#WFH? Security Considerations for Working Remotely

Mar 23, 2020

Categories:

Blogs
Coronavirus Response Team
Technology Blog

Authors:

Michael E. Nitardy

As the coronavirus continues to quickly spread across the United States, employers are following CDC guidance and implementing strategies calculated to protect their workforce while ensuring continuity of operations. In many cases, employers are allowing – and in some cases requiring – employees to work from home. While working remotely helps containment of COVID-19, it also presents an opportunity for bad actors to attack information systems, users to make mistakes when adjusting to a new environment, and outdated or unpatched systems to fail.

All executives must consider the threats to their organizations presented by COVID-19. But, while allowing employees to work from home may be a seamless transition for big companies or specific service industries, smaller, family-owned companies, or companies providing certain services, may have never considered providing this option to employees. Regardless of their size, organizations are required to protect and maintain information, especially when being shared and transmitted online. This obligation does not change when employees are working from home.

Ideally, a company has an established written information security program (WISP) with policies to minimize risks that can be reviewed and deployed for remote work. However, for those now faced with having to organize impromptu virtual offices and meetings and to move operations to an online environment, here are some issues to consider that will help prioritize risks and follow best practices even in times of crisis.

1. What information would employees be working with from home?

In crafting a policy for working remotely, a business needs to first identify the information it must protect, including personal information of employees, customers, vendors, and other individuals, as well as proprietary intellectual property

FBT Gibbons

and other confidential business information. If employees have hard copies of this information, they need to ensure these copies are physically secure and should destroy/shred the copies when appropriate.

Sensitive or highly confidential information should be encrypted in transit and at rest on devices. A company does not need a sophisticated information system to encrypt information. Companies using Windows 7, 8 or 10 in their computers already have Microsoft's BitLocker available to do a full-disk encryption. Smartphones also have encryption settings, and Microsoft Office 360 allows the encryption of emails.

2. What equipment would employees use?

Ideally, an organization has already adopted a bring your own device (BYOD) policy and installed Mobile Device Management (MDM) and Mobile Application Management (MAM) software. But no two organizations are the same, and some small businesses do not have such policies or software. In addition, while the use of laptops throughout an organization has become more prevalent, many organizations still use desktops at the office.

Several issues are presented with asking employees to use their home computers for work. First, employees may be forced to save important information in their own computers, which increases the chances of wrongful disclosure or loss. What type of anti-virus software does the employee use on the home computer? Could the information become infected and consequently infect the company's systems? Is access to the computer password protected? How strong is the password?

Second, home computers are often family computers, and others may unwittingly stumble upon information and accidentally use, change, delete or disclose it. Most importantly, multiple users of one device may accidentally open the doors to unauthorized parties to access the information.

Third, there may be software compatibility and connectivity issues if the remote device uses software or systems that the organization does not support or cannot integrate with. If

employees are using their own computers or devices, basic security features that come with the device should be enabled like the PIN, fingerprint, or facial ID features. Additionally, Wi-Fi networks should be secured with a strong password.

3. How would employees be connecting to the network?

Even when employees will not be working remotely with personal information or proprietary information, bad actors could target employees in order to gain access to a company's network. Once an unauthorized party enters the company's systems, the company could be hit with ransomware attacks, phishing, or the takeover of email accounts for fraudulent transactions. As a result, a company needs to consider how its employees are accessing the network while working remotely.

Many employees have access to the internet from home without having sufficient firewall protection. The preferred way around this is to setup a virtual private network (VPN), which allows employees to connect securely to the company's network via virtual encrypted communications. But not even VPNs are fool-proof and must be properly used and administered.

Recognizing that companies will be adopting telework options, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has issued Alert (AA20-073A) regarding "Enterprise VPN Security." While the alert recognizes that remote work will increase, and VPN usage will also increase, the alert "encourages organizations to adopt a heightened state of cybersecurity" that addresses the issues faced by VPNs, including the fact that malicious actors are actively looking for VPN vulnerabilities, that VPNs must still be patched and updated when necessary (which may require limiting 24/7 access), and that certain VPN networks may offer a limited number of connections.

4. Have employees been trained?

Proper training can prevent many problems. CISA also released a bulletin warning individuals to remain vigilant for scams related to

COVID-19. With an increasing number of coronavirus-based phishing emails, organizations need to train employees on how to detect phishing emails and other forms of social engineering involving remote devices and remote access to company information systems. When information security safeguards are loosened up to be more flexible, proper training may help maintain a small margin of user error.

Organizations will face a number of difficult decisions over the next several weeks and months. Taking the time to consider the threats posed by working remotely may save your organization an additional headache during this uncertain time.

For questions and assistance regarding this topic, please feel free to contact any member of our Privacy and Data Security Team.

To provide guidance and support to clients as this global public-health crisis unfolds, Frost Brown Todd has created a Coronavirus Response Team. Our attorneys are on hand to answer your questions and provide guidance on how to proactively prepare for and manage any coronavirus-related threats to your business operations and workforce.

FBT Gibbons