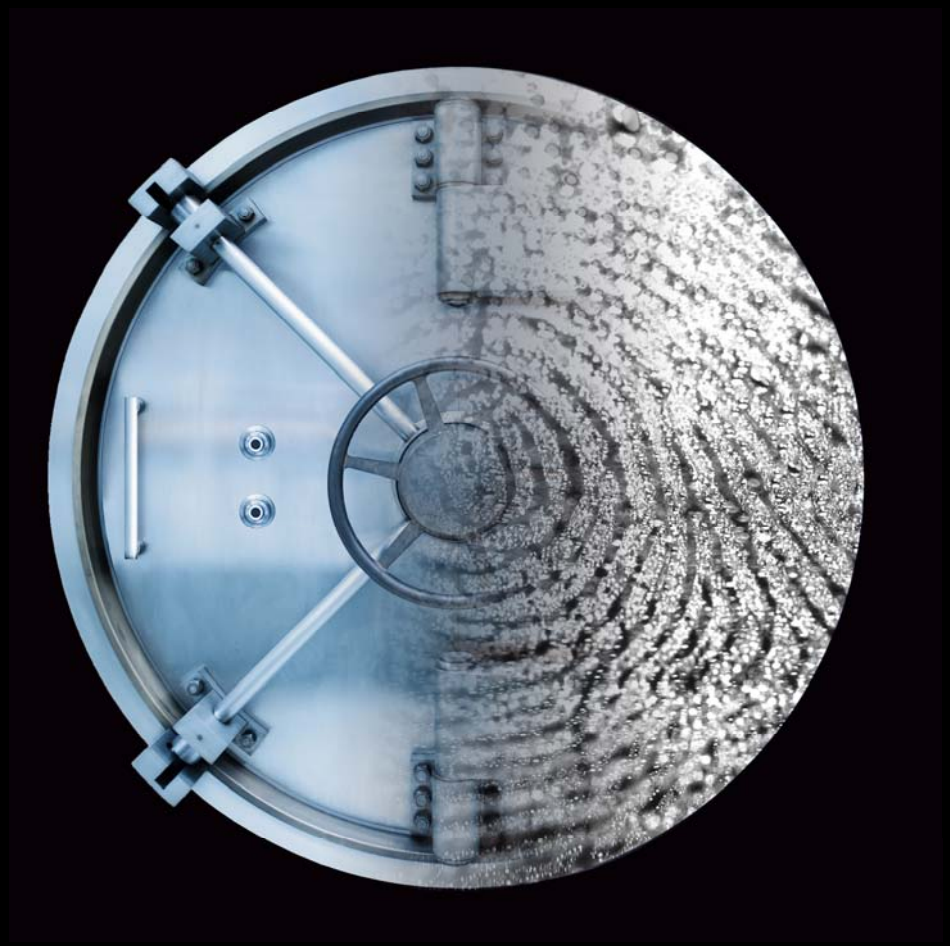
Deloitte.



Standing Together for Financial Industry Resilience

Quantum Dawn IV after-action report

June 2018

Contents

Background

In November of 2017, the Securities Industry and Financial Markets Association (SIFMA), in conjunction with Norwich University Applied Research Institutes (NUARI) and SimSpace Corporation, hosted the fourth iteration of Quantum Dawn exercises, Quantum Dawn IV. The exercise provided a forum for participants to exercise their technical and crisis response capabilities in response to a sector-wide cyberattack. This Exercise built on the lessons learned from previous Quantum Dawn exercises and included over 1000 participants from over 50 financial institutions, government agencies, industry groups, and market utilities.

Quantum Dawn IV was designed to strengthen the readiness of the financial services sector to respond to cyberattacks in a coordinated manner. Day 1 provided a real-life "hands-on-keyboard" exercise for participating financial 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 sector-wide coordination capabilities.

Deloitte Risk and Financial Advisory observed the simulation and prepared this after-action report with recommendations aimed to strengthen sector's readiness to defend 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 the Sector should consider for a coordinated response to cyber incidents.

Exercise objectives

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

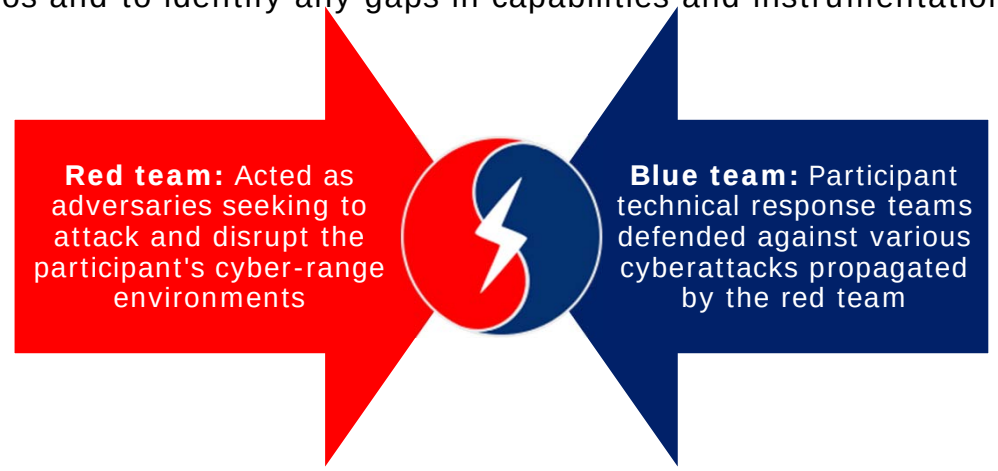
1. Exercise readiness of financial institutions across multiple business-lines, as well as staff within information security, information technology, business continuity, privacy, legal, risk, operations, human resources and others.
2. Exercise firm connectivity and communication protocols to the sector and government through established playbooks.
3. Provide information security staff with an optional “hands-on-keyboard” experience utilizing a “cyber range” provided by SimSpace.
4. Exercise, and determine the utility, operability and potential overlap of existing playbooks and protocols including the Securities Industry Financial Markets Association (SIFMA) Protocols and the Financial Services Information Sharing and Analysis Center (FS-ISAC) All Hazards Playbook.
5. Determine the role of regulators, government agencies, and law enforcement such as the Department of Homeland Security (“DHS”), Department of Treasury (“Treasury”), Federal Bureau of Investigation (“FBI”), White House and others.

Day one—Cyber-range exercise

While prior Quantum Dawn exercises focused on simulations to test the crisis management and coordination capabilities of participants, this year, in collaboration with SimSpace Corporation, SIFMA introduced a cyber range exercise in which a "red team" of adversaries attempted to infiltrate a specialized sandbox environment, the "cyber range". Each participating institution set up their defenses using the same security tools available on their production network. The "Blue Team" from the institution operated those tools and worked to thwart the attacks.

This exercise was a technical one, and it measured the blue teams' ability to block, detect, and eradicate the advances of the red team. The red team attempted a rich array of cyber-attacks ranging from low-level simple attacks to more sophisticated scenarios.

The exercise was followed by an information sharing session where participating firms and SimSpace Corporation red team attackers shared their in-game strategies and reactions. Participants identified the simulation as an optimal mechanism to test their technical preparedness, to train their incident response staff on real-life scenarios and to identify any gaps in capabilities and instrumentation.



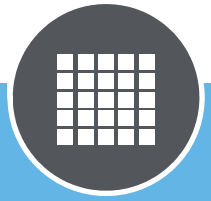
Day two—Cyberattack scenario

The Day 2 scenario simulated a “bad day” on Wall Street through a large-scale targeted cyber-attack against numerous financial institutions, with rolling impacts for the sector, markets, and customers. Firms experienced targeted malware attacks that corrupted payments-related messages and then lost the ability to transmit payments altogether.

Breaking news reports throughout the day brought attention to the turmoil in the financial sector causing the industry to exercise its media response protocols. At a point, a major news outlet was hacked, and fraudulent news stories overstated or misstated the events in the sector, causing potential panic for customers and contagion in the markets. Later in the day, firms were also presented with scenarios such as theft of funds and exfiltration of private customer data through ransomware, watering-hole, and other attacks.

QDIV stands out from less integrated exercises by:

Allowing the Sector to exercise roles and responsibilities of sector bodies such as SIFMA and FS-ISAC



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

Providing opportunities for firms to coordinate their response to the cyber incident with law enforcement and regulatory bodies

Day two—Cyberattack scenario (cont.)

The cyberattacks participating organizations received included the following:

Attack name

Payment fraud	Distributed denial of service (DDoS)	Data exfiltration	Payment system compromise (malware)
			
• Firms discovered that funds were mistakenly or fraudulently transferred without appropriate operations controls. • Previously cancelled transactions were modified to execute transfer of funds.	• Adversaries attempted to render services unavailable by overwhelming systems with abnormal traffic from multiple sources. • Internet-facing systems of participants were targeted using DDoS attacks.	• Firms were targeted with a data theft/ransomware breach attack that compromised a heavily used website/application hosted by a critical third party. • Firms discovered that international bank account numbers, including passwords and other personal information of many customers, had been exfiltrated.	• Firms experienced targeted malware attacks on core payments infrastructure, which resulted in corrupted payment messages. • Malware morphed and firms were then unable to send or receive payment instruction messages.

Quantum Dawn IV benefits the industry

QDIV demonstrated many positive results and continued to enhance sector-wide cybersecurity readiness. The Sector should continue to build on these results and successes:

More than 50 organizations and over 1,000 industry experts built muscle memory within their crisis response by exercising DDoS mitigation, ransomware response, and payment system recovery. The firms exercised both their technical response capabilities and sector coordination procedures.

Institutions, along with the FS-ISAC, SIFMA, law enforcement, government, and regulatory bodies, enhanced their working relationships and exercised the public/private collaboration that will be required to respond to a large-scale attack.

The cyber range exercise led by SimSpace Corporation added a new dimension to the Quantum Dawn series by giving firms the opportunity to exercise their technical response capabilities.

The exercise helped identify areas of improvements for both public and private sector to strengthen crisis coordination and communication during a sector-wide cyber incident.

Recommendations

The exercise was designed to identify areas where firms and the Sector as a whole can continue to improve their incident response processes. Below are the high-level recommendations:

Sector-wide coordination, communication and decision-making:

- Simplify the complexity of Sector response and coordination playbooks to enable a seamless, rapid and coordinated response and recovery from cyber events.
- Define clear roles and responsibilities for Sector bodies such as SIFMA, the FS-ISAC and public-sector partners.
- Clarify roles and responsibilities pertaining to the delivery of timely Sector-wide communications and messages to the financial sector, the media and the public.
- Ensure that all Sector-wide coordination calls and incident response meetings have a formal definition and structure to seamlessly manage communications and decision-making during a cyber event.

Coordination with public sector agencies (e.g., government agencies, regulators, law enforcement):

- Define the roles and responsibilities of public-sector agencies during a cyber event and ensure they are clearly understood and actively tested through cyber simulations and exercises.
- Provide clarity around the detailed information the US government requires from the private sector in order to be able to respond and react to systemic cyber events.
- Promote better communication to the private sector participants in order to provide situational awareness and support incident mitigation during a cyber event.
- Clarify the protocols to be used during public sector crisis management coordination calls.

Acknowledgements

Participating financial institutions and associations:

- **Federal contributors:** US Department of Treasury, US Securities & Exchange Commission (SEC), 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)
- QDIV was organized and designed by Norwich University Applied Research Institutes (NUARI) and SimSpace Corporation, and hosted by SIFMA

Contact information

SIFMA

Thomas Wagner
Managing Director
SIFMA
+1 212 313 1161
twagner@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

Tyler Morris
Associate
SIFMA
+1 212 313 1261
tmorris@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.
www.sifma.org

Deloitte

Edward W. Powers
Principal
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 5599
epowers@deloitte.com

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

Kevin Gallagher
Managing Director
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 6072
kevgallagher@deloitte.com

Deloitte Advisory's Cyber Risk practice assists many of the world's leading organizations to be Secure.Vigilant.Resilient.TM in the face of cyber threats.
www.deloitte.com/us/cyber-risk

SIFMA is the voice of the U.S. securities industry. We represent the broker-dealers, banks and asset managers whose nearly 1 million employees provide access to the capital markets, raising over $2.5 trillion for businesses and municipalities in the U.S., serving clients with over $18.5 trillion in assets and managing more than $67 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.

Deloitte.

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.