FIA MARKET TECHNOLOGY

2018 Cyber and Operational Resilience Scenario Workshop

"Operation Blowback"

Summary Report

November 15, 2018

A. Executive Summary

- FIA Market Technology division moderated a cybersecurity and operational resilience workshop. The simulation provided a forum for participants to discuss their respective responses to a systemic market disruption.
- Representatives from major FCMs, exchanges, clearinghouses and key service providers attended. The workshop was attended by a cross-section of 40 industry participants, representing 12 FIA member organizations.
- The workshop presented a disruption scenario that takes place two years into the future (Q4 2020) when a fictitious back-office service provider has successfully migrated all its clearing firms to a new cloud-based back-office system, away from an on-premises technology model. The service provider supports nearly 50% of clearing firms. An operational oversight failure during scheduled system maintenance leads to a significant business disruption on Sunday evening during a period of heightened market volatility. Due to the interconnectivity of participants, clearing firms not using the service provider are also affected by their peers' inability to process trades.
- A breakout session was held with the participants divided into three working groups, each led by a moderator. The breakout groups were presented with questions on the impact of the disruption and its ramifications to their business, technology and operations. At the end of the breakout session, the moderators presented the groups' findings to the audience.
- The breakout sessions and subsequent discussion highlighted the following points:
  - Multiple industry participants would start working on the issue in isolation.
  - Workarounds for problems of this magnitude would not be easy, as clearing firms would not have the levels of staffing to manually process the trades in question.
  - If such an issue were to impact a large percentage of clearing firms, it is likely that firms would tend to reach out and try to help each other. Communication and coordination are key.
  - FIA can play a critical role providing a trusted conduit for emergency communication.
  - FIA should look at developing a futures-specific crisis team and playbook to respond to industry disruptions, and FIA should bring those tools to future workshops.
  - Future workshops should invite non-industry groups to share their experiences (e.g. FS-ISAC, [1] ChicagoFIRST,[2] etc.)

[1] Launched in 1999, FS-ISAC was established by the financial services sector in response to 1998's Presidential Directive 63. That directive - later updated by 2003's Homeland Security Presidential Directive 7 - mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure.

[2] ChicagoFIRST is a nonprofit association that provides critical firms a collaborative forum to address private sector resilience and emergency management planning and response with relevant local, regional, and national public sector agencies.

B. Introduction and Workshop Overview

On Oct. 16, 2018, the Futures Industry Association's Market Technology division moderated a cybersecurity and operational resilience workshop. The workshop was held at the Chicago Hilton hotel.

The simulation provided a forum for participants to discuss their respective responses to a systemic market disruption.

Representatives from major futures commission merchants (FCMs), exchanges, clearinghouses and key service providers attended.

The workshop was attended by a cross-section of 40 industry participants, representing disciplines from 12 FIA member organizations: Business Continuity Management, Clearing Operations, Compliance, Credit Risk, Information Technology, Service Providers and Trading Operations.

C. Scenario Summary

The workshop presented a disruption scenario that takes place two years into the future (Q4 2020) when a fictitious back-office service provider, Dunn-Rite Automated Clearing Systems, LLC ("DRACS") has successfully migrated all its FCM and clearing firms on to a new cloud-based back-office system, away from an on premises technology model.

After significant research and lengthy due diligence, DRACS has chosen one of the major cloud service providers to host their "Moneypenny" back-office system.

The cloud service provider Universal Exports Co. ("Universal") operates 38 state-of-the-art data centers globally. They now host the Moneypenny system for DRACS and its user firms.

Due to a major operational oversight during a regularly scheduled systems maintenance and upgrade process, a significant business disruption is created that impacted the users of the Moneypenny system.

The system upgrade occurred on a Saturday afternoon, and the disruption started to be noticed shortly after the commencement of trading on global derivatives markets on Sunday evening.

Market participants and their clearing firms were impacted by the disruption and were not receiving executed trade messages via the Moneypenny back-office. A large backlog of trade messages began to build, impacting those firms and clients that traded during the disruption on Sunday evening.

Large volumes of M1 trade messages began to queue up at the clearinghouses that these firms and their customers traded with.

The background, storyline and the scenario were presented to the audience. The disruption began and evolved over two days.

A breakout session was then held, with the participants divided into three working groups, led by a moderator. The breakout groups were presented with questions on the impact of the disruption and its ramifications to their business, technology and operations.

At the conclusion of the breakout session, the moderators presented the groups' findings to the audience.

Discussions were held as to how participants would anticipate being notified of this type of event, what capabilities are in place to investigate what has been reported, and some of the actions they would take in response.

Problem escalation, industry notifications, media communications and recovery considerations were discussed for all market participants, including the exchanges directly impacted by the disruption, as well as those firms that did not use the DRACS Moneypenny system.

D. Scenario Recap

Day 1:

- A large, fictitious back-office systems provider ("DRACS") has migrated all its FCM and clearing firms to a cloud-based environment, hosted by Universal Export Co. ("Universal").
- The back-office system called Moneypenny resides across multiple system modes in the Universal cloud.
- As part of normal system maintenance, Universal performs system upgrades, and introduces new system nodes and retires certain older ones. The upgrades are performed on Saturdays, when no major derivatives markets are open.
- Universal reports back to DRACS on Saturday PM that all went as planned and that Moneypenny is ready for regular processing when Sunday trading commences.

Day 2:

- Over the same weekend, a major geo-political event occurs, when the Iranian Revolutionary Guard attacks oil tankers in the Straits of Hormuz.
- The result causes oil prices to spike when global derivatives markets open for trading on Sunday around 6:00 PM.
- The spike in trade volumes impacts Universal's systems and message loads.
- Under the increased volumes, the system launches more cloud environments of Moneypenny. The infrastructure starts to re-route to network nodes that were either not updated, or no longer exist. Messages are re-directed, triggering a spike in re-transmission requests.
- The outage adversely impacts the DRACS virtual servers and numerous web-based tools they use.
- As a result of the failed update, DRACS realizes that the Moneypenny routing tables have become corrupted.
- Proprietary trading firms' internal risk systems are not seeing offsetting (cross market) hedge transactions, and neither do their FCM firms.
- Service disruptions to user firms start to become wide spread. FCMs notify their clients about delays in back-office processes.
- By 9:00 PM on Sunday, there is a lot of finger pointing between the FCMs, DRACS and Universal. There is an apparent abdication of controls as a result of poorly documented contingency procedures.
- DRACS has a 2-hour service level objective with their FCM user firms for the recovery and continuance of *Moneypenny*. They have obligations to immediately notify their user firms if a significant disruption impacts their systems and operations.
- At 9:30 PM DRACS management invokes their BCP and declares the problem to be a significant business disruption.
- By now DRACS has hundreds of thousands of M1 trade messages backing up.
- Clearinghouses start to be concerned that multiple members cannot process trades. FCMs continue to notify their clients about delays in back-office processes.
- DRACS and Universal's staff currently estimate that it could take 12-18 hours to implement a fix, before restoration of the systems and data files can begin.
- DRACS fails over to their fully-redundant back-up systems. These are dynamically updated with the primary production systems data.
- In consultation with their CEO and key board members, DRACS management notifies their user firms, the exchanges and the CFTC.

- By 10:00 PM they announce publicly that *"…we have serious processing problems, and as a result, have invoked our BCP and commenced fail over to our back-up systems".* They start to address the reputation management with the media.
- The CFTC will be concerned about the implications of concentration risk and issues such as give ups, take ups and allocations across multiple participants.
- Major news outlets report that the Middle East shipping disruption begins to contribute to volatility across all energy markets.
- However, because of the DRACS problem, the markets are not as deep and wide as they should be.
- Up until now, there has not been any social media chatter about the DRACS/Universal problem.
- Universal's managed operations and support teams continue to work feverishly and methodically with DRACS to assess why some data is flowing correctly and why some isn't. It's the middle of the night, and various operational work-arounds are considered.

Day 3:

- By early Monday AM, the exchanges begin to schedule calls with DRACS and the major FCM and clearing firms.
- At this point, firms that use Moneypenny endeavor to contact their key clients to tell them that they have a serious processing problem and their trades are not being reported to the back-office.
- By Monday, DRACS has contacted the CFTC, the NFA and all its user firms and briefed them on the extent of the problems and potential timelines.
- FCM and clearing firm operations teams are overwhelmed by the magnitude of the problem.
- The process to pull the data directly from the exchanges or clearinghouses is very labor-intensive, and can only prove what the net positions were, not what is reflected real time.

E. Breakout Sessions and Feedback

Participants were divided into three discussion groups, moderated by a facilitator. The groups discussed the following questions:

1. ***When would the FCMs start to reach out to exchanges?***

   FCMs noted that they would first assume that the problem was theirs and would start to research the cause. They felt the exchanges would notice the problem before they would.

   Personnel analyzing the problem would likely notice a pattern of those firms that utilize DRACS/Moneypenny as a common thread. They felt the problem should be caught early on.

   A service provider in the group noted that their Risk group would most likely see the problem as it started to evolve.

2. ***How might FCMs attempt to throttle trading, if at all?***

   FCMs stated that they would most likely not throttle trading. Traders are receiving fills, so they may have a sense of their positions, depending on the volume of business they do. There may be implications to the price discovery process.

It may be riskier to slow down/throttle trading for not knowing the status of positions, rather than to allow traders to get out of risky positions.

The FCMs indicated that they would be reluctant to notify their clients until the cause of the disruption is better understood and the potential duration thereof.

The FCMs further stated that they may look at risk profiles by client types and give a heads up to those clients where the problem may create the highest risk.

3. What are the regulatory reporting requirements under this scenario? Who should notify them if required?

If an FCM suspects that the disruption is potentially a reportable event, they would most likely call their regulators and give them a heads up that they were analyzing the problem and trying to resolve what could be a troublesome issue.

However, since the source and facts behind the disruption were unknown, it is unclear if it would be a reportable event or what would be described in a formal report.

Participants indicated that within 24 hours is the requirement, however, the start of that timeframe would be unclear, given what was known.

There would be no formal declaration of a disruption that would trigger the BCP, unless the firm felt that it was their system. There would be no regulatory requirement to report a DR/BCP event.

In any case, no formal report would be filed until there was a clear and thorough understanding of the cause/effect of the disruption.

4. When, in the lifecycle of trading, would the back-office be potentially impacted, and what would be the work-arounds?

Participants agreed that the impact of the disruption would be noticed almost immediately.

The first major milestone for this would be the intraday filing.

Workarounds for problems of this magnitude would not be easy, as FCMs would not have the levels of staffing to manually process the trades in question.

The firms indicated that they could get estimates from Clearing or Risk departments via drop copies or spreadsheets. Some risk systems are independent from the back-office system and may be better set up to research or reconstruct the circumstances.

5. What key processes could be run, if at all?

Participants agreed that until clean and complete data is available, no key processes could or should be run.

They indicated that the worst-case scenario would be for firms to roll back to the prior business day and rebuild the positions.

It was questionable if drop copies have all the requisite fields required to accomplish this.

6. What about those firms that do not use the DRACS Moneypenny system?

Participants indicated that under a disruption scenario such as this, that firms would tend to reach out and try to help each other.

Furthermore, participants felt strongly that those firms that were not impacted by the disruption should not ethically take advantage of their position to the detriment of others.

F. Participant Feedback

The attendees were very engaged in the breakout sessions. While many had previously attended a tabletop scenario workshop, several the participants had not.

Several attendees indicated that their firm's BCP incudes operational processes and procedures that address this type of disruption event.

Broad participation and lively conversations ensued. The participants addressed the scenario and its impact as real.

Here are some key findings and feedback from scenario participants:

1. FIA Should Coordinate Industry-Wide Communications

- As during past events, FIA should be a single point of contact to help disseminate messages, and to protect the integrity of the markets under adverse conditions.
- FIA should provide the same communications to members as from the entity that was disrupted, as well as progress updates.
- FIA would be an additional, trusted conduit of emergency communications to the broader industry.
- The industry should have a futures-specific crisis team and playbook to respond to disruptions (for example, like the FS-ISAC All-Hazards Playbook). FIA should convene a working group to discuss and develop such a playbook.

2. Proactive Communications During Such a Disruption is Key

- In this scenario, DRACS and the FCMs that use its system should be the initial points of contact for communications about the nature of the disruption.
- Communicating with clients as to the scope and nature of the problem is key.
- There is a need to establish confidence as quickly as possible, when the facts are known.
- Public statements should include remediation intentions, if possible.
- Communicating frequently and broadly is an important factor.

G. Suggestions for Future Events

- The breakout sessions were very interactive. This was an important factor to the success of the workshop. Future events should strive for the same audience engagement.
- A wider cross-representation from all three FIA divisions could help future events. Cross-functional perspectives and teams will be key to discussing and resolving disruption events.
- To impact potential turnout, make the title of the workshop more enticing (e.g., have an attention-grabbing headline).
- Consider inviting representatives from non-industry groups to share lessons learned from similar exercises they have conducted within their industries (ChicagoFIRST, FS-ISAC, DTCC etc.).

- Include more cybersecurity experts in the design of the problem hypothesis, to make it more reliable.
- For a scenario such as this, include more senior operations representatives
- Consider expanding the workshop timeframe to 2-1/2 hours, if possible.
- Consider a ransomware scenario or a virus that is replicated between production and back-up environments that creates the need to abandon or rebuild in a tertiary data center.

H. Acknowledgements

Special thanks to the working group members and the participating FCMs, exchanges, clearinghouses and key service providers

The workshop was designed and moderated by Tellefsen and Company, L.LC.