SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

COVID-19 Resources

2020 - 2021

Selected Highlights

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

SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Phases of Pandemic

with Action Items for Security

1 No detected transmission

- Regularly review business continuity plan
- Align roles/responsibilities of Incident Management Team
- Conduct tabletops with internal and external resources
- Conduct research on risk likelihood and preparedness
- Inventory pandemic preparedness essentials
- Build/strengthen relationships with public health agencies
- Develop expat playbook and update crisis evacuation plans

2 First human transmission

- Notify Critical Incident Management Team
- Gather reputable situational awareness sources
- Engage company communication resources
- Track incidents
- Gather situational risk intelligence

3 Isolated transmission

- Stand-up Critical Incident Management Team
- Business impact analysis
- Business travel analysis
- Supply chain disruption risk analysis
- Develop work from home procedures and communication
- Analyze stakeholder impacts
- Acquire adequate PPE and cleaning/disinfectant supplies

4 Continental transmission

- Stand-up 24x7 GSOC support
- Decide thresholds for restricting travel and closing sites
- Visitor controls
- Evaluate essential services contracts to ensure they meet new guidelines of standards of care for their employees

5 Global transmission

- Build/strengthen relationships with public health agencies
- Document "essential workers" exclusion requirements for individual countries and states and link to plans
- Coordinate temp/symptom screening logistics
- Stagger workforce and create additional space to ensure redundancy of essential services

6 Regional deceleration

- Define thresholds for reopening
- Business resumption/modification planning
- Office re-entry procedures and communication
- Travel resumption/modifications plan
- Secondary infection monitoring
- Define cleaning, sanitization, disinfection, and QC procedures per govt or health agency guidelines
- Communicate to C suite the capabilities of existing security technology for social distancing, contact tracing
- Work with leased property managers to understand/influence their cleaning protocols

7 Planning for the new normal

- Survey constituencies and ask for thoughts and concerns about reopening
- Coordinate with HR to define or support security and safety plans for remote workers, incl. domestic violence, mental health, emergency response
- Re-evaluate risk transfer and mitigation strategies
- Communicate revised safety and security support, guidelines and requirements
- Conduct community readiness assessments to determine whether governments and schools in site locations are prepared

8 Phased recovery

- Access insurance & government relief programs
- Hire/recall staff from furlough
- Supply chain disruption risk analysis
- Commend company frontline workers
- Qualitative/quantitative cost analysis

9 Intense monitoring

- Monitor for reoccurrence
- Survey stakeholders for recommendations
- Address preparedness and competency gaps
- Maintain a Contagious Illness Working Group made up of business unit leaders and executives

Throughout All Crisis Phases

- Document lessons learned and actions taken
- Document technology and resource investments that, had they been in place, could have eased or assisted in managing the crisis

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

COVID Work from Home Guidance

Considerations for Security Leaders

Introduction

The COVID 19 pandemic caused many companies around the world to shift from conducting work on company premises to almost entirely a work-from-home (WFH) environment in a matter of weeks. While some companies allowed small numbers of employees to WFH periodically or permanently prior to the pandemic, the notion of full-time teleworkers across all industries and the globe was a first in human history.

Because of this, the term “workplace” has taken on a whole new meaning. For today’s teleworkers, a “place of work” can be wherever they are at the moment, whether at home, in a vacation home, at a café, in an RV, or wherever they ideally have secure VPN internet access to their work files, colleagues or clients.

The expansion of the WFH dynamic introduces new and increased risk to the organization. It requires modification of behavior and demands flexibility from all concerned. Understanding what has changed, adopting new processes, observing new policies and meeting new requirements—all while meeting business objectives—is a challenging adaptation that many organizations and individuals will be called upon to execute.

In this paper, we will outline how the WFH environment may be impacting organizations in a variety of risk categories.

Communications and Training

By Jim Hutton

Arguably, the most important aspect of addressing the risk management elements of a work-from-home scenario is communications. Messaging and electronic exchange between and among employer and employees, vendors and suppliers, customers and prospects, and family and friends take on more importance in the absence of face-to-face engagement.

Employers and employees need to redouble their efforts at creating or modifying clear channels of communication to identify and manage exposures and risks in this new employment scenario. Particularly important will be those processes related to alerting, coordinating, and responding to threats and incidents.

To help ensure full communications support for teleworking employees, organizations will be well-served to validate processes and tools such as

- Alert lines
- Ethics and compliance hotlines
- 7x24 communications
- Dispatch functions
- Alarm and broadcast capabilities
- Monitoring technologies

All these should be reviewed to ensure interoperability and efficacy within the work-from-home environment.

GSOCs will play a critical role in communicating with teleworking employees by continuing to provide travel advisories, weather monitoring, alarm response, access control and executive protection support activities.

The velocity of changes in policy, process and workflow in the new environment can be daunting. Organizations must leverage technology in new and creative ways to ensure that appropriate notification, training, and compliance requirements are addressed, presented and understood by a dispersed audience. Paramount among these messages are instructions and guidance on both emergency and routine processes. Organizations can leverage virtual platforms to communicate with employees regarding training, certification and assurance programs, and life safety programs.

Physical Security

By Jim Hutton

While the organization's workplace-centric demands such as food service, parking and HVAC may diminish in a dispersed worker scenario, certain core physical security activities remain vital to reducing risks to the organization. Life safety systems, alarms and surveillance technologies and personnel and property protection systems remain pillars of enterprise risk reduction.

Appropriate staffing levels should be maintained to operate and maximize the risk management infrastructure. Regular preventive maintenance should be continued, or perhaps accelerated – especially those potentially disruptive projects that always seem to be deferred. Maintain a robust and agile liaison with property management teams as well as public safety officials.

Many of the considerations listed above may need to be extended to alternate work locations and homes as well. Responsible staff should ensure that employees working from home are able to access company tools, technologies, and counsel appropriate to emerging exposures presented by their new work setting. Education campaigns or refresher opportunities should be made available to extend a level of protection consistent with the organization's risk appetite.

Pay particular attention to the nature of activities teleworkers will be conducting off-site.

- Does the work require ergonomic support?
- What first aid and medical resources are available?
- Are additional physical protective devices required to minimize the exposure to workplace violence scenarios?
- Will business appointments or small groups require health and hygiene protocols?
- What are the requirements for secure storage of documents, samples, prototypes, etc.?
- Are home-based network requirements adequately protected? (More on this in **Information Protection and Recovery.**)

In sum, responsible organizations will need to re-think the physical security boundaries of risk mitigation that have traditionally been defined in duty of care and safe and healthy workplace requirements. Enlisting the employees in an awareness campaign to jointly identify and manage these areas will maximize available resources and demonstrate commitment to a safe and healthy organization.

Investigations

By Jim Hutton

Fact-finding, assurance, due diligence, employee relations and compliance investigations must now be conducted in a new paradigm.

In a dispersed work environment, investigations may be hindered by intermittent availability of information, evidence, exemplars, witnesses, and technologies.

This new investigative landscape demands renewed and perhaps modified policy and procedures. The organization must examine and restate its expectations and requirements for investigations. Legal and Human Resources must be enlisted to calibrate and approve proposed approaches and the organization must anticipate and adapt to new legislative requirements and adjustments to best practices.

Changes and modifications to traditional processes should be highlighted and communicated to the workforce. Follow this up with training and validation, as necessary. A particular area of emphasis could be the restatement or inauguration of a "duty to cooperate" with an inquiry as part of the organization's renewed mission and values.

Organizations that are subject to inspection, audit, or validation by third parties need to consider how best to facilitate the ongoing investigative interface with these key partners. Understanding the updated protocols used by government authorities such as tax and inspection functions, law enforcement and regulatory agencies, and processes for external certification or operating licenses will facilitate timely, effective, and efficient outcomes.

Investigations may be challenged significantly by the work-from-home model; understanding the changes to traditional processes will limit exposure to litigation, fines, and disruption. This "new normal" may also provide an opportunity to examine the efficacy of historic practices, to evaluate new technologies, to audition new partners or operating models, and to restate what investigative outcomes remain critical to a healthy operating environment.

Business Resiliency and Continuity

By Dan Sauvageau

Let's explore some of the considerations and challenges that teleworking poses from a business resiliency and supply chain perspective.

For decades companies spent enormous sums of money to ensure their buildings were safe and secure and that business operations could run smoothly, efficiently, and uninterrupted when faced with crisis events. Investments were made to harden building infrastructure such as power, telecommunications, HVAC and computers systems to ensure backup systems were in place so that employees had access to the tools and equipment needed to run the company and service clients. In recent decades a new profession emerged where Business Continuity and Disaster Recovery professionals were hired, or dual-hatted individuals engaged, to conduct Business Impact Analyses (BIAs), drills and exercises to identify and mitigate threats to business continuity and build resiliency and recovery strategies into enterprise business operations and supply chains.

Since the COVID pandemic, the more immediate threats to business resilience come from the fact that much of the work across companies is being done at home without benefit of the robust, hardened, and time-tested infrastructure to support operations. Teleworkers share limited internet and Wi-Fi bandwidth with family members or roommates. Most don't have backup power generators and are solely reliant on Wi-Fi and/or cell towers for their communications. Moreover, teleworkers are often ill-prepared with basic food and supplies to manage through a natural disaster such as a hurricane, earthquake, wildfire, or flood. In past crisis events, many companies would proactively or reactively house critical staff in hotels close to the office. Due to COVID challenges, that may not be a viable or health conscious strategy.

Other traditional crisis and business resilience tools companies rely upon include critical incident tracking systems that geo-fenced their buildings, weather alerts, and employee mass notification systems. All of these are largely rooted on company premises as the primary workplace. Companies may want to consider helping teleworkers better understand and be prepared for crisis events that may impact their home office. A more prepared, resilient teleworker is more likely to return to a business-as-usual state than an unprepared person when confronted with a crisis. Ensuring one has essential living supplies, backup batteries to charge computers or phones to use as a hot spot when power or Wi-Fi are down will make them more able to address their personal and company needs during and following a crisis impacting their home and community.

This work-from-home (WFH) landscape also demands a renewed and modified look at how dependent companies are on critical suppliers and supply chains. Even the best prepared and resourced multi-national corporations have faced some challenges adjusting to the WFH paradigm. Some companies reacted and responded well while others still struggle to find their way or survive.

Think about your small but critical supplier. How prepared are they to deliver products, services, or support to your company in the face of a natural or manmade disaster with their employees teleworking?

- How financially solvent are your critical suppliers given the economic hardships posed by COVID?
- If their business is struggling to survive financially, how likely are they to cut corners to save costs? Would you even know before it's too late?
- Will their quality control suffer under austerity measures?
- If they anticipate a problem with their service delivery to your company or experience a breach of your company or customer information that jeopardizes their contract, will you be alerted in a timely manner, or at all?
- How would any of these potential scenarios impact your business operations, customers, share price, or brand?

Vendors and suppliers that are subject to inspection, audit or validation by your company's risk, audit, or Q/A teams should consider how best to facilitate their work in the WFH environment and with the limitations and economic challenges brought about by COVID. Refreshing BIAs of your operations and those of critical suppliers, and perhaps including non-traditional partner stakeholders as part of the BIA process, may be worth considering.

The challenges every company is forced to address in this new operating environment, whether it's their own internal operational readiness and resiliency or the limitations of their suppliers, partners or other stakeholders, is cause to evaluate old and new business practices, BIAs, SOWs and contracts. Not doing so could have a significant impact on your company's bottom line, brand, reputation, or even survival.

Information Protection and Recovery

By Dan Sauvageau

Safeguarding a company's sensitive or proprietary information while teleworking requires more care and attention from employees than safeguarding data in a company office. While security controls, culture and risk tolerance clearly differ across companies, traditional safeguards and measures are within reach of most companies, regardless of their size and resources. Such measures include:

- Physical ones such as access controlled perimeters/doors/rooms, CCTV, video analytics, visitor controls, shredders or secure bins, locking files and guard posts.
- Robust IT systems with controls to thwart intrusions, breaches, data loss and insider risk attempts to cause harm.
- Less visible controls such as background checks, clean desk policies, formal management and informal peer oversight of employee activities.

Apart from IT VPN and PC controls, virtually none of the measures listed above are applicable in a typical WFH environment. While some fastidious or seasoned teleworkers no doubt go to great lengths to protect information they work on at home, they are the minority. Think for a moment of likely WFH settings: active children afoot, students remote learning, family members, roommates and friends coming and going, and all the other distractions within a home compared to a calm, controlled, relatively secure office environment. The chances of information unintentionally being lost, shared, improperly disposed of, or unprotected are great. So are the opportunities for intentional misdeeds, such as theft by external parties or rogue employees looking for personal gains. How can employees and organizations protect information in such environments?

The topics and suggestions below can help protect information that a company's risk management team deems appropriate to send off-site with teleworkers. These suggestions are not intended for extremely sensitive or classified information that does not belong anywhere outside a company's secure offices, labs or classified working areas. If teleworkers feel the information they are taking home is too sensitive to protect, encourage them to consult with their manager, risk or security.

Education and Awareness. Companies use many different methods to differentiate between internal, sensitive, proprietary, trademarked, confidential and proprietary information. It's the responsibility of company management to ensure employees understand what information is sensitive and how to safeguard it when in use, at rest, in storage and in transmission. A company may remind teleworkers of their obligations to safeguard company information through a variety of methods including:

- E-mail reminders
- Screen pop-ups
- Awareness campaigns (October is National Cyber Security Month!)
- Messaged coffee mugs, mouse pads, post-it notes

- Periodic team/management meetings

Policy. It may also be prudent for a company to create a telework policy that clearly spells out the special circumstances and risks of working from home and an employee's unique responsibilities. (This policy would complement existing codes of conduct and ethics documents.) A telework policy would aim to ensure sensitive information has distinct methods of data and information protection in hardcopy or electronic form while considering a less controlled WFH environment.

Telework policies would also need to address any unique governmental laws, regulatory guidelines or mandates pertaining to information or data privacy, such as HIPPA, GDPR and other information protection acts that govern their company locations. Security leaders may want to remain current with changes, updates and court rulings on as the world navigates through this pandemic and its far-reaching implications.

Dedicated workspace. To the extent possible, encourage teleworkers to dedicate workspaces that are private and separate from highly active or travelled parts of the home to safeguard company information even more so in an environment of reduced controls.

Clean desk policy. Encourage teleworkers to clear desks and work surfaces. This will keep company information out of sight of casual home visitors, domestic help, and service and repair persons. This is especially important for employees who live with roommates.

Visual security. Keep PC screens and sensitive information out of the view of other occupants and ensure PC cameras used for video conferences don't have a field of view of sensitive information.

Lockable files. Keep work material in a lockable file or drawer separate from personal information or files.

Manage and appropriately dispose of sensitive documents. Encourage employees to eliminate or reduce the need for printed materials. If this isn't practical, require the use of a company-approved cross-cut shredder. If a printer is required for work at home, consider supplying employees with company printers to allow for greater control. This way if the printer requires servicing or reaches end of life, it can be effectively managed as a corporate asset rather than discarded and potentially retrieved by someone looking for sensitive information from its internal storage.

Computer security and controls. According to published reports by U.S. intelligence and law enforcement agencies, cyber actors are watching for opportunities to exploit the weaknesses created by the new COVID teleworkers. Simply put, it's much easier for cyber thieves to hack into hundreds of millions of less secure home computing environments than fewer, often better defended company systems.

Computer security controls for teleworkers will vary depending on many factors, including the size and resources of the IT department, whether teleworkers use personal or company equipment, hosted virtual desktops (HVD) or VPNs. Some of the more basic and fundamental considerations that are not beyond the reach of companies with limited IT security capabilities may include:

- **Phishing scam awareness**: Educate or re-educate teleworkers on the risks posed by phishing scams as well as how to recognize and avoid them. Remind teleworkers to promptly notify their IT department of phishing scams and other anomalies.
- **Safeguard passwords:** Just because teleworkers are in familiar settings at home doesn't mean they can become lax with passwords, leaving them exposed or systems logged on unattended, especially if the home has other tenants and visitors.
- **Avoid Public Wi-Fi**: Remind teleworkers of the risks posed by open, unsecured public Wi-Fi, especially as they tire of being confined at home and look to get out and change their scenery.
- **Avoid or protect local storage back-ups:** If teleworkers locally back up computer files in addition to or aside from the cloud, they must remember to properly safeguard those files.
- **Secure home Wi-Fi routers:** This will reduce the risk of unauthorized access to home networks. Also remind them to take care when joining or signing on to known Wi-Fi networks, as scammers can create similarly named systems to trick them into entering their password for capture.
- **Use only company VPNs to conduct company business:** Company VPNs will hide IP addresses, properly encrypt data, mask locations, and provide other essential controls.
- **Update anti-virus software**.
- **Avoid USBs:** Unless they are from a trusted source or company provided with password protection, USBs can be altered to upload malicious code or steal information. Companies may consider disabling USB ports on company-provided computers altogether to eliminate risk of introducing malicious code through them and to control data loss through their use.

Layer security for executives and key personnel. Due to their positions and access to sensitive company information, these individuals may require additional, heightened levels of controls in to their WFH environment. For decades, security executives spent considerable time identifying and assessing the risks to these groups of employees and designing and installing myriad visible and stealth security controls and devices around C-suites, private offices, and secure labs. Now and for the foreseeable future, many of these people will spend more time in home offices.

Most will not have anything close to the safety and security features they have in place while on company premises, not to mention a quick-response security staff. These individuals are the face of your company. They possess knowledge and access to valuable company secrets, client assets or sensitive strategic plans. They remain potential targets of disgruntled employees,

customers, violent activists, criminals, and competitive intelligence interests. The WFH environment with its fewer security safeguards requires security professionals to reassess the threats and risks posed to these individuals. Updating home risk assessments to take a fresh look at physical, operational, and technological risks and threats may be prudent, especially with the ever evolving and rapid adoption of technical and home automation tools.

Workplace Violence Mitigation and Executive Protection

By Dan Sauvageau

What implications does the new workplace have when it comes to managing and mitigating violence to employees or protecting executives?

For countless years, the strategies that companies employed to safeguard employees included measures such as gates, access-controlled doors, CCTV, staffed lobbies, mass notification systems, guards, and education. Executives were often surrounded with an enhanced level of physical and technical security features within the C-suite. Furthermore, companies relied on an educated and trained workforce to recognize and report early warning signs for potentially violent acts. Many companies tested their workplace violence plans and security systems with drills, exercises, internal partners and law enforcement agencies.

What is a company security team to do now that the employees they are supposed to protect are scattered across hundreds or thousands of homes that serve as their workplace? To what lengths does a company go to protect employees working away from traditional offices? What is the scope of their responsibilities and duty of care? At some point these questions will likely be answered through legislation or tested in court cases. Should a company wait for either of these occurrences or be proactive in considering how their workplace violence (WPV) policies, practices and approach may be altered to address a geographically dispersed workforce?

Internal threat assessors and WPV management teams, along with employees, will need to create or modify clear channels of communication to identify and report potential and actual incidents of threats and violence. Without traditional building controls and notification systems, new processes related to alerting, coordinating and responding to threats and incidents will need to be developed. Organizations may be well served to create partnerships with law enforcement agencies across communities where employees reside, rather than just with the few that have jurisdiction over a company building or campus. Education and training efforts will need to be reviewed and modified. Companies may need to reassess the responsibilities and expectations they place on employees when it comes to their safety in a WFH environment.

In addition to a broad programmatic review of their approach to WPV, companies will have to decide what to do when faced with known, imminent, or foreseeable threats to employees and executives. In the past, on company premises they may have increased security vigilance, guard patrols, or hire off-duty police to patrol a building or campus. Should those same measures be redirected to a teleworker's home or other remote work location? Does extending security protection to WFH locations increase or decrease a company's liabilities should something go wrong? Would it be preferable for a company to equip the targeted employee with safety tips and information or leave it to them to contact law enforcement?

Should security provide executives with some measure of security at their homes now, whether or not they did prior to the COVID pandemic? Given the amount of time executives are now

working from home and the increase in civil unrest and violence occurring across some cities, is it worth re-examining their existing home risk assessments, alarm systems and emergency procedures to see if they remain appropriate in light of the potential changes in the threat landscape and police response?

These are all risks that must be re-imagined and assessed along with questions that should be discussed among stakeholders such as Legal, HR, and Security. Ready or not, organizations will be called upon to understand what has changed, adopt new processes, modify policies, re-double and re-work education and awareness campaigns.

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

The Top COVID-19 Security Concerns of Security Leaders

As the world continues to grapple with the impact of the COVID-19 pandemic, we continue to listen to the concerns of security leaders who are trying to do all they can for their organizations and communities.

Here are the nine most common requests for information we've been receiving.

- Statistical analysis of data, including trend analysis and data reporting dashboards.
- "Return to" strategies, including triggers and indicators for phases of return or reopen
- Technology and tools that are proving worthwhile in COVID-19 risk management, including symptom self-attestation apps, kiosks, CCTV, temp scanners, touchless options for access, contact tracing, identity and access management.
- Entrance screening strategies and best practices that meet HIPAA requirements.
- Reorganizing the building space for social distancing, to include elevator use, bathrooms, stairwells, zoning and environmental design.
- Travel safety, including triggers for return to travel and post-travel self-quarantine concepts.
- Cleaning procedures and protocols.
- Managing risk in the remote environment – including domestic violence, mental health, secure cloud, and data privacy.
- Dealing with new waves of infection.

Many security leaders are looking for best practices and input from peers about what works and what doesn't, from process to technology. Keep in mind that while such advice is useful, it isn't a substitute for a realistic and vigorous assessment of your own organization's capabilities, resources, and needs. Just because a strategy or technology works for others doesn't mean it will work for you.

Particularly if you decide to pursue technology as a solution to COVID-19 related issues, don't neglect to do your due diligence. In a time of crisis, vendors or media may claim certain technologies as quick fixes to problems, but testing and time may show they are far less effective than expected. For instance, many institutions rushed out to buy thermal camera systems for speedy noninvasive temperature checks, but it's since been shown that their margin of error still requires a backup method of screening for accuracy. It's also become clear that a high percentage of cases are presymptomatic or asymptomatic, so some companies have spent $20,000 on systems that don't save them much time or mitigate much risk.

There are some considerations, however, that can be of common benefit across organizations. These three points have been raised consistently by our subject matter experts over the last few months.

1. **Don't wait to do your after-action reviews.** This isn't like a storm or an earthquake. It is an ongoing crisis with a long tail, and if you wait until it's over you will have lost the memory of many of the issues you could have improved along the way. It would be wise to do reviews at least once a quarter, and as often as once a week if possible. Make sure to include which tools you used to greatest benefit and what would have helped you do better, and track your costs continually.

2. **Consider how you can enhance employee care.** Make sure your people know you are there for them and they can trust you with their health and safety. Communicate this intention clearly and often. Remember that your tone and follow-through will impact employee trust in the long term.

3. **Prepare for changes in Security.** Redefining the workplace will continue to redefine security's role in the organization. Be thinking now about how reductions in physical space may affect your function. How will security protect remote workers and assets? How will a changing Security function impact staffing and required skill sets?

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

SECURITY EXECUTIVE COUNCIL
A research and advisory firm

COVID-19 Security Response Tactics and Strategies to Consider for Business Resumption Plans

Created by Dan Sauvageau, SEC Subject Matter Expert.

Many security departments are currently busy focusing on the immediate needs of managing their COVID-19 response plans, assessing their resources, evolving their tactics, and fielding questions from employees, executives, and other stakeholders. Some may have not had the time or opportunity to think about what the next two, six or twelve months may look like or what measures they should consider taking when officials allow non-essential businesses to open and employees return to work. With some countries already starting to slowly end lockdowns and the U.S. government's three phased re-opening plans recently announced, now is the time for companies to get into high gear with their next phase of business resumption plans. In the spirit of helping our community to "see around the corner," the SEC is taking the opportunity to share thoughts and ideas that security teams may want to consider as part of their near- and longer-term strategic plans to manage through the COVID-19 pandemic and beyond.

This is a critical time for Security to rise to the occasion to assist their company in managing this crisis and demonstrate their value over the long term. This can be done by demonstrating their considerable crisis management experience, talents, and 24x7 presence, leveraging their tools, delivering excellence, and offering creative solutions to novel problems to keep a company safe, secure, and successful.

Realizing that companies vary in industry, size, location, layout, and resources, some of the suggested items below may prove more or less challenging for some than others. Also, given the dynamic nature of the COVID-19 virus and fluid recommendations and guidelines coming from local, state and federal agencies, the security department should work closely with its internal stakeholders in HR, Facilities, Safety, Legal, Corporate Affairs and specialized licensed health care experts before implementing specific measures. These functions are also best positioned and informed to adopt measures and controls that best fit their corporate culture and risk appetite. As the company quickly evolves from a *response* to *recovery* mindset, it should be prepared for the numerous yet unknown challenges in the weeks and months ahead. It is time to move beyond the tactics, see through the fog of the battle, and be strategic and creatively flexible in one's planning process. Think of it like a COVID-19 employee return experience where all aspects of returning to one's place of business are clearly thought out, risks carefully assessed, action plans made and communicated, and done with unprecedented teamwork and collaboration amongst business functions.

The centerpieces of the planning process are trust, transparency and the health and wellbeing of all employees, both in the words and actions of a corporation. Maintaining those three focal points should go a long way to engaging employees for the challenges that lie ahead and enabling security teams to be successful.

The suggestions outlined in this document fall into five general categories:

1. **Preparing for re-entry**
2. **Re-entry logistics for employees, vendors, and governance considerations**
3. **Ways to best leverage security teams and their tools**
4. **Staggering the workforce and staging the workplace differently**
5. **Post-business-resumption risks and preventive measures**

Well-resourced and robust security functions will likely have documented procedures and guidelines for re-entry and business resumption well underway, while some may have not yet started. The suggestions outlined below may be helpful for both groups as they are meant to stimulate the thought process and accelerate discussions between security and their business partners.

1. Preparing for Re-Entry

There are many things for a company to consider prior to re-entry to its workplace, but arguably one of the first is how to do so in as safe a manner as possible for all employees. The term "employee" is used to broadly cover employees, contractors, interns, or anyone who accesses the workplace on a routine basis. Once plans are solidified for the employees' safe return to the workplace the company can focus on undertaking the necessary longer-term efforts to mitigate the risks of a further business disruption or closure due to a possible future virus outbreak. Local, state, and federal government guidelines are the first ones to consider when moving to a phased business re-opening, but such guidelines are designed to be general and for a diverse set of industries and institutions. Government guidelines will lack the specificity that companies will need to fit their unique business requirements, workplace environment and culture. Government guidelines are also meant to be the minimum requirements or hurdles to overcome; a company always has the option to do more and go above and beyond to ensure the safety of their employees while regaining momentum for its business. Employees will count on and expect their companies to do everything possible to ensure their safety in the workplace or while on company business, and companies have a duty-of-care responsibility to not let them down.

Symptom screening - Aside from the myriad of reactionary company policies and practices developed by companies thus far into the crisis, symptom screening of people prior to returning to the workplace is a logical first step to consider. The objective is simple - keep the infected out to avoid further infections; however, the means to do that are complex. A company has many options to consider when it comes to screening its employees. Here a just a few approaches that some companies are doing or considering:

- Employees take their own temperatures and answer CDC or appropriate government health official COVID-19 symptom questions at home - before coming to work.
- Employees take their own temperatures and answer symptom questionnaires upon arrival at work, which are then validated/supervised by a designated person(s).

- Designated, trained, and properly equipped company employees perform the screening at the entrance to the workplace.
- A subcontracted licensed, qualified healthcare provider performs all screenings at the entrance to the workplace.
- Employees answer other symptom questions before arriving at work, and thermal cameras installed at designated entrances read temperatures of people as they enter, followed by other measures.
- Any combination of above

If a company chooses to have its security staff perform screening and temperature taking of employees, vendors or visitors, the staff should be properly trained and equipped with CDC recommended PPE and would be well advised to only perform that work under the direction of competent and licensed medical health care provider. This option also comes with significant other risks and challenges that should be carefully considered by all company stakeholders.

If screening is done in the workplace, stations and queues may be set up to allow for social distancing and, where necessary or practical, with separate entrances for employees, vendors and visitors to facilitate throughput and allow for social distancing and some degree of privacy. Ultimately, a building's size, configuration, population, and use will determine what approach works best, and one should expect to modify their approach through some amount of trial and error. Security is typically well positioned with the access history tools, data and experience to estimate "normal" volume throughput in pedestrian entries to help inform decision makers on what approach makes the best sense for them.

A company may also ask their healthcare provider experts if two levels of temperature tests are prudent – infrared followed by a secondary, more precise temperature screen to minimize false positives. A trained, equipped, and experienced healthcare provider will know the best practices to employ and should be consulted. Security and their business partners should, however, be part of the planning process to assist the healthcare provider by understanding the business environment, organization, and its culture to allow for a streamlined, positive employee experience. Healthcare providers that offer such services are already being placed under contract or will be in extremely high demand as more companies develop return to business plans. The SEC suggests that security teams conduct their own due diligence and needs assessment when determining what health provider is best suited for them.

Secure internal web portal for incident tracking – Keeping track of individuals who have been out of work with symptoms, confirmed cases or quarantined from recent travel can be a daunting exercise for a company, especially one with thousands of employees. A secured, database-driven portal could be set up and made available to employees to self-report updates on their conditions or changes in health (e.g., recovering at home, in hospital, elapsed quarantine time, more recovery time needed). Professionally trained HIPAA HR staff or others could manage the portal and act accordingly on the information collected. As previously noted, Corporate Legal and/or HR would be important stakeholders to ensure all HIPAA rules are followed.

Discontinue unassigned seating and locking conference rooms – Inform employees ahead of returning to work that unassigned seating will be discontinued. Consider locking conference rooms or areas where large groups of people might consider gathering. Place signage on areas designated as off limits. Designate or render select fixtures inoperable in common use areas such as restrooms, cafés, or outdoor patios to allow for and encourage social distancing. More information on this topic is included in section 4 below.

Proactive communication - Communicate to employees as to what they can expect to experience on day one of their re-entry experience so they can be prepared, understand, and gain comfort in the actions your company is taking to protect them. This may help reduce their anxiety and that of their loved ones by detailing all the measures your company has taken and will undertake on a go-forward basis, such as cleaning protocols, social distance markings, building occupation limits, entry screening, and package handling.

Consider creating "wellness coordinators" - To assist with reinforcing messaging and mitigation efforts being taken as part of the overall re-entry experience, companies may consider developing a system whereby designated individuals across enterprise HR functions and/or business units serve as wellness coordinators. Similar to having knowledgeable, trained employees serve as emergency/floor wardens to assist in a fire or other building emergency, wellness coordinators who are trained and versed in the company's unique COVID-19 measures and protocols could be a force multiplier for the HR, Facilities and Security departments. These coordinators could serve as knowledgeable ambassador points of contact for the broader employee population - adding clarity to communicated messages or funneling questions and concerns of co-workers to the proper individuals with responsibilities to address an issue. This approach would supplement other avenues such as intranet web portals or microsites for employees to voice concerns or comments. It would also add a human dimension to the communication process. As with any delicate matter involving employee privacy, Corporate Legal would be an important stakeholder to ensure privacy and HIPAA and other privacy laws are followed.

2. Re-entry logistics for employees, vendors, and governance considerations

Make hygiene apparent and accessible and cleaning visible– Ensure hand washing signage reminders are ubiquitous throughout the workplace, not just in restrooms. Hand sanitizer or disinfecting wipes should be readily accessible and re-stocked at all entrances, exits and throughout highly trafficked common areas. Place disinfecting wipes or disinfectant near all commonly used office equipment, e.g., printers and copiers, and other high-touch surface areas. Consider adding periodic checks of these stations to security's patrol duties to avoid employee frustration and reduce risk if they run empty.

Instead of relegating housekeeping staff duties to off hours, make them visible and available throughout the day, especially in the early days of return to business. Frequent cleaning of common areas and high-touch surfaces will help put employees at ease. Employees should see cleaning taking place and smell it in the air. The early days of re-entry will all be about gaining employee confidence and trust for the sanitary nature of their work environment, and these duties will likely fall on the shoulders of lower-paid vendor staff. It is important to pay close attention to cleaning and sanitization practices. Without question, some employees will be looking for gaps and perhaps even taking pictures of practices and areas they are critical of or find concerning.

Vendor controls and oversight – For many companies, on-site vendors are essential partners in allowing a business to carry out its important day-to-day operations. However, a company has little if any control over the outside practices, behaviors, and policies of the vendor staff they use and who enter their workspace. Ahead of re-entry would be a good time to understand and validate what measures, controls, policies, and procedures vendors have for their employees. After all, their presence and behaviors will impact a company's ability to maintain a safe and healthy work environment. Perhaps the Procurement department, which is best positioned to know every vendor contract, could coordinate, and take ownership of this task. In many companies the Facilities and IT functions often have the greatest number of vendors, so that may be another logical place to start.

Strict guidelines may be needed for vendors, especially those with unknown, limited, or questionable benefits or practices to mitigate virus spread. For example, a company can incent its sick employees to stay away from the workplace by offering generous paid sick or quarantine leave or extend work from home abilities. What if a vendor does not extend this or similar benefits to its employees, especially those who live paycheck to paycheck, and they come to your workplace sick for fear of missing out on pay? Every effort should be made to ensure service staff, especially housekeeping, food, and other close-contact service functions, are not spreading virus through their normal duties. This is especially important for the housekeeping staff who are entrusted with vital cleaning and disinfecting duties. The importance that trust has on the employee experience and their perception of a safe/healthy workplace cannot be overstated here. It would be a serious impact to business operations and employee trust if that critical vendor who chose to ignore or not reveal their symptoms came in and infected others in a critical operation, or if a housekeeper responsible to clean and sanitize workspaces was instead contagious and spreading virus, making people sick and causing a workplace shut down.

Housekeeping staff should follow government health officials' guidelines regarding PPE while performing their duties and be instructed on the proper use and disposal of them. Also, they should properly dispose of other potentially contaminated items they use or come across in performance of their duties. Typically, the Facilities department will be responsible for ensuring the work practices of housekeeping staff, but they may not be around to ensure they are always carried out. Consider whether security can add value by serving as a secondary check

and balance control measure to ensure that designated areas are cleaned and/or disinfected after hours and housekeeping staff are wearing PPE as appropriate. Security could capture their findings and share them with their Facilities partners to address non-compliance before larger problems emerge. This is a terrific opportunity for Security and Facilities to partner closely and demonstrate teamwork to employees and senior management for the benefit of all.

Consider having conversations with vendors now about whether they have plans to notify your company in a timely manner of any confirmed COVID-19 cases that occur among their staff who access your premises. Would you want to leave it to chance that a contractor who has COVID-19 symptoms and calls in sick to their company will proactively also notify your company? Consider working with your Procurement and/or Legal partners about adding addendums to existing contracts emphasizing new or additional COVID-19 controls and measures that your company deems important and that vendors must follow while on property to avoid virus spread resulting from their behaviors.

Shipping/receiving/packages - While health experts consider the transmission of the COVID-19 virus from package surfaces to be low compared to social contact and droplet spread, the risk still does exist, and measures should be evaluated against the company's risk tolerance. Consider allowing any inbound packages to remain untouched for a period of time until surfaces are considered free of viruses according to published CDC or equivalent health agency guidelines. If parcels are deemed important, adopt disinfecting procedures for parcels in accordance with healthy agency guidelines. Discontinue internal hard copy mail services until the pandemic risk is over. Ensure shipping/receiving and internal mail staff are properly trained and understand established guidelines and restrictions concerning package handling. Post external signage (multi-lingual as appropriate), instructing infrequent delivery personnel of the established measures and controls in place prior to them entering your facility or offloading materials. Greater care and more stringent measures may be appropriate for packages destined for high security and critical areas such as data centers, GSOCs, R&D labs, trading floors, wire transfer rooms and executive offices.

Leverage existing plans, or start plans, to create virtual GSOCs to create flexibility in the event of future outbreaks. If virtual GSOCs do not exist, re-arrange existing workstations to increase social distancing. Some GSOCs are built atop a raised floor which may make rearrangement easier. Split work teams and have them perform at-home self-assessments of symptoms prior to workday shifts to prevent spread and contamination of this critical function. Designate the GSOC and all critical areas frequented by people as regular disinfected areas for housekeeping staff to address. See the SEC's COVID-19 GSOC & General Security Risk Mitigation Checklist.

3. Ways to best leverage security teams and their tools

Most corporate functions are not available or on-site on a 24x7 basis like security. Yet business partners such as HR and Facilities have already been and will continue to be deluged with

employee calls concerning questions about COVID-19 plans, policies, controls, and measures. Many expect COVID-19 to be an ongoing crisis/challenge to manage well into the year 2021. Such a long-tailed event will no doubt create fatigue across teams. The more cross-functional support and collaboration there exists amongst business partners, the more enduring and resilient people and teams will be for the marathon journey that lies ahead. Let's look at some ways Security can assist and continue to add value in the long term.

- Leverage your CCTV system to conduct periodic after-hours spot checks of housekeeping staff to ensure they are employing safe hygiene practices while cleaning the workplace. Alert facilities staff of improper practices before larger problems set in. Some housekeeping firms are small with limited resources and training to manage a crisis of this magnitude and complexity and offer limited supervision of their duties. Security can be an extension of the eyes and ears of a Facilities team.
- Leverage your CCTV system to monitor if social distancing practices are being maintained in the workplace upon employees' return and future phases of increasing population. If your system has video analytic capabilities determine if it could detect for breaches of pre-set social distance parameters.
- Proactively have the GSOC team run end-of-day building access reports to inform stakeholders of occupancy rates.
- Ensure that all access systems and CCTV equipment are working and recording properly as they will be essential contact tracing requests/needs.
- Consider installing "exit" card access readers to help assist with building occupancy counts at any given time and contact tracing when warranted.
- Be vigilant in keeping visitor and vendor sign-in and access records up to date and accurate. Records will be essential in flagging individuals who are temporarily not allowed access if they failed temperature/symptom screening and for contact tracing.
- To the extent possible and balancing the needs of security with safety, consider allowing normally closed, non-critical interior doors to remain open to reduce the number of commonly touched surfaces. Note: It is important to follow local fire code requirements and not to impede the operation of fire door closures. Also, taking normally active card reader-controlled doors offline will limit access history records for potential contact tracing so the risk/benefit decision to leave doors open should be carefully assessed.
- As appropriate, consider replacing card access door release buttons with hands-free, passive infrared door releases.
- Depending on your buildings' unique entrance configurations and/or security requirements, consider leaving main entrance doors open and staffed with a security officer during times of increased foot traffic while still having employees use their access cards to create access records for population counts and contact tracing.

Companies that have already experienced confirmed COVID-19 cases in their workplace are reporting that important contact tracing requests from health officials is taking a huge amount of time and taxing their staffs, who are already stretched thin. Depending on your access system's

capabilities, consider creating pre-programmed software shortcuts or routines to quickly assist with contact tracing if needed. Also consider ramping up with additional contract staff now – ahead of incidents requiring contact tracing when large numbers of people return to the workplace. If your visitor management system is not up to the task, make note of this and hold onto it for future capital requests. Records of all persons accessing a facility will also prove helpful should health officials need to conduct contact tracing for infected individuals and subsequent communications to building occupants about necessary appropriate actions and measures to be taken.

The risk of malware and computer viruses being introduced into company equipment used while working from home in a less controlled environment may have increased. Consider partnering with your IT department and use access systems to disable badges (i.e., block access) of individuals who need to have critical equipment scanned for virus or malware before it returns to the building and is connected to the network.

4. Staggering the workforce and staging the workplace differently

Just as some employees experienced anxiety returning to work in high-rise buildings or flying on planes following 9/11, some will have anxiety or concerns about returning to a workplace filled with people compared to the controlled environments of their homes for the past six or more weeks. Look at how businesses that are deemed essential, like grocery stores and pharmacies, have evolved their controls to limit virus spread in recent weeks, such as shortening store hours, setting special times for the elderly to shop, limiting the number of people allowed in a store, routine disinfecting and social distancing inside and outside. The workplace may consider employing similar measures that limit spread and make employees feel more at ease. Hands-free access control systems such as facial biometrics have existed for some time, but their throughput limitations or cost were often prohibitive. Eventually, these and other technology solutions that enable touchless controls will become more practical and less expensive. Since perimeter security and access controls are the domain of security departments and often require physical contact, security leaders should be vigilant in researching practical hands-free or soc called “friction-less” solutions suitable for long term use. Now may be an opportunity to try out virtual receptionist and self-serve, voice-enabled kiosk assistance stations.

Consider the following measures that help address and or complement government guidelines for phased re-openings and/or your company’s other needs:

a. Discontinue unassigned seating altogether or at least until pandemic risk is completely over at which time the risk/benefit can be re-evaluated. Consider assigning seats to individuals and allowing for social distance spacing in the work environment with social distance marking prominently displayed in work areas as appropriate. Some of the large commercial real estate service providers already have robust plans and ideas available on the web for companies to consider accommodating social distancing in the workplace

b. Continuing some measure of work from home strategies to minimize building occupancy and keep more vulnerable staff away from the workplace will ease pressure on any symptom screening checkpoints and other building services needed to keep the environment and occupants healthy.
c. Apply signage markings on floors in lobbies, common areas and other typical gathering areas to designate 6 ft. social distancing.
d. Create social distance markers around workstations as friendly reminders in co-worker interactions.
e. Stagger work hours to limit office population and ease traffic at entry symptom screening stations.
f. Section/designate parts of the building as no-work/off limit areas to serve as relocation spaces for areas that get closed down temporarily if/when confirmed cases occur. Disable access control readers to these and other temporarily restricted areas.
g. Modify contractor card access privileges for times of day or days of week to limit them from showing up off schedule or wandering in temporarily off limit areas.
h. Divide critical functions into 2-3 components, allowing only one to work on any given day/shift to ensure "people continuity" if one becomes infected.
i. Consider limiting elevator occupancy or restricting their use to only mobility restricted employees. Explore the feasibility of upgrading elevators to touchless controls.
j. Consider making long corridors one-way to allow for social distancing.
k. Consider individualized take-out meals from favorite restaurants to build staff morale, reduce cafeteria populations and help small businesses.

It's important to ensure frontline supervisory staff and all full-time and contracted service support staff such as Security, Facilities, etc. are well informed of any changes ahead of re-entry so they can properly support, communicate, and help employees comply.

Leased space - If you occupy leased space as a tenant you may have no control over the cleaning or hygiene practices in place for common areas such as lobbies, building reception, stairwells, and elevators. Also, a tenant may have little if any control over the quality of work, cleaning supplies used, or procedures employed by the housekeeping staff for your immediate office environment. Given these limitations while still being responsible for the safety and health of your employees in the workplace you might ask yourself the following:

- Are landlords and their housekeeping staff following CDC or other equivalent gov't health official's workplace disinfecting guidelines?
- The Buildings Owners Management Association (BOMA), a property management oriented professional industry association has many informative on-line resources and best practices that a company may leverage, especially one that doesn't have its own professional Facilities department.
- Are they using EPA-approved products that are effective to eradicate the virus and safe for employees?

- Is the landlord or their vendors conducting symptom checks of their cleaning and support staff before entering the building or tenant space to perform their duties?
- Are landlord vendors encouraging staff to self-quarantine with paid sick leave or other benefits if one is sick or symptomatic, so they don't spread virus to your offices or common areas?
- How confident are you that Illiterate and poorly trained housekeeping staff understand and properly carry out their duties to your expectations?
- How are all the above issues playing out in international leased spaces of less developed countries, where local government guidelines are non-existent or lax compared to those in developed countries? What about countries with a high level of corruption?
- How can you be assured they are not cutting corners with products and procedures to save money?

Now is the time to review your lease agreements and enter into proactive conversations with your landlord to understand and request specific measures when it comes to routine office cleaning and disinfecting work areas, both as a matter of routine and after it is known that someone was symptomatic and/or confirmed for having the COVID-19 virus. If you are not an anchor tenant, determine where your company stands on the prioritization scale for requesting disinfecting of workspaces in a time of need or high demand. Inquire if the landlord has a practice to notify all tenants if they are made aware of confirmed COVID-19 cases among tenants, vendors, or their own staff. It is better to know what is in place or lacking before the rumor mill gets started or you are caught off guard by employee questions on the topic.

5. Post-business-resumption risks and preventive measures

Business travel – Once business re-opening phases commence, companies will have a need to resume business travel to check on suppliers, service clients, and generate new business. With reduced commercial routes, fewer direct flights, continued interest in social distancing, and a desire to avoid airport congestion, private aviation may become more popular among travelers for critical business needs. A company may consider which roles are travel critical, such as sales, business development, manufacturing, and executives and inquire if they plan to use commercial or private aviation. If private or charter aviation is used more frequently, the security department should look into whether their current automated travel tracker systems do or do not track employees on such flights.

Regardless of whether travel is undertaken on commercial or private aircraft, it will be important to remain current and vigilant on continued travel bans, restrictions, and changes. Once travel restrictions are eased or lifted, a company should closely monitor the appropriate government travel advisories, WHO and CDC guidelines, and third-party global risk providers as health officials caution against the emergence of a second pandemic wave and/or virus "hotspots" which could catch business travelers off guard if not kept properly informed. Particular caution should be placed on allowing travel to developing countries that reported

few initial outbreaks of the virus, since some countries may have adopted internal policies to not test for the virus or have insufficient tools and protocols for tracking virus spread.

Prior to resuming business travel, a security leader and their business stakeholders should agree upon what factors could be used to determine when a destination is appropriate for business travel. A fully thought out and agreed upon set of controls and strategies should be devised, and a pre-trip safety briefing given to every traveler. Contingency and travel emergency plans should be revised and refreshed accordingly. The important difference with plans now versus pre-COVID-19 is that the security, safety and health infrastructure across countries may have changed, in some cases dramatically. Security leaders will need to ensure their travel security teams or services remain current with all the changes that a business traveler may encounter. For example:

- What changes can a traveler expect upon airport arrival/departures?
- Have existing travel visas been cancelled due to COVID -19 controls thereby requiring new ones?
- Will there be a requirement to download tracking apps on smart phones?
- Are mandated quarantines upon arrival still in place? If travelers become symptomatic while away and forced to self-quarantine in a foreign location, are they properly equipped, prepared, and briefed with the best access to healthcare information and hospitals?
- Is the healthcare system or previously recommended hospitals at their destination stressed and short of supplies to the point they can't provide adequate care if needed?
- Have ground transportation logistics and rules changed for taxis, ride share services or public transit? Should use of public transit be prohibited for business travel for a period of time?
- What changes can travelers expect at hotels?
- When and if effective, medically approved COVID-19 antibody tests are available, should a company consider only allowing business travelers who have been tested to travel to riskier locations? What employment concerns enter into that discussion?
- Should all business travel be voluntary or require secondary levels of approval?
- If hot spots emerge and flights are cancelled with short notice, stranding travelers, how is the company prepared to manage such occurrences?
- Should a company consider requiring versus suggesting certain actions by business travelers, such as:
    a. Enrollment in the U.S. Department of State's Smart Traveler Enrollment Program.
    b. Updating or validating emergency contact information prior to travel.
    c. Reporting of personal travel to known international or U.S. "hot spots" before being approved for business travel.

Being a prepared traveler will be more important than ever. Security travel teams should equip business travelers with the most current information prior to and during their trip. It may also

be beneficial to debrief early travelers upon their return from a trip to learn from their experience and identify tips and information that may not have been included in government or third-party global risk briefings. Debriefing travelers early on will also demonstrate a sense of care for the employee and perhaps yield useful information for future travelers to a region.

Maintain a contagious illness working group - After the current wave of the pandemic has passed, a company may want to keep a small team of internal stakeholders (e.g., Security, Safety, HR, Facilities, Legal and Corporate Communications) in an 'on-call' status to manage virus issues, incidents and concerns that emerge or are raised by employees. While I was with my previous employer, we had contagious illness working group made up of HR, Security, Real Estate, Business Continuity, and Legal in place for over 18 years. Working dozens of small and larger-scale contagious illness incidents over such a long period developed muscle memory and a disciplined approach of trust, expediency, and professionalism when handling a variety of cases. When the COVID-19 crisis passes, maintaining a contagious illness team at the ready will help prepare a company for any future incidents, small or large.

Leverage employees' experience and suggestions - Consider keeping employees up to date with a company's efforts to manage COVID-19 until a vaccine and/or therapeutics are widely available. Also call on employees to share their inputs, suggestions, and concerns for ways they need to stay informed and engaged to help boost productivity and morale. The priorities of this crisis remain health and safety followed by business resumption, with the latter intrinsically dependent on the former. Employees are at the center of both priorities, and it is their experiences, real and perceived, that will help a company keep people healthy and return to business operations as efficiently as possible. A company's internal crisis team will benefit greatly by keeping the pulse of the employee experience throughout the coming months. This pulse will inform the crisis teams on what measures are working, which require modification, and where new ones are needed to navigate what will be a bumpy journey forward. Leveraging employees also emphasizes the importance the corporation places on those centerpiece focal points of trust, transparency, health and wellbeing of employees.

Prepare After-Action Reviews (AAR) – Because of the length of this crisis, smart companies will perform AARs at certain points throughout it and when it is finally over. Performing AARs on a recurring basis will help capture important details while memories are fresh. Aside from answering the usual "what worked and what didn't" questions, security teams may want to also consider the following:

- What resources, equipment, protocols and strategic external business partners and experts, were needed, and at what different stages during the crisis?
- How can these things be leveraged differently for potential future waves of COVID-19 or entirely different contagious illness events – small or large?
- What new technology should security be aggressively advocating for to reduce cost and to provide better control and management of a similar crisis? Are hands-free access controls, robots, integrated visitor management systems, smartphone apps, voice-

enabled kiosks, others practical and cost effective? Security should be prepared with a "shovel ready" list of those capital and operational expenses, complete with ROI calculations for each.

- Were critical security vendors able to perform satisfactorily and support all your needs at the outset of the crisis? If not, were they able to adapt quickly?
- Some companies may be also be evaluating their organizational structures to assess how well they responded and managed this crisis, especially business continuity and resilience. Security should be poised and ready to accept any new responsibilities that they could assume which play to their core strengths, talents and experience managing crisis events.

It may also be beneficial as part of an AAR for a company to look back at what actions, controls, and measures Countries and individual U.S. states adopted as they passed through the apex of their pandemic curves. Creating a timeline of the macro issues of what happened externally and internal to a company with the benefit of hindsight may provide helpful markers to consider for the future.

Until we know what re-opening will look like for business, industry, or even society, it will be difficult to fully plan for longer-term strategies to mitigate and battle deadly future contagious illnesses. There is much talk amongst health experts, governments, and business leaders that we will not return to business as we knew it for quite some time. We may come to realize that avoiding future work stoppages from health crises – not only future pandemics, but perhaps even seasonal flus that pose a higher risk to vulnerable groups and for which there is no effective vaccine - will require us to employ many of the tactics we are using now to combat COVID-19. For example:

a. Not shaking hands
b. Increased work from home for high risk individuals
c. Increased workplace sanitization routines
d. Wearing masks
e. Social distancing
f. Splitting work functions
g. Restricting travel to/from locations that experience large outbreaks

<u>Pro-active campaigns for vaccines and proof of immunization for critical roles</u> - Consider socializing the idea amongst internal stakeholders to push for more education and awareness and to consider making vaccines available to employees. Vaccines have been an increasingly polarizing topic amongst many groups, so this is not one to be taken lightly or without healthy debate amongst stakeholders to fully consider the laws, health considerations, individual beliefs and business needs. Consider the pros, cons, legal and other challenges of having critical function staff maintain immunization records and/or blood titers during outbreaks of contagious illnesses (e.g., coronavirus, MMR, and chicken pox) that could prompt closure or quarantine by health officials. Work with HR and Legal to ensure HIPAA, religious sensitivities,

and other laws are respected. HR and Legal would also be knowledgeable of whether immunization records for critical functions constitute a bona fide occupational qualification for certain critical roles or circumstances.

Communications and on-going contagious illness awareness - Consider keeping active campaigns, awareness, and messaging in multi-media and multi-lingual formats as we move through COVID-19 phases and safe hygiene messaging into the future. Employees will have a strong interest in company actions pertaining to COVID-19-related workplace actions and will likely have a heightened concern and interest in all future contagious illness outbreaks impacting the workplace. Just as we prepare for seasonal natural disasters such as tornados, hurricanes and wild fires having a site with links such as helpful FAQs, travel advisories, internal policies, and hand hygiene will help keep people informed, vigilant, safe, and better prepared for endemic, epidemic and pandemic health issues.

Increased workplace and domestic violence spillover - According to the International Association of Chiefs of Police, many law enforcement agencies are reporting increased domestic violence since stay-at-home orders were issued. Will more domestic violence spill over into the workplace when stay-at-home orders are lifted? Will the increase in job losses, financial stress, mental disorders, post-traumatic stress disorder, and grief increase the potential for more of the following in the workplace?

a. Hostile behavior
b. Threats
c. Violence
d. Substance abuse
e. Threats to self-harm or suicide
f. Erratic behavior/inappropriate conduct
g. Theft

If you do not have a documented workplace violence plan or existing program, now would be a good time to prepare one. If you have one, now is the time to refresh it. Security should remain informed of all trends brought about by this crisis with the potential to impact the workplace and should make stakeholders aware of them.

Potential for civil unrest - Globally and within the U.S., drivers for civil unrest can arguably fall into the categories of political, economic, and social. Though not currently a problem, essential supply chain (e.g., food and medicine) or utility disruptions could result from COVID-19 repercussions. Security teams would be well served to remain vigilant, looking for signals of potential unrest across regions globally and in the U.S. where they have operations. In the U.S. for example, federal stimulus money is not going to certain groups like the homeless. Would U.S. cities with large homeless populations and known active civil rights supporters be at a higher risk for protests and/or unrest? Could the cities that had high numbers of Occupy Wall Street protests back in 2011 be the likely locations for potential COVID-19-related unrest to

occur? What about in countries with a history of civil unrest, large populations with fragile infrastructures or political institutions, or where U.S. multi-national corporations have significant operations?

Increased fraud, insider risk, product diversion, counterfeiting - Recently, U.S. Federal Agencies announced enhanced enforcement efforts to combat potential increases in transnational crime, drug and terrorist activities as criminal and terror groups look to exploit the COVID-19 pandemic for their benefit. Companies may want to increase their vigilance in monitoring known hot spots of past crime (traditional and cyber) for upward trends of fraud, counterfeit, and theft of their products and intellectual property. Combatting these challenges and efforts to protect a company's brand, customers and bottom line have become more difficult with COVID-19, especially as law enforcement agencies are stretched thin and forced to focus on higher priority issues.

In Conclusion

This is understandably a great deal of information to digest and by no means should be considered an exhaustive list of security, safety, and other business functions' items to consider when looking to construct tactical and strategic plans to manage the ongoing COVID-19 pandemic. Also, as was mentioned at the outset, every company's culture, business operations, and risk tolerances are different. Moreover, the laws, regulations and guidance coming from local, state, and federal governments are different and quickly evolving as everyone comes to grips with this novel virus. Assembling the proper stakeholder functions within a company, assisted with the right health and subject matter experts to formulate realistic and actionable plans that meet a company's needs and comply with applicable rules, regulations and guidelines, will best position them to be resilient and successful.

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

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

General Security Risk Mitigation Strategies: COVID-19

The coronavirus disease 2019 (COVID-19) has spread rapidly across the globe. Security leaders, along with internal stakeholders, must think several steps ahead of this deadly virus and implement measures designed to mitigate risk to people and company reputation.

The collective knowledge of the SEC has put together a summary of general security-related action items to be considered to minimize risk and to begin implementing safeguards and measures that can mitigate or reduce risk. Relatedly, an SEC paper has been created that is dedicated to business resumption, which outlines what security leaders and other stakeholders should consider for an orderly return to work: "COVID-19 Security Response Tactics and Strategies to Consider for Business Resumption Plans"

The following information regarding general risk mitigation strategies is provided with the understanding that not all companies have a professional security staff, or a Global, or even a local, Security Operations Center (SOC). We recognize that not all suggestions identified apply to all companies. However, whether you are the only security person at your company and wear many hats or you are the Chief Security Officer with a staff of security professionals, we all need to focus on risk mitigation in the most challenging of environments. We must also contemplate what controls and measures we will need to put in place to reduce risk now, and ultimately plan for the return to the '*new* normal' of business operations.

Now is the time to consider the daily tactical initiatives as well as the strategic path regarding the next steps that are right for your company. These steps must include aligning your strategy with the many new requirements imposed by federal, state, and local officials.

Note: This checklist should not be construed as a means to establish any legal standard of care or identify what reasonably prudent security precautions should be taken in any specific situation. The actions to be taken for individual situations will vary depending on the corporate culture and individual circumstances at the time. Ultimately, every individual must assess any given situation, choose a response and manage the consequences.

	Strategic Partnerships
☐	1. Develop an Infectious Disease Preparedness and Response Plan, to include establishing plans and protocols with HR, Legal, Safety, and Operations that address an actual and potential infected building occupant. The strategies you generate should be cultivated from authoritative sources such as the WHO and the Centers for Disease Control and Prevention (CDC). Monitor and adjust your policies (as the guidance from these resources evolves and changes frequently.) Derive your information from these reputable resources and align your plans with their up-to-date recommendations; doing so will put you in a position of following the guidance and advice of the experts should your company be challenged regarding the response measures implemented.
☐	2. Collaborate with Legal to ensure workers' rights and employers' responsibilities that may apply to prevent occupational exposure to COVID-19 are followed in accordance with federal and applicable state guidelines (for instance, OSHA's Occupational Safety and Health Act of 1970, prohibits employers from retaliating against workers for raising concerns about safety and health conditions.)

☐	3. Develop procedures and protocol with Legal, HR, and others, when an employee makes a claim (under federal, state, or local regulations or laws) about safety and health conditions that do or could impact them, others, and the company brand.
☐	4. Identify alternate work areas (include coordinating with IT) multiple drops-in alternative areas for phone/computer/other that can be quickly occupied with all new equipment should the GSOC/building be contaminated.
☐	5. Identify a process and protocol with local hospital(s) should a building contract or be suspected of having contracted, COVID-19.
☐	6. If you are a tenant, coordinate COVID-19 response protocols with the property management team.
☐	7. There has been a sharp rise in domestic violence (spousal and child abuse), due to the pandemic. Team with HR, Legal, and others to ensure EAP resources and support are made available to those impacted.
☐	8. Devise a procedure and protocol with Facilities regarding HVAC and other air handling unit devices, regarding measures they will take to slow, or prevent, the spread of COVID-19, should it become necessary.
☐	9. Monitor and evaluate social media postings with Communications to ensure that you understand the pulse of employees and the public. It is essential to stay ahead of any negative postings about the company and to have the opportunity to address, immediately, any actual or potential adverse impacts to the company.
☐	10. Send policy and rule reminders to all employees about the remote use of information technology for the company and, if applicable, personally owned devices; update and distribute any new policies related to working remotely.
☐	11. Partner with IT; provide education and training regarding phishing, social engineering, common attack vectors, or vectors specific to your industry. Remember, the best hardware and software cannot prevent a person from clicking on a link that will compromise your or your customer's intellectual property and tarnish your companies name.
☐	12. Devise a law enforcement and emergency response call list. Maintain communications with local health department and emergency services to keep informed of the ever-changing conditions and response protocols.

	Situational Awareness
☐	1. Explore whether you can establish policies and practices, such as flexible worksites (e.g., telecommuting) and flexible work hours (e.g., staggered shifts), to decrease group gatherings and increase the physical distance between/among employees and others, in accordance with applicable federal/state/local guidelines. Working remotely is perhaps the most effective response that can rule out the possibility altogether, of a person becoming infected: try to avoid in-person contact at every possible juncture.
☐	2. Create a COVID-19 response team to address and expeditiously consider, evaluate, and appropriately address actual or potential concerns. Quick, thorough, and detailed procedures and protocols are vitally important. Note: Please recall that there are OSHA and perhaps state guidelines that prohibit employers from retaliating against workers for raising concerns about safety and health conditions.
☐	3. Assess all workspaces and common areas that do not readily allow for appropriate physical distancing and devise interim measures that provide the recommended six feet of separation.

☐	4. Educate employees about COVID-19 specific phishing scam emails that have been designed to take advantage of the pandemic to compromise personal and company assets/information, to include "Zoom bombing" and other warnings issued by the FBI and other law enforcement.
☐	5. As an interim measure, and until a contact tracing program can be decided upon and implemented, require that all staff take their temperature at home just before departing for work.
☐	6. Devise an educational awareness campaign about COVID-19 mitigation plans to be in full swing (such as printed materials, email reminders), in anticipation of the resumption of business.
☐	7. Plan for an increase in mental health issues impacting employees and for a potential rise in workplace violence. Workforce reductions should be monitored closely, and "at-risk" cases should be given priority attention as soon as possible.
☐	8. Ensure a written protocol is in place should there be an actual or possible COVID-19 contamination. This should be a well thought out process and protocol, requiring a team to assess and address any concerns. No one person should have the authority to dismiss a possible or actual concern.
☐	9. 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.
☐	10. Require sick employees, or employees with sick household members, to either work remotely or stay at home.
☐	11. Partner with your procurement department and conduct due diligence checks to avoid fraud regarding new vendors who claim they can provide hard-to-get items. Items include personal protective equipment and other items in high demand. Often, in addition to the provider urging you to place an order immediately, combined with payment is required upfront, this combination of events typically results in a fraudulent transaction. These conditions of obtaining hard to find resources should be scrutinized and given careful consideration due to the vast amount of fraud due to the pandemic.
☐	12. Provide detailed instructions for the use (or restriction) of videoconference platforms such as Zoom and other online teleconference center services.
☐	13. Develop a contingency plan for key staffing shortages or consider how services offered may be adversely impacted and communicate any impacts before the resumption of business.
☐	14. Consider using drones to monitor key areas and when responding to alarm conditions outside the building.

	GSOC and Social Distancing/Hygiene/Cleaning
☐	1. Devise cleaning intervals for all keypads, biometric surfaces, and other vulnerable areas throughout the facility: stay abreast of updated and ever-changing cleaning and disinfection guidance.
☐	2. Consider having staff work virtually, or separate staff into at least two different physical work areas (and do not allow cross-contamination of spaces).
☐	3. If staff separation is not possible in the GSOC and all other workspaces, separate staff work areas 8 feet away from each other.
☐	4. Have cleaning supplies next to each phone/keyboard/work area and require full cleaning prior to, and after, each use.

☐	5. Issue headphones/keyboards, phones, etc., to each person. Prohibit equipment sharing.
☐	6. Do not allow non-staff in the GSOC (devise and promulgate the means of communicating with the staff other than face-to-face).
☐	7. Practice and communicate the requirement of handwashing after a person touches their eyes, nose, or mouth, and after blowing one's nose, coughing, or sneezing.
☐	8. Close as many entry/exit points as possible. Post "open door" maps at all entry/exit points.
☐	9. Schedule cleanings for GSOC (with focus on handled equipment and all surfaces touched) prior to, during, and after each shift change.
☐	10. Prohibit eating in the GSOC; provide a designated area for meals outside of the work area.
☐	11. Provide cleaning supplies (including three sizes of gloves). Consider mandating the use of gloves for the GSOC staff. Include a supply of facial tissues for each workspace.
☐	12. Devise a protocol should someone in the GSOC becomes infected or responds to a person who has or is presumed to have contracted COVID-19.

	Increase Security Services & Bench Strength
☐	1. Devise a procedure using your access control system to permit those to enter the building (employees, consultants, contractors, vendors) that have tested negative per your contact tracing policy.
☐	2. Prepare for increased absenteeism by training/cross-training personnel for temporary duty reassignment to assure continuous coverage of essential duties.
☐	3. Run daily building/area access histories to inform management of building occupancy trends.
☐	4. Educate officers on techniques to minimize exposure to infectious disease, to include immunization and proper use of personal protective equipment such as wear, removal, and disposal.
☐	5. Address officer physical and emotional well-being; increased pressures and continued obligations in and outside of work; create additional awareness of employee assistance programs (EAP) resources available.
☐	6. Use CCTV and security patrols to audit and review housekeeping staff adherence to established cleaning protocols.
☐	7. Leverage GSOC 24x7 presence to collect and collate actionable news items and provide key stakeholders each morning with overnight developments.
☐	8. After hours GSOC staff can monitor the Overseas Security Advisory Council (OSAC), WHO, CDC, and other government health and travel updates to assist in assessing future restricted travel locations and add relevant information to morning reports.
☐	9. Leverage visitor management systems to track/record records of visitors/vendors who passed/failed screening.
☐	10. Partner with IT to you have a well-defined cyber-attack prevention plan that can be immediately implemented and acted upon.
☐	11. Use building cameras and patrols to monitor and enforce applicable social distancing guidelines promulgated by state public health orders, stay-at-home orders, and any prohibitions or the maximum number of people in group gatherings (both inside and outside company property).

☐	12. Do not greet building visitors face-to-face. Instead, post contact instructions at all entry/exit points and on company website.
☐	13. Perform security work from home or at an alternate remote location.
☐	14. Provide information about isolating a person who has, or is perceived as having, an infectious disease.
☐	15. Implement a mass emergency notification system (such as Send Word Now or Everbridge) to provide emergency notifications to employees/visitors, should this become necessary.
☐	16. Consider pay increases for essential staff due to the exigent circumstances created by COVID-19.
☐	17. Set up an independent cost center to track all expenses related to COVID-19.
☐	18. Partner with HR to leverage the GSOC to manage/field employee calls, leverage FAQs from past HR inquiries, and be the on-call 24X7 support center.
☐	19. Devise a plan with IT to address FAQs regarding safe return of computers into the workplace. GSOC serves as 24x7 central clearing point for cataloging computer equipment being scanned for malware, virus etc.

	Virus Spread Mitigation
☐	1. Provide hand sanitizer/wipes at all entries, high traffic, common areas, office equipment, cafes, etc. Factor in that pilferage may occur.
☐	2. Minimize package delivery and eliminate inter-office mail. Establish cleaning and safe package opening procedures, (e.g., proper use of gloves, hand washing).
☐	3. Create and distribute awareness reminder of social distancing, hand washing/hygiene posters, CDC flyers, computer pop-up messaging specific to your business. Distribute these now and upon resuming business.
☐	4. Encourage staff to pack their own lunch. Coordinate safe foods with café and increase (possibly mandate) takeout orders in accordance with any federal or state guidelines.
☐	5. Balance security with safety; consider leaving interior doors open to common/non-critical areas to minimize surface contact, while maintaining full compliance with ADA, NFPA, and Life Safety Code.
☐	6. Increase the frequency of disinfecting patrol cars, locker rooms, break rooms, and other facilities.
☐	7. Review all areas where multiple touches typically occur each day and devise mitigation procedures for these surfaces (e.g., machines that dispense newspapers, coffee, and other items, as well as water coolers, elevator buttons, microwaves).
☐	8. Disable requirement for PINs to be used for non-critical internal areas of the building. For areas requiring a PIN, consider disabling the use or provide wipes at each PIN pad; post instruction to clean PIN pad and hands before and after entering PINs.

	Critical Vendor Reliance
☐	1. Indoctrinate key vendors and any others regarding cleaning/separation protocols for entering/working in the GSOC.

☐	2. Contact key vendors now regarding business resumption plans and gauge their current staff levels and support capabilities.
☐	3. Open channels of communication with key vendors and providers to ensure continuity of operation discussions take place.
☐	4. Inventory supplies, stock, and other essential items to ensure sufficient amounts are on hand or are available from vendors now, for when business resumes.
☐	5. Order necessary inventory of cameras/card readers, etc., that require typical preventative maintenance or replacement.
☐	6. Assess critical vendors' contagious illness protocols and benefits as they pertain to their ability to service your account, to ensure vendors approach is consistent with CDC guidance.
☐	7. Assess housekeeping staff training about cleaning procedures, staff education (language abilities), equipment usage, and benefits, to allow ill staff to stay out of the workplace. Ensure the cleaning team is educated on the proper use, removal, disposal of gloves, and any other potentially contaminated items they use or come across.
☐	8. Consider sending a letter to all vendors outlining your expectations to be notified, in writing, should one of their employees working at your facility contract, or is suspected of having contracted, COVID-19.

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

Program Best Practices > Policies and Guidelines >

Addressing COVID-19 Related Complaints and Reporting

By the Security Executive Council

Businesses continue to reopen under new and changing guidelines for mitigating the spread of COVID-19, even as cases spike in many regions. As employees and visitors re-enter the workplace, they are undoubtedly anxious about the new normal and what they will need to know to avoid the risk of infection.

Organizations need to be prepared to respond to questions and concerns about new risk mitigation procedures and protocols. They also need to outline the channels for communicating any observations, concerns, or suggestions regarding personal protective equipment use, screening, distancing, sanitization, and other related topics.

Businesses must also outline the steps they will take to address the non-compliance of the newly implemented procedures, many of which are required by local, state, or federal guidelines.

Here are some basic questions to consider.

What must every employee and visitor know?

- The details of each new policy/guidelines and what each person must do to be compliant.
- The responsibility of each person for reporting a concern that might lead to contamination.
- The steps the company will take if a person is observed or said to be acting outside of the policies/guidelines.

- Any reporting requirements (in or outside the company) the business must meet in accordance with regulatory guidelines.

Information regarding new risk mitigation measures must be provided to all who enter your buildings. Will your company require a formal acknowledgment from all employees and visitors entering your property? What about in leased space? If your company has organized labor unions, consider sharing any new procedures or controls with union representatives ahead of time to avoid unforeseen challenges.

How will you receive questions, concerns, and complaints?

- Reporting hotline
- GSOC
- Online form
- Phone call
- E-mail
- Private meeting

Ensure that incoming concerns or questions are fully documented; any records could be subject to disclosure if legal proceedings follow. Also, consider providing a statement about whether anonymity can be provided.

Who will respond to questions, concerns, and complaints?

- Security alone
- HR alone
- Individual function leaders
- A multidisciplinary team of responsible parties
- Outside third party

Include as much transparency in your response protocols as possible. Proactively state what you will and will not share about reports received, knowing that many employees and visitors will be anxious about rumored concerns that get further socialized at work. No feedback is often understood as "no action taken."

How will complaints be resolved if confirmed by interview or investigation?

- Verbal reprimand
- Escalating written warnings
- Termination
- Removal from property

Outline the process, steps, and documentation maintained. If security is involved in enforcement, it is critical that HR or other responsible functions support the process with well-defined procedures for disciplinary action.

How will the response and resolution plan be communicated?

- Posters
- Emails/Company newsletter
- Link on company intranet
- Verbal reminders
- New hire orientation
- Company town halls

The response and resolution plan must be clearly and broadly articulated to the visitor and employee population. Make it clear employees have a responsibility to report concerns and identify any reporting requirements the business must meet in accordance with regulatory guidelines.

Your response and communication processes are essential to ensure that employees and visitors have confidence in the team responsible for responding to concerns and maintaining compliance with regulatory guidelines.

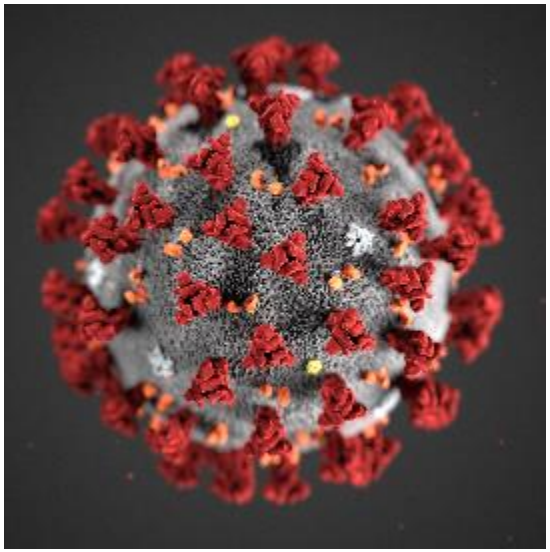
About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence**.**

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

Redacted Summary: COVID 19 – Are we ready?
Considerations and Implications

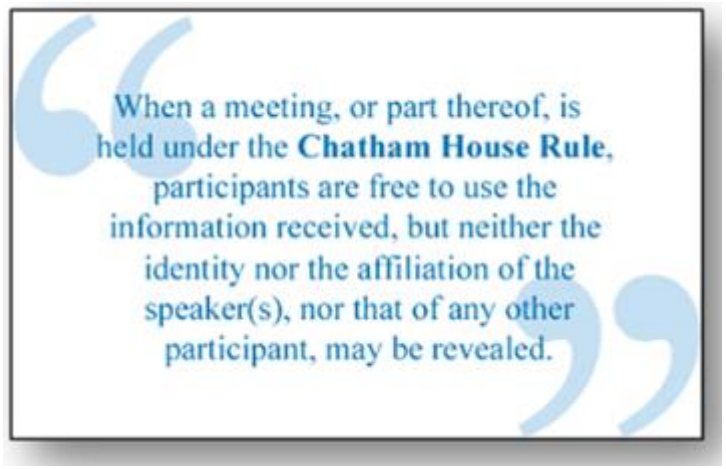
Next Generation GSOC (Fusion Center) Group
Virtual Advisory and Research Forum
March 19, 2020



SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Welcome Next Generation GSOC (Fusion Center) Group

- 62 active member organizations
- 130+ research participating companies
- Industries – banking, government, healthcare, tech, manufacturing, NGO, pharma, retail, utilities, Etc.
- Global, national and regional brands
- $0 NGOs - $535B market cap multinationals



5 Member Surveys to Date

Plan? Planning? Planned?

- Regardless of where business continuity resides (e.g., IT, Manufacturing, Ops, CAO, etc.), Security has a role to play and incredible opportunity to prove its value. **Plan.** Continuously improving operations lend confidence.
- Few functions aside from Security have the experience, expertise, and muscle memory to manage small and large-scale crisis events. The skills, competencies, and leadership traits required to manage a crisis are transferrable. Pandemic teams just need to import health/medical expertise into the mix.
- Organizations likely already have plans.
- It's never too late to mitigate…
- Every SMART organization will be doing thorough After-Action-Reports to modify and improve their operations.
- To borrow a phrase from the National Preparedness Leadership Institute – what's needed is "swarm intelligence" coordinated actions by disparate teams and clear leadership.

George Campbell and Dan Sauvageau
SEC Emeritus Faculty, formerly Fidelity Investments

Group Discussion

- Best Practices Topics
  - Virtual GSOC
  - Redundant locations
  - Staffing/scheduling modifications
  - Issued headsets, keyboards, etc.
  - Cleaning intervals
  - Access protocols e.g., testing for employees, Visitors prohibited
  - Supplies/provisions for shelter in place
  - Virtual intelligence / remote guarding
- Considerations and Implications
  - How many of us are proactively providing intel to the business?
  - Are we also looking past tactical to strategic implications?
    - To the business?
    - For our teams?
    - For us as Security leaders?
  - What if you need to close your GSOC? Impact to business?

Select Next Generation Service Competencies to Mitigate Threats/Situational Risks…

Remote Critical Facility, Supply Chain, Travel & Special Events - Dynamic Risk Assessment and Threat Recognition

GSOC/Fusion Center Integration (Aggregated or Distributed) for All-hazard, Unified Risk Oversight (URO) & Mitigation Response

INTERNATIONAL SOS

JOHNS HOPKINS SCHOOL of MEDICINE

everbridge

SureView systems

topo.ai

CAP Index® OUTSMART CRIME

Two-way mobile alerts, warnings, and advisories

LIFERAFT

SECURITAS

NC4

Technology-equipped Uniform Services

Autonomous Assistance

ROBOTIC ASSISTANCE DEVICES

Intelligence Informed

G4S

PROTOS SECURITY

911 SECURITY

eLUMINATE CRIMINAL ALERTS

Friction-reduced, if not frictionless

ENDERA

Persistently Informed for Insider

Smart, analytic, audio/video edge devices for 3D Access Control

Contributing Attributes:

- AI / + Human + Machine Intelligence
- Analytic alarm, anomaly, and exception detection
- Integrated and inter-operational risk reporting, communications, dispatch response and critical incident mitigation management
- Performance & Value Metrics
- After Action-informed continuous improvement

Perspective?

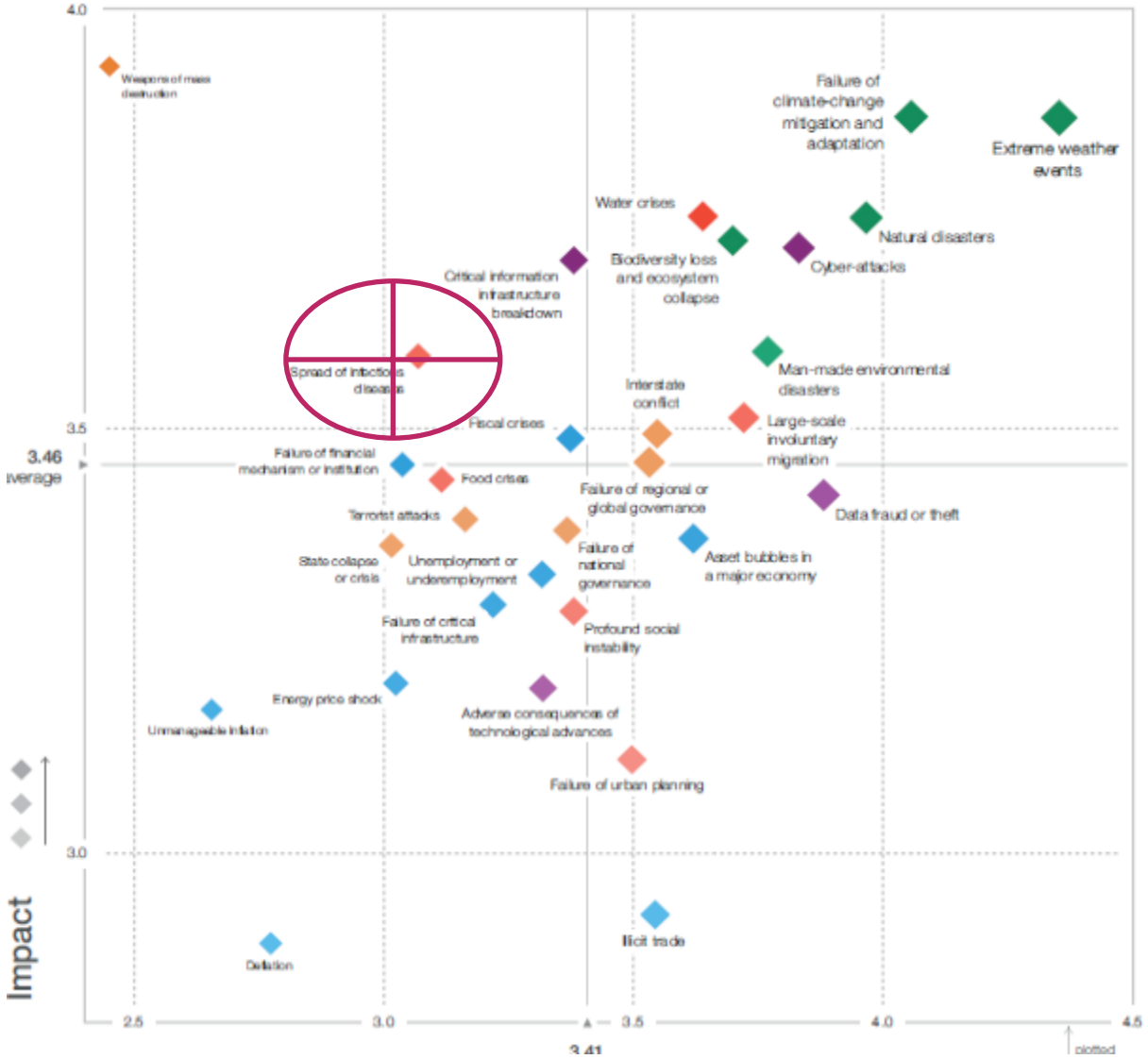
Global Level Risks 2020

Few Surprises…

Pandemic or Infectious Disease Risk has been on radar since 1918

The Spanish flu pandemic of 1918, the deadliest in history, infected an estimated 500 million people worldwide—about one-third of the planet's population—and killed an estimated 20 million to 50 million victims, including some 675,000 Americans.

Spanish Flu - Symptoms, How It Began & Ended - HISTORY



Is Security Ready to Contribute and Lead Where Required?

The Challenge - What are the Security-unique demands this pandemic presents to your company? How well have you assessed the opportunity to serve?

- Is Security effectively at the table with all of its capabilities?

Risk to Security Employee and Teams- Monitoring and action for red flags.

- Established procedures and protocol with contract security staff – They may have the most contact; are they equipped, informed, and ready for the challenge?
- Cleaning crews- inherent risks and need for more aggressive facility cleaning processes – Instructions and SOP's in multi-lingual format?

Addition of qualified medical expertise on crisis teams – MNCs should be prepared for varied response, guidance and direction in foreign countries.

Is Security Ready to Contribute & Lead Where Required?

Containment- What is a smart perimeter and what is Security's role? Are your visitor management and access control systems up for the task and ready to flag, monitor, track, or contain?

- Who are persons with access at highest risk and how to engage them?
- What are the implications of an enforced area lockdown?

Address Information Security threats and proactive IT engagement from expanded work at home.

Aggressive engagement of GSOC in situational monitoring of proximities around corporate sites and working populations.

The Security Executive Council is the leading research and advisory firm focused on corporate security risk mitigation strategies and plans. We work with security leaders to transform security programs into more capable and valued centers of excellence.

Get to know the SEC: Watch our 3-minute video for a quick overview. Read what your peers have to say about working with us. Or contact us at: contact@secleader.com

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

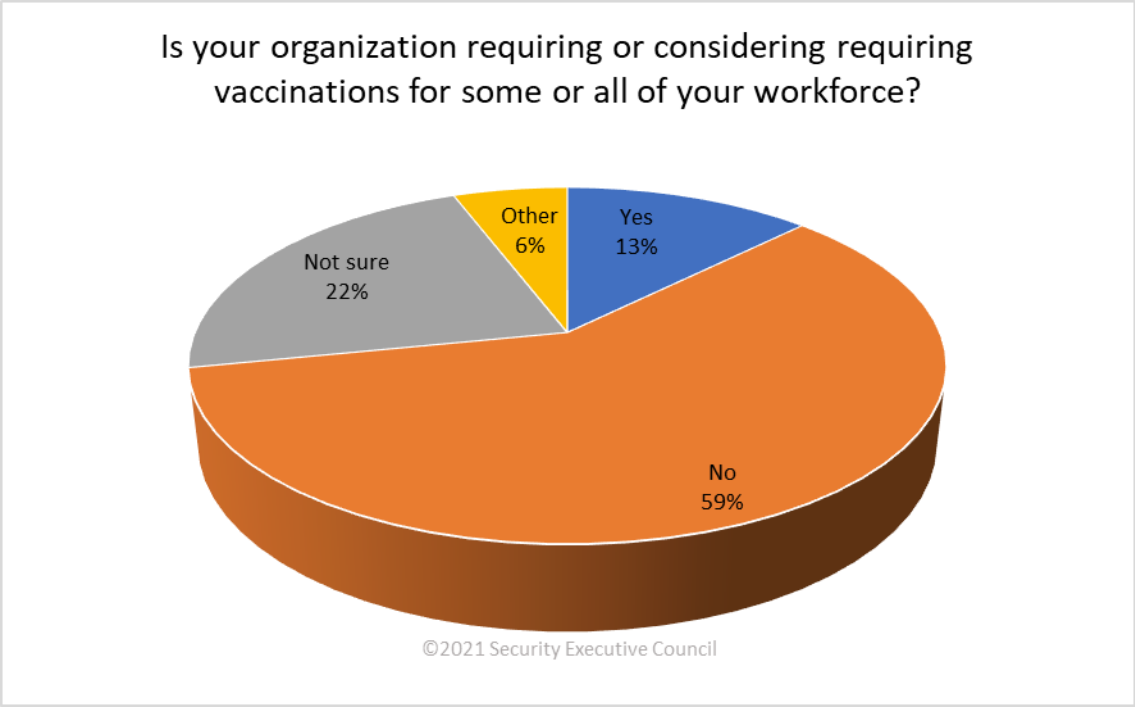
Program Best Practices > Policy and Guidelines >

Expected Employee Response to Mandatory COVID-19 Vaccinations

By the Security Executive Council

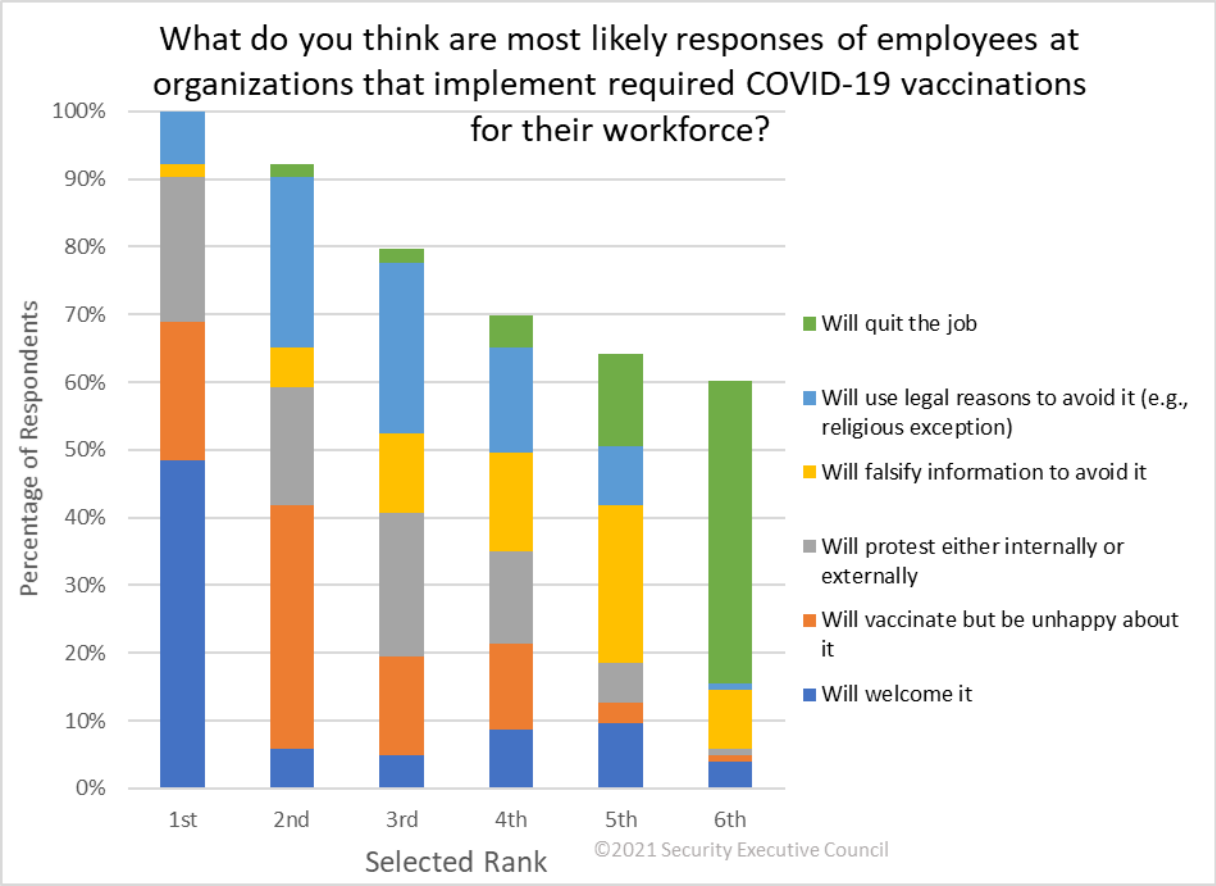
As COVID-19 vaccinations rollout across the world it is unclear whether all people will voluntarily choose to be vaccinated. Businesses may be faced with a decision to mandate vaccinations to keep their workforce safe and healthy.

In this Security Barometer we asked your peers what they thought the likely fallout may result from required COVID-19 vaccinations.



Some survey participants commented that their organizations were making vaccinations mandatory only for front-line workers, not required unless customers required it, or only requiring vaccinations based on health authority's guidance.

The survey participants were asked to rank what they thought would be the most likely employee responses if organizations instated mandatory COVID-19 vaccinations. (Respondents did not have to rank all options).



The voting resulted in the following ranking:

1. Employees will welcome mandatory vaccinations.
2. Employees will vaccinate but be unhappy about mandatory vaccinations.
3. Employees will protest either internally or externally about mandatory vaccinations.
4. Employees will use legal reasons, such as religious exception, to avoid mandatory vaccinations.
5. Employees will falsify information to avoid mandatory vaccinations.
6. Employees will quit their employment rather than submit to mandatory vaccinations.

The following contains selected and edited commentary from survey participants:

- Different rules by country, and possible within US state cause concerns for organizations in requiring or promoting.
- Rather than put the focus on the person, our organization is putting the requirements into the role. For example, if a role requires international travel and a vaccine is required by the destination countries, then the employee will have to have the vaccine or look for another role that does not require travel and the vaccine.
- We are not mandating unless required by government. Our HR and legal staff have offered guidance advising against mandating the vaccines from and ethical, administrative and litigation risk perspective.
- Our organization is taking the approach that this is a health decision that needs to be made by the individual. In addition, as a global company, each country will have access to different vaccines of varying degrees of efficacy and transparency of the clinical trial data. However, the company will abide by any local government mandates.
- Our organization offered vaccinate all since Dec 17th. Was not mandatory. We are coming to an end of willing vaccinations. We are at 16,500 out of 24,000 Employees and contractors.
- The answers above will be influence with passage of time. The longer the period of time the elapses without vaccine issues, the likely to shift my answers to "will welcome it"
- We strongly considered requiring the vaccine but after much internal discussion, decided not to require it, but to put significant efforts behind a positive vaccine campaign to get the vaccine. We took steps to inform our teams about it, creating a dedicated promo and FAQ page within our internal Covid response website (intranet). We are having CDC and local Medical Center experts available for our virtual town hall meeting where the employees are able to submit questions in advance and participate in a Q&A. Our internal culture will be more prone to accept and proceed with it in this manner versus a required vaccination policy.
- We will follow local authorities' guidance and adapt our policies accordingly.
- Employee response will vary depending on company country and industry sector. Some employees will be greatly relieved, believing that a vaccinated workforce will be protected against virus transmission. Setting vaccine mandates risks hardening the position of employees who were otherwise ambivalent, and opposition to such a mandate can be exhibited in either protest or seeking out legal protections. Companies need to be careful about mandating any medical procedure - all medical procedures carry a degree of risk, which means any company requiring vaccination is also taking on liability if an adverse event should occur.
- Irrational responses will largely reflect the sources of propaganda employees use to misinform themselves.

Visit the Security Executive Council web site to view more resources in the Program Best Practices series.

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Risk-Based Security > Risk Assessment >

Reimagine Risk and Security: Evolving Beyond COVID

By the Security Executive Council

A recent SEC Security State of the Industry event for Tier 1 leaders explored how practitioners must reimagine risk and security to envision a post-COVID future.

Here are some of the highlights of the discussion, which featured Bob Hayes, SEC Managing Director; Kathleen Kotwica, EVP and Chief Knowledge Strategist; Dan Sauvageau, Emeritus Faculty - Executive Influence; Francis D'Addario, Emeritus Faculty - Strategic Innovation; and Jim Hutton, Emeritus Faculty - Strategy and Leadership Development.

Security Success

If we want to adapt to an uncertain future, we first must look at what we're doing now, why and how we're doing it, and then examine whether that model matches the reality we are facing.

It's useful to first revisit how we achieve security success in any environment.

- Success requires you to recognize Security's current conditions, culture, circumstances, and resources (your C4R). You may have great plans, but if you don't consider the C4R, you'll likely fail to gain traction.
- Successful leaders develop a compelling story for Security. They set expectations and give examples of what success looks like. They use it as a tool to gain strategic input. Now, more than ever, our story is important; however, it is likely to change due to the current environment.
- We need to understand the entire realm of Security. The SEC has outlined the Universe

of Security Success (see figure 1). This is the accumulation of 15 years of research and collaboration with thousands of leading security practitioners. Not all elements in this universe are necessary for everyone. The trick is to find the elements that will provide your organization the most value.

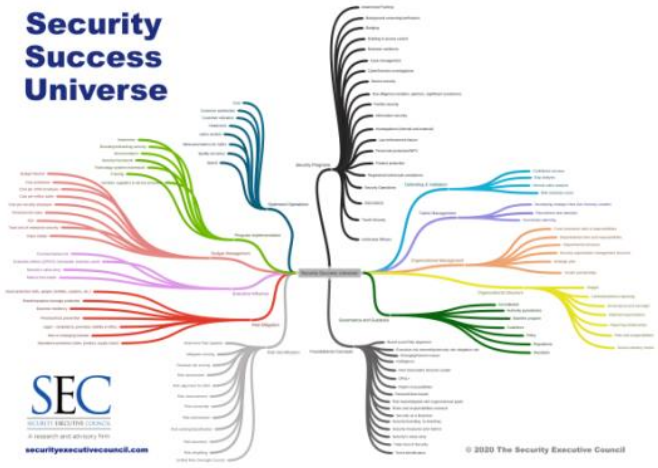


Figure 1 The Security Success Universe

Security Success Universe

The image to the left contains the universe of possible elements for security practitioners to consider. Our research based on security thought leaders' key success elements resulted in 13 categories:

- Foundational Concepts
- Risk Identification
- Governance/Guidance
- Risk Mitigation
- Executive Influence
- Organizational Structure
- Organizational Mgmt.
- Budget Management
- Program Implementation
- Talent Management
- Optimized Operations
- Defending/Validation
- Security Services/Programs

In total there are 115 unique elements to consider for your success equation. Consider implementing the ones that can bring value to your organization.

Why Reimagine Risk and Security Now?

A worldwide pandemic of this scale has not been seen in our lifetime. It has produced a tremendous amount of change. Organizations and security departments clearly have their hands full reacting to twists and turns. But we need take the time to be prepared for an alternative future state.

Your company today is not the same company it was last year. A recent McKinsey report claimed that a majority of businesses have changed how they go to market since the pandemic started.

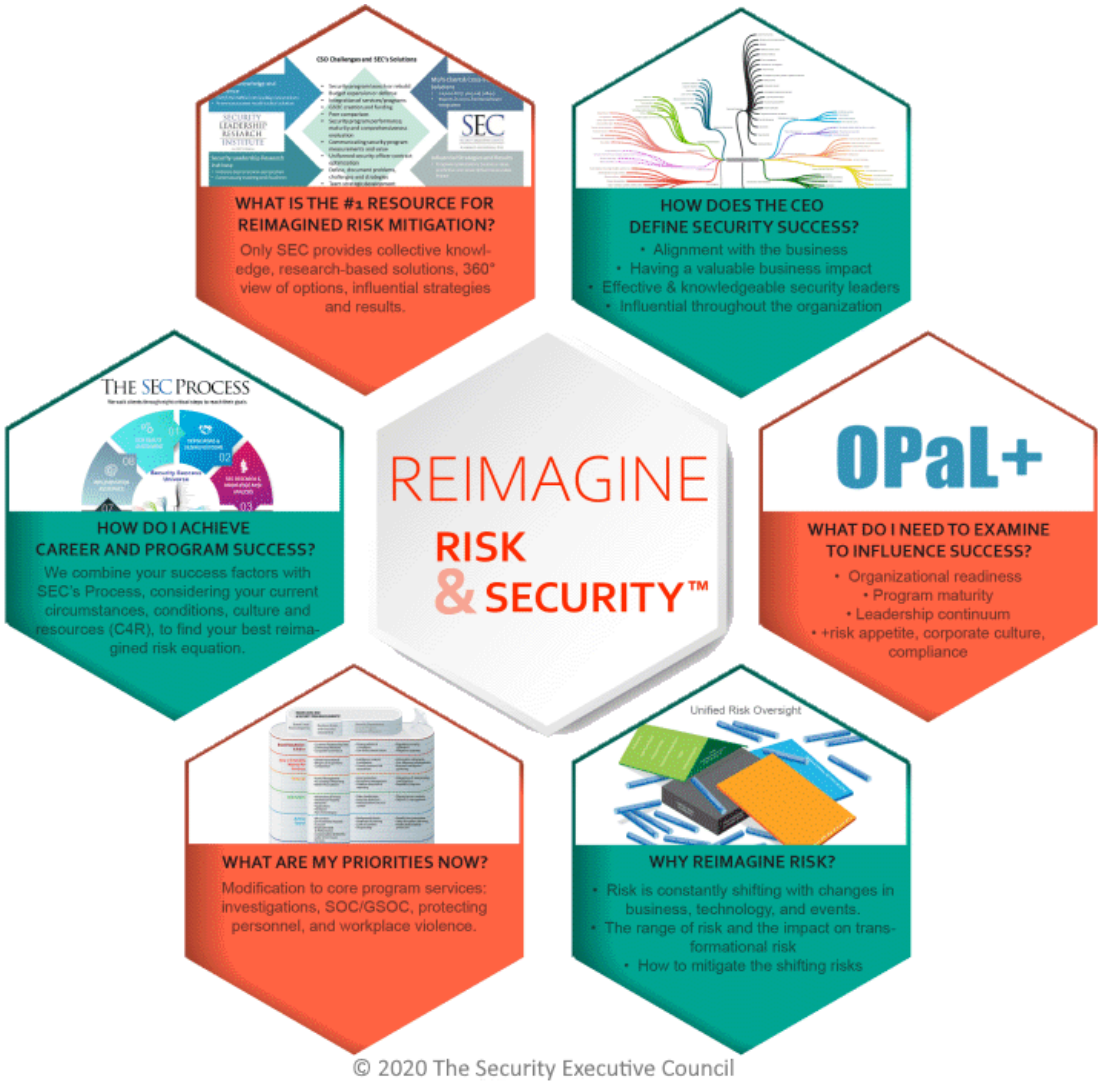


Figure 2 Reimagine Risk and Security

Reimagining risk and security (figure 2) means:

- recognizing risk shifts based on current events, company changes, social, economic, and political changes.
- re-assessing your organization's security risks and revisiting your programs, services, and mitigation strategies informed by these changes.
- prioritizing any modified plans while aligning with the organization's new directions and goals.

Security needs to look ahead. What may permanently change, and how will core security programs adapt in a VUCA (Volatile, Uncertain, Complex, and Ambiguous) world?

Executives are Looking for Opportunities

According to McKinsey's Innovation Through Crisis survey, most executives see new opportunities for growth right now, but few feel confident they'll be able to harness them. Security can be a partner in this endeavor. Opportunities exist in moving fast and taking on more risk. Security can help in the reimagining process by doing what we do – objectively articulating the potential security risks that may derail new growth.

Security must adapt its core programs to meet the company's new requirements and the need to leverage new opportunity.

Risks from Continued Work from Home

The continuing work from home model brings both physical and Information risk.

On the information protection side:

- Employees working from home are unlikely to use safe practices on their own.
    - A CyberArk study shows that 60% of remote workers use unmanaged BYOD to access company assets; 89% use the same password across platforms; and 57% insecurely store passwords in browsers.
- Vendors are also using remote workers.
    - Are you comfortable with their workers' remote security?
    - Do you trust they will contact you in the event of a breach?
    - Do they have the capacity to meet your security requirements at all?
- Insider threats
    - In the brick and mortar environment, security often gets tips on insider risk from coworkers who see red flags. In a work-from-home environment, that resource is lost. How do we replicate that informal environment in a remote world?

On the physical security side:

- The economic forecast shows a potential increase in crime; should companies install home security systems to keep staff and assets safe?
- Hiring concerns - the intuitive behavioral signals that occur during an in-person interview will be harder to assess on video meetings. Perhaps we will be able to use automated behavioral analysis applications?
- What will access control, video surveillance or medical emergency procedures look like? How do we accomplish that in a work from home environment? Or can we?
- The security control center (SOC) or GSOC is one tool that could help you reimagine some risk processes. Will it take calls from all employees? Will the GSOC take on situational awareness, coordinate responses, or send individualized advisory

information to help remediate potential issues?
- Investigations – how will we handle hostile interviews, equipment recovery, or searches for material or information? Do employees sign a condition of employment document that ensures Security can come and get the equipment if the employee does not return it?
- Risk mitigation is the responsibility of many functions across the organization. Working from home will make cross-functional teams even more important for coordinating handling events. This may also include updating or developing new policies.

At-home employees continue to share responsibility for security. It's important to communicate that responsibility and articulate exactly what they need to do to manage security in their workspace. It's also important to solicit their feedback. Companies are pivoting –from auto parts to ventilators, distillers to sanitizers – and those solutions may be coming from the shop floor. Find out what employees are thinking and what they need. Be culturally relevant. Use apps to let them provide input and feedback about their own safety, security and health.

Further Resources

For more information about some of the foundational concepts of security mentioned in Figure 2:

Unified Risk Oversight

Board-Level Risk

OPaL+

Program Continuums

Security's Value Potential

Maturity Model

Visit the Security Executive Council web site to view more resources in the Risk-Based Security: Risk Assessment series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

