SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

COVID-19 Decision Insight

Our thanks to all the COVID-19 frontline workers

Issue: Preparing for the Future - Adapting to the “New Normal” with COVID-19.

Contributor: Jeremy M. Baumann, CPP, SEC Subject Matter Expert, former Director, Enterprise Security, Discover Financial Services

Where this issue fits in the phases of the pandemic: Regional deceleration, Hot spots/flare-ups/next waves, Phased recovery, Intense monitoring and planned improvement.

Summary: The Coronavirus disease, COVID-19, has overtaken the globe and is causing unprecedented disruption in many aspects of life. Security Leaders, most of whom have been amid the fray, leading their top executives and organizations through this crisis, now need to refocus on planning for the future and preparing their organizations for what may come. The Spanish Flu of 1918 saw initial detection in March 1918 and two much more deadly waves - first in fall 1918 and again in winter and spring 1919[1]. Security leaders must consider similar circumstances to effectively prepare for the future. The few questions that follow serve to lead a contemplation to benefit this effort.

What is the new normal?

- What about our way of working has changed permanently and what will return to “old normal?”
- We’ve been viewing this as temporary; how could our business function in this mode for 6-24 months?
- How do we track those who have recovered and do these people have an immunity against the virus?
- Will these people with some immunity become “in-demand” human resources in a practical future?
- What are the challenges around immunity information from a health privacy and legal standpoint?
- How will sick people in the workplace be treated? Do we need employee awareness training for this?
- Do we need reporting hotlines for sick people; or for reporting symptoms observed in the workplace?
- Do we need to change to a new sick policy and benefit?
- How can we prepare for more resilient monitoring of staff for symptoms at home and campus entrances?
- Is using personnel to screen for symptoms viable/sustainable or is self-screening better at entrances?
- Are we monitoring Employee Assistance Program information for intelligence?

What has reviewing how we’ve handled the last few months tell us about what we should plan to change?

- What do After Action Reviews[2] of activities over the last 90 days tell us? Are we requiring they be done?
- Are we tracking metrics, cost, time spent and business impact to share with the business?
- What were the gaps in our intelligence, human resources, internal communications, decision making/management, record keeping, business and information technology, and finance programs?

[1] “1918 Pandemic Influenza Historic Timeline.” *Centers for Disease Control and Prevention*, Centers for Disease Control and Prevention, 20 Mar. 2018, www.cdc.gov/flu/pandemic-resources/1918-commemoration/pandemic-timeline-1918.htm.

[2] An after-action review (AAR) is a structured review or de-brief (debriefing) process for analyzing what happened, why it happened, and how it can be done better by the participants and those responsible for the project or event.

- What worked well, and where were our successes? How can we incorporate those more permanently?
- What internal and external stakeholders should we have developed a tighter cadence with?
- Are there additional resources that we should have had like staff, or other resources that were missing?
- What changes must we consider immediately to be successful should there be another wave?
- When should we have first briefed leadership about this issue? Do we have the credibility needed for this?
- How did some companies get so far ahead on this issue while so many others lagged?
- How do we identify those leading companies and incorporate their intelligence into ours?
- Were our Business Continuity Programs (BCPs) effective at managing our risk and 3rd party risk?
- Is BCP positioned effectively in the organization within a strong Crisis Management (CM) program? If not, what changes need to be made immediately to re-position these programs?
- Were BCP and CM team roles and responsibilities correct? Are teams too large? Too small?
- Were we able to communicate effectively to our crisis teams and to our employees? If not, what tools or processes need to be added now to bolster this gap?
- Were risks properly disclosed in our 10-K? What new disclosures do regulated companies need to make given impacts related to this crisis and anticipating future uncertainty?
- What corresponding internal changes need to happen and be disclosed to show we are being responsive to this new risk? How can we show the business value of these changes?
- Have we effectively tracked all COVID-19 costs? Are there government relief programs can we leverage?

How has this crisis impacted my company and what changes do I need to be planning for proactively?

- How is my company impacted? Revenue? Supply Chain? Profitability? Taking on more debt?
- If revenues were increased because our company provided necessary goods/services, how can we act appropriately now to leverage this to make much needed enhancements?
- If revenues declined, how can we accelerate proactive changes to reduce our expenses without impacting Security service delivery? Are there investments in technology we can make to reduce future expense?
- How can we reset our team goals to meet these new challenges? How does our program vision change?
- What questions will our Board of Directors be asking company leaders? How will we answer these questions? Have we located and reviewed available resources to prepare for these questions?[3]
- What will our recruiting efforts look like based on assumption that a percentage staff will not return?
- What type of mental wellness checks are we conducting on staff as they return?
- What new risks have emerged that we need to account for? Supply chain, counterfeiting, fraud, domestic violence? Do we need an external risk assessment? What new vendors might we need to onboard?
- Did we have impact that should have been foreseen? Are mitigation strategies defensible? What improvements need to be considered to show we are responding and preparing effectively?

These questions and others like them should be considered by Security Leaders, their teams, their peers and their stakeholders. Seeking proven practice is more important now than ever. Time remains a most precious commodity. If there is a second, more impactful wave, will we wish we had spent our present time more effectively preparing for it?

Contact us if you need assistance in COVID-19 strategic planning, response or recovery at contact@secleader.com

[3] "Assessing Management's Effectiveness in Responding to the COVID-19 Crisis: A Quick Checklist for Boards." *Home*, 2020, www.nacdonline.org/insights/publications.cfm?ItemNumber=67340.