2020 Cybersecurity Scenario Workshop

"Operation Chimera"

Summary Report

December 2020

A. Introduction and Workshop Overview:

On 10 November, 2020, FIA's Market Technology division moderated the fourth annual cybersecurity scenario workshop. The workshop was conducted in a virtual environment via Zoom conference.

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

Representatives from major futures commission merchants (FCMs), proprietary trading firms, exchanges, clearing houses, hedge funds and key service providers attended.

The workshop was attended by a cross-section of 34 industry participants, representing 18 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 to return 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, and understand what improvements should be made for the industry to be more resilient.

C. Target Audience, Attendee Recaps:

The audience for this exercise included those that would be impacted by the disruption and those who would need to collaborate during such an event. The workshop attendees represented multiple disciplines and functions, including:

- Business Continuity Management
- Business Systems
- Clearing Operations and Collateral Management
- Compliance and Legal
- Executive Management
- Information Security
- IT Management
- Operations Management
- Product and Applications Management
- Trading and Risk

Participants represented a cross-section of the industry:

- Clearing Houses
- Exchanges
- Futures Commission Merchants
- Industry Consultants
- Proprietary Trading Firms
- Regulatory Services
- Service Providers
- FIA

D. Background:

Over the last 15 years, various market participants in the Financial Services industry have migrated their mission critical order management, trading, risk, clearing and market data systems to data centers at managed service providers (MSPs), to be in close proximity with exchanges' infrastructures.

In the futures industry, market makers, proprietary trading firms, liquidity providers and market data vendors all have co-located their systems into hardened data centers that are either owned or managed by the exchanges, or at a site where an exchange has housed its matching engine.

These data centers have been engineered with rigid physical and information security controls, redundant power, network and telecom providers, environmental controls, etc.

Concurrent with these trends, there have been numerous mergers and acquisitions of data center providers, combined into publicly traded real estate investment trusts (REITs).

Today, the top 30 managed services providers operate over 1,100 physical data center facilities worldwide.*

From a risk perspective, some firms and regulators have become concerned that there is too much concentration of industry participants.

As strategically important market utilities (SIFMUs), U.S. exchanges and clearing houses are required by regulators to have business continuance and disaster resilience capabilities in their processes, procedures, infrastructure and mission critical systems and applications.

The Commodity Futures Trading Commission (CFTC) and the National Futures Association (NFA) have business continuance regulations that exchanges/clearing houses and market participants must adhere to, in cases of significant business disruption (SBD) or emergencies.

Source: Enterprise Management 360, February 2018

E. Scenario Summary:

The workshop presented a disruption scenario where a domestic terrorist group attacked a major data center complex used by a futures exchange, its clearing house, members' connectivity and their mission critical systems infrastructures.

As part of the attack, a fictitious derivatives exchange and clearing house - the Boston Futures Exchange (BOFEX) and Future Clear (FC) - are destroyed by an explosives-laden drone.

Day 0, 8:00 AM EST

BOFEX houses its mission-critical trading, risk management, market data and clearing systems in a hardened co-location data center operated by GoogEquiniZure Web Services (GEZ).

GEZ ranks in the top 3 of global managed services providers, based on their revenues and global footprint.

Major futures commission merchants, proprietary trading firms, software-as-a-service providers and market data vendors are also co-located in GEZ, as are numerous dark pool automated trading systems and crypto trading platform providers.

The GEZ BOS12 complex is a state-of-the-art data center located outside of Boston in central Massachusetts. It is classified as a "Tier 4" data center, with full redundancy throughout.

Like most hardened data centers, the building has redundant power distribution units, transfer switches, multiple paths for utility power and telecoms connections, as well as multiple back-up generators with bio-diesel fuel tanks.

BOFEX and other GEZ clients are cross-connected from BOS12 to secondary (backup) sites, telecom and market data vendors etc.

In the last few years, cyber terrorists have stepped up their attacks on various soft targets, including banks and high-profile corporations.

An extremist group called the *Texas Raiders* has vowed to conduct vicious attacks on symbols of capitalism and America's financial infrastructure. They are seeking retribution for the income inequality in America.

They have been responsible for cyber and ransomware attacks on numerous global entities and have recently espoused more violent approaches.

Day 1, 7:00 AM EST

Using their war-chest of bitcoins amassed via corporate ransomware, the Raiders acquire a Hermes "*Silver Arrow*" drone on the black market. They have recruited a former military drone pilot to operate it.

The Hermes is a medium-sized drone with a 49-foot wingspan, capable of delivering up to a one-ton payload from altitudes of up to 30,000 feet.

They previously disassembled the drone and smuggled it into the U.S.

The Raiders also employee a high-explosives weapons scientist sympathetic to their cause. He has previous experience in developing bis-oxadiazole ("*BIS*"), for the U.S. Army Research Labs at the Aberdeen Proving Grounds.

As a highly explosive substance, BIS is proven to be 1.5 times more powerful than TNT. It is known for its stability, density and highly concentrated destructive power.

Day 1, 8:30 AM EST

When the Hermes drone components arrived in the U.S. at the Port of Boston, they were trucked to a non-descript warehouse in a remote part of Rhode Island. It was re-assembled and its components prepared for its solo mission.

They dub their drone the "Chimera" after a mythical fire-breathing monster.

They set up the Chimera to quickly launch it from Rhode Island and hit its target, with no time for counter measures from the authorities.

The Raiders load the Chimera with a thousand-pound payload of BIS.

Day 1, 2:30 PM EST

They remotely pilot their deadly cargo towards it intended target – BOS12.

- *The flight time to target is only 7 minutes!*

The stealthy Hermes technology evades major East Coast radar systems and U.S. Homeland Security detection, until it's too late… *Within minutes of takeoff, the drone crashes into BOS12 at 2:49 PM EST.*

Instantly, numerous alarms are generated from the data center environmental sensors, physical security systems, power generators, network equipment and applications software. They are sent to network and operations staff in multiple GEZ operations centers.

Alarms are also generated to client firms and vendor contacts at those firms for whom GEZ provides managed services.

The failure of the BOS12 data center triggers automatic failover mechanisms to secondary data centers.

These include other GEZ datacenters (secondary sites), as well as clients' designated secondary sites hosted in non-GEZ data centers.

The recovery time objective to failover to the secondary site for such a large data center is expected to tax or exceed service level agreements or contractual recovery time objectives.

The auto-failover to the backup data centers is contingent upon the state of the site-to-site connectivity.

The critical path to the failover and recovery is the telecoms infrastructure.
From a triage perspective, data center clients who have split their managed service providers between sites (e.g., GEZ = primary and Amazon, Microsoft or Google = secondary), may not necessarily be addressed as a first priority.

Day 1, 3:30 PM EST

The attack has caught Homeland Security and other government agencies flat-footed.

- *There are concerns that other high-profile exchanges and financial services entities and critical infrastructure may the next targets.*

Conference calls are quickly organized with high-level representatives from the FBI, the White House, Homeland Security, Treasury, FSISC the CFTC, SEC and major market regulators.

Major U.S. cash and derivatives markets are still open. There is significant volatility in all asset classes.

Orders are flowing to other exchanges and trades are being reported back from clearing houses across the globe. Transaction volumes are heavier than normal.

- *Will the data center attack impact other markets and major financial infrastructure?*

BOFEX has a 2-hour objective for the recovery and continuance of their mission critical trading, risk management and clearing systems.

- *Can BOFEX failover to their secondary site, process today's business and be ready to open their market tomorrow?*

They have obligations to immediately notify their users and regulators if a significant disruption impacts their systems and operations.

By 4:00 PM, BOFEX management declares the problem to be a significant business disruption, and invokes their BCP.

- *What are the potential implications relative to BCP? Will they be able to process today's business?*

- *When do regulatory notification requirements suggest this should happen?*

Day 1. 4:15 PM EST

The BOFEX Risk and Settlements Committees hold emergency meetings to discuss what to do about pending settlements, the posting of margins and related processes.

In consultation with their CEO and board members, management notifies their member firms, the CFTC, other government agencies and the media.

They announce publicly that *"As a result of an attack on our primary production data processing facilities, we have invoked our BCP and will not open our markets until further notice"* …

They start to address the incident and incident management with the media.

The CFTC is concerned about the implications of closing the market, BOFEX's ability to regain control of its systems and infrastructure, and how quickly they can re-open the markets.

By now, major news outlets and social media channels have picked up on the story. They report that BOFEX and numerous financial entities have been the subject of a vicious and deadly terrorist attack.

POTUS issues a statement:

"This is a direct attack on American capitalism. The FBI and DHS are actively searching for the source of this terrorist attack. We must re-open our markets as soon as possible... and hunt down the terrible nasty people who perpetrated this heinous crime!"

Day 1, 5:30 PM EST

Regulators are concerned about the potential for further acts of terrorism and widescale, systemic impacts to other global financial markets.

A follow up call is scheduled for later in the day.

BOFEX posts a notice on its website that its markets are *closed* until further notice.

BOFEX has contacted the major market regulators and all of its member firms via conference calls, and briefed them on the extent of the problems and potential timelines.

They have reached out to as many industry contacts as possible.

Day 2, 8:00 AM EST

The BOS12 data center has been totally destroyed.

There is airborne PCB contamination in the area, as a result of the burning building and its toxic contents of computing equipment, electrical wiring and components, ethylene glycol etc.

GEZ, in concert with its insurers, has declared the BOS12 data center and its contents to be a total loss.

They are actively working with their client firms to re-establish business and connectivity to other sites.

BOFEX participates on an all-hands call with the FBI, DHS, outside agencies, market regulators and representatives from financial sector partnerships to discuss the status of the attack and efforts to re-open the markets.

They describe the efforts that their staff has taken, in concert with help from GEZ and outside agencies and vendors.

Regulators want to know when BOFEX will restart its markets

* * * * * *

F. Breakout Discussions:

Breakout sessions were held, with the participants divided into three teams, each lead by a moderator. Each team was presented with questions on the impact of the disruption and its ramifications to their business, technology and operations.

At the conclusion of the breakout sessions, the moderators presented the teams' 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 happened and some of the steps and actions they would take in response.

G. Breakout Sessions Feedback:

The groups discussed the following questions:

1. ***Do existing BC/DR playbooks address such a catastrophic event? Has this scenario been addressed in prior BC/DR tests?***

   Some firms have this scenario covered in their BCP playbooks and have accounted for this in prior BC/DR testing.

   Most firms keep their key contacts up to date in their BCPs via automated tools (e.g., In Case of Crisis).

   Firms would expect BOFEX to contact the CFTC and NFA as soon as possible.

   Respondents would expect FIA to coordinate multiple conference calls with BOFEX management, GEZ, market regulators, key service providers and market participants.

   Following the failover, various teams would be involved in the response and recovery: IT support, network operations, clearing operations, legal/compliance, etc.

   Overall, the IT infrastructure and software should be in lock step in both production and back up. IT replicates to DR every 15 minutes; main response. The other methods were to clone the VMs or hot copies of data.

   Firms should practice drills/rehearsals/exercises to refine and reinforce the playbook to cover worst case scenarios.

   Plans/playbooks should be available that can be accessed by key people by any modalities. Storage of the playbook, should be in the cloud or stored separate from the primary data center, so it is not lost in this catastrophe.

Planning and more importantly rehearsing the scenario; irons out the details and 'gotchas''. You can alternate staff to perform the testing quarterly to minimize Key Man Risk and provide more chances to come back sooner.

Diligence in keeping the emails and contact numbers updated regularly for those partners noted above. Keep internal key contacts fresh by performing EMS tests for employees regularly (e.g., quarterly).

2. ***How would user organizations (member firms, providers of SaaS solutions, other users of BOS12 managed services) be notified of the failure?***

The loss of physical connectivity to BOS12 would be the initial trigger of alarms to BOFEX and any firms connected to GEZ. Firms indicated that data loss and loss of electric power would also generate alarms. Firms expect to be contacted via phone calls, email. Also, via news broadcasts and social media.

Firms would expect that clearing members' customers would contact their clearing banks, shortly after the clearing firms find out.

Regulatory agencies would be contacted by the clearing house.

Assuming phones, power are all consistently working. Cell phones may be impacted if bandwidth is taken over by DHS etc.

The initial notifications would likely come to the IT support and operations staffs and the data center teams.

Question - what is BOFEX's message to the public about the attack and disruption to its markets?

3. ***How/when would a secondary data center be notified of the failure?***

The loss of physical connectivity to BOS12 would be the initial trigger of alarms to BOFEX and any firms connected to GEZ. The initial notifications would likely come to the IT and IT operations staffs.

The crisis team would be activated; becoming or assembling a Task Force to protect the exchange, market and firms and regulators.

Immediate notification was the consensus by multiple alarms and alerts due to constant monitoring of the infrastructure, middleware and software. Priority to the clients and regulators would be first and foremost.

To remedy that steps would be taken to call and notify skilled resources to begin analysis as soon as possible assuming secondary site is not in the same region. This way the hazardous chemicals would not impact safety of those employees, or the power grid to the data center.

IT would likely perform gap analysis and troubleshoot throughout the night and provide ongoing status by phone/email/IM.

Concurrently, the crisis team of member firms would convene. It is likely an open line would be started by the FIA and attended by exchanges, firms and regulators to come together to share what is known, when and help to target the response on this in order to resume operations next day.

If any deadlines, positions, margins, collateral and risk-based information would cause Legal/Compliance to request regulatory relief.

4. Given the loss of life, would GEZ's ability to failover and recover be impacted?

Market participants would be sensitive to staff welfare and the loss of life from the attack. Did firms have any technical staff on site at GEZ that day, as well as GEZ staff?

Loss of colleagues naturally impact the circle of people with emotion, grief and despair. In addition, concerns for the toxic chemicals in the immediate area that will harm the community and fire fighters.

Most firms indicated that they would corroborate/verify their employees' safety and welfare as an initial step. They would quickly review the data center site schedule for any hardware/software installs scheduled for that day and attempt to contact those that were expected to be on site.

Is there any "key man" risk at GEZ, due to the loss of life? Is there continuity for those key roles that were lost in the attack?

Concerns were expressed that the failover from production to DR may not go as planned, given the need for some level of manual intervention.

As for manual steps, SME skills for any manual troubleshooting or simply verification of the key infrastructure, routing, middleware and applications.

There is a need to verify that a golden source of data exists and has not been corrupted or adversely impacted.

Traders would be concerned that any orders in flight generated by algos may still be live and may cause risk. They would also want to verify the current state of their positions to assess any hedging requirements.

There would likely be an all-hands effort to reconstruct last set of transactions; time stamps of the transactions. This will help assess any loss or risk for asset classes; hedge, cleared swaps, futures, etc.

Skillset of task force may come from industry professionals who volunteer to help pull things together is a possible lifeline for BOFEX.

Consider a grace period to cover gaps, issues, time needed to recreate any margins or positions from the day before the explosion.

Limbo for the overnight is likely for both IT and business staff; while pulling together what is known so focus on out-trades can be done by a smaller set of people (assuming they are okay and available) at BOFEX; while others keep the rest of business going.

Running processes to get settlements, positions and statements to clients to what extent possible.

Firms would be guarded until they can determine the net exposure to the entire exchange and its markets. Ideally, Day 2 is at least a partial trading day.

5. ***What is the state of collecting margin, cash movement, completing the daily settlement, end of day processing and regulatory reporting requirements, given the time of the attack?***

BOFEX/Future Clear would likely notify its clearing banks of the disruption ASAP.

There may be a need for regulatory relief for the impacts to the BOFEX end of day processing cycles.

Teams would be needed to review and reconcile any pending or incomplete M1 trade messages, margin calls, the movement of collateral, statements, customer seg etc.

Questions:

How would firms handle their end of day processing for BOFEX trades?

Can/would clearing firms and their service providers process their end of day for all markets except for BOFEX?

Are firms' back office manuals (written procedures) up to date?

Could clearing firms produce estimated risk parameters and margin files on Day 1 for BOFEX trades that were booked prior to the attack (2:49 PM)?

Would the business step up and help out GEZ, given the extent of the disruption and loss of life?

6. ***What are the implications on the overall market and other global, inter-connected asset classes?***

What exposure would market makers and prop trading firms have that typically have huge intra-day positions?

The industry would likely come together to address any missing trades, data etc.

Question - would BOFEX continue to be viable if some clearing members start to default due to their exposure?

Given the extent of the damage and time to recover, would BOFEX announce a "Declared Holiday"?

Firms are concerned that the size of BOFEX and the extent of the disruption would have a knock-on effect on other markets. The availability of credit could have an effect on liquidity.

Volatility on other markets is expected to increase, but volumes may trail off. Traders may take advantage of panic selling that may temporarily impact liquidity and volatility.

Customers and traders will look for alternate ways to hedge risk, but may be limited by availability of credit and lack of fungibility at other exchanges.

7. ***Could other critical financial infrastructures (clearing houses and exchanges) be at risk for a similar attack?***

Market participants should now be initiating their own operational work-around plans, i.e., procedures in place in the event of an outage at BOFEX.

Question - what would the CFTC Part 190 bankruptcy protections and CCP recovery resolutions be, given the extent of the disruption?

This is something that we should already know, but if not - then pulling the contracts to confirm failover obligations, recovery time objectives, etc., would be good to confirm at this time.

With the flurry of emails generated by this disruption, there may be further opportunities for phishing or random ware attacks.

Participants noted that during the last update that the organization was in full BCP mode and "closed" util further notice so whatever the contractual commitments are they may not be relevant as everyone is in the same boat.

More questions should be asked, related to the anticipated length of the temporary closing.

From other exchanges' perspective:

- Crisis management teams should be engaged and trying to assess if other SIFMUs are also being targeted based on public / private, FS-ISAC, etc., available information available.
- Is there a pending threat based on classified intelligence?
- Ascertain the interconnectedness of market ecosystems and potential impacts to:
    - Settlement prices / settlement banks
    - Other clearing members like prop trading firms and FCMs needing to know what is their risk
    - Margin risk exposure
    - Locked liquidity
    - Open transactions
    - End of day positions

Start playing out scenarios to address if X is unavailable past Y timeframe.

8. ***What are the contractual ramifications for BOFEX' member firms and those SaaS firms who were housed in BOS12?***

Discussions quickly shifted to the "force majeure" language within insurance contracts:

- Several interpretations were exchanged on this topic with a question related to would this scenario trigger the condition or not
- Given this may not be perceived as an "act of war" nor a "foreign terrorist" attack compared to a "domestic terrorist" attack, (i.e., the Texas Raiders).
- Question - would be relevant at this recovery stage of the scenario?

- The group decided to leave this debate for "the lawyers" and return to the scenario at hand.

By 8:00 a.m. the next morning:

- Assess if "close of business" processes were completed became a priority.
- The question of pending settlements resurfaced.

9. ***What is the message to the public from BOFEX management and any other firms who were co-located at BOS12?***

Assumptions are that most crisis management or business continuity communications are pre-scripted and leveraged accordingly as many organizations of this size practice scenarios to be prepared to manage.

- Several shared what they do for preparations, etc.
- Crisis management communications teams include C-suite, marketing, legal, etc.

Communications would likely include information related to:

- Internal communications to staff confirming an accounting of all staff
- Acknowledgment of loss of life, condolences, etc.,
- Appeal to assist in environmental cleanup efforts
- Current status indicating progress
- When to expect the next update

It is uncertain what would be communicated to those market participants that did not have redundant capabilities at the BOFEX secondary location.

- High frequency trading firms typically house closest to matching engine and also in the secondary location.
- FCMs and others will likely only have a presence at the primary location without redundant infrastructure at secondary location
- What percentage of industry intermediaries and other critical services to them could be impacted in this manner?

Assumptions are that there would also be some type of Industry wide information sharing underway, e.g., FIA role.

- Assess the collective efforts needed toward seeking regulatory relief.

10. ***Would this attack impact the opening of other domestic financial markets?***

There were some mixed responses here but overall a general feel that the impacts would be minor:

- There may be some delays with cash markets due to risk management and price discovery challenges
- Potential interconnectedness / interoperability issues
- Little/no direct impacts to equity markets

Expect increased volatility across other markets:

- Discussed that other markets would allow for traders to lay off some of their risks through hedging strategies
- Crisis mgmt. communications teams include C-Suite, marketing, legal, etc.

* * * * * *

H. Participants Feedback:

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

Several attendees are in a line of business that does not regularly expose then to business continuity management, information security, data center operations and back up sites.

Attendees reported that the virtual workshop format was well presented and well-orchestrated.

A number of attendees indicated that their firm's BCP incudes operational processes and procedures that do address this type of disruption event. However, some acknowledged that theirs does not (yet).

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

1. ***Ensure that Response to a Data Center Failure or Loss of a Cloud Service Provider Scenario is Addressed in Business Continuity Plans and Training:***

    - Ensure that existing business continuity plans and table top exercises address the responses to cybersecurity attacks and data center failure scenarios.
    - Pre-determine the message(s) to clients, counterparties and the staff, and who is authorized to make them.
    - Ensure that ongoing BCP and cybersecurity training to the staff address best practices for cyber and computing.
    - Several attendees commented that small-medium sized FCMs who are housed in co-located data centers may or may not be architected with data replication capabilities and automated failover mechanisms to a secondary (back-up) site. Larger FCMs and high frequency trading firms would.

2. ***Under Similar Disruption Scenarios, the FIA Should Coordinate Industry-Wide Communications:***

    - Most participants assumed that in a scenario such as this that FIA would open a "war room" via conference calls, and be a focal point to communicate with market participants.
    - As during past disruption events, the FIA's role should be a single point of contact to help disseminate a message, and to protect the integrity of the markets under adverse conditions.
    - FIA should invoke its disruption playbook and provide the consistent 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 with the industry.

3. ***Proactive Communications During Such a Disruption is Key:***

- Communicating with staff and 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.

I. Suggestions for Future Events:

- The breakout sessions engaged the audience and was very interactive. This was an important factor to the success of the workshop.

- Participants indicated that the size and composition of the audience was conducive to a good dialogue.

- Continue to invite and engage a wider cross-representation from all three FIA divisions to attend. Cross functional perspectives and teams will be key to discussing and resolving disruption events such as this.

- Consider inviting representatives from non-industry groups to participate to share their lessons learned from similar exercises they have conducted within their industries.

- Continue to market this to a wider part of the industry.

- For future workshops, consider:

    - Aligning the scenario with current technologies, architectures and best practice areas for mission critical systems (e.g., auto-failover mechanisms, dynamic IP addresses, resiliency mechanisms).
    - A region or location outage scenario that impacts internet service providers (ISPs), member firms, financial technology service providers, and telecommuting capabilities (i.e., users working from home) etc.
    - Cyber and operational risk issues associated with a large remote workforce (disruptions to users' home computing capabilities).
    - Post-COVID return to the office challenges.

J. 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.