March 17, 2020

Transition to a Remote Work Environment

With the current concerns regarding the spread and impact of COVID-19 (“Coronavirus”), many companies are asking or requiring their employees to work remotely. If your organization is considering this option, it needs to consider data security and privacy implications. In order to assist you with potentially making this transition, here are some issues to discuss before you make the decision of how to proceed forward during this time:

1. Home WiFi Networks

The only way for an employee to connect to your network is likely through a home WiFi connection. Your employees’ will likely connect to their home Wi-Fi networks, which can be less secure. Encourage employees to change default router settings and passwords before connecting to the business’ network.

2. Personal Devices

Unless you already maintain a large number of business devices, your employees will likely be using personal devices to work remotely. The IT teams need to work with the HR teams to ensure that appropriate “Bring Your Own Device” or BYOD controls are in place, and employees are trained (most likely remotely) on those policies. Even if your organization already maintains a BYOD policy, it should be reviewed and updated to reflect a more long-term work from home requirement.

3. Physical Security

Physical security is critical when addressing cybersecurity concerns. For example, there are employees who may be talking loudly on the phone while working in public places, exposing their laptop’s screen for the entire crowd inside a coffee shop to see or even leave their devices unattended. Employees should be trained on best practices for ensuring both devices and paper documentation.

March 17, 2020

4. Consider who should work from home

Not all employees should and can work remotely. Your company should consider which job functions can be moved to remote work, and which require in-person involvement. Consider decreaseing in-person requirements, and rotating employees who are required to come to the office on a given day.

5. Provide a list of tools remote workers are required or permitted to use

Remote working creates opportunities for “shadow IT” to become very prevalent. Make sure to communicate to your employees regarding approved tools for communications and operations, such as cloud storage platforms, communication/video conferencing tools, project management tools, etc.

6. Provide employees with steps to follow at the first signs of account compromise.

Train, train, and train. You cannot over communicate to your employees when working in a remote environment. Remind your employees, and provide detailed information on company protocols in the event of an actual or suspected system or account compromise. This should include clear guidelines to follow, such as how to report, where they should report, etc.

At XPAN, we hope that your employees remain safe and healthy during this trying time. It is easy during times of crisis to forget basic cyber and privacy best practices. However, cybercriminals do not rest and they are opportunistic. They will use the distraction of Coronavirus to exploit any weaknesses. Take the time to review your current policies to see if they adequately address the "new normal" that we are facing. We want to ensure that our clients do not contract another virus while it protects its workforce from the Coronavirus.

March 17, 2020

As a virtual law firm, our team is prepared to continue to operate throughout the development of the Coronavirus. Our team uses tools and an infrastructure that supports our employees to continue to provide our services to clients across the globe.

For additional information, and to learn more about how to create a secure and private remote environment, please feel free to contact us. If we can help, we will.

Rebecca L. Rakoski, Esq.
rrakoski@xpanlawgroup.com
267.388.0897

Jordan L. Fischer, Esq.
jfischer@xpanlawgroup.com
267.536.9376