MARKS PANETH

ACCOUNTANTS & ADVISORS

PREPARING FOR THE CORONAVIRUS: BUSINESS SURVIVAL PLANNING

MARCH 2020

Melissa Ouari, CISA, CBCP
Senior Manager, Technology Services
Marks Paneth LLP

PREPARING FOR THE CORONAVIRUS: BUSINESS SURVIVAL PLANNING

As the coronavirus continues to spread, businesses are struggling to keep their employees safe and healthy while minimizing disruptions due to workforce shortages, travel bans and the inability to rely on products and services they use as part of their daily operations.

Many organizations have made great strides in technology recovery capabilities since there is so much reliance on computer systems and networks, but can your business survive if there are impacts to your people and the supply chain that your business relies upon? Organizations, especially those in densely populated areas, will have to consider how their people will work if they are afraid of traveling to and from the office and must understand why they need to incorporate pandemic planning into their business continuity efforts to address situations like the coronavirus. This article will highlight the key components around people, process and technology that need to be considered to reduce the risk of a business shutdown.

Today's business landscape is one with interrelated and interdependent systems and processes, and the coronavirus is already having a significant impact on the global economy. A pandemic typically begins with a shortage of people due to illness and employees staying home to prevent exposure. Because of this, business operations and processes are hindered by the lack of or reduced interaction with customers/clients, onsite collaboration, data processing and business travel.

Since pandemics have far-reaching global impact and are not localized incidents, organizations must understand the potential external risks and their impact should supply chains and key third-party vendors, suppliers and business partners also have disruptions. During a pandemic, It is necessary for organizations to think through the right course of action that addresses people, processes and technology. Having a business continuity plan is a good start, but a pandemic presents some unique constraints that are not common in other disaster scenarios.

People

The most immediate apparent impact during a pandemic is the people shortage. Pandemic planning begins with building robust communication procedures and alternatives. Effective internal and external communication is crucial at any time but increases during a personnel shortage. As a next step, business continuity plans need to be enhanced and specifically tailored to the various personnel shortage scenarios. This may include cross-training strategies to offload work for people who are not available, use of temporary staff and coordination with staff who are working remotely. In conjunction with this, organization workflow, as well as the roles and responsibilities for primary and backup support personnel, must be addressed.

Human Resources plays a key ongoing role in the communication efforts and should set protocols around attendance such as requiring employees to stay home if they are sick. Decisions should be made about what happens if extensive sick time is needed--i.e., if the maximum paid sick time is reached. These considerations need to be addressed and communicated.

Process

A pandemic has the potential to handicap business operations and even bring them to a halt. Organizations need to identify the key components supporting business processes, including dependency on third-party vendors, suppliers and business partners. You must know your suppliers and understand any critical vulnerabilities, and it is important to assess and prioritize these dependencies so that contingencies can be put into place if they are truly critical to the organization. Strategies or workarounds can then be developed for continuation of the business process.

Technology

PREPARING FOR THE CORONAVIRUS: BUSINESS SURVIVAL PLANNING

Although it may not be immediately apparent, technology, too, can be impactful in many ways. Many organizations today may acknowledge that employees work from home/remotely from time to time. However, if you have a significant number from your workforce working remotely at the same time, it may result in extensively larger remote connectivity traffic than normal. The company's access points to the Internet, capacity on interfaces and security mechanisms need to be addressed, to name a few. What happens if your vendors supporting your networks and telecommunications experience capacity issues because of the extensive number of resources on the system?

Even in the world of virtual technology, human intervention and support is required if there are job errors or configuration needs. If IT support resources are unavailable, systems could potentially be impacted. This also holds true of cloud technology. If your cloud provider is experiencing people issues because of a widespread pandemic, your systems may be impacted.

Final Thoughts

We cannot predict the spread of the coronavirus and how bad it could potentially be. There is growing concern that a pandemic may ensue, and the World Health Organization recommends completing plans to address this possibility. The ability to address people, process and technology issues that may arise because of a pandemic will enable your organization to survive even in the worst-case scenarios.

Melissa Ouari, CISA, CBCP
Senior Manager, Technology Services
P. 212.324.6850 F. 212.324.6851
mouari@markspaneth.com

MARKS PANETH

ACCOUNTANTS & ADVISORS

CYBERSECURITY BEST PRACTICES WHILE EMPLOYEES WORK REMOTELY UNDER COVID-19

MARCH 2020

Melissa Ouari, CISA, CBCP
Senior Manager, Technology Services
Marks Paneth LLP

CYBERSECURITY BEST PRACTICES WHILE EMPLOYEES WORK REMOTELY UNDER COVID-19

Among all of the concerns facing businesses in the COVID-19 crisis, cyber threats loom larger than ever. Predators are looking to exploit overlooked security measures within businesses under intense pressure to operate during the pandemic. Consider how many IT departments are racing to keep up with technology needs in order to support the alternative/ remote solutions that many organizations have deployed. The rigid testing guidelines typically followed before the deployment of such technology may have been compressed in order to support the sudden rush of remote users that many companies had. It is more vital than ever to address these new risk scenarios in order to protect your organization.

Best Practices

Right now, organizations need to *enhance* and *communicate* their IT security policies, especially regarding security standards in the new "Distributed Organization" environment with a remote workforce. The same level of security controls that exist in an office setting need to be managed across a distributed team. This is not so difficult to manage if employees are working on company-issued equipment, but not every company issues laptops to all employees, and some may work from a home device. Be aware that personal devices are significantly less secure than organizational ones, making them **more vulnerable to a malware attack**. Be sure to issue a policy on personal devices and guidance for the security standards of remote workers, if your organization has not already done so.
Employees want to stay productive but should only do so safely. If a remote worker experiences internet trouble at home and their service provider advises lowering the security settings, your policies should require them to reach out to IT, who would determine what risk that would present to your corporate data.

IT teams should:

- Ensure that multi-factor authentication is in place for 100% of employees 100% of the time.
- Ensure that employees connect to corporate networks using a secure means (e.g., a virtual private network), and store data on available encrypted network drives to avoid loss in the event of a computer virus or other malfunction.
- Ask employees to be wary of suspicious emails, downloads, USB drives or other things that could introduce malicious software onto the network. These could include spoofing and phishing attacks from hackers pretending to be IT personnel asking for credentials.

Additionally, IT teams could provide the following guidance to employees to help mitigate threats:

- Promptly install patches and updates, including to anti-virus software, to all devices on your home network.
- Check individual Wi-Fi router management software to ensure it's running the latest firmware, which can update security flaws.
- Establish a strong password on home Wi-Fi networks unrelated to your work computer password.

In the past, Business Continuity and Cybersecurity risks were addressed and managed as separate disciplines. In today's business landscape, IT risks need to be managed holistically so that threats and the ability to react and respond are integrated. Lessons learned in the initial days and weeks of the COVID-19 related crisis are validating that organizations need to be actively managing their cyber risk and continuously communicating to system users their role in maintaining a secure digital environment.

CYBERSECURITY BEST PRACTICES WHILE EMPLOYEES WORK REMOTELY UNDER COVID-19

Melissa Ouari, CISA, CBCP
Senior Manager, Technology Services
P. 212.324.6850 F. 212.324.6851
mouari@markspaneth.com