Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

A Strategy to Get Started with a Cybersecurity Program: Working from Home

Patrick Rost prost@dopkins.com

Published December 23, 2020 – This is the latest in Dopkins series of Cybersecurity posts. These blogs will introduce various topics, related terms, importance of reviewing the topic and hopefully raise some questions you should be asking.

At the dawn of the COVID-19 pandemic, Dopkins **published an article on best practices** for employees to help them remain diligent about cybersecurity while working remotely. As working from home is expected to remain the new normal for so many, this post will expand on the topic and take a further look into the cyber-risks of working from home from a business perspective.

Read our other recent issues covering:

- **Cybersecurity Awareness Training (November 2020)**
- **Data Backups (October 2020)**

Since March, the pandemic has caused companies to make world-wide changes to how they conduct business. Seemingly overnight, a workforce of unprecedented size was unable to report to work. This led to companies exploring options to allow employees to work from home in order to keep the business functioning.

Under so much rapid change, one of the first questions company leadership likely asked is how they can keep doing business, a difficult task without employees! With on-site workplace access often restricted, employers were left with little choice but to allow employees to work from home. With many of the initial questions having to do with continuing to conduct business, the **security** of functioning this way may have taken a back seat. Hopefully by now you have had a chance to address these concerns. **If not, the following IT issues should be addressed as soon as possible.**

Device and Firewall Risks

A major security risk is employee use of their own personal computer for business purposes. The pandemic compounded this issue for businesses as a result of supply and demand: laptops were on backorder due to overwhelming orders! As a result, the shortage of laptops brought even more concerns: *Was it possible to send a desktop computer home with employees and trust they can set it up on their own? Or do you have the IT resources to have someone go into their home and set it up for them?*

After going through these questions, it is plausible to see how a decision to allow an individual to use their personal computer for business purposes would be made. However, this decision leads to several risks.

Where are the files stored? Employees who are using their own computer are likely to save files on their computer in order to perform work functions. These files are now outside of the company network and will remain on that employee's computer until they manually delete them, and then empty their recycle bin.

Also, does the employees' spouse or children then use this computer with the business files residing on it? If they have access to the files, they can view them or potentially share them (unintentionally). In addition, what kind of virus protection does this computer have, if any? If a virus compromises the computer, it opens the possibility of an outsider accessing the files. Then, even after completely deleting the files it is possible for these files to be recovered. Company policies that dictate how hard drives are destroyed to prevent data from getting out cannot be applied to an employee's personal computer.

What protections do the employees have on their personal computer? In addition, remote employees' computers will not be protected by the company's firewall. This is true regardless of what computer is being used. Hopefully they have an adequate endpoint protection (that includes more features than just anti-virus), but that does not replace the protection of a hardware firewall. Firewalls have features like content filtering, geo-filtering, Intrusion Protection System (IPS), etc. Employees will have to be extra cautious when browsing the web and when reviewing emails. A simple mis-click can lead them to a site that would have otherwise been blocked inside the protection of the company network.

Connectivity Risks

Another possible risk is how the employee is connecting back to the company network, also regardless of which computer the employee is using. Hopefully the connection is using an encrypted **virtual private network** (VPN) to ensure the data being passed is not viewable to the outside world. *If an encrypted VPN is being used, are secure passwords being enforced?* A VPN connection allows someone outside the company's network to connect to it and access resources. If this password is weak it can be guessed and will allow an outsider to gain unauthorized access. One way to help prevent this (which should be used with a secure password) is **multifactor authentication** (MFA). Enabling MFA will require employees to enter another randomly generated code that is sent by text message or is available on an authenticator app, which only the employee has access to.

Cloud Access Risks

In recent years there has been an increase in moving to hosted or cloud solutions. There are many benefits to these solutions and companies may have taken advantage of the benefits this year as they looked for new ways to operate. Risks of using these solutions are similar to those while connecting back to the company network. By nature, cloud solutions are available from anywhere with an internet connection. This means that it is vital that they use the same secure password requirement previously discussed and that MFA is enabled. This is significantly more important for privileged accounts. Losing access to an administrator account on a cloud solution compromises the entire system.

File Sharing Program Risks

If users do not have a way to connect back to the company network, or independently determine it is too difficult, they may look to a file sharing program available online to help them store and transfer files. Programs like Google Drive, Dropbox, etc. could be used. The problem is that this allows company documents and information to be stored outside of the company network. Once documents are stored in these locations they are no longer under the control of the company, possibly without the knowledge of IT or leadership within the company. There is no enforcement of secure passwords and MFA as previously discussed within these programs. This leaves the account open to being compromised and all of the documents stored being lost to an attacker outside of the company. Company data can easily be **breached without the knowledge of the company**. Use of these applications should be limited by both policy and technology constraints to help ensure data is not compromised.

Part of the evaluation of what the right choice is will depend on how much longer the pandemic will affect everyday life – unfortunately this appears to be continuing well into 2021. After health concerns are alleviated will these practices stay or will everything return to its prior state? Many companies are eager to get everybody back in-house like they were a year ago. However, many more are making permanent changes to support employee's abilities to continue to work from home even after it is not a requirement. **Regardless of this answer, even temporary circumstances need to be setup with security of company data in mind**. As we discussed in last month's post about **User Awareness Training**, cyber-attacks are at an all-time high in 2020 and will continue to increase in frequency and success.

If you would like to have a conversation and review your working from home policies check out our STARTegy page for more information about our Strategy for Getting Started with Information Security.

Stay tuned for our next blog which takes a look at the cost of a data breach!

For more information, contact Patrick Rost at prost@dopkins.com.

© Dopkins & Company, LLP