SEC

Security Executive Council

A research and advisory firm

COVID-19 Decision Insights

2020 - 2021

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

About This Resource

From the very beginning of the COVID-19 crisis, Security Executive Council staff and faculty worked to provide actionable guidance, information sharing, corporate security-specific research, relevant strategic insight, and access to tools to help security leaders protect people and assets in the unprecedented new global risk environment.

Early in 2020, the SEC created a special COVID-19 landing page on www.securityexecutivecouncil.com that linked to all these new resources for easy access from the security community. Now, we've compiled them into two downloadable resources: **COVID-19 Resources** and **COVID-19 Decision Insights**.

COVID-19 Resources includes pandemic-related security checklists, visuals, research results, slide decks, guidance documents, and collective knowledge.

COVID-19 Decision Insights is a collection of short articles created by SEC faculty to address questions they heard from security leaders every day through the height of the crisis.

While the resources in these compilations were created to apply a specific pandemic event, their message is ever relevant: corporate security leaders have the crisis management experience, 24x7 presence, and tools to help lead their organizations with agility through uncertain times. And it's those moments between crises when corporate security must be diligent in using its resources to improve cross-functional teams and creative solution-building to prepare for the next round of the unexpected.

The Security Executive Council stands ever-ready to help its clients and the security community as a whole weather the crises to come. For more information, contact us or visit https://www.securityexecutivecouncil.com/about/overview today.

Contents

Multi-national Corporations with Operations in India – Considerations for the Next Phase of the Pandemic........ 4

Measuring Security Risk and Response to COVID-19 6

Access Control, Contact Tracing and Unified Risk Oversight 9

Cyberattacks Resulting from COVID-19 - Information Security Risks 12

Preparing for the Future - Adapting to the "New Normal" with COVID-19........ 14

How has COVID-19 Changed the Threat/Risk Register at your Company? 16

How will COVID-19 Inform Your Future All-hazards Resilience? 17

COVID-19 Decision Insight

Issue: Multi-national Corporations with Operations in India – Considerations for the Next Phase of the COVID-19 Pandemic

Contributor: Dan Sauvageau, SEC Subject Matter Expert, former Chief Security Officer, Fidelity Investments

Where this issue may fit in the pandemic scheme: Regional Deceleration – Overseas Operations

On March 24th, India's Prime Minister, Narendra Modi, ordered a 21-day lockdown for its entire population, appx 1.3 billion people. Unlike more developed countries coping with their own struggles posed by shutdowns, India is further challenged by having limited critical infrastructure, health care services, and emergency first responder services. Unless PM Modi extends the lockdown, it is set to end on April 14th. Exactly what a re-opening would entail remains unknown.

Multi-national corporations (MNCs) have a lot to gain or lose from how quickly and effectively their operations can return to normal. With four times the population of the U.S. and known for high levels of corruption, poverty and poor infrastructure, India will likely be faced with even greater challenges than the U.S. when it comes to this pandemic. Security leaders and their risk mitigation colleagues must figure out how they will assess, prepare and respond to India's attempt at resuming normal operations weighing all these factors in their decisions while safeguarding their associates, expatriates and workplaces. Please note that some of the items listed below may apply to MNC operations regardless of location while others are unique to the India operating environment.

Since MNCs have different operations, organizational structures and risk tolerances, there is no one size fits all approach. Below are questions and facts that may evoke thoughts, ideas and creative solutions to assist a security team in managing this unprecedented health and economic crisis.

Health/Security/Safety/Risk Management

- With limited public safety, law enforcement, infrastructure capabilities, the Indian government pushes much of the responsibility for employee safety and security to corporations. Is your company prepared to step up to overcome the shortcomings in all these areas to keep your staff safe in transit and at work? Now is the time to test ALL building and transport security devices, systems and procedures to ensure they are working.
- Companies rely heavily on contractors to support their operations such as housekeeping staff, food service, transport drivers, and security. Many are poorly trained, equipped and supervised. Ensure that your contract security providers have ample surge capacity should a number of people contract the virus. Insist that vendors step up their supervision of guards, drivers, housekeepers, etc., to ensure they are competent and properly performing their normal and any unique COVID-19 related duties.
- What controls are in place to ensure contract staff who live paycheck to paycheck are not showing up to work sick and infecting others?
- Do you have established, communicated and understood protocols should an associate be confirmed to have COVID-19? What if the virus is suspected or confirmed to have been in a building or neighboring office? Since cleaning is different from sanitizing - do housekeeping staff have proper instruction and tools to perform their duties? Are the chemicals they use safe? Guidelines, if any, and their enforcement differ from strict EPA ones found in the U.S. Are your supply chain subject matter experts informing procurement guidelines for CDC, WHO approved products?
- Will your company limit the number of employees in transports or at the office at any given time?

- If you plan to conduct temperature and symptom screening for associates entering the workplace, who will do that work? A healthcare provider, contract guards? Ensure they have the proper training and equipment to carry out these duties as they will be the front line of defense, keeping contagious people away.
- The use of office “tea boys” is common, but rubs against social distancing; will that service be suspended?
- If you have expats and families in India and the hospitals run short of beds, have you considered plans for if they get ill and need medical treatment? Do you have multiple vetted hospitals to choose from?
- Expats rely heavily on domestic help and drivers for their daily activities. Do you have processes and procedures in place to screen them for symptoms, so they don’t infect families?
- Protests or “Bandhs” can happen with little or no notice and can turn violent quickly. Is your transport, building or campus security up for the task if civil unrest erupts?
- What changes will be made to in-country travel practices when stay at home orders are relaxed?
- Are your visitor management and access control systems up to the task if health or law enforcement authorities request them for contact tracing of confirmed cases? This has been quite taxing for security staff in other companies across the globe: do you have extra staff available for this work that requires precision and speed?
- Consider the Security Executive Council’s GSOC and General Risk Mitigation Checklist that contains many risk mitigations actions you can consider now.

Legal Risk Mitigation

India has many laws and regulations that an MNC must comply with that are often difficult to understand and interpreted differently.

- Has your in-house or external Legal counsel been involved in all your pandemic planning response and management to date? Are they current with and keeping stakeholders informed of changes to laws, regulations resulting from the Governments COVID-19 response/measures?
- What are the implications of Force Majeure and contractual non-compliance both by the company and third parties, e.g., contract guards, transport and housekeeping? Companies share the responsibility for ensuring third parties properly compensate their staff for wages and over time. What additional challenges will result with the complexities and challenges brought about by the pandemic?
- What is the enforceability of foreign judgements and multi-jurisdictional contracts?
- Labor and employment (issues with wages, surplus labor and retrenchment) should be understood by the security team as needed/appropriate.
- Are COVID-19 compliance expectations being communicated with duty to report expectations?

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

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

COVID-19 Decision Insight

Our thanks to all the COVID-19 frontline workers
SEC

Issue: Measuring Security Risk and Response to COVID-19

Contributor: George Campbell, SEC Subject Matter Expert, former CSO, Fidelity Investments

Where this issue may fit in the pandemic phases: Hot spots, next waves, Phased recovery, Intense monitoring

COVID-19 has focused the world on metrics. We are bombarded every day with grim counts of victims, percentages of testing and other business and home front statistics. Your organization should be intimately involved with the overall corporate crisis management activities and, as such, you will need to be crafting a responsive set of measures for reporting on key areas of risk exposure and Security's planful response.

Until a suite of effective COVID-19 treatments or vaccine are widely available you need to focus on measuring Security's contribution to virus risk mitigation and remediation efforts as well as anything that promotes or threatens business resumption and continuity. We are seeing many of our colleagues leveraging the information from reliable public health resources to aid in decisions related to business re-entry/resumption, travel and plans for hot spot contingency plans. As you develop a tactic, program, or process in response to COVID-19, assign the appropriate performance measures for reporting.

Because this pandemic has driven significant work away from the traditional workplace into employee homes, businesses will be challenged to assess our legal and programmatic definitions of corporate duty of care. Within that new context, Security should be addressing how their company's approach to safety and a "secure workplace" should be measured and what metrics should be reported. Some of the ideas you will see in the Security measures below go to our simply trying to measure what issues are being raised to level of measurement and reporting. If they previously have seen something suspicious in the office or factory floor, there was a protocol for reporting (''see something, say something"). We now need to know if there are threats and issues that impact our people and business operations in this new venue called home.

Since this crisis demands teamwork, a collaborative approach is essential for building a responsive set of actionable metrics with your HR and governance colleagues as well as business stakeholders. Many of the following fall into that enterprise-level profile. Finally, this is a financial crisis presaging a recession. The pressure is on every business element to demonstrate how it is directly contributing to the bottom line. Security's value metrics have never been more critical to our people and programs. When you demonstrate that a safeguard Security employs is directly preventing or measurably contributing to the protection of critical assets, tell the story.

ENTERPRISE MEASURES FOR COVID-19 RISK DRIVERS

- % of total workforce tested positive
- % of daily or weekly increase/decrease in workforce reported cases and fatalities
- % of essential workforce tested positive and unavailable
- % confirmed capability for local testing (local on-demand testing)
- # of key executives and key personnel tested positive by location
- % of sites with established local protocols to assure timely availability of reliable public health information
- % of required PPE available per site for approved duration of operations
- in-house operations (e.g., Security guards, cleaning, IT) audited for compliance with communicated guidelines

- % trend increase in EAP calls and by category –depression, attempts of self-harm, suicide, victim of domestic violence, substance abuse, anxiety.
- # of staff, visitors, contractors denied access due to COVID-19 symptoms screened at workplace entry locations
- Days facilities remain operational without COVID-19 incidents or outbreaks
- # of domestic and international business trips deemed essential
- # of essential on-site vendors (e.g., data center, housekeeping, facilities) tested positive
- # of special disinfecting cleaning incidents from suspicious COVID-19 incidents
- # of social media comments posted by associates regarding COVID-19 work topics. Number of negative and positive comments.

SECURITY MEASURES FOR COVID-19 SECURITY RESPONSE

- % of Security staff hours directly linked to COVID-19 response
- # of sources monitored by the GSOC or Security teams to maintain authoritative and actionable COVID-19 risk reporting for management
- Month over month % increase in advisories, alerts and warnings issued by the GSOC directed to COVID-19 risk management operations
- # approved home-based business applications compromised and investigated and % with successful closure per reporting period
- # Business applications loaded by those working at home that contributed to a breach or caused a risk event
- # security-related issues reported by remote workers per reporting period
- # of at-home work infosec and physical threats identified and % of confirmed for mitigation per reporting period
- % of remote workforce PCs, laptops and mobile devices with endpoint protection including VPN tools and encryption
- # domestic violence or restraining orders reported to law enforcement and/or Security by at-home employees per reporting period
- # employee residential physical and logical security enhancements requested and performed per reporting period
- # of workforce notifications or alerts to address critical health and safety information
- # warnings or disciplinary actions taken per location to enforce communicated COVID-19 policy and guidelines
- % of threats from furloughed, laid off, or dismissed employees (including vendor employees) investigated and closed with positive results per reporting period
- % throughput capacity at facility/building entry points with tested safeguard countermeasures in place
- Month over month % increase/decrease in cyber-attacks- all sources
- % of incoming mail and packages being screened and treated per site
- % of owned spaces (by site) prepared consistent with guidelines for re-entry and approved operations
- % of leased space confirmed as meeting guidelines for re-entry and approved operations
- % of primary and back-up COVID-19 on-site protection team staff trained and available
- % of required plans in place and tested for crisis team response to a confirmed contamination in the workplace.
- % of key GSOC/other critical response Security personnel with trained and available back-up
- # COVID-19 phishing emails reported by remote workforce
- Call trends to GSOC for COVID-19 related issues
- % of shift coverage gaps for contract security due to COVID-19
- Call trends for employee confidential hotline regarding COVID-19
- Increase of contractor overtime due to COVID-19 illness
- % change in number and types of reported security and safety incidents assignable to COVID-19
- % of data loss prevention alerts and origin (home or office)
- Total time it takes to respond to health official contact tracing requests

- Number of systems and applications used to complete contact tracing
- Number of security spot checks of housekeeping cleaning protocols. Number of infractions found, or behaviors corrected.
- % of at-home workforce who have acknowledged security policy and procedures for remote work
- Identify where Security operations have been modified, scaled back, and reduced in response to COVID-19 with direct impact on “must” do mission operations

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

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

COVID-19 Decision Insight

Our thanks to all the COVID-19 frontline workers

Issue: COVID-19 Technology Innovations: Access Control, Contact Tracing and Unified Risk Oversight

Contributors: Neil Johnston, SEC Subject Matter Expert, former Senior Manager of Security Technical Operations, The Boeing Company and Francis D'Addario, SEC Subject Matter Expert, former VP Partner and Asset Protection, Starbucks Coffee

Where this issue may fit in the pandemic phases: Phased Recovery, Intense Monitoring

Summary: Operational health, safety and security innovation is alive and well with COVID-19; as automated, frictionless (touchless) access control and infection contact tracing are added to unified risk oversight opportunities[1]. Optimized capabilities to meet evolving Duty of Care brand expectations remain a primary driver. Global risk and safety/security operations centers (GROCs and GSOCs) are gearing up for continuously improving situational risk intelligence capabilities to meet COVID-19 and other global hazards. See World Economic Forum 2020 Global Risk Report[2].

Privacy concerns, voiced from those who worry about government and private-sector over-reach and the very real perceptions of "big brother/big sister" espionage, will closely follow. Mobile app contact tracing featuring "voluntary" privacy features are being perfected by tech firms including Apple and Google's joint solution offer[3]. MIT and other university laboratories are weighing in.[4] Security leaders and their cross-functional teams (e.g., HR, IT, Legal, Ops) must be fully informed for benefits and risks of all solutions. Transparently communicating the issues/opportunities, diligence, and surveying our cross-functional teams will help. Proven protocol testing will be key. Considerations will include:

Access Control

Adapting and modifying current technology supplemented with COVID-19 temperature checks or validation of test results.

Returning to the workplace and use of access control could include:

- Use access control only on exterior doors.
- Consider for non-sensitive areas to leave interior doors propped open, evaluating risk of not having data on those doors. It is important to still meet fire codes requirements
- Turn off dual authentication where you can reduce infection with less surface touching such as pin pads and fingerprint readers.
- Control exterior access to the building by locking all doors; requiring contractors, employees and visitors to only access doors that are staffed with officers to conduct or oversee temperature checks prior to allowing access to the building.
- Use existing video software but consider adding infrared cameras for temperature checks if cost is not a detriment.

[1] https://www.securityexecutivecouncil.com/spotlight/?sid=31750
[2] World Economic Forum 2020 Global Risk Report https://www.weforum.org/reports/the-global-risks-report-2020
[3] https://bgr.com/2020/04/27/coronavirus-news-apple-google-contact-tracing-app-wins-in-europe/
[4] https://pact.mit.edu/

The new normal, business case support for frictionless access control:

- Biometric access control solutions verify the identities of people entering a building or other defined area. Organizations have been moving in this direction over the last several years, now we can mitigate virus infection transmission with technologies including touchless fingerprint matching, retina scanning, and facial recognition.
- Quality biometric access control systems can provide reduced exposure to COVID-19 by:
  - Confirming identities quickly and accurately, even in low light levels and darkness.
  - Tracking multiple faces simultaneously to ensure all people are authenticated before entering a protected area.
- Frictionless biometric access control facilitates faster identification so that employees, contractors, guests and other building occupants can be processed quickly and enter securely. This is especially important in high traffic buildings.
- Biometric access control is a people, process, technology approach widely used among industries such as aviation, financial services, healthcare and manufacturing. Applications include:
  - Aviation enterprises rely on biometrics to verify identities of people entering tarmacs, air traffic control towers and restricted areas of airports.
  - Corporate applications for biometric access control for verifying the identities of people who attempt to access data centers.
  - For healthcare, highly vulnerable personnel (patients, staff and visitors) and assets from controlled medications to confidential medical records are protected.
  - Biometric technology can also be used in time management and payroll optimization.

No doubt, next generation service and technology roadmap requirements will be further informed by pandemic innovation demand. Deploying more autonomous devices to preclude infection may enable long sought, cloud-based, data aggregation and anomaly detection opportunities. For example, smart acoustics in public lobby and other spaces may enhance video facial and voice analytics for hands-free access while providing blast, glass break, gunshot or raised voice threat recognition. Similarly, infrared temperature sensing and prohibited device or weapons detection may evolve concurrently. Fixed and mobile device app integration and interoperability will allow smarter, remote all-hazards protection monitoring once privacy concerns are addressed.

Contact Tracing

Change management, transparent communications, testing, and training are required.

- Automated contact tracing, like frictionless or touch-free access control, can be optimized by mobile applications when diligently vetted by cross-functional compliance teams.
- Bluetooth, global positioning systems (GPS) and other features detail network and personal device proximity to help trace infected personnel.
- If organizational or statutory compliance requires illness reporting, tracing, and or tracking, communicate requirements transparently with frequently asked questions and feedback loops to help ensure fluid policy or guidance change management.
- Existing health, safety and security apps may suffice in lieu of other requirements when GPS protocols are leveraged to produce an informative itinerary trail
  - Risk mitigation teams are reintroducing existing apps for additional opt-in subscription
  - Investigate low cost apps like LiveSafe to allow all-hazards reporting
- Health, safety, and security concerns should ideally be aligned and balanced within the context of potentially conflicting cultural, compliance, and regulatory expectations. Focus groups help.

- Less automated and potentially less integrated approaches to contact tracing include access logs, calendars, diaries, shift deployment schemes, time and attendance systems.
    - Some nation states may require health tracing apps that could be leveraged for espionage. Solicit cyber security team subject matter experts for app benefit/risk evaluation [5]assistance.

Unified Risk Oversite (URO)

Ensure that all-hazard risk mitigation, practices, protocols, systems, and technologies are subject to cross-functional leadership compliance oversight.[6] Governance scrutiny for change management, cultural alignment, regulatory compliance and under-anticipated vulnerabilities is always prudent.

Traditional compliance operating silos must be overcome to manage pandemic and other widely anticipated global risks. Regardless of people, process, and technology risk mitigation choices, continuously improving cross-functional teams will continue to drive all-hazards awareness and next generation innovation solutions. Data-centric, common operating practices will inform defensible strategic and tactical decisions; but organizational culture, vision, mission, and values will determine collaborative objectives and performance requirements.

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

[5] https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

[6] https://www.securityexecutivecouncil.com/spotlight/?sid=26462

COVID-19 Decision Insight

Issue: Cyberattacks Resulting from COVID-19: Information Security Risks

Contributors: Herbert J. Mattord, PhD, SEC Subject Matter Expert, Professor of Information Security and Assurance, Kennesaw State University and Keith Jones, SEC Subject Matter Expert, former CSO for The Charles Stark Draper Laboratory, Inc.

Where this issue fits in the phases of the pandemic: Hot spots, flare-ups, next waves, business resumption

Summary: Security leaders and other stakeholders can have a positive impact on employees and the workplace by considering and implementing risk control and mitigation techniques designed to protect computers, technology, and the company brand.

Many employees have been sequestered with shelter-in-place orders with little notice (and if fortunate enough to still be employed) are working remotely. Given the situation we are all in, security leaders can mitigate risk by evaluating, identifying, and improving their information security policies to counter the aggressive actions of cybercriminals and advance persistent threat (APT) groups taking advantage of the COVID-19 pandemic. According to the Verizon 2019 Data Breach Investigations Report (https://enterprise.verizon.com/resources/reports/dbir/):

Threat actors consist primarily of three types - and involve the corresponding threat actions that are focused on data breaches:

1. **Actors external to the company**: Account for ~ 65% of data breaches (social engineering, accessing unsecured networks, physical theft, or data exfiltration).
2. **Actors internal to the company**: Account for ~ 30% of data breaches (insider and privilege misuse, ignorance of policy existence, physical loss, or data exfiltration for unauthorized use).
3. **Partners of the company**: Account for ~ 5% of data breaches (negligence, data misuse, malicious intent, or accidents).

Alarmingly, the report also highlights that 56% of breaches had long periods of activity taking months or longer to discover. Prior to the pandemic, some companies implemented well-defined and mature information protection controls. These controls include multi-factor authentication, end-point protection, unified threat management, VPN connectivity, data loss prevention), and security event and incident management (SEIM). Many also have implemented bring your own device programs that provide partitioned and controlled access from personally owned hardware. The most mature companies maintain security operations centers (SOC) or global security operation centers (GSOC) to monitor, detect, and respond to cyber incidents.

However, some organizations have implemented only a few of these controls. Meanwhile, cybercriminals and APT groups have done everything but shelter in place; they are moving boldly across the globe at internet speed while actively taking advantage of the COVID-19 pandemic to gain access to companies sensitive, proprietary, and customer information. A recent FBI report stated that "Scammers have used websites and mobile apps to implant malware to steal financial and personal information. Other criminals have used COVID-19 as a lure to deploy ransomware for payments." (https://www.fbi.gov/news/pressrel/press-releases/fbi-and-secret-service-working-against-covid-19-threats).

Technical systems, even if equipped with all the “best-in-class” cyber defenses, are still vulnerable to cybercriminals who will leverage social engineering to compromise information technology resources and the information contained within. The best hardware and software cannot prevent people from being helpful on the phone, responding to emails they think come from their superiors, or clicking on a link and infecting their or the company’s computers. The following recommendations should be considered now to minimize risk:

- Have a well-defined cyber-attack response plan that can be immediately implemented and acted upon. Given many labels, this is often called an incident response plan.
- Implement an augment awareness program; send policy and rules reminders to all employees regarding the use of information technology resources provided by the company and, if applicable, personally owned devices.
- Update and invigorate your end-point protection so that malware/virus scanning software is operating in all resources used for business purposes; this may require employees to connect to your network overnight, so that each device can be scanned, and patch management upgrades can be provided. This should be done periodically, or upon detection of a significant vulnerability.
- Give detailed instructions for the use (or restriction) of videoconference platforms such as Zoom and other online teleconference center services. Consider allowing only signed-in users to attend, turning off file transfer, locking the meeting, and requiring unique passwords for each meeting to reduce the chances of hackers eavesdropping on private sessions; not doing so is an easy path to corporate espionage.
- Increase network monitoring consistent with the threats facing your industry; update and dial up the sensitivity on every technical control system and augment staff accordingly.
- Provide education and training regarding phishing, social engineering - especially business email compromise using typo squatted domains, common attack vectors, or vectors that are specifically targeting your industry. Employees must be reminded to be cautious of all emails and text links. They should be required to examine the full content of a message looking for anomalies before opening or clicking. Remember: the best IT systems cannot prevent a person from clicking on a link that can compromise your or your customer’s intellectual property and tarnish your companies name.
- Require employees to report any suspicious or anomalous activity related to any computer used for business purposes. Increase the degree and sensitivity of your SEIM logging as well as additional staffing levels at the call centers to enable highly vigilante responses.
- Contemplate cyber and ransomware insurance policies to cover losses, notification costs, credit monitoring, defending claims from customers and applicable regulators, as well as any fines or penalties.
- Implement mandatory and frequent password changes and specify complexity requirements.
- Ensure your call center and SOC/GSOC are fully staffed and ready to respond to, or escalate, a cyber-incident.

We recommend you collaborate, now, with stakeholders in IT, Legal, Audit, and perhaps others, to understand the capabilities you currently have in place. Then, identify any gaps and corresponding actions you can implement short-term that can reduce or prevent the risks such as outlined above.

Once the dust has settled, and things get nearer to a steady state, it will be time for an after action report. This should be a thorough macro-level, wide-area review of your information protection game plan. If that litany of technical control options we rattled off at the top of this article sounds like geek technobabble, you need to get your IT and InfoSec leadership in to explain why these features are missing from your environment. Ask some tough questions but be ready for the tough answers. You may find that insufficient resources or inadequate investment may have adversely impacted your organization’s ability to reduce risk when it mattered most.

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

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.

COVID-19 Decision Insight

Our thanks to all the COVID-19 frontline workers

Issue: How has COVID-19 Changed the Threat/Risk Register at your Company?

Contributor: George Campbell, SEC Subject Matter Expert, former CSO, Fidelity Investments

Where this issue fits in the phases of the pandemic: Global transmission (pandemic)

Summary: In one form or another, most Security executives maintain a risk register as a tool to identify, assess and manage risk to acceptable levels. COVID-19 is diverting everyone's attention has become a risk multiplier. We must not lose sight of our mission and pay attention to how current events are morphing the probability of threat and risk from internal and external adversaries. In your organization, how has likelihood morphed by adversary source, location, critical process/asset or other vectors? Consider the following list, probe considerations with your team and your key stakeholders and then build this list to suit your unique organizational risk environment.

- Key skills and competencies in the global risk mitigation team permanently or temporarily lost
- Diversion of skilled resources and priorities to address immediate COVID-19 implications
- Increased levels of individual stress coupled with furlough or lay-off incent insider threats
- Outright elimination or reduced external response resources
- Perceived areas of reduced levels of protection provide incentive to adversaries
- Assets outside the envelope - remote access without tested and resilient remote safeguards
- Inability or limited ability to respond in time and with requisite internal resources to risk events
- Lapses in adequate vetting of temporary workers
- Ability of less sophisticated attacks to penetrate established safeguards undetected

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

COVID-19 Decision Insight

Issue: How will COVID-19 Inform Your Future All-hazards Resilience?

Contributor: Francis D'Addario, SEC Subject Matter Expert, former VP Partner and Asset Protection, Starbucks Coffee

Where this issue fits in the phases of the pandemic: Phased Recovery

Summary: Security leaders and their operational risk mitigation colleagues learn valuable lessons from rigorous after-action reviews. Importantly, brand reputation and stakeholders agree that risk mitigation confidence relies upon continuous improvement. COVID-19 after-actions will continue to inform our balance for a steady state readiness and fast-follow resilience. The evidence that most companies, governments and other institutions were/are relatively un-prepared seems inevitable. Analyses and books will be written, yet critical catastrophic events loom. The World Economic Forum Global Risk report warns that other catastrophes are increasingly likely. Our questions going forward must probe beyond what worked and what didn't in the response to COVID-19. The answers and critical few prioritized adjustments are within our grasp right now and for the months to come. Most importantly, they will likely yield the highest value for future all-hazard continuity and resilience. We are inclined to offer full marks for heroic ingenuity and work arounds. Those must be celebrated if not rewarded. How we work them into our planning, automate and scale for continuous improvement for lasting value remains the opportunity. Let's ask…

Was a pandemic equivalent to the magnitude of COVID-19 properly forecasted in the company's 10K or risk plan documentation? How might we improve or better align mitigation services against future board level risks?

- Was the corporate crisis management team the right mix of talent and leaders? Were they properly exercised in the past to build muscle memory to tackle this crisis? Were they stuck in their silos and not benefitting from open collaboration and creative problem solving?
- Was business risk intelligence properly deployed to identify pandemic-relevant impacts as it emerged over the horizon? Are our resources adequate, agile and redundant?
- Were environmental health, safety and security needs properly anticipated and provisioned? How might ae cross-functional team help facilities and supply chain to improve readiness for any catastrophic event?
- Was risk mitigation acumen and competency sufficiently available and distributed to inform or advance the plan on a global and regional basis? If not, is this an individual talent, organizational, service or training opportunity?
- Was the systems/technology tool-box good enough to communicate planned changes, monitor critical facility access or flex to new operational requirements? What solution innovation tools including APPs might have cost effectively improved our competencies?
- Were performance assessment tools or value metrics automated, robust and timely to inform decision makers? If not, what was adapted or adopted?
- What services or technologies might have been better arranged or contracted in advance for critical processes or oversight redundancy

- What dependencies on private/public responders require renewed or revised efforts contractually, or by service level agreement, to meet or exceed new performance expectations?
- Was your public/private network up to the task and robust enough to reach out to when needs arose?
- Were your internal business partnerships established and the capabilities, services and trust of the security team know ahead of the crisis to best be leveraged?
- What are the benchmarked proven practices?

Resources: World Economic Forum Global Risks Report 2020

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