Bloomberg Law®

Professional Perspective

Secure Telecommuting While Social Distancing

Joel Schwarz, The Schwarz Group, LLC

Secure Telecommuting While Social Distancing

Contributed by Joel Schwarz, The Schwarz Group, LLC

For more information, see Bloomberg Law's Data Security Checklist, Secure Telecommuting Controls.

Due to "social distancing" requirements that arose from the 2020 coronavirus pandemic, a large part of the American workforce traded in their cars and train seats for makeshift home offices. This sudden shift to telecommuting caught the attention of cybercriminals and state-sponsored actors in China, North Korea, and Russia, who have been using coronavirus-related phishing tactics to infiltrate computer systems.

With this new work paradigm, we therefore need to turn our focus to better securing the home office environment, thereby improving our overall cumulative cybersecurity posture. But how would good cybersecurity look in this new paradigm?

Securing the Home Office

Few of us actually follow through with the obvious security steps and recommendations that are familiar to us. Whether it's a desktop, laptop, or tablet, it's vital that employees use an operating system (O/S) firewall and anti-virus program with the most recent software manufacturer updates, and each still supported by the manufacturer. Otherwise the employee's system is more vulnerable to compromise, which in turn becomes an exploitable point of vulnerability where a criminal may gain access to the corporate network. Bear in mind that Microsoft's Windows 7 just reached its end of life at the end of 2019, so it's no longer supported and poses a higher risk to any system still running it.

Illustrative of the danger, consider when Microsoft stopped supporting Windows XP in 2014. Soon after they ceased support, a security gap was identified that posed such a high risk to customers—including 75% of the water utilities still using XP that Microsoft back-pedaled and issued a patch. But it's unlikely that Windows 7 users can count on the same intervention from Microsoft.

Next, employers should consider requiring employees to create separate account personas on their home computers, if possible—this can be done in Windows. While separate personas don't necessarily block others from accessing data saved on the hard drive, they do automatically segregate the data to a file folder unique to the persona. When users open or save files for work purposes within a given persona on a home computer, their data is not automatically intermingled with personal data. Likewise, to the extent an employee uses an internet browser for work, the cookies and transactional data are saved to a folder within that persona, and don't bleed over to one's personal browsing activity.

Finally, for purpose of risk mitigation, it's advisable to avoid holding conference calls or virtual meetings in a room where there's a smart device, such as an Alexa or Google Home, because as we learned back in 2016, there's a distinct possibility that the device might record and retain the conversation. While some companies have since ceased this practice, others have merely changed their privacy policies to more explicitly disclose that this is occurring, creating a potential vector for compromise of corporate secrets and other proprietary information.

Employers should therefore mandate that any work-related calls or video conferences be done in a room where either these devices have been manually turned off, using the on/off button, or in a room where there are no smart devices located. And just as a reminder, similar concerns have been raised about smart TVs, such as the Samsung smart TV, which was identified in 2015 as having a propensity for recording conversations via its "always on voice detection" service.

Securing the Home Network

Next, consider the way employees will access the corporate network. Today, they're likely to use one or more wireless routers in their home network. But wireless connectivity introduces vulnerabilities that don't exist in hardwired (i.e., ethernet) connections. So, if using a hardwired connection is an option, it's certainly the more secure method. But assuming this isn't an option, there are at least four basic security steps every employee should take to better secure their wireless router, because a vulnerable router invites intruders, who can then ride the employee's compromised connection into the corporate network.

First, if employees aren't already using a password to secure their Wi-Fi, they should enable one immediately. That password should adhere to traditional password requirements, such as using a combination of letters, numbers and characters, not too short, and they shouldn't be easily guessable (i.e., no family name, home address, telephone or license plate number, etc.)

Second, employees should disable broadcasting of their Wi-Fi network ID (which is also known as the SSID); disabling the broadcast makes the network invisible to passersby. Employees can still log in without any difference, but in order for others to log in, they'd need to know the network name and manually enter that information to connect. This in turn reduces the likelihood that an intruder will find the network and attempt to breach it.

Third, employees should change the default accounts pre-programmed into virtually every router (and every Internet of Things device). Usually those accounts come with names as creative as Admin, Administrator, or Default. People often leave these default accounts in place, sometimes even leaving in the default passwords as well. But these default accounts are the first thing a virtual trespasser looks for when trying to gain entry to a network.

They're also vulnerable to malware attacks programmed to try default account names and passwords as part of an exploit. For example, the now infamous Mirai and Dyn DDoS attacks in 2016 were perpetrated by exploiting the default user name and passwords in IoT devices like home routers, air-quality monitors, and personal surveillance cameras, crippling a number of high-profile websites, including Netflix, Spotify, and CNN.

More recently, leaked documents from Russia's Federal Security Service described a project under development to enable them to coopt devices with the goal of taking down key servers in various countries, using nothing more than a dictionary of the usual default passwords used for these devices.

Finally, employees should enable a functionality available on almost every wireless router, called “MAC address filtering.” Every computer and IoT device today has a Wi-Fi card inside. And every Wi-Fi card has a unique identifier, known as its “MAC address.” To find the MAC address for individual devices, just a simple search is needed on YouTube. Once MAC address filtering is enabled, and the MAC address of authorized computers entered into the router's software, this becomes an exclusive list of the only computers allowed on the network. Think of it as “the list” at a nightclub, where only those on “the list” get in. Should someone else try to log in, even if they know or guess your router's SSID, the router won't let them in. This provides an additional layer of security on the network, and by extension, the corporate network.

Account Logins and Communication

With the mass transition to telecommuting, there are many ways to exploit employee laxity in their homes. As such, every employer should mandate the use of multi-factor authentication as a pre-requisite for gaining access to the company email, or other corporate system. This can be done using a random number generator offered by various authentication apps (both Google and Microsoft offer free authenticator apps), a physical token held by the employee, such as those issued by RSA, or even a temporary one-time code texted each time the individual attempts to log in.

When accessing the corporate network, employers should also require use of a virtual private network, enabling end-to-end encryption between the employee's computer and the corporate network; think of it as a secure tunnel on the otherwise inherently insecure network. If your company doesn't already have a VPN, there are many options out there to choose from, to include a number of free VPN picks.

But a VPN is not foolproof. For employees logging in using a public Wi-Fi hot spot like Starbucks, they should be cautioned against conducting business of a confidential nature, even on a VPN. That's because anyone on that Starbucks network can potentially intercept an employee's communications, to include keystrokes, as they enter their VPN credentials to initiate the VPN. And with an employee's credentials, that individual can now gain access to the corporate network. In addition, they can potentially use those credentials to access other accounts, under the premise that people tend to reuse passwords and account identifiers.

Of course, some employees may express interest in using their personal email accounts, instead of the employer's email system. While this is an employer-specific decision, there are significant downsides to consider. Anything sent through a personal email account hosted by a provider like Outlook or Gmail is stored outside the corporate firewall, on their servers, meaning that all work-related communications and any confidential, proprietary or otherwise sensitive company information is now accessible/readable by the provider, depending on the specific provisions set forth in their privacy policy and terms of service.

For example, if an employee uses Outlook, they should know that Microsoft collects the content of all emails sent or received through their service, as well as any audio and video included with the email, and shares this data with its affiliates and subsidiaries, as well as with vendors or agents. Microsoft also reserves the right to disclose personal data it has collected as part of a corporate merger, or a sale of assets. To be clear, this is not to intimate that there's anything nefarious here. Rather this is meant to point out how an employee's use of a personal email account for work can result in an employer's loss of possession of, and control over, confidential or otherwise proprietary information.

Next, given that meetings are a regular part of many jobs today, it's reasonable to assume that this will continue. For companies that don't have a dedicated telephone conference line or video conferencing functionality, or if employees don't have the necessary equipment at home, online web-based video conference services are certainly an option. But before jumping all in, it's important to become familiar with their TOS and privacy policy.

Zoom became popular in this niche marketplace during the pandemic with its free video conferencing services. But if one looks at Zoom's privacy policy – the data they collect and retain, as well as what they share with others – an employer may have second thoughts about allowing the use of Zoom for sensitive or confidential conversations. For example, according to Zoom's , not only does their platform collect personally identifiable information such as name, email address, phone numbers, etc., but also "information provided by the customer to Zoom through the usage of the service," which includes the "content contained in cloud recordings, and instant messages, files, whiteboards, and shared while using the service."

Moreover, Zoom's privacy policy states that it "may use identifiers, employment information, payment information, Facebook profile information, technical information, demographic information, usage information, and user-generated information" for targeted marketing or promotional activities by Zoom and/or its affiliate websites, and they share this data with 3rd parties who may then use it "for their own business purposes."

Employers should therefore use Zoom's service, and others like it, with eyes wide open, and consider the TOS and privacy policies before authorizing such use.

In addition to concerns with Zoom's privacy policy, a number of security concerns with Zoom recently came to light, best summed up by an investigative report released by the Citizen Lab at the University of Toronto, to include:

- Zoom clarifying that when it claims to use "end-to-end" encryption, it means encryption between an individual's device and the Zoom server, not the entire communication. In other words, not "end-to-end" encryption as industry uses the term.
- Zoom uses custom encryption, which does a poor job of masking everything, is predictable, and is potentially breakable given their use of weaker than industry standard encryption keys (AES-128 vice traditional AES-256).
- In making Zoom dummy-proof ("low friction"), Zoom gave rise to a number of additional security vulnerabilities and privacy concerns. For example, Zoom allows the host of a call to record the conversation, potentially unbeknownst to others (although, other participants should "generally hear a notice or see an on-screen notification when recording is in progress"), the recording of which is then at the disposal of the host to use, post or otherwise disseminate as desired.
- Even with all parties to a call located in the U.S., Zoom's encryption keys come from China, creating the risk that the Chinese government may force Zoom to share those keys and gain access to all communications.

Employers should carefully read the TOS and privacy policies before authorizing employee use of web-based conferencing services, and potentially consider limiting the use of such services to certain business purposes that do not involve confidential or proprietary information.

Risks to Corporate Data and Systems

Many employers use cloud services to host their email and store data, whether by Amazon, Microsoft, IBM, or another, something employees can do just as easily from home. But given that many people use personal cloud storage, it's important that they be instructed to save data on the employer's cloud, and not auto-default to saving on their personal cloud. Much like the issue with Zoom, and use of personal email, the TOS and privacy policy for those private cloud providers will govern how the provider can access, use and share this data, which is something employers may not be willing to risk. To that end, it's also important to stress that employees not save data to their personal computer's hard drive, where there is always a risk that others who use that computer might access the information or accidentally disclose the information to others.

Of course, the biggest potential threat to corporate data (and systems) remains phishing scams, ransomware, and other malware attacks, whether by cyber criminals or nation-state hackers. And in addition to the traditional threats, 2020 has now seen coronavirus/Covid-19 scams.

For example, during the first day of mandatory social distancing in some states, a coronavirus phishing email circulated, masked as a map of infected areas and death rates, but was trojanized to carry malware (the name of the file was corona-virus-Map[dot com][dot exe]). Ransomware has also played a prominent role in coronavirus pandemic exploits. For example, on March 23, a Spanish paper reported that the Netwalker ransomware was making the rounds of Spanish hospitals, masquerading as an informational email on the coronavirus in an attachment called "Coronavirus_Covid-19.vbs."

While there's no magic bullet here, employers can do three things to minimize this threat.

First, to the extent an employer uses a service designed to test the susceptibility of employees to phishing attacks, this test should be run immediately, for all employees, without waiting for the next regularly scheduled cycle. Likewise, these tests should be customized for the pandemic. Finally, employers should undertake to send out weekly emails to employees reminding them to be vigilant against Covid-19/coronavirus phishing and, ideally, include updates on the latest exploits, using resources from trusted publications, or those put out by an anti-virus companies such as Norton. While this may be more frequent than traditionally practiced, it's especially important right now, given the relaxed environment most employees are working in, far removed from the traditional office setting.

Update Corporate Policies

Finally, employers should review and update their corporate policies regarding remote access, remote data management, authorized and prohibited resource usage, etc. to reflect this new paradigm. And to ensure every employee is aware of the updates, employers should consider sending out a short, Cliff-notes-type summary of the changes along with the new policy, so that employees absorb the high points immediately.

Relatedly, its important employers explicitly specify what employees can and cannot do and use many examples to illustrate. Understanding and enforcing policies at the office is already a challenge. To get remote employees to understand and comply in the current environment, given all the potential distractions of home—such as home-schooling children —it's especially important for employers to provide clear and concise guidance that cannot be misinterpreted.

Risk Mitigation

In the world of cybersecurity, the primary goal is to mitigate risk as best you can and accept or offset the risks you can't mitigate. And the good news here is that all of the steps laid out in this article are simple, basic security protocols, easily within the employee and employer's control. At the end of the day, the goal is to raise your overall cybersecurity posture and make your company and its systems a less attractive target, in the hope that the bad guys will move on to another potential victim who requires less work and is easier to breach.

As such, the steps laid out in this article should be considered the minimum an employer accepts when allowing an employee to work from home and access the corporate network in this new age of social distancing.