straight answers + bright solutions

General Guidelines for Business Continuity During a Pandemic Quarantine

A well written business continuity plan, thought out and planned-in-advance of an actual execution, will save business productivity while avoiding as much confusion and miscommunication as possible. However, it's not always possible to include every scenario that might cause a business disruption and require you to put your Disaster Recovery (DR) or Business Continuity Plan (BCP) into action.

We all know COVID-19 (Coronavirus) has taken over the media, especially suggestions of a potential outbreak or quarantine situation, and many of our clients are wanting to have a plan of action should employees not be able to come into the office. With a suddenly remote workforce, you need to be sure your IT infrastructure can support the same levels of productivity, security, and compliance that it does when everyone is working from the office building.

We thought it might be helpful to give some general overall guidelines for you to consider as you review your BCP and particularly around an extended work at home situation. These suggestions follow best practices around security; however, your network environment may differ depending on your configuration and business applications in use.

Specific to COVID-19, we are providing an outline of key preparedness activities to ensure continued service delivery during this event. The three areas of focus during any situation that challenges normal operations are as follows:

- Impact to systems – does the event have a potential impact on our systems used to deliver and support our same level of service to our clients?
- Impact to location – are the locations from which we deliver, and support service effected and what is our response? This is the most likely area impacted by a quarantine order.
- Impact to people – are we prepared should there be impact to the individuals responsible for delivering service to our customers? Could be a factor should employees become ill.

While there could be multiple areas impacted, the COVID-19 situation will most likely focus on the Impact to Location, as noted above, should employees not be able to come into the office.

- Remote workers need the right tools to complete their work and we recommend a company issued laptop that is monitored and managed by True North Networks. We cannot remote to employee owned equipment to assist or troubleshoot issues.
- Ensure you have SSL VPN configured on your firewall and enough connection licenses for all employees to connect at the same time. Ensure employees know how to connect from home.
- For best results, home Internet service should meet a certain speed requirement, otherwise productivity will be hindered and, in some cases, impossible for things like video conference.

- Bandwidth limitations may prevent video conference calls or VOIP phones from working as expected. Also, when entire regions or local areas are quarantined, home-bound people can overload local phone switches reducing call quality and interrupting connectivity. Internet bandwidth can be impacted in much the same way.
- Management should establish how they want to communicate, for example, are there organized times when everyone should check in, what is expected from remote workers each day, how to collaborate with your coworkers in the most effective manner, will phones be forwarded, etc.
- It's important to communicate that the employee has a shared responsibility in ensuring the ongoing security of company data and resources. A vigilant mindset is required, as cybercriminals are watching industry trends and news or company announcements about remote work plans. This information allows them to devise new scams and social engineering methods adapted to these evolving circumstances.
- Implement a layered approach to security with multi-factor authentication, next generation AV, DNS filtering, continuous monitoring for things like account privilege escalation, new user accounts, suspicious processes, anomalous login behavior, etc. Many of these security layers are part of our SecureWorkplace® cybersecurity program. Ask how we can help you implement.
- Be aware of leaving PII out in the open and dispose of any printed material in a secure method such as shredding.
- Your organization does take on an added security risk with the introduction of a much broader remote access footprint. When employees work outside the safety net of the corporate network, it opens the organization up to devices and Wi-Fi networks that are potentially insecure – as well as users who no longer think they are "at work".
- Perform an actual dry run through your remote work plans to reveal any unforeseen issues so they can be resolved before an actual emergency.

Finally, understand what regulations your organization is subject to, and know what's required to protect that regulated data. Ensure you still have security controls in place and the ability to monitor when those controls are not upheld. Keeping information confidential is much easier in a controlled and protected workspace such as the office. When information is taken out of the office, security and confidentiality are not guaranteed, however, you are still responsible and required to protect the data.

The key to success is having policies and technologies
(that support remote work)
in place before a disruption occurs.