

5 Business Resiliency Tips for COVID-19

Consider taking precautions to keep your business running.

As concerns about the COVID-19 outbreak and its impact on the global market mount, so does the potential for service disruptions. From supply chain interruptions to employee health concerns, unanticipated developments can threaten your core business and result in losses.

It's impossible to predict exactly how your business will be impacted by the COVID-19 outbreak, but preparation is critical. Consider the following tips to help steer your business safely through uncertain times.

1. Prepare for a Work Environment Change

Employee connectivity is a crucial tenet of any business resiliency plan. If remote work is recommended, it's important that all employees have access to necessary technological equipment to do their jobs properly. Make sure network connectivity is available to essential employees, and work with internal personnel to ensure that data protection practices are replicable away from central office hubs. Ensure that all video conferencing and telephone systems are functioning properly. Employee absences can also increase during uncertainty, as they manage adjustments to daily life, so make sure employees in essential functions have trained backups who can cover their workload.

2. Prepare to Pivot your Plan

Your business resiliency plan is not a final document that represents your total response. Conditions can change quickly, so be prepared to make adjustments to your resiliency plan based on new information. You can seek the help of trusted experts in public health, emergency preparedness, treasury, payments, communications, legal, operations and others to help you monitor and react to sudden changes. For example, the CDC offers resources such as its [Interim Guidance for Businesses and Employers to Plan and Respond to Coronavirus Disease 2019](#). Because information moves fast and professional opinions can differ, be sure to consult multiple expert sources to get a well-rounded perspective on how to act.

3. Communicate Clearly

The 24-hour stream of information that accompanies global events like COVID-19 can be difficult to navigate. If a serious business disruption occurs, your clients, partners, vendors and employees need clear and concise messages about the scope of impact.

Delivering the right message at the right time starts with designing a robust communications strategy for both internal and external audiences. You may consider creating a small task force or communications team to lead the charge of drafting and vetting all information sent from your

organization. Additionally, it's important to work with internal partners to identify secure communications channels that are accessible even during prolonged or increased disruption.

4. Commit to Continuous Learning

Remember that even with a plan, unanticipated issues can arise. It's important to document all developments, impacts and responses for the sake of learning. Even if your business successfully weathers the storm, a future outbreak could result in even worse interruptions. That's why collecting data and insights in real time is beneficial. Look for areas where communications failed, bureaucratic inefficiencies were exposed or a lack of response resulted in negative impacts. These can become learning experiences to prevent losses during future business disruptions.

5. Stay Aware of Cyberattacks

Cybercriminals and fraudsters often take advantage of business disruptions such as COVID-19 to launch highly targeted attacks. Employees are always your first line of defense against cyberattacks, but take steps to re-educate them on strategies to protect your business. Often, these events can be a distraction and lead to increased risk. To combat this, provide employees with tools and resources on ways to spot different cybersecurity threats, including business email compromise (BEC), phishing, ransomware, social engineering and more. It can also be helpful to outline procedures for reporting threats, and reiterate company policies around password security. Stay mindful that cybercriminals and fraudsters are keen to capitalize on the chaos caused by unanticipated global events. You are your best defense!