FIA TASKFORCE ON CYBER RISK

After Action Report and Findings

September 2023

TABLE OF CONTENTS

About FIA

FIA is the leading global trade organization for the futures, options and centrally cleared derivatives markets, with offices in Brussels, London, Singapore and Washington, D.C.

FIA's mission is to:

- *support open, transparent and competitive markets,*
- *protect and enhance the integrity of the financial system, and*
- *promote high standards of professional conduct.*

As the leading global trade association for the futures, options and centrally cleared derivatives markets, FIA represents all sectors of the industry, including clearing firms, exchanges, clearing houses, trading firms and commodities specialists from about 50 countries, as well as technology vendors, law firms, and other industry service providers.

© FIA, SEPTEMBER 2023

Introduction

In March 2023, FIA created a Cyber Risk Taskforce to recommend ways to improve the ability of the exchange-traded and cleared derivatives industry to withstand the disruptive impacts of a cyberattack. This Taskforce consisted of subject matter experts and business leaders of the exchange-traded and cleared derivatives industry, including members from exchanges, clearinghouses, clearing firms, vendors, and end users.

This decision to form a Taskforce was taken in response to a significant disruption one month earlier in the processing of trades executed on multiple exchanges around the world. This outage was triggered by a ransomware attack on a single third-party service provider used by many clearing brokers globally.

Although cyberattacks in the financial services sector are far from new, this attack was notable for the scale and severity of the impact. The attack demonstrated that an outage at a single service provider can have damaging effects across a wide range of firms and threaten the orderly functioning of markets.

The attack also demonstrated in vivid detail the complexities of restoring normal service. For some firms impacted by the disruption of services, it took as long as two weeks of intensive work to gather and process missing trade records and to reconnect systems to the rest of the marketplace.

Ransomware attacks work by taking control over a company's systems and preventing the company from operating those systems until a ransom is paid. When a service provider is the target, a ransomware attack disrupts the operations of companies that rely on that service provider. For this reason, this type of attack can be particularly disruptive in highly interconnected sectors, such as the exchange-traded derivatives markets.[1]

That makes it all the more important to focus on resilience. For this reason, the Taskforce worked from the presumption that future attacks will succeed, focusing on steps to improve the recovery process.

It is important to note that the Taskforce did not conduct its work in a vacuum. Many market participants already have well-developed policies for cybersecurity, third-party risk management and resiliency, and prudential and market regulators have requirements in place for addressing cyber risks. In addition, financial market infrastructures such as exchanges and clearinghouses, and regulated financial entities such as banks and brokers, are forward looking in their response and recovery strategies and already comply with many regulatory requirements related to information, technology and operational risks.

© FIA, SEPTEMBER 2023

It is also important to note that the issue of resilience is far from new for firms in the exchange-traded and cleared derivatives markets. Over many decades these markets have demonstrated a very high level of operational resilience with respect to other types of outages, such as those caused by terrorist attacks, extreme weather, pandemics, power outages, and disruptions to communication networks.

This report therefore focuses on the operational resilience issues raised by the ransomware attack that took place earlier this year. In particular, the report focuses on steps that firms in the exchange-traded and cleared derivatives industry can take to improve their ability to respond to future attacks as well as opportunities to increase coordination and information sharing in all aspects of operational resilience.

Summary of Findings

First, communication is key in a crisis. The exchange-traded and cleared derivatives industry needs well-established and secure channels to share information and coordinate responses during and after a cyber incident. This need is also evident in other types of incidents that cause industry-wide disruptions. The Taskforce therefore recommends that FIA should create an "Industry Resilience Committee" to encourage the development of such channels with respect to all forms of operational resilience, including but not limited to cyber resilience.

Second, the Taskforce highlights the importance of connecting the exchange-traded and cleared derivatives industry with sector-wide groups that specialize in operational resilience across the financial services sector. During cyber incidents, these groups serve as trusted forums for the sharing of information. They also meet regularly to share threat intelligence and promote preparedness, and they partner with the public sector to enhance cybersecurity and resilience of the financial sector as a whole.

Third, the Taskforce recommends that market participants should review their policies and procedures for reconnection to impacted parties during and after a cyber incident. The Taskforce recommends using existing guidance and frameworks developed for use in the financial services sector and considering how they apply to the exchange-traded and cleared derivatives industry.

Fourth, the Taskforce encourages service providers, market participants and market infrastructures to establish procedures for sharing critical data and other information with their counterparties and clients in a timely manner during a cyber incident. A clear understanding of those procedures ahead of an incident can streamline information-sharing during an incident and accelerate the recovery process.

© FIA, SEPTEMBER 2023

Fifth, the Taskforce recommends that the industry should identify ways to make the assessment of risks to operational resilience more efficient. It is already common practice for firms to question their third-party service providers about their cyber protections. Greater standardization in these questionnaires would make the process more efficient.

Sixth, the Taskforce believes that the exchange-traded and cleared derivatives industry should participate in regular cyber preparedness exercises. This includes both direct participation by key stakeholders, such as clearing brokers and market infrastructures, and indirect participation through FIA. The Taskforce recognizes that it would be most effective to leverage existing programs for these types of exercises, rather than create a new program.

Background: A Timeline of the Attack

On Tuesday, January 31, during the early morning hours of the London trading day, FIA became aware of an outage at ION Markets impacting the trading and clearing of exchange-traded derivatives. FIA immediately began working with members to identify the scope of the outage and assess the potential impact on markets.

ION is a third-party software service provider that offers front-, middle- and back-office products to a number of clearing firms that are active in futures markets in Europe, Asia-Pacific and the Americas. Those services are embedded in the execution and clearing workflow at these firms, and any disruption makes it difficult for firms to process their trades in a timely and efficient way.

As the day progressed, it became clear that this outage was not insignificant. To provide its members with updates on the situation, FIA held four conference calls that first day, including an evening call with members in the Asia-Pacific region – many of whom were just waking up to news about the outage. FIA also notified several market regulators, including the Commodity Futures Trading Commission in the US, the Bank of England in the UK, the Bundesanstalt für Finanzdienstleistungsaufsicht in Germany, the Autorité des Marchés Financiers in France, and the Finansinspektionen in Sweden.

ION confirmed the attack via a press release on January 31 and the following day it revealed via a broadcast communication that LockBit, a type of ransomware, has been used.

In 2022, LockBit was the most deployed ransomware variant across the world, according to the Cybersecurity and Infrastructure Security Agency, a branch of the US government. The organization that developed the LockBit software functions

© FIA, SEPTEMBER 2023

on a "Ransomware-as-a-Service" model where affiliates are recruited to conduct ransomware attacks using LockBit ransomware tools and infrastructure.[2]

Shortly after the attack, ION began providing updates with its clients and qualified contacts via regular daily calls and a dedicated mailbox. At the industry-wide level, FIA continued holding regular calls to coordinate with the association's global membership. By the week's end, the FIA calls included more than 700 individuals from clearing firms, exchanges, clearinghouses, service providers and regulators. These calls were critical for the sharing of important information among market participants to keep the markets open and functioning. The calls also served to identify regulatory and reporting challenges.

On Monday, February 6, the industry began the reconnection phase of the incident. To assist firms, FIA shared industry protocols and best practices for reconnecting systems, such as the guidance developed by the Financial Services Sector Coordinating Council (FSSCC) in coordination with the US Treasury Department as well as guidance developed by the Cross Market Operational Resilience Group in the UK.

Even after ION completed its recovery, impacted firms needed several days to finish their internal recovery processes and reconnect with market infrastructures. One obstacle was the time needed to gather and process trade records that were not captured during the outage. Another obstacle was the time needed to complete attestations. Due to the disparate internal requirements of each affected firm, there was no single form of attestation that was acceptable, and navigating the disparate requirements added delay. Obtaining these attestations is one of the critical steps in the reconnection process.

The disruptions to trade processing at impacted firms also had a ripple effect on regulatory reporting. During the first week of the incident, the Commodity Futures Trading Commission, the primary regulator of derivatives in the US, announced that its widely used Commitment of Traders report would be delayed. The CFTC was not able to resume publishing this report until February 24, more than three weeks after the incident began.

© FIA, SEPTEMBER 2023

Regulatory Landscape

As mentioned above, financial market infrastructures and other regulated financial entities are subject to an array of regulatory requirements that relate to cyber risk and operational resilience. In several leading jurisdictions, market regulators and prudential regulators are moving to update these requirements.[3]

United States

- The Securities and Exchange Commission recently adopted new requirements regarding the disclosure of cyber incidents.
- The Commodity Futures Trading Commission is preparing to propose rules related to cyber resilience.
- The three federal banking regulators—the Federal Reserve, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation—jointly issued final guidance in June 2023 on how to manage risks associated with third-party relationships.

European Union

- EU policymakers enacted the Digital Operational Resilience Act in November 2022, which establishes technical standards that financial entities and their critical third-party technology service providers must implement in their information and communication technology systems by January 2025.
- The European Systemic Risk Board recently published a report on "advancing macroprudential tools for cyber resilience."

United Kingdom

- The UK Financial Conduct Authority set out final rules and guidance on new requirements to strengthen operational resilience in the financial services sector in March 2022.
- The Bank of England, the Prudential Regulation Authority and the Financial Conduct Authority jointly published a discussion paper in July 2022 that sets out potential measures to oversee and strengthen the resilience of services provided by critical third parties to the UK financial sector. A further consultation is expected later in 2023.

© FIA, SEPTEMBER 2023

APAC

Australia

- In July 2023, the Australian Prudential Regulatory Authority completed its new prudential standard CPS 230 which focuses on enhancing operational risk management for banks, insurers, and super funds. The new standard will commence from 1 July 2025.

Hong Kong

- In 2022, the Hong Kong Monetary Authority issued Regtech Guide on Third-Party Risk Management to help banks implement regtech solutions to address the risks associated with third-party relationships.
- In 2022, HKMA issued Supervisory Policy Manuals OR-1 on Operational Risk Management (Jul 2022) and OR-2 on Operational Resilience (May 2022).

Japan

- In April 2023, the Japan Financial Services Agency issued a Discussion Paper on Ensuring Operational Resilience to set out a basic framework for ensuring operational resilience with reference to international trends.
- In February 2022, JFSA published its "Policy Approaches for Enhancing Cybersecurity in the Financial Sector (Version 3.0)" (only in Japanese) to address new issues and challenges in ensuring cybersecurity posed by growing cyber threats, such as increasing cyberattacks including sophisticated ransomware attacks and other threats in cyberspace.

Singapore

- The Monetary Authority of Singapore has various guidelines on third-party risk management and business continuity management. They include Technology Risk Management Guidelines, Guidelines on Outsourcing, and Business Continuity Management Guidelines. The TRMG is the primary set of cybersecurity regulations covering financial institutions in Singapore.

International Standard-Setting Bodies

- The Financial Stability Board recently issued a consultation on a "toolkit" for enhancing third-party risk management and oversight.
- In November 2022, the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions issued a joint report on the "cyber resilience" of financial market infrastructures.

© FIA, SEPTEMBER 2023

In this paper, the Taskforce is not making any recommendations or comments related to specific regulatory proposals or existing requirements. Instead, the paper offers some general observations that may shape industry response to such consultations.

First, the Taskforce encourages regulators and legislators to take a principles-based approach to cyber risk and operational resilience. That approach may not be sufficient in all areas, but such a flexible approach is well suited to a threat landscape that is likely to continue evolving at a rapid rate. Unlike other areas of operational risk, cyber risk stems from the activities of malicious actors who are constantly probing for weaknesses and refining their tools. This threat requires regulators to exercise a high degree of nimbleness and adaptability.

Second, it is important to note that many entities in the exchange-traded and cleared derivatives markets are subject to overlapping layers of regulation. This is especially true for intermediaries, such as banks and brokers, that provide services to customers across asset classes, including futures, options or swaps. Any regulatory proposal must recognize existing global regulatory requirements in its design of policy objectives.

Third, in large and complex organizations, cyber risk is managed at an enterprise level. It is therefore important to avoid conflicts between rules that apply to one business unit within such an organization and rules that apply to the organization as a whole. Such conflicts could make it more difficult for organizations to comply with the rules and could delay an organization's response to a cyber incident.

Lessons Learned

One of the most important lessons learned was the need for communication during a crisis. ION provided frequent updates to impacted clients via daily calls and a dedicated mailbox, and at the industry level FIA was able to centralize information, dispel rumors and urge calm, and share practical advice and experience.

It is also important to recognize the crucial role of market infrastructures in the recovery process. Exchanges and clearinghouses from around the globe, from Australia to North America, deserve a lot of credit for their response to this incident. They showed flexibility in extending their deadlines, helping firms recover data, keeping clearing windows open, and maintaining confidence that the markets would continue to function.

Regulators also showed flexibility during this outage, providing relief to market participants on certain regulatory filings and compliance obligations. Industry and

© FIA, SEPTEMBER 2023

regulators shared information throughout the process to protect the integrity and operations of markets and expedite recovery processes.

That said, the incident demonstrated that the industry can improve the response and recovery process. There was no centralized secure platform for communication in place to allow vetted firms in the exchange-traded and cleared derivatives industry to share information. Several firms were forced to rely on painstaking manual reconstruction of trading records that took many days to complete. In some cases, reconstructed data was incomplete or inconsistent, making the resumption of normal operations challenging.

The incident also demonstrated that a critical component of managing cyber and other third-party risks involves having robust, regulatory compliant and up-to-date contractual provisions that address a variety of resilience scenarios to mitigate exposure for firms. In the aftermath of the incident, many clearing firms commenced a review of the contractual terms that they have in place with third-party service providers and customers.

Since its formation in May, the Taskforce has discussed the problems observed during this cyber incident and various ways to make the reconnection and recovery processes faster and more efficient. The Taskforce has developed several recommendations for market participants.

Findings and Recommendations

With this background, the Taskforce makes the following findings and recommendations:

1. **Form an "Industry Resilience Committee" as a standing industry-wide group.**
    - The Taskforce agrees that the industry must have a trusted forum for key stakeholders to discuss cyber incident management and resilience planning and recommend best practices for the industry, within the bounds of relevant sensitive information sharing protocols, data protection and anti-trust regulations.
    - The Taskforce therefore recommends that FIA should form an "Industry Resilience Committee" (IRC or Committee) to serve this function. Although the recent incident involved a cyberattack, the issues it highlighted are broader. The Taskforce therefore recommends that this group should focus on all forms of operational resilience, including but not limited to cyber resilience.

© FIA, SEPTEMBER 2023

- With respect to cyber resilience, this Committee should have two sets of functions: one set during business-as-usual (BAU) periods when there is no ongoing cyber incident, and one set when there is an urgent need to respond to an ongoing cyber incident.
- During BAU, the IRC should focus on leading the industry's operational resilience preparedness, including but not limited to cyber resilience. This includes engaging with other organizations, building greater awareness of standards and guidance, and supporting efforts to rehearse responses to cyber incidents. This also includes planning periodic "roundtable" discussions on topics related to cyber resilience.
- During a market disruption event when a cyber incident is causing a market-wide outage in key services or functions, this Committee should function as a "trusted group" for sharing information and coordinating responses. By meeting on a regular basis during periods when there is no crisis, the Committee members will develop strong relationships across the industry that will allow for quick and effective action during a cyber incident.
- When dealing with the disruptive impacts of a cyber incident, the IRC should focus on addressing the "Three R's: **Response** - coping with the immediate impact of a breach; **Recovery** - rebuilding and restoring systems and databases; and **Reconnection** - reconnecting to market infrastructures, service providers and other organizations.
- While cybersecurity issues are often at the heart of major outages or disruptions to the financial sector, the response is often led by the executives who oversee business operations and technology infrastructure rather than cybersecurity experts. The Committee therefore should meet regularly and consist of a cross-section of subject matter experts from around the globe, including experts in information security, technology, and operations as well as business heads and lawyers.

2. **Engage with sector-wide groups on cyber and operational resilience through FIA.**
   - The Taskforce highlights the importance of connecting the exchange-traded and cleared derivatives industry with groups that specialize in operational resilience across the financial services sector.
   - During cyber incidents these groups serve as trusted forums for the sharing of information. They also meet regularly to share threat intelligence and

© FIA, SEPTEMBER 2023

promote preparedness, and they partner with the public sector to enhance cybersecurity and resilience of the financial sector as a whole.

- Examples of these type of groups include the Financial Services Sector Coordinating Council (FSSCC)[4], the Financial Services Information Sharing and Analysis Center (FS-ISAC)[5] the Cross Market Operational Resilience Group (CMORG), and the Securities Industry and Financial Markets Association (SIFMA).

3. **Encourage alignment with reconnection guidelines developed by leading US and UK groups.**
   - Several financial sector groups have developed guidance, frameworks and tools to guide firms through the process of reconnecting to impacted firms in the aftermath of a cyber incident. These include the CMORG in the UK and the FSSCC in the US.
   - A review and adoption of these reconnection guidelines could help facilitate a more efficient recovery process for the exchange-traded and clearing derivatives industry. These guidelines should be promoted and practiced through the Industry Resilience Committee and other industry forums.
   - In this context, the Committee could take a leading role in examining whether existing reconnection guidelines fully account for the differences between trading and clearing and whether those differences impact the reconnection process.
   - FIA should work with other groups in the financial sector to ensure that the guidelines are aligned with the specific characteristics of the exchange-traded and cleared derivatives industry.

4. **Support the sharing of information with connected parties regarding contingency plans in the event of a cyber incident or other type of outage.**
   - To optimize the success and timeliness of a market recovery after an incident, market participants need to have an ex-ante understanding of the reconnection contingency plans of various market participants, market infrastructures, and third-party service providers.
   - The Taskforce encourages service providers, market participants and market infrastructures to establish procedures for sharing critical data and other information with their counterparties and clients in a timely manner during a cyber incident.

© FIA, SEPTEMBER 2023

- Equally important, the Taskforce encourages service providers, market participants and market infrastructures to provide their clients and counterparties with visibility into those procedures. Having a clear understanding of those procedures ahead of an incident can streamline information-sharing during an incident and accelerate the recovery process.
- In particular, exchanges and central counterparties play a critical role in the front-to-back trading and clearing ecosystem. In any outage that affects post-trade processing, reconnection to exchanges and CCPs is an essential step in the recovery process.
- Cyber incidents can force impacted firms to reconstruct part or all of their databases. Much of the data in these databases consists of trade records provided by exchanges and CCPs. Access to those records is therefore critical to the database restoration process.
- Recent experience has shown the value of an ex-ante understanding of how exchanges and CCPs will make data available during a recovery from an outage. This includes an understanding of policies, procedures and data formatting and templates.
- It is recognized that each exchange or CCP may take a different approach to making data available to its members during the recovery and reconnection phases. Equally important, each clearing member may have different data needs from other clearing members.
- The Taskforce believes the recovery and reconnection phases can be completed much more quickly and efficiently if clearing members and CCPs discuss in advance how data will be made available and in what format.
- The Taskforce recommends the Industry Resilience Committee should work with market participants on developing guidelines for all participants, including but not limited to exchanges and CCPs, to provide such information to their members, customers or counterparties in a secure, timely and accurate manner.[6]

5. Improve risk assessment of third-party service providers.

- Many participants in the global exchange-traded and cleared derivatives markets rely on third parties for services essential to their participation in the markets. These services include market data, trade processing, reconciliation, collateral management, and risk calculations.

© FIA, SEPTEMBER 2023

- The reliance on third-party service providers creates an exposure to cyber risk, in the sense that a cyber incident at a service provider can disrupt functions that are critical to operating the business.
- While some jurisdictions such as the European Union have already introduced or proposed comprehensive regimes for a sound management of information and communication technology third-party risk, it is important that firms in all jurisdictions establish a risk management policy that covers third-party service providers, especially critical third parties. Rather than one universal set of risk management practices that applies to all service providers equally, the policy should allow the risk management practices to be calibrated to such factors as the type of service that is provided, the nature of the relationship, and the potential impact of a disruption to that service.
- This should include a plan for managing the risks in these relationships, a process for conducting due diligence, and a plan for ongoing oversight and monitoring. This also should include a plan for dealing with cyber incidents that affect service providers.
- The Taskforce recommends that the industry should identify ways to make the risk assessment process more efficient. It is already common practice for firms to probe their third-party service providers about their cyber risk management policies. Greater standardization in these questionnaires would make the process more efficient.
- The Taskforce also recommends that firms should review the contractual terms that they have in place with third-party service providers and customers to ensure that they address a variety of resilience scenarios.

6. Participate in regular cyber preparedness exercises.

- Resilience planning must be practiced to be effective. While playbooks are helpful, they must be exercised to discover unintended consequences, uncover real-life limitations, and identify evolving threats.
- The financial services industry already conducts several cyber risk exercises yearly. However, these exercises tend to focus on the broader financial services industry, rather than the exchange-traded and cleared derivatives industry.
- Such exercises are time-consuming. The Taskforce therefore recommends that the exchange-traded and cleared derivatives industry should

© FIA, SEPTEMBER 2023

participate in existing cyber exercises, rather than creating a new exercise. The Taskforce recommends asking the organizers of these exercises to incorporate exchange-traded and cleared derivatives scenarios and situations. This would allow the industry to practice its responses to such outages without creating a significant new burden on operational risk professionals.

- These exercises include the Hamilton Exercise organized by the US Treasury Department and the Quantum Dawn exercise organized by the Securities Industry and Financial Markets Association. The Taskforce recommends that both exercises should incorporate scenarios related to the exchange-traded and cleared derivatives markets.
- The Taskforce also believes that the Industry Resilience Committee can play an important role in this context. As mentioned above in recommendation one, this includes planning periodic "roundtable" discussions on topics related to cyber resilience. This also could include addressing any lessons learned from the exercises described above.

© FIA, SEPTEMBER 2023

Conclusion

The recent cyber incident presents a meaningful opportunity to improve the operational resiliency of the exchange-traded and cleared derivatives industry. It disrupted operations across the industry and the recovery and reconnection phases took much longer than expected.

It is now clear that the industry must presume that the risk of another cyber incident is not an "if" but a "when". The Taskforce believes that the recommendations outlined above will help the industry prepare. The formation of an Industry Resilience Committee will be particularly important in carrying these recommendations forward.

The recent cyber incident also showed that FIA itself has an important role in industry communications. This includes not only functioning as an "information clearinghouse" during an incident but also encouraging preparedness across the industry. This role also could include the development of guidelines or the organization of periodic exercises to test preparedness.

Over many decades, the exchange-traded and cleared derivatives industry has developed a comprehensive playbook for dealing with the consequences of a default. Defaults do not happen very often, but when they do, the risk of financial loss is high. For this reason, a wide range of protections are in place to protect customers and markets, and clearinghouses and clearing members constantly test their risk management processes to make sure that any potential losses can be absorbed. In sum, defaults are rare, but default management is normal.

It is now the challenge for the industry to make cyber risk management just as routine as default management. For many firms, it already is. Whether because of regulatory requirements or their own commitment to operational excellence, they have made cyber risk management a routine part of their contingency planning. But even for these organizations, it is essential to practice those procedures and evolve them over time. And as the recent cyber incident showed, even the most highly protected organizations can be exposed to the risk of disruption by a cyber incident at a third-party service provider.

© FIA, SEPTEMBER 2023

Endnotes

1 According to the US Treasury Department, financial institutions in the US suffered $1.2 billion in losses from ransomware attacks in 2021, three times the amount in the previous year, and the frequency and sophistication of these attacks continue to increase.

2 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

3 There are also several organizations that issue guidelines and coordinate work in this area across the private sector. These organizations include the Cross Market Operational Resilience Group in the UK and the Financial Services Information Sharing and Analysis Center as well as trade associations such as the Securities Industry and Financial Markets Association in the US and the Investment Association in the UK.

4 https://fsscc.org/about-fsscc/

5 https://www.fsisac.com/who-we-are

6 Subject to contractual terms between the parties and in compliance with personal data and anti-trust laws

BRUSSELS
Office 502
Square de Meeûs 37
1000 Brussels, Belgium
+32 2.791.7572

SINGAPORE
One Raffles Quay North Tower
Level 49
Singapore 048583
Tel +65 6622.5781

LONDON
Level 28, One Canada Square
Canary Wharf
London E14 5AB
Tel +44 (0)20.7929.0081

WASHINGTON
2001 K Street, NW
Suite 725, North Tower
Washington, DC 20006
Tel +1 202.466.5460

FIA.org