TALGLOBAL

# Reopening and Staying Open

## Planning, Execution, and Compliance

*TAL Global is an elite security consulting and risk management firm that protects human and physical assets around the globe. We are a team of world-class, interdisciplinary security experts that join forces to identify, analyze, and mitigate risk for our clients and their organizations from every vulnerability – inside and out.*

## Contents

Nations around the globe, including the United States, are in the process of reopening. However, many businesses will confront numerous challenges as they attempt to resume business operations.

Further, these challenges may change as conditions change—businesses will need to be agile and able to pivot quickly, should conditions warrant.

This includes challenges surrounding corporate operations, and investigating and addressing possible threats, along with overall security. Some of the issues corporations may be confronting in the coming months include the following:

**Ensuring Cybersecurity**

COVID-19 has caused millions of workers in the United States to stop commuting to their places of work. Instead, remote working has become the norm. Further, some organizations have already announced their intention to make this standard operating procedure going forward.

Just to see how quickly things have changed, as recently as March 1, 2020, the idea of having entire companies shift to remote work was unheard of. In fact, many organizations considered it an impediment to corporate culture. COVID-19 has changed all this, possibly forever.

An excerpt from a *New York Times* article published in June 2020 reports that before the pandemic, no more than 10 percent of Accenture's 500,000-plus employees worldwide worked remotely on any given day. By mid-March, nearly all of them were working remotely.

Supporters of a remote work program (RWP) believe it has many benefits, such as the following:

- Greater flexibility for workers
- Real estate cost savings for businesses
- Reduced travel costs for staff
- Enhanced worker productivity
- Positive impact on the environment

Because of these and other benefits, Kate Lister, president of Global Workplace Analytics, estimates that 30 percent of the U.S. workforce will be working from home—one or more days each week—by the end of 2021.

This migration to remote work was born of necessity. It happened so quickly that many IT professionals did not have time to implement data security programs that would allow people to cooperate safely and securely from home.

Now, however, as businesses accept remote working, they are beginning to revisit current cybersecurity programs and practices. The goal is to put in place new systems and procedures to help ensure that their businesses, clients, and staff are protected from unwarranted online intrusions, or what are referred to on the internet as “bad actors.”

To help address this situation, the first thing corporate managers must do is assess whether their current cybersecurity practices meet industry standards. Then, they must take the next steps and investigate the following:

- Does the company have a formal RWP in place, including policies and procedures for remote work?

- How does the RWP integrate into the company's existing/pre-COVID cybersecurity program?

- Does the organization have the proper cybersecurity tools in place for the RWP?

- Are these tools capturing all data “at rest, in use, and in motion”? **(See Sidebar: What Is Data at Rest?)**

- Does the business incorporate mobile device management tools, especially for BYOD (bring your own device) situations?

Further, there are several proactive measures all corporate managers must consider when it comes to ensuring cybersecurity. These include the following:

- Active prevention controls are in place to protect data transmission systems.

- Requiring “credential verification,” having an authorized third-party system that requires proof of an individual’s permission, knowledge, and qualifications to be involved with a specific project.

- Implementation of multifactor authorization for all VPN (virtual private network) connections to increase security.

- Recognition that each company is part of a chain. If one business is attacked by hackers, others doing business with that organization may also become a target.

**Guaranteeing a Healthy Reopening**

Businesses and employers should plan to protect the health of their staff when they return to work. Fortunately, OSHA reports that most

American workers will likely experience low- or medium-exposure risk levels at their job or place of employment.[2]

However, businesses must still take proactive steps to protect their staff. Further, in their efforts to remain open, they must continue to monitor credible news sources that provide information about the virus. They must also strictly adhere to the guidance provided by government and public health authorities.

In preparing to reopen and stay open, businesses should do the following:

- Identify a workplace coordinator who will be responsible for COVID-19 health issues and their impact in the workplace.

- Review all cleaning strategies in place to ensure they are designed to minimize the spread of the infection.

- Implement flexible sick leave and supportive policies and practices for employees.

- Determine how the business will operate if absenteeism spikes from increases in sick employees.

- Decide what steps to take if staffers must stay home to care for sick family members or children unable to go to school.

- Implement protocols to ensure adherence to mask wearing and social distancing.

**Reducing Transmission Among Employees**

One of the primary goals of businesses preparing to resume operations—and stay open—is to take active steps to reduce transmission of COVID-19 among employees. Some of the guidelines offered by the Centers for Disease Control and Prevention (CDC) to accomplish this goal include the following:

- Actively encourage sick employees to stay home.
- Require temperature checks as employees come to work.
- Identify areas in a facility where workers might be exposed to COVID-19 at work; this could include areas where staffers tend to congregate.

· Require employees that test positive to the disease or feel ill to self-isolate immediately.

· Educate employees about how they can reduce the spread of COVID-19.

Other considerations to help reduce the possibility of transmission of the virus between building users include the following:

**Ventilation:** Improve building ventilation systems by increasing ventilation rates throughout the facility. This should also include increasing the percentage of outdoor air that circulates in the system.

**Respiratory etiquette:** Encourage if not require respiratory etiquette and effective hand hygiene practices for employees, customers, and worksite visitors. This may require training and education to ensure compliance.

**Employee travel.** Minimize employee travel. In-person meetings and other gatherings should also be reduced or eliminated.

### Physical Security

When we discuss physical security, we are referring to the bodily protection of an organization's staff and executives, on- and off-site. This would also include when they are traveling for the organization.

According to experts at the Carnegie Endowment for International Peace, several main aspects of site security are likely to change in the post-COVID-19 period, such as the following:

- Demand for security guards will increase sharply. This will be accompanied by a change in the employment profile and requirements of the newly employed guards. For instance, additional training in crowd control will be needed along with training related to "temperature monitoring" of crowds attending civil events, accurately reporting on these events, overcrowding prevention, and how to control situations *before* they get out of hand.

- Some organizations, such as retailers, will need to provide curbside delivery for customers while still ensuring minimal points of contact, and contactless delivery of products will need to be developed. In all cases, practicing social distancing and personal and site hygiene will be required. Such practices will also need to be in place when vendors make deliveries to an organization.

- New passive and active monitoring, reporting, and enforcing technologies will be necessary to offset the high cost of paid guards; however, guards will be required to become familiar with existing and evolving physical security solutions, allowing them to optimize their adoption and use.

- While physical safety is the goal, existing and evolving technologies must still comply with privacy requirements.

These changes will dictate revisions to best practices, which will then have to be taught to management and staff. Special facilities, such as retirement, assisted-living, and elder-care facilities, will require a complete reconfiguration of site security practices. These organizations will need to outlay significant resources to enact these changes.

Further, to ensure physical security, organizations will need to make several changes to their facilities, most of which were not even a consideration just a few months ago. These will include the following:

- Compartmentalization of staff to help minimize personal interactions
- Social distancing markers
- Plexiglass barriers and other social separation devices
- Temperature monitoring stations

These changes and others are not only recommended but may be required in some jurisdictions, making businesses and other organizations responsible for their proper implementation. Security teams are trained in these areas and can help ensure best practices are followed.

**Business Continuity**

We know there is hardly any business that has been immune to the disruption and damage inflicted by COVID-19. We also know that organizational resilience and the ability to make changes when needed, and to do so quickly, are keys to successful business reopening and continuity.

If there is one thing we can learn from this pandemic, it is that in future crises, businesses must avoid late activation of continuity plans. This means adopting and practicing strategies now to help mitigate against late activation.

To accomplish this, we suggest a solid business continuity strategy that includes the following three-pronged approach:

- **Prepare.** Get ready for what is coming next. Allocate resources, assign roles, set priorities, establish a command center, train, and practice.

- **Predict.** Create the tools required to monitor vulnerabilities and threats and bring them to the attention of decision-makers.

- **Prevent.** Prevention will largely depend on established organizational resilience, procedures, and preparations to help leverage in crisis.

This three-pronged approach, as well as everything previously discussed, should help ensure a safe, secure, and healthy reopening for businesses around the globe. Further, and just as important, it can help ensure that they stay open.

Too many businesses already have fallen by the wayside because of the virus. Our goal here is to help ensure yours is not one of them. We are here to help.

### Sidebar: What Is Data at Rest?

Data at rest refers to information that is stored physically, in a digital format. Data at rest tends to be a favorite target of hackers. Data in use or in motion refers to information that is being accessed in-house or online. Typically, this data is encrypted for safety.

Sources: Guidance on Preparing Workplaces for COVID-19, prepared by OSHA (https://www.osha.gov/Publications/OSHA3990.pdf)

Based on Igor Ivanov, "Rethinking International Security for a Post Pandemic World," Carnegie Endowment for International Peace, April 20, 2020. (https://carnegieendowment.org/2020/04/20/rethinking-international-security-for-post-pandemic-world-pub-81584T)