Keeping Your Business Operational

Voice Data Security is a DFW based Professional IT Service company providing services to many small to medium businesses in Texas.

The COVID-19 (Coronavirus) pandemic caught all of us off-guard and it continues to disrupt the healthcare, government and economic system. Voice Data Security hopes you and your loved ones take precaution to be safe and healthy.

We wanted to share our thoughts on how you can keep your business operational during and after this difficult time.

1. **Should I allow my employee to directly access to their office computers using remote access tools?**
    - While remote access tools can be an option to accomplish accessing to the office computers, VDS recommends having a VPN connection to office network with SSL based secure client before allowing access to the computers. Allowing direct access to the computers may also create interfaces for hackers to access your network. VDS recommends using multi-factor authentication access to your VPN connections, using strong anti-virus, firewall applications with central control on home computers and making sure these computers are patched with the latest security updates.
    - Using office computers might be a good alternative if anti-virus, firewall and patching on those computers are managed and monitored day-to-day basis. VDS recommends using VPN connections on these computers as well.
    - Using VPN technologies creates an encrypted connection between your home PC to the office and it makes it difficult hackers to gain access to your business.
    - Use of home computers may cause cyber security incidents.

2. **I am allowing my employee to access to my network securely. What happens if the ISP stops functioning at our business location or at the houses of my employees?**
    - It is very critical to have a functioning Internet connection during this time if your employees are accessing your network to perform their functions. Services like Microsoft Office 365 and Cisco WebEx do not require your office location to be operational. However, accessing file servers or application servers in office will require the office infrastructure to be fully operational.
    - If you do not have redundant connection at your office location, it is advisable to have a redundant connection so that office infrastructure will be completely operational in case of ISP failure.
    - If remote employees lose their connection, hotspot-based connections on their phones can be used temporarily to gain access to the corporate network. It may be slower than the regular connection, but it will allow employees to re-gain access to corporate resources.

3. **I have only one router/firewall connecting my office to Internet. What happens if we have a hardware failure?**
    - Hopefully, you will not experience this problem. If your router/firewall stops functioning, your employees will not have any type of access to your office and until the problem is resolved, your business may stop functioning.
        i. To prevent this happening, you may want to cluster your device by adding one more of identical device to your network. If clustering is not an option, having a spare device in hand with identical configuration will prevent long term business outages.
        ii. Almost all VPN technologies run on edge router/firewall devices and even when a VPN is not used, remote access to the network will only be available via these devices.

4. **How can I have a reliable communication between my employees?**
    - If you are using a VOIP based phone system, it may offer a soft client which enables users to use their phones on their computers at remote locations.
    - If your phone system is not VOIP based, you may prefer to forward all incoming calls to cell-phone of the designated person.
    - VDS recommends using technologies like Cisco WebEx or Microsoft Teams to have group meeting among your employees.

5. **How can I make sure that my corporate data is safe during this time?**
    - VDS recommends having a monitored backup solution. Your data should be kept at your office locations for at least 30 days and the data should also be replicated to an off-site location.
    - Enabling remote access to the data brings additional risks to your environment. Monitoring the data health and making sure infected data is not overwritten to backup sets are critical.

6. **We are relying on technology more and more these days. What happens if one of my critical systems stops functioning?**
    - VDS recommends having a structured and documented professional engagement in place for fast recovery. While it is very common to have issues with IT and many people can continue functioning while they are in the office, faster recovery of service outage is critical while functioning with part or full set of remote workers.
    - System monitoring, maintenance schedules and other IT related activities should be modified to accommodate remote users.

7. **Should I allow my employee to access to corporate email and other resources on their phones or tablets?**
    - VDS recommends to management capabilities on employee devices to make sure your employee can securely access to your corporate resources. Before allowing access, setting policies and procedures for remote access will be a good idea to set the expectations and address privacy related concerns.
    - It is advisable to have multi-factor authentication on end-user devices to prevent un-authorized access.

8. **I need to be compliant with regulations like HIPAA, PCI and SOX. Will I be violating any rules if I enable remote access?**
    - VDS recommends having your remote access plan verified so that you will not be faced with issues with your compliancy requirements. For example; PCI requires to have certain controls in place before having remote access to your network. You may not be using remote access in the past but under the circumstances, you may have to enable access and that will cause issues with your auditors.
    - It may be a good solution to start using Virtual Desktop solutions which basically means that your employee will be working within the boundaries in your office and they cannot access the data directly from their home computers.

9. **I enabled access for all my employees. What if one of my employees has a breach, would they be a security issue for me?**
    - If you do not have the proper monitoring functions and controls in place, you may face with the same infections on your network and it may affect everybody at the same time. Working remotely requires the main network to be protected from remote computers in case they are infected. Remote users should only have access to systems that they are normally allowed access while they are in the office. Mapping shared network drives should be prevented as it may allow crypto-ware types of malware to spread to all corporate files.

10. **I do not have any policies and procedures for remote access. Should I come up with one?**
    - VDS recommends having a policy for remote access to corporate resources. This document will explain to employee what they should or should not do while they are accessing the corporate network. Some VPN designs may route all user traffic through the corporate network. If a user is streaming audio or video to their PC, they may block all other employees from accessing the corporate resources as it will utilize the bandwidth at the office as well.

Please email support@voicedatasecurity.com for a free remote consultation on how to keep your business operational while we all have to work from our homes and find out how your business can be protected from potential Cyber Security risks.

Keeping your system operational requires a professional organization who is available and capable to resolve the issues remotely and quickly. If you need any help, please do not hesitate to contact us.

(972) 426-7102 www.voicedatasecurity.com
5899 Preston Road #301 Frisco, TX 75034