Preliminary Lessons Learned from COVID-19

Nina Neer / Jason Harrell
Cybersecurity Subcommittee - CFTC Technology Advisory Committee

July 16, 2020

Pandemic vs Cyber Operational Impacts: Differences

While the COVID-19 pandemic tested firms ability to respond to a material operational event, there are some caveats to this teaching moment that make it different from a cyber event

Differences include*:

- Financial Institutions could see the event coming giving time to prepare prior to being effected
- All Financial Institutions affected symmetrically by the event
- All supply chain entities were affected symmetrically by the event

* Preliminary, non-exhaustive list

Technology and Cyber Risks in the context of COVID-19: Impacts

The unprecedented and rapid global shift to remote working due to COVID-19, as well as the significant increase in market volatility/trading volumes, amplify existing technology and cybersecurity risks.

Impacts to Technology and Cyber risks include*:

- Greater vulnerability to phishing attacks by overstretched employees working in new environments
- Increased adversary scanning on internet facing infrastructure
- Increased requests for exceptions to previous prohibitions such as printing at home or USB rights
- Managing processes that previously required physical proximity such as onboarding and renewing hard tokens for two-factor authentication
- Rapidly build and shift to remote working and increased dependency of remote working IT infrastructure
- Supply Chain resilience: Country Risks
- Work-life balance (e.g., virtual classrooms, child care)
- Increase in working from home with limited supervision, including for employees previously restricted to office access only

* Preliminary, non-exhaustive list

Technology and Cyber Risks in the context of COVID-19: Actions

Actions which address these risks enable businesses to develop new ways of working, which can be leveraged in the longer term, where appropriate.

Actions which address these impacts include* (1 of 2):

- Increase external threat monitoring (regardless of evidence of successful cyber attacks)
- More frequent vulnerability and configuration scanning on internet-facing environment
- Heighten internal communications on increased cyber/phishing threats; Provide employees with verified links for pandemic information
- Provide guidance to staff on home working set up (e.g., firewall security settings, disable IoT, clean desk)
- Communicate / train managers on importance of and tips for remote supervision
- Quickly take action to contain new risks, such as an increase in the use of new collaboration tools such as Zoom or increase in remote printing
- Provide a robust framework for approving exception requests and strong controls on use of new platforms (consider ability to chat, whiteboard and communication retention requirements)
- Monitor print actions including volume and frequency to identify odd patterns
- Create process for holistic, retroactive review of exceptions granted during pandemic

* Preliminary, non-exhaustive list

Technology and Cyber risks in the context of COVID-19: Actions (cont)

Actions which address these risks enable businesses to develop new ways of working, which can be leveraged in the longer term, where appropriate.

Actions which address these impacts include* (2 of 2):

- Provide employees with resources for mental wellbeing
- Ensure resilience across remote working infrastructure with a fail over strategy across and/or within regions
- Implement change freeze when needed to ensure focus on rapid scaling of remote working capacity and maintain system stability by limiting non-essential changes during times of high volatility
- Heighten monitoring of critical applications and batches
- Pro-active engagement of critical third party suppliers to validate their operational and financial resilience

* Preliminary, non-exhaustive list

Preliminary Lessons Learned from COVID-19

Response to COVID-19 across the industry reinforced the importance of a number of key practices and highlighted both strengths and areas for improvement for many firms in risk governance, corporate culture and technologies that need to be addressed in the longer term.

Preliminary Lessons Learned include*:

- Increased horizon scanning capability and extreme scenario modeling (including what-if stress testing tools) are vital to assess tail end risk scenarios, such as pandemic or cyber, to understand organizational resilience and exposure
- Accurate inventory of assets (systems, 3rd parties, data) are essential to effective crisis response
- With the need for timely decisions following new requirements (such as printing at home or collaboration tools), risk governance bodies must have capability to address non financial risks in a global, cross-functional, timely & practical manner
- Resilience of IT systems are dependent on agility and commitment of IT and other staff; "Never waste a good crisis" and consider opportunities to increase capability for new ways of operating

* Preliminary, non-exhaustive list