Coronavirus and its effect on business continuity planning

February 3, 2020

Health scares, especially instances where a new threat arises and spreads quickly, cause a public panic, but can also impact global markets and businesses everywhere. The latest concern arises from a new virus identified as a novel coronavirus (2019-nCoV) – a strain that originated in Wuhan, China and has not been previously identified in humans.

The World Health Organization (WHO) defines coronavirus as "a family of viruses that cause illness ranging from the common cold to more severe diseases such as Middle East Respiratory Syndrome (MERS-CoV) and Severe Acute Respiratory Syndrome (SARS-CoV)." Coronaviruses are spread between animals and humans. Infected individuals will likely experience respiratory symptoms, fever, cough, shortness of breath and breathing difficulties. More severe cases of infection can lead to pneumonia, severe acute respiratory syndrome, kidney failure and even death.

The reactions to 2019-nCov have varied from heightened anxiety to calmly understated assurance. This state of anxiety is not unexpected given the newness and poor understanding of the transmitted contagion.

LOCKTON®

FDI consulting ...problem solved

What has become clear is that the fear of a new, unknown virus, which has been declared a global health emergency, could greatly impact business operations across the globe.

This situation has drawn the attention of many businesses and is forcing an evaluation of their preparedness to the potential impact an illness or global event, like 2019-nCov, may have on their operations and supply chain.

Preparing your business

Organizations today, more than ever, should make the wise investment in developing, implementing and maintaining a viable continuity management program. When developed correctly, a continuity management program takes an 'all hazards' approach to providing a layer of protection for your most important assets: people, information, cash flow and reputation.

Pandemic/Biological preparedness planning is one aspect of a continuity management program, just as continuity management is one aspect of enterprise risk management. It relies upon the creation and maintenance of a business continuity plan, technology/disaster recovery plan and a crisis communications plan to be effective.

Continuity management creates the highest levels of preparedness for potential health and other threats. Given the current WHO standard recommendations for 2019-nCov, current employee prevention actions and business preparations should be communicated.

Prevent

- Frequently clean hands by using alcohol-based hand rub or soap and water.
- When coughing and sneezing, cover the mouth and nose with a flexed elbow or tissue – throw the tissue away immediately and wash hands.
- Avoid close contact with anyone who has a fever and a cough.
- If you have a fever, cough and difficulty breathing, seek medical care early and share previous travel history with your health care provider.

- When visiting live animal markets in areas currently experiencing cases of 2019-nCov, avoid direct, unprotected contact with animals and surfaces in contact with animals.
- Avoid consumption of raw or undercooked animal products; raw meat, milk and animal organs should be handled with care to avoid cross-contamination with uncooked foods, as per good food safety practices.

Educate

- Provide current information and training on prevention of pandemic infectious disease outbreak to your employees.
- Provide a summary or review of your current pandemic preparedness plan.

Review

- Review and prepare a work from home strategy for those areas of your business that can telecommute. This includes access to essential technology components and communications among employees.
- Review and prepare a work-transfer strategy for functions and processes that can be transferred to other office locations or external entities outside the geographical region.
- Review technology, including bandwidth, security and connectivity, needed to support increased traffic associated with telecommuting and work from home strategies.
- Review business continuity plans for process and functional priorities, recovery time objectives, work instructions and resource requirements.
- Review current insurance coverages with brokers and carriers to insure adequate coverage along with what may or may not be covered.
- Reach out to your supply chain (critical vendors and suppliers) to understand their preparedness capabilities.

Monitor

- Monitor WHO, US Department of Health and Human Services (HHS), Center for Disease Control (CDC) and local health official's reports and status updates.
- Monitor current staff absenteeism levels and provide regular reporting to management and executive teams.

Analyzing your business impact

Organizational preparedness starts with an executive commitment communicated throughout the organization, followed by implementing the appropriate process or methodology (e.g., best practices) to alleviate and address potential business interruptions.

Ensuring your organization is prepared begins with a business impact analysis (BIA) to evaluate the potential effects of an interruption to your business operations. The BIA is the foundation of an effective enterprise continuity management program. The analysis from a BIA provides a wealth of information to help minimize operational and financial risks.

However, it is not a standalone solution and shouldn't be confused as an alternative to either a business continuity plan (BCP) or technology disaster recovery plan (DRP). Without full support, including approval and backing from the highest levels of management, a BIA or DRP/BCP will not achieve its full potential or benefit to your organization. A well-executed BIA can make the difference between a fully developed, robust continuity management program and a mediocre one.

Measuring your risk

A risk assessment is another key component to developing a continuity management program. This process involves identifying the most probable threats to an organization which could result in a loss of ability to perform critical and essential processes identified in the BIA. The risk assessment involves evaluating existing physical and environmental security and controls and assessing their adequacy relative to the potential threats to the organization.

When examined together, these two components will give an organization a picture of what it does, what it needs, the cost of not being able to perform and how the threats, which if materialized, would cause an operational interruption. Once the information from the BIA and risk assessment are available, then the process of developing high-level recovery strategy options for the restoration of people, technology and information/data can begin.

Putting the pieces together

With this information gathered, the business continuity plan, technology disaster recovery plan, crisis communications plan, emergency action plan and pandemic preparedness plan can be crafted to provide the most effective approach to restoring and resuming critical and essential functions and processes.

LOCKTON FDI consulting ...problem solved