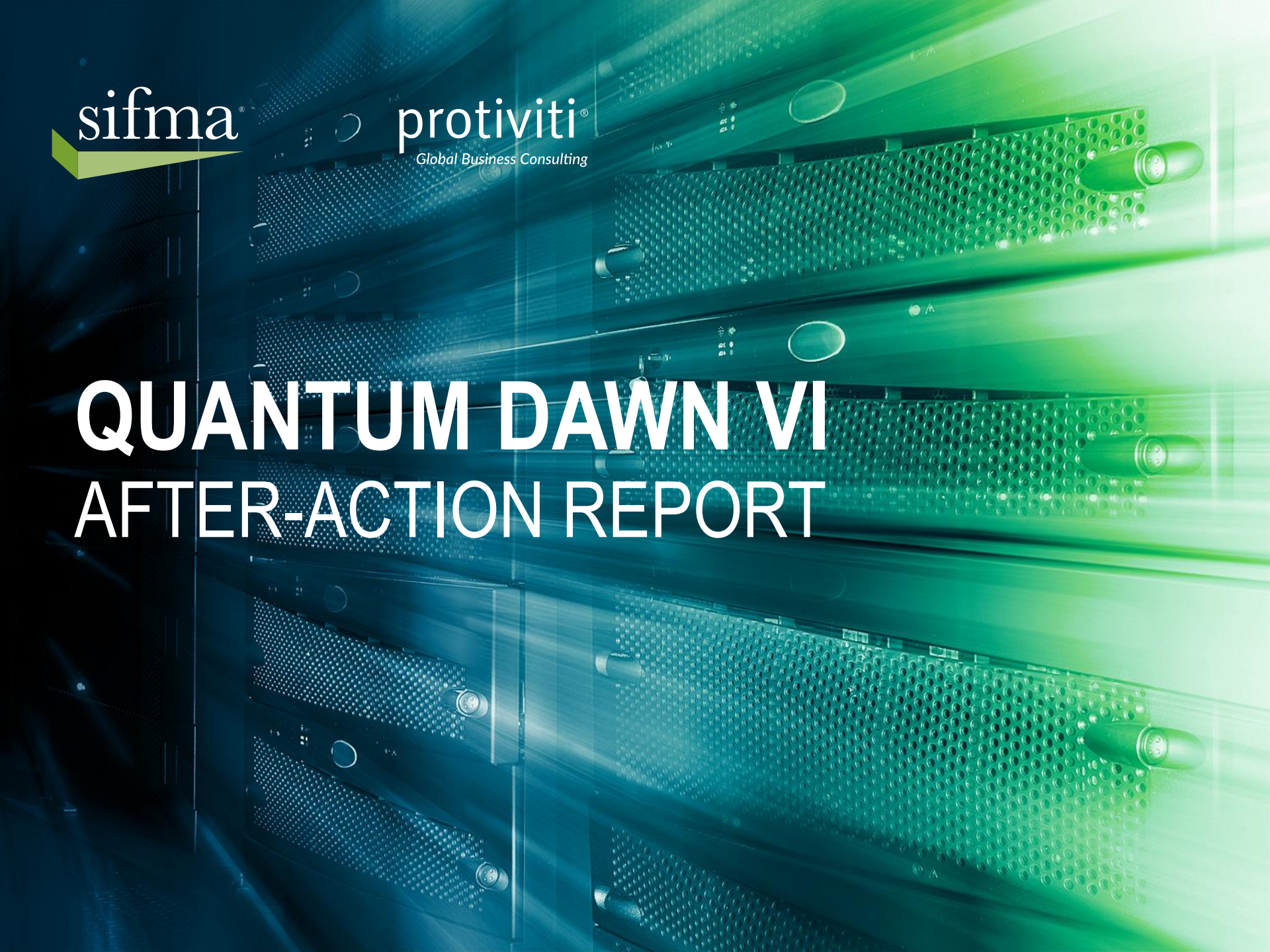
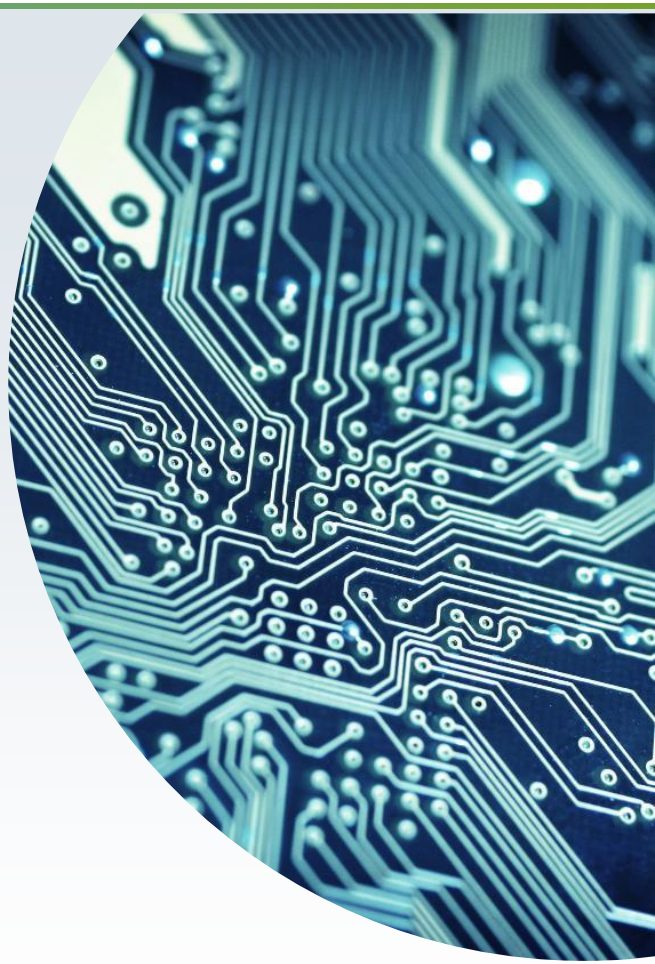

sifma
protiviti
Global Business Consulting
QUANTUM DAWN VI
AFTER-ACTION REPORT

TABLE OF CONTENTS



A DECADE OF TESTING AND RESILIENCE

Over the past 10 years, the Securities Industry and Financial Markets Association (SIFMA) has coordinated a series of industrywide resilience exercises known as Quantum Dawn. These exercises provide a forum for financial firms, regulatory bodies, central banks, law enforcement, government agencies, trade associations and information-sharing organizations to respond to simulated cyber and/or physical attacks.

QDI
2011
November

Quantum Dawn I & II

QDII
2013
July

In November 2011 and July 2013, the financial services sector, in conjunction with service provider Norwich University Applied Research Institutes (NUARI), organized two marketwide cybersecurity exercises called Quantum Dawn I and Quantum Dawn II, respectively. Those events provided a forum for participants to exercise risk practices due to a disruption in equity trading and clearing processes in response to a systemic attack on market infrastructure.

QDIII
2015
September

Quantum Dawn III

Whereas Quantum Dawn II focused on decision making for closing the equity markets, Quantum Dawn III, held in 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 on 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.

QDIV
2017
October

Quantum Dawn IV

In November 2017, SIFMA introduced the concept of integrating cyber range capabilities into industry exercises and engaged the SimSpace Corporation's Cyber Range software for the simulation. Day 1 of Quantum Dawn IV provided a real-life "hands-on-keyboard" experience for participating institutions to test their technical cyber response capabilities, while Day 2 involved participants engaging in a sectorwide simulation to test their crisis response, communication, and coordination capabilities around a large-scale targeted cyberattack against numerous financial institutions and news organizations.

QDV
2019
November

Quantum Dawn V

SIFMA's first global cyber exercise, held in November 2019, 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 sectorwide global cyberattacks. The exercise helped identify the roles and responsibilities of key participants in managing global crises with cross-border impacts and began development of its Global Directory of key crisis management contacts across the public and private sectors.

QUANTUM DAWN VI: EXECUTIVE SUMMARY

On November 18, 2021, more than 1,000 participants from both the public and private sectors, representing over 240 financial institutions across 20 countries, participated in SIFMA's global Quantum Dawn VI exercise. The industrywide exercise simulated a large-scale ransomware attack by a state actor against several major global financial institutions and regulatory bodies.

The scenario began with a state actor successfully infiltrating a major global bank's custody servicing infrastructure, causing a suspension of the trading system used to process incoming messages from clients around the globe. The attackers made a triple-extortion[1] ransom demand for $100 million worth of Bitcoin within 24 hours.

Participants confronted the potential for a systemic event that could cause a widespread liquidity crisis and global financial instability. They grappled with crucial questions like the following:

- What key decisions should be made during a ransomware attack?
- Who are your initial points of contact internally and externally once an attack is confirmed?
- What communication lines can be leveraged to help firms coordinate responses in the heat of the moment?

The focus on ransomware in this exercise underscores the increased frequency of this type of cyberattack, the growing sophistication of the attackers, and severity of risk to financial institutions, governments, global markets and technology infrastructure. According to a study published last year, ransomware attacks increased at a rate of 41% during the first six months of 2021 and 93% over the 12-month period ending June 2021.[2]

Overall, the exercise provided an opportunity for financial firms to assess their existing response playbooks, identify leading strategies and processes, and examine internal and external communications plans for responding to a ransomware attack. The latest learnings on coordinating a response at a country, regional and global levels were shared, along with communication channels and strategies to liaise with relevant stakeholders, including the media.

1. *The New Ransomware Threat: Triple Extortion*, Check Point.
2. "*The Vexing Tech Challenge of Fighting Ransomware: A Battle of Milliseconds*," Bloomberg, June 17, 2021.

QUANTUM DAWN VI: OBJECTIVES

The intent of the exercise was to assess public and private sector-wide communications and information-sharing mechanisms, crisis management protocols, and decision-making, as well as legal and regulatory considerations as exercise participants responded to and recovered from significant ransomware attacks targeting the financial sector. The scenario emphasized global cross-jurisdiction information sharing among financial firms, central banks, regulatory authorities, trade associations and information-sharing organizations.

SIFMA gathered information from participants in real time and post-exercise and worked with global consulting firm Protiviti to analyze the data. The results of the survey,[3] summarized in the key findings below, provide significant insight into the industry's capabilities for handling major disruptions.

The following key objectives were achieved:

Incorporated after actions and lessons learned from Quantum Dawn V, as well as recent disruptions including the SolarWinds and other breaches, third-party outages, and ransomware attacks.

Assessed the industry's ability to respond to and recover from a ransomware attack affecting financial firms and the sector at large.

Exercised the interaction and information-sharing amongst Global Directory members with a focus on managing global ransomware attacks and potential impacts to the sector and financial markets.

Provided a forum for financial firms to challenge internal incident response playbooks and share best practices for managing a ransomware attack.

3. Survey respondents included representatives from both public and private institutions, as well as organizations that are considered noncritical.

QUANTUM DAWN VI: KEY FINDINGS (1/5)

I. Ransomware recovery plans are common

Approximately 93% of financial institutions that participated in the recent Quantum Dawn exercise have developed ransomware recovery plans or integrated ransomware incident response procedures into existing crisis or cyber incident response plans.

Typically, the plans cover data recovery and internal and external communications with clients, law enforcement, government resources, legal and compliance teams, regulatory authorities, trade associations, and information-sharing bodies.

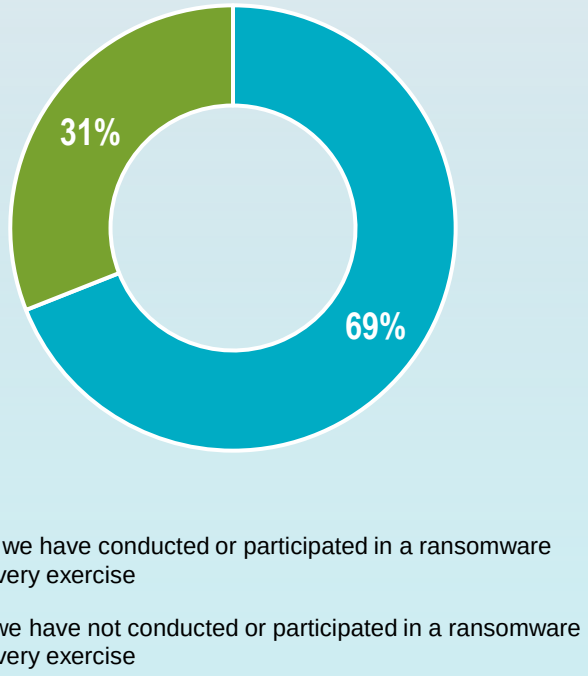
Does your organization have a ransomware recovery plan?

QUANTUM DAWN VI: KEY FINDINGS (2/5)

II. Have you conducted or participated in a ransomware recovery exercise?

Prior to Quantum Dawn VI, nearly 70% of participating financial firms indicated that they have exercised their ransomware recovery plans. The event provided an additional opportunity for participants to exercise their plans and gain a deeper understanding of ransomware recovery time frames and processes.

Have you conducted or participated in a ransomware recovery exercise?



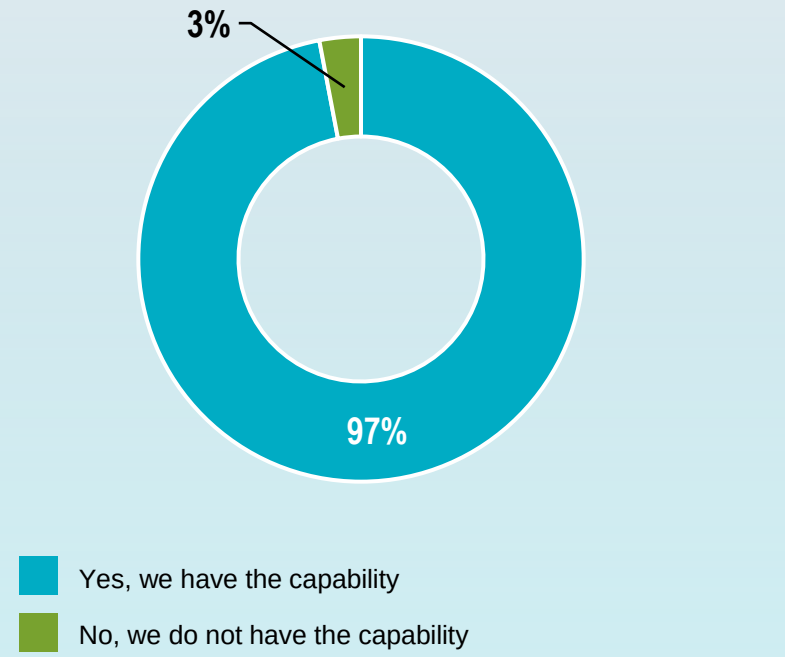
QUANTUM DAWN VI: KEY FINDINGS (3/5)

III. Many firms have critical data recovery capabilities

Firms should continue to protect critical data through replication and backup, as well as prioritize testing strategies that allow for adherence to established recovery objectives (i.e., recovery time and recovery point objectives).

Approximately 97% of respondents reported that their firms have the capability today to recover critical data within their recovery time and recovery point objectives under normal circumstances.

Do you have the capability to recover critical data within your recovery time and recovery point objectives?



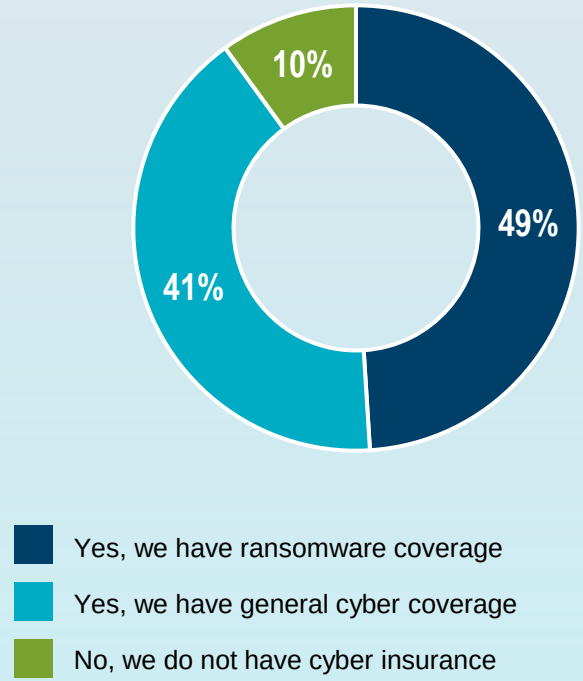
QUANTUM DAWN VI: KEY FINDINGS (4/5)

IV. Ransomware and general cyber insurance are widespread

As shown in the graphic, 90% of firms have a form of cyber insurance -- 49% have ransomware cyber insurance, while another 41% have general cyber insurance that would cover business interruptions.

While cyber insurance does not protect firms completely in all instances, it is a risk transfer strategy that could be implemented and maintained over time.

Does your organization have cyber insurance?

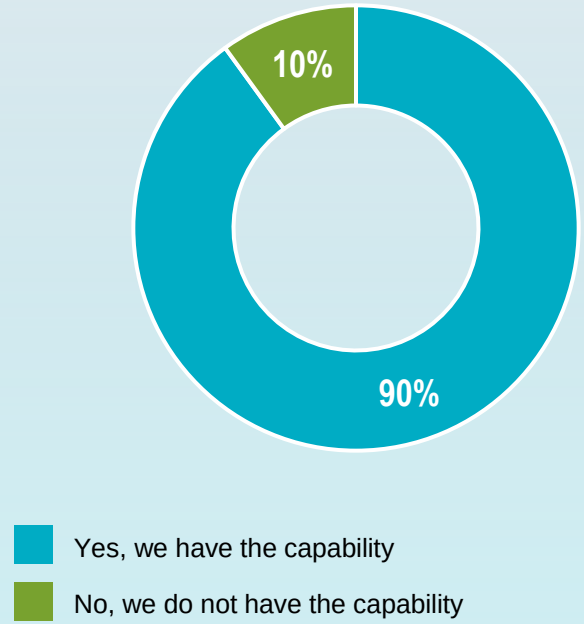


QUANTUM DAWN VI: KEY FINDINGS (5/5)

V. Bare-metal restore capabilities

Although responses varied by type of institution, many respondents (90%) indicated that their organizations have the capability to bare-metal restore critical business functions in the event of a cyberattack.

Do you have the capability to bare-metal restore your critical business functions?



QUANTUM DAWN VI: RECOMMENDATIONS (1/2)

An active defense — including assessment exercises, threat hunting and tabletop exercises —can improve any organization's ability to quickly detect and react to evolving cyber threats. The following recommendations are based on the lessons learned from Quantum Dawn VI.

I. Make critical investments in capabilities

Institutions should continue to invest in robust ransomware recovery and cyber, business continuity and information technology incident response plans and strengthen these plans based on frequent exercises and tests.

II. Create an alternate communication channel for worst-case scenarios

In the event a regulatory authority is impacted by a ransomware event and goes offline, firms should have processes in place to use alternate communications channels.

III. Beware: Ransom payments may not lead to data recovery

SIFMA does not recommend paying a ransom. Executives need to carefully consider the realities of taking such actions, including the possibility that they still may not recover compromised data.

QUANTUM DAWN VI: RECOMMENDATIONS (2/2)

Resources:

- **Action Fraud (UK):** RansomAware
- **Department of Homeland Security:** StopRansomware.gov
- **FBI:** Internet Crime Complaint Center (IC3)
- **FS-ISAC:** Tips to Defend Against Ransomware
- **NIST:** Ransomware Risk Management

IV. Join global directory of critical stakeholders

Financial firms are strongly encouraged to join SIFMA's Global Directory of critical stakeholders. This directory was created to identify critical public and private sector organizations and key contacts that play a role in crisis management and global information sharing.

V. Follow best practices

- Validate that critical infrastructure assets are not exposed to the public internet.
- Institute self-service password management controls requiring a second factor to avoid being socially engineered.
- Require multifactor authentication (MFA) everywhere.
- Deploy modern-day Identity Governance and Administration (IGA) systems to detect backdoor accounts.
- Use a privileged account management (PAM) system to check in-and-out access to accounts or deploy even more advanced defenses for critical admin-level accounts.
- Isolate and disconnect infected machines immediately.
- Develop threat hunting capabilities to proactively search for potential security incidents within the IT environment.

CONCLUSION AND ACKNOWLEDGEMENTS

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. Firms should continually test their crisis management, incident response and data recovery plans to ensure rapid response and recovery from ransomware or other types of cyberattacks.

Visit sifma.org to learn about SIFMA's Quantum Dawn exercises, its annual industry business continuity tests and ongoing efforts to improve the industry's cyber and operational resilience.

SIFMA would like to acknowledge the hundreds of organizations and individuals who helped design and execute the Quantum Dawn VI exercise. Special thanks to global consulting firm Protiviti for helping to analyze participant feedback and prepare this after-action report.

Finally, SIFMA would like to thank all the participants who engaged in the exercise and provided valuable insights, ensuring its success.

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

sifma.org

Protiviti

Kim Bozzella
Managing Director
Global Leader of Technology Consulting
Protiviti
+1.212.603.5429
kim.bozzella@protiviti.com

Andrew Retrum
Managing Director
Technology Consulting
Security and Privacy
Protiviti
+1.312.476.6353
andrew.retrum@protiviti.com

Douglas Wilbert
Managing Director
Risk & Compliance
Protiviti
+1.212.708.6399
douglas.wilbert@protiviti.com

protiviti.com

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. 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 SIFMA.org.

sifma®

Protiviti (protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Through our network of more than 85 offices in over 25 countries, Protiviti and its independent and locally owned Member Firms provide clients with consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®