RISK
MANAGEMENT

3 Tips for Protecting Remote Employees' Data

Brian Schrader
July 7, 2020

As the COVID-19 pandemic continues to force many employees to work from home, both now and in the future, it is crucial for companies to take precautions to protect sensitive data from the cyberattack vulnerabilities introduced by this new "normal." That means establishing organization-wide data-security policies that take remote workers into account and inform them of the risks and how to avoid them. The following are three tips for keeping your organization's data safe during the work-from-home era:

continued next page

1. Be Wary of Open and Public Wi-Fi Networks

Employees probably did not set up their home Wi-Fi networks expecting to spend months working and viewing sensitive company files from home (take a look at these steps to better secure routers). Some may not have access to Wi-Fi at home, requiring them to use public networks and hotspots. In either case, companies can safeguard corporate data with a few simple measures:

- **Encrypt employees' sessions with virtual private networks (VPN):** A VPN creates a secure connection over a public or unsecure network by encrypting the data that flows to and from the device. Company leaders should establish a policy requiring all remote employees to use a VPN, which costs around $3 to $10 per month per user, depending on the plan you choose. Keep in mind that work-from-home policies are likely to become more popular in the future. Now that companies have established remote working capabilities due to the pandemic, employees may expect to continue that practice long after the pandemic has passed, so it is wise to set up protocols now.
- **Use a personal Wi-Fi puck:** If company leaders are not confident in their employees' home network security (or if they do not have one in place), employees can also use a personal, secure Wi-Fi hotspot device, also called a puck. This device is available through all the major cellular providers and acts as a hotspot that connects through a cellular device. More expensive than a VPN, a puck is around $100 (plus the monthly fee for internet access), but it is small (sometimes the size of a USB key) and portable. These devices can prove essential in avoiding spoofing attacks, which is when a bad actor impersonates a service or device to access your data, and man-in-the-middle attacks, when a hacker intercepts (and possibly even alters) information between two parties.
- **Use multi-factor authentication (MFA):** Multi-factor authentication ensures that access is granted only after an individual presents at least two pieces of "proof" that they are who they say they are. The validation process requires fulfilling at least two of three categories: something they know, something they have and something they are. For example, it might require a password and a texted code or fingerprint. It is a simple security measure your company should have in place whether employees are remote or not, but if you do not already have it implemented, now is the time to do so. Consider using authenticator apps or systems that send access codes via text to minimize the risk of cyber criminals stealing sensitive data.

continued next page

2. Establish Personal Device Policies

It is likely that many people will use their personal devices to work from home during the pandemic. While this may not seem like a problem, consider where those devices will go when stay-at-home orders end—coffee shops, hotels and more. Without the proper security measures in place, all the data accessed on these devices (including emails, files and the cloud) is susceptible to data breaches. With so many remote employees, it is wise to create company-wide policies that:

- **Require standard security protocols:** Organizations should require multi-factor authentication, security timeouts and password complexity for any employee using personal devices for business matters. Passwords should contain capital and lowercase letters, numbers and characters, none of which are easily guessable. Employees should avoid using their dogs' names and instead choose something like "OrangeLagoon18!". They also should not use the same password for multiple accounts. Suggest that they use a password manager that generates and stores login information to ensure passwords are complex and varied (without relying on memory).
- **Use a need-to-know basis:** Grant access to sensitive files and systems only to those whose roles and responsibilities rely on them. You can also limit privileges, such as editor and administrator roles, if necessary. Opt for "read only" access for as many employees as possible to keep malicious actors from viewing, altering or deleting critical or sensitive files.
- **Outline the company's right to access devices:** Create a contract for all employees to sign stating that the company owns and controls all corporate data. The contract should allow the organization to remotely wipe even an employee's personal devices if they are lost or stolen and contain corporate data. Mobile device management platforms can be programmed to only wipe company data and leave personal data untouched, so the employee will not lose anything if this step is taken.

3. Educate Employees on Threats

An educated workforce is the best defense against cyber-attacks. Many organizations now hold regular training sessions on cybersecurity best practices, whether or not employees are working from home. Because of the recent increase in phishing and malware attempts, managers need to communicate more often with employees, sharing tips, updates and other

continued next page

information to combat the threats. Once workers are back in the office and the risk level returns to normal, this training can be a part of employee onboarding and yearly company-wide planning meetings. The program should address:

- Common types of internal and external data threats
- New technologies that assist in hacking
- How to respond if your device has been breached
- Defenses against attacks, such as strong passwords and multi-factor authentication
- Using common sense while online and keeping security top-of-mind

We have certainly never experienced anything like this pandemic before, but fortunately we have advanced technology that allows many of us to continue our jobs in much the same way we would in an office. By taking these cybersecurity precautions, you can keep your organization's data safe through the pandemic, and you will be prepared for whatever happens next.

Brian Schrader, Esq., is president and CEO of BIA, a provider of eDiscovery services and digital forensics.