

# Factoring Coronavirus into Your Business Continuity Plan

By Mark Bednarz, CPA, CISA, CFE, Partner

We work with for-profit, not-for-profit and governmental clients, and the majority of these organizations have either a business continuity and/or disaster recovery plan in-place. In constructing these plans, most threat scenarios typically cover natural disasters such as hurricanes and earthquakes, power grid outages and major cyberattacks. In recent years, some entities have had to activate their plans to deal with Hurricane Sandy and ransomware incidents.

Almost no organization has ever dealt with the outbreak of a new virus like COVID-19 (coronavirus) and the adverse impact it can have on employee health and their families, contaminated workplace facilities, questionable food sources, stockouts of essential goods due to supply chain disruptions and other facets of business operations. Management should take immediate action in either developing or revisiting their business continuity plan (BCP) because no industry is immune to this coronavirus because little is known about how it spreads, how long it remains potent on surfaces, the human incubation period and what safeguards beyond quarantine are truly effective.

While some companies are already taking precautionary actions, such as disinfecting offices and conference rooms, sending communications to customers, cancelling non-essential travel, prohibiting large group meetings, converting face-to-face meetings to web conferencing and splitting the workforce between multiple facilities, it is becoming clear that so much more will likely be required.

## Planning and Risk Management

In facing a crisis, planning is critical. A good starting point is using business continuity planning as a foundation for deciding how to address catastrophic events that can negatively affect an organization. The strategy that management puts in place must – at a minimum – consider its employees, critical processes, customers, suppliers and other stakeholders. While most events are confined to a specific geographic area, the response to a pandemic is more complex and forces management to strategize on different severity levels, requiring assumptions about the anticipated spread and duration. COVID-19 is an example of how a threat that appears to have its origins in China has evolved into a global issue due to travel and transportation.

With every BCP, there is a risk assessment component that identifies the potential threats and vulnerabilities and prioritizes the severity of each business disruption. Management needs to involve employees in multiple areas and departments to understand the risks and the associated likelihood and impact. The specific risks related to the pandemic must be incorporated into the business impact analysis (BIA) portion of the BCP, which should include:

- Assess and prioritize the critical business processes and locations affected by the coronavirus
- Determine the impact of the coronavirus on the business processes, employees, customers, service providers, technology and regulations
- Estimate the recovery time objective (RTO), which is the target time management sets for the recovery of the organization's IT and business activities after a pandemic

## Pandemic Considerations

Due to the complexities associated with any pandemic, management should develop a pandemic plan, which requires careful planning, preparing, responding and recovery. Numerous internal and external factors and interdependencies should be considered including:

- Assign a group to monitor the stages of the virus outbreak
- Identify possible work-related exposures to the coronavirus
- Monitor absenteeism, which can be a result of quarantined households, ceasing public transportation and school closings

- Educate employees on preventive care and human resource policies or topics (i.e., workplace and leave flexibility, non-essential business travel)
- Identify key individuals at different locations who will have the authority to take appropriate action that is documented in the pandemic plan
- Make procedure manuals available and consider cross-training for critical functions or processes
- Identify and establish communication protocols with employees, investors, customers and suppliers

Responding to a pandemic requires significantly more collaboration between management, employees and outside parties than other types of events. Pandemic events will likely last far longer than typical BCP threat scenarios so communication is essential as the pandemic continues to evolve. Assigning individuals to closely monitor the situation and communicate with key stakeholders should be a top priority.

## Testing

Though an organization may have a well-documented plan with detailed analysis, testing is a critical component in the program. Testing allows the identification of issues and promotes employee confidence. By performing tabletop or other testing methods, it allows individuals to understand their roles and responsibilities.

We have seen situations where management has run into issues or technical challenges related to inadequate technical resources, lack of communication with outside parties, the inability to properly identify or classify events due to environmental and other changes, and the lack of coordination with employees. In addition, a crisis takes a toll on an employee's mental health and physical stamina as they try to balance their work commitments with their fears and concerns about their homes and families.

One example of a technical challenge is the heavy reliance on remote access if an office is closed and personnel must work from home. [Refer also to our article [Dealing with the Cybersecurity Challenges of Coronavirus](#).] The information technology department should work with management to test their remote access capabilities and determine whether their infrastructure has the capacity to handle the workload and that users are aware of the steps to access network-based computing resources. This assessment should extend beyond on-premise systems to those applications hosted by software as a service (SaaS) providers where less may be known about their capabilities under such circumstances.

## Takeaway

Benjamin Franklin's words – ***By failing to prepare, you are preparing to fail*** – still hold true today. Your well-considered, well-documented and well-tested BCP can help protect both your business and your workforce.

## Contact Us

For assistance in developing a business continuity plan with the coronavirus or any pandemic top of mind, please contact the partner in charge of your account or the author:

Mark Bednarz, CPA, CISA, CFE  
 Partner, Risk Advisory  
[mbednarz@pkfod.com](mailto:mbednarz@pkfod.com)

[www.pkfod.com](http://www.pkfod.com)

## About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, twelve offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 800 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 29th on *Accounting Today's* 2019 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today*. In 2020, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.