FIA MARKET TECHNOLOGY

2017 Cybersecurity Scenario Workshop

"Operation Blow Torch"

Summary Report

November 7, 2017

A. Introduction and Workshop Overview:

On Tuesday October 17, 2017, the Futures Industry Association's Market Technology division moderated a cybersecurity workshop. The scenario simulation provided a forum for participants to discuss their respective responses to a systemic cybersecurity attack.

Participation in this inaugural workshop was on an invitation only basis. Representatives from major futures commission merchants (FCMs), exchanges, clearing houses and key service providers attended.

The workshop was attended by a cross-section of 50 industry participants, representing 20 FIA member organizations.

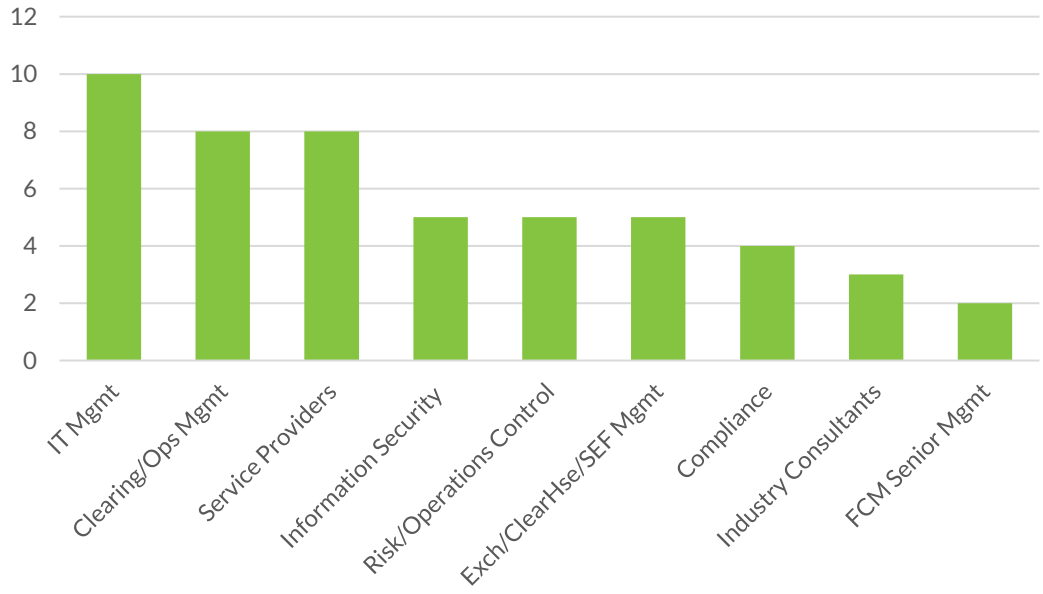
B. Workshop Objectives:

- Present a futures industry-specific cyber disruption that poses systemic risk to the market and participants.
- Heighten industry awareness to the importance of proper planning and coordination of a response to significant business interruptions.
- Discuss participants' understanding of the current state of data and systems recovery processes for returning to a normal state.
- Identify additional resources that may be required to better prepare and facilitate incident response and coordination.
- Engage the audience and get them thinking about how prepared their organizations are.
- Assess the collective response to a major disruptive cybersecurity event, understand what improvements should be made to be more resilient.

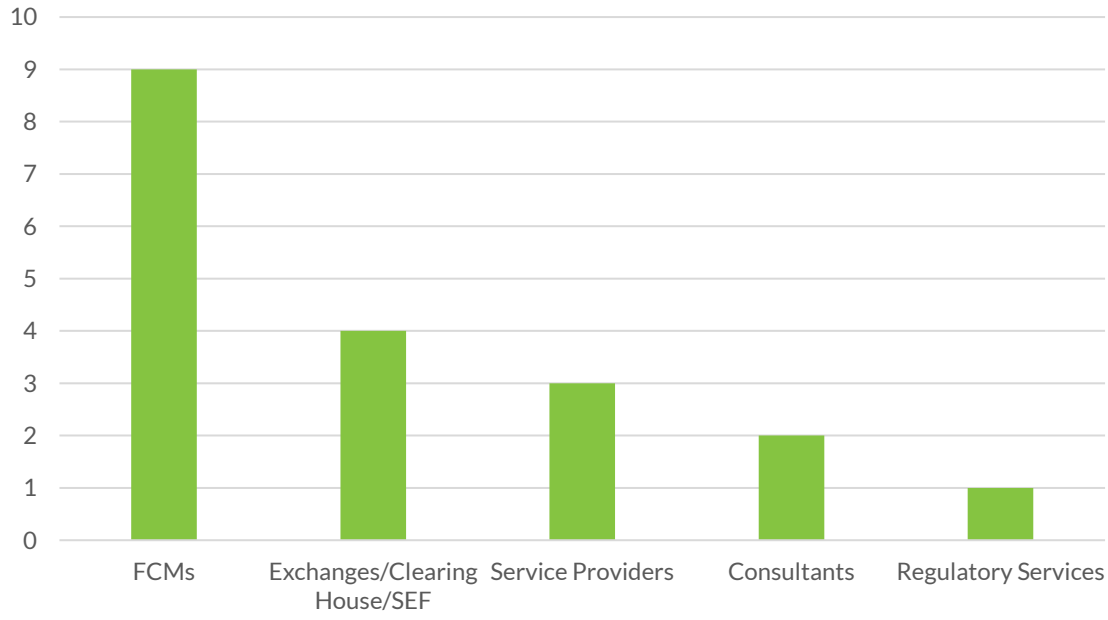
C. Target Audience, Attendee Recaps:

The audience for this exercise included those that would be impacted by, and would need to collaborate, during such a disruption (i.e., business, client services, operations, risk, technology, service providers, etc.).

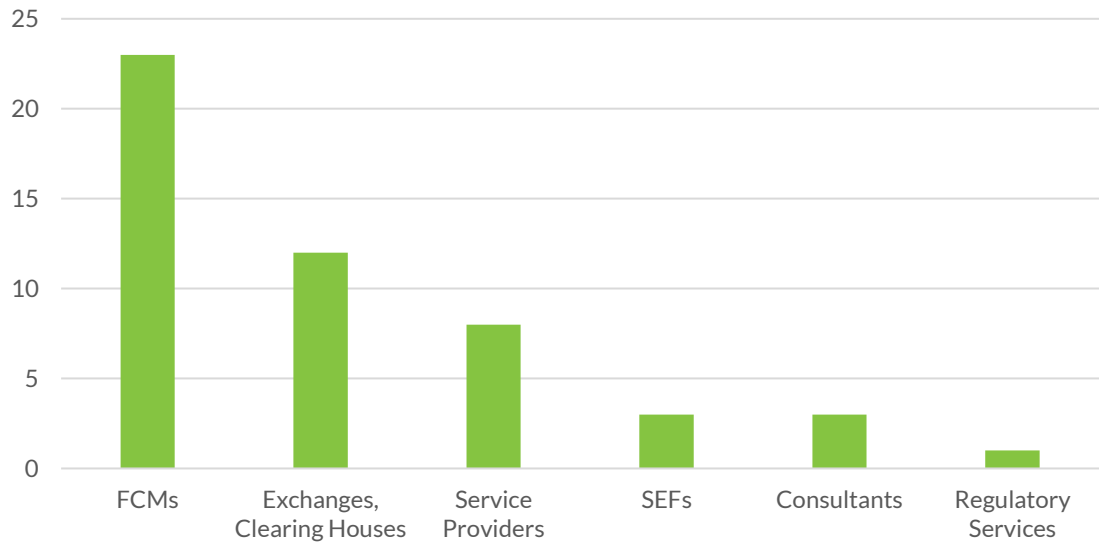
1. The workshop was attended by multiple disciplines and functions:



2. A cross-section of futures industry entities participated:



3. The majority of participants were from FCM firms:



D. Scenario Summary:

The workshop presented a cyberattack on a fictitious derivatives clearing house (Future Clear) and an exchange - the Boston Futures Exchange (BOFEX), and the resultant impact on market participants, the risk management and price discovery processes and the underlying cash markets.

The scenario evolved on an hour-by-hour and day-by-day basis; it consists of four modules separated by two 15-minute moderated Q&A sessions.

Market participants, clearing firms and key service providers were impacted by the disruption, where a malware attack targets the central trade database of Future Clear and slowly starts to erode cleared trade data. The erosion continues for over a business day.

Decisions were made as to how to isolate the infected data, reconcile and resolve impacted trades, continue business, close or reopen the market, deal with customers, regulators and the media, etc.

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 steps and actions they would take in response.

Crisis escalation, industry notifications, media communications and recovery considerations were discussed for all market participants, including other exchanges not directly impacted by the malware attack.

A discovery process evolved, and the root cause of the malware attack was eventually uncovered.

E. Scenario Recap:

Day 1:

- A large, fictitious exchange and clearing house (BOFEX, Future Clear) are attacked by a vicious malware called *Blow Torch* on the last trading day of a settlement period.
- The worm attacks Future Clear's data warehouse, data files and top day trade messages. The malware attack starts at the start of day and the disruption evolves over 2 business days.
- Given the expiration, there is a heavier than normal amount of volume.
- Anomalies with trade executions are initially identified by a large buy-side firm (Good Will Holdings) that trades across numerous futures commission merchants.
- Technology specialists and operations teams attack the problem and attempt to identify the cause/effect of the malware. Deadlines to kickoff key processing events are fast approaching.
- Potentially, hundreds of thousands of trade breaks exist, and major clearing processes and settlement prices have been impacted.
- By late afternoon, BOFEX determines that the malware has only impacted its clearing system, not the trading system. The malware has not propagated to members' back office systems (the clearing house data was corrupted, not the back-office systems).
- The exchange's management team wrestles with the decision to open/delay or close the market. Calls to the CFTC take place.
- By 4:00 PM on Day 1, the exchange announces that it will not open for the evening trading session that starts at 5:00 PM.
- The exchange initiates a situation recap and updates its member firms, clearing banks and market making firms.
- There is significant buzz and fake news on the major social media channels.
- The perpetrators of the malware insinuate that there are huge market losses that may not be covered by the clearing house default fund.

- The exchange's crisis management team gears up and crafts various media messages.
- The exchange and FIA conduct several conference calls.
- Emergency communications with clients and the general investing public kicks in. Entities that traded today may have positions at risk.
- By 5:00 PM, evening trading has started on other global markets.
- There is a significant impact to the underlying cash markets, as a result of the lack of risk management and price discovery created by the malware attack.
- The cash equities, ETF, fixed income, interest rates and commodities segments are all adversely impacted.
- FCM firms and key service providers wrestle with processing their other business around the effects of the malware at BOFEX.
- Forensic data scientists at Future Clear work feverishly to identify the root cause of the malware.
- By the end of Day 1, BOFEX and Future Clear have conducted 5 conference calls with its members and 3 calls with the CFTC and other market regulators.

Day 2:

- By the morning of Day 2, the source and impact of malware is finally identified.
- The perpetrator of the malware is identified as the clearing system Database Administrator.
- The IT staff develop an inoculation for the malware, test it and are confident that it can rectify the problem.
- BOFEX conducts 2 more situation recaps with the CFTC and other market regulators.
- By the end of day, the clearing system is back and successful EOD processing is completed.

Days 3 and 4:

- Over the course of the day, BOFEX conducts 3 more calls with regulators.
- With senior management approval and CFTC concurrence, BOFEX uploads the fix and the production system data starts to recover – clean.

- Future Clear processes the Day 1 (problematic) trades on Day 3, as-of Day 1. With the data files cleansed of the malware and the clearing system restored, Future Clear requests a margin true up from its clearing members.

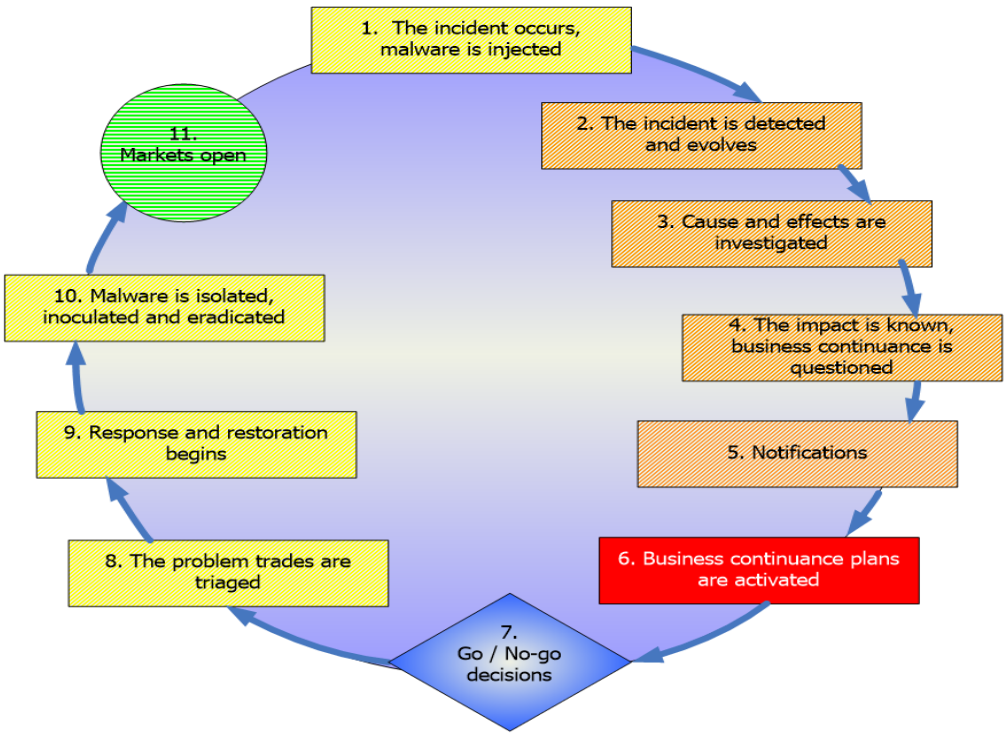
- BOFEX announces that its markets will have a staggered re-open at 5:00 PM, with a limited number of products.

- By the evening of Day 3/morning of Day 4, BOFEX markets are reopened and Future Clear has been restored to service.

- BOFEX and Future Clear have committed to implement tighter production access controls, processes and procedures to prevent a recurrence of the problem.

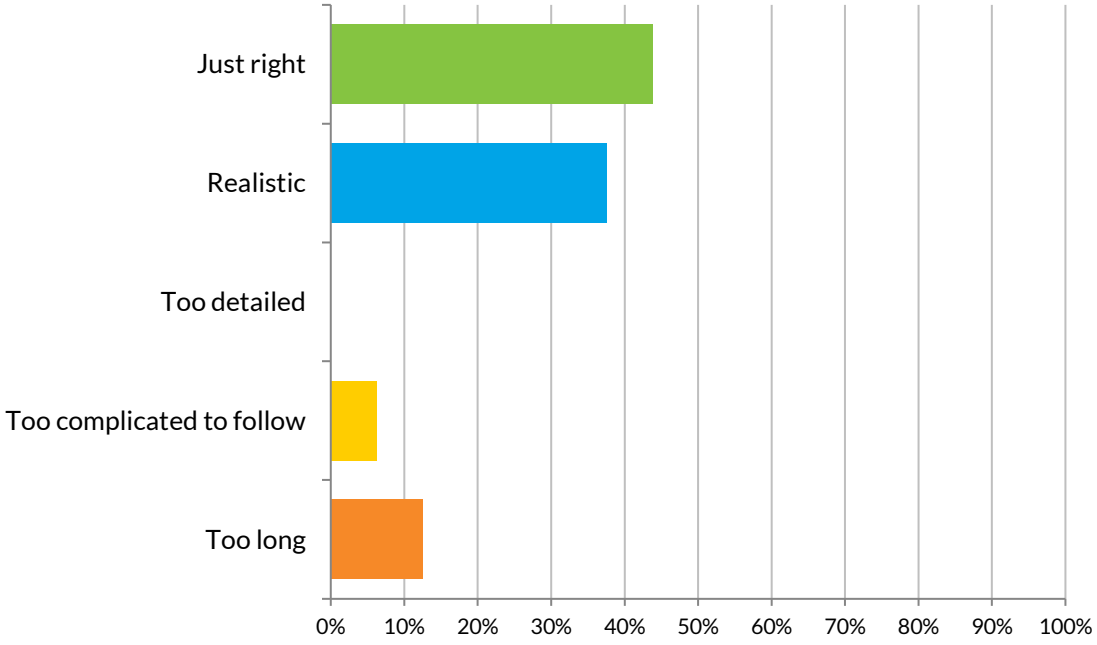
- Forensic post-mortem reviews are conducted.
  Market volatility is expected to continue across most global markets

The Incident Detection and Response Flow:

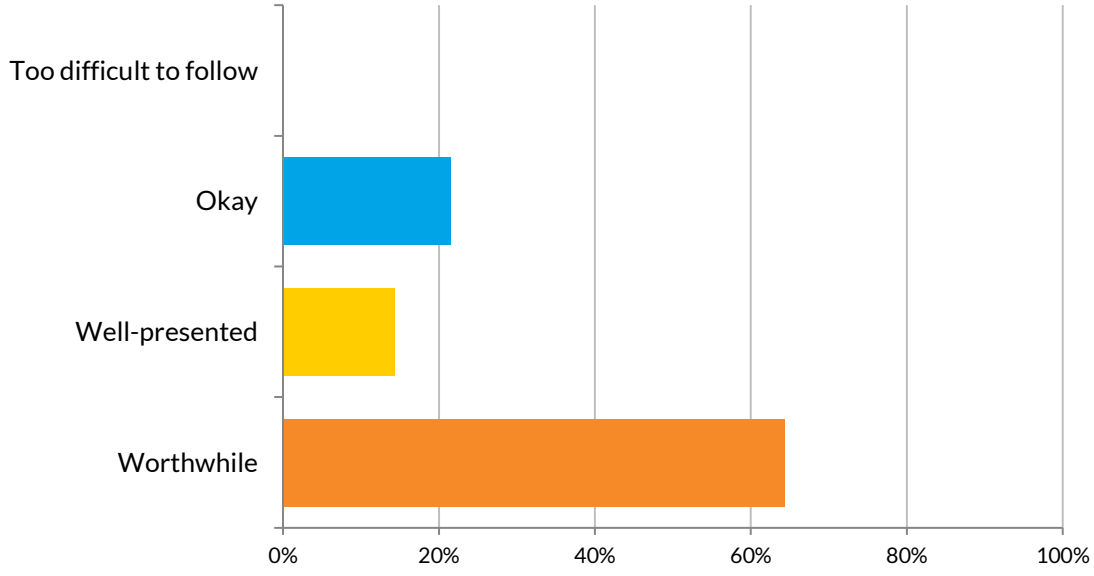


F. Participants Feedback:

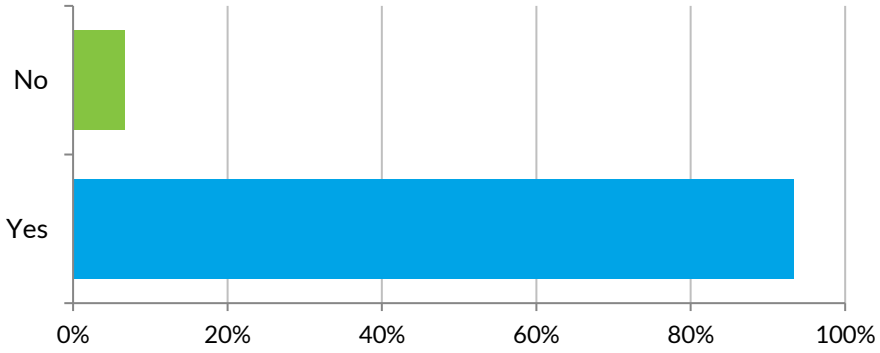
1. Overall, The Workshop Was Rated as Being Realistic and Plausible:



2. Those Participants That Had Not Previously Attended a Table Top Exercise Found the Experience Worthwhile:



3. The Majority of Existing Business Continuity Plans Address the Responses to Business Disruptions and the Restoration of the Business:



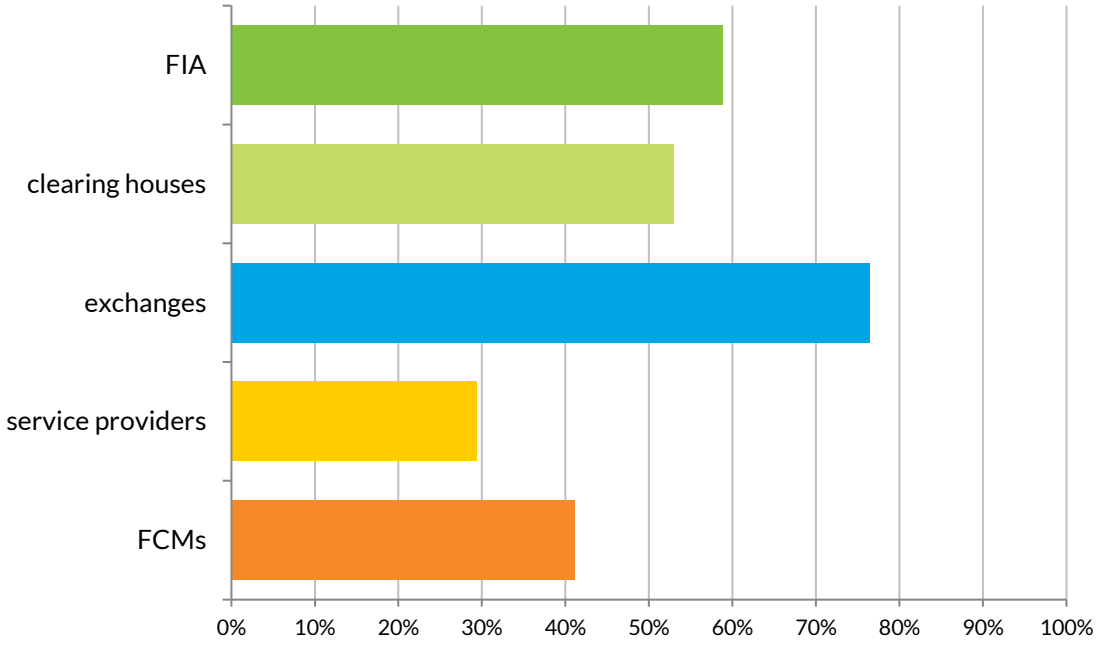
4. Procedures Exist to Address and Reconcile a Large Number of Out-Trades:

   - FCM clearing operations managers indicated that they may have sufficient staff and procedures in place to reconcile a large number of trade breaks.
   - They also indicated that they could/would do this if they felt confident that their records were not corrupted.
   - FCMs would expect the clearing house to declare force majeure to extend the clearance and settlement cycle, processing windows.
   - Clearing operations managers indicated that there are alternative methods in place to compute the daily settlement prices (e.g., using the prior business day's settlement prices).

5. Computing and Issuing Margin Calls Would be Problematic:

   - Clearing operations managers questioned how initial and variation margin could be determined, if positions cannot be validated.
   - FCM participants indicated that they could use a volatility matrix to compute margin, but realistically would wait for the clearing house to declare force majeure.
   - Under a worst-case situation, the FCMs would use the prior day's positions and prices, assuming they corroborated that prior day's data has not been corrupted also.

6. Exchanges and Clearing Houses Should be the Focal Point for Crisis Communications, Under Similar Disruptions:



7. The FIA Should Coordinate Industry-Wide Communications:

   - As during past events, the FIA's role should be to help disseminate a message to protect the integrity of the markets under adverse conditions.
   - 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.
   - FIA should help coordinate emergency communications between BOFEX, Future Clear and the industry.

8. Proactive Communications is Key:

   - 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.
   - Corroborate that clients are/are not seeing anomalies with BOFEX and other markets' trades.

- The consensus among participants was to tell clients to "…go with what you believe your (BOFEX) positions are, and we will straighten out the clearing house…"

- From there, disseminate the fact that the problem is solely with the clearing house.

- Public statements should include remediation intentions.

- Communicating frequently and broadly is an important factor.

9. FCMs Have the Ability to Run Their Back-Office Systems for All but the Impacted Market:

    - FCMs indicated that they could run their back-office processing on a selective basis (i.e., process trades for all other market *except* BOFEX)

    - They would need to manually override the system and set parameters to select out the market in question.

    - Once it was determined that the malware was in the clearing house systems only, firms could consider using drop copy records from the BOFEX trading system as the "*golden record*".

10. Firms Would Suspend Trading on the Affected Market, During a Disruption of This Magnitude:

    - Given the uncertainty at the outset of the attack, some firms would stop or suspend trading on BOFEX.

    - Participants also indicated that, from a trader's perspective, positions would be most likely be liquidated or hedged on other markets, if possible.

    - However, it will be near-impossible to control what hundreds (or thousands) of traders will do when they see market-moving news breaking on social media platforms.

    - Communicating that the extent of the malware was limited - just in the clearing system – should have some limited effect on the market.

11. Settlement Pricing and Regulatory Reporting Would be Thorny Challenges:

    - With the extent of the malware, the clearing house would most likely declare it a *force majeure* event.

    - Based on this, they would extend the settlement cycle for those trades.

- Alternatives and precedents exist to compute settlement prices (e.g., a variation of the prior business day's prices).

- FCM managers said that they would use a volatility matrix to facilitate this.

12. Operational Work-Arounds May Not Be Effective:

- With the growth of electronic trading and trade volumes over the years, operational work-arounds may be limited, as back office systems and processes have been geared for a relatively low percentage of exceptions processing.

- Given the timing of when the extent of the malware became known and the sheer volume of trade breaks, the ability to react to the problem trades and process other business may be highly challenging.

13. Market Participants Should Have a Media Strategy, Prepared Messages:

- Exchanges and market participants have incident management teams in place to communicate (internally) under similar disruption scenarios.

- Participants should have a crisis management system and framework for communications during significant business disruption events.

- The crisis management framework should be deployed to disseminate their message to clients, regulators, the media etc.

14. Other Markets Should be Introspective Under Similar Circumstances:

- This malware disruption was targeted at one market.

- Given the magnitude of the situation and the rapid proliferation of news, it is incumbent that all other markets "look inward" to see if they are seeing similar behavior with their processes and systems.

- As part of their emergency communications strategy, exchanges should keep their peers in the loop.

15. The Malware Attack Would Cause an Immediate, Cascading Effect on the Cash Markets:

- Given the inter-relationship between the underlying cash and futures markets, there will be an immediate, fast-moving effect on price discovery, risk management and liquidity.

- Volatility will spike, due to the absence of liquidity and order flow providers.

- Capital flight will be swift under similar market disruption circumstances.

- Major market regulators will likely confer with cash market operators to assess the effects of the disruption and the orderliness of the markets.

16. Trading in BOFEX Stock Would be Halted, Pending Large Order Imbalances, News Dissemination:

- BOFEX, a listed company (NYSE: BFX), is also included in numerous financial ETF portfolios, as well as the S&P 500 index.

- Under similar disruption circumstances, the primary market (NYSE) will likely have a large imbalance of sell orders that may trigger a halt in trading, pending the dissemination of news from BOFEX.

- This will also have a cascading effect on the underlying ETFs and S&Ps.

G. Suggestions for Future Events:

- Participants felt that the workshop was well developed and presented. However, there should have been a third Q&A breakout, possibly with a discussion on the return to normal by Day 3, internal cleanups etc.

- Expand the composition of the working group to include representatives with cross-industry, cross-domain expertise (e.g., the Operations Division).

- Speed up the timeline.

- Consider engineering the scenario in lesser detail as this one, possibly create a cyber situation premise and have the attendees flesh it out (i.e., "who dun it?")

- The physical set up of the room should be conducive to facilitate the dialogue.

- Consider setting up roundtables or horseshoe style tables.

- Structure the setup of the room/tables and questions as to how the industry would respond, as opposed to individual organizations (neutral facilitation) - by functional areas.

- Have each functional team attack the problem from their area of expertise (e.g., IT and information security, clearing operations, exchanges/clearing houses, service providers).

- Set up problem-solving break out groups that would share their feedback with the larger audience.

- Provide more open-ended questions in the presentation.

- Future events should continue to be by invitation only, with ~50 attendees.

- Expand the overall workshop time to a maximum of 3-4 hours in length, to allow for breakout sessions, Q&A etc.

- Include more cybersecurity experts in the design of the problem hypothesis, to make it more bulletproof.

- Security concerns were raised about what might be discussed in a WebEx (i.e., on an open conference line) workshop.

- Providing an executive summary overview to attendees in advance is helpful in understanding the scenario and focusing participants' attention.

H. Response and Recovery Considerations:

1. For FCMs and Key Service Providers:

   - Activate an operations recovery team to address the questionable trades and another team to continue to process the ongoing business.

   - Allocate/provide adequate staffing to attack the problem. Identify other internal departments to collaborate with.

   - Invoke the FS-ISAC "*All- Hazards Crisis Response Playbook"*

   - Consider running your back-office processing for all other markets except the affected one, to minimize your risk exposure.

   - Based on the update from the exchange, craft media message(s) to your customers, including when and how.

   - Review your firm's BCP to ensure it encompasses cyber disruptions such as this.

   - Have a cybersecurity breach plan.

2. For Other Exchanges and Clearing Houses:

   - Determine how/when you collaborate with Future Clear and BOFEX staffs to coordinate the response to the problem and how best to attack it.

   - Determine how/when you would conduct a similar review internally to look for similar malware or system behavior.

   - Determine what you would do if you find the malware, or were attacked in a similar manner.

   - Develop/enhance a marketing communications and emergency PR strategy, including identification of key spokespersons and the crisis response team.

- Identify key contacts in your BCP that regulatory and compliance teams would need to communicate with.
- Ensure your BCP encompasses cyber disruptions such as this. Have a cybersecurity breach plan.

3. For Legal/Regulatory Services:
   - Identify other internal departments to collaborate with to address and resolve the problem.
   - Create a file and carve out information for potential evidence for legal discovery and to build a case for (ultimate) prosecution.
   - Identify tools that exist to support this process.
   - Identify who needs to be involved on this team from your organizations (functions and skill sets).
   - Determine how/when you would contact the FBI and other government agencies.
   - Determine how/when you would collaborate with other agencies and services (CFTC, FBI, Fed, FS-ISAC, FSSCC, NFA etc.).
   - Assess the frequency of communications between regulators, markets and the FIA.

I. Acknowledgements:

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

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