Guarding the Gateway: Internet Safety for Your Mobile Workforce

Work-related cybersecurity can pose special challenges when employees work at home or while traveling. Here are suggestions for safeguarding data and devices regardless of staff members' locations.

BY JAMES PEARSON

Global pandemics can change things. Drastically. Not all effects of the COVID-19 pandemic were bad, though. The forced shift to remote work and the reliance on cloud-based technologies during quarantines had several positive outcomes. Rural areas in Wisconsin experienced improvements in internet access, and overall, internet connections became more stable as grant funds were made available to improve access and infrastructure.[1]

How and where many people work and what people now find acceptable (such as video meetings with local clients) have been permanently altered. Only 5% of the population was telecommuting pre-COVID; now, as much as 20% of the population remains working remotely. A full 30% of respondents to a study on the topic stated that they would consider a career change if forced to return to in-office work. The good news is that the reduced commute times and other factors have led to an estimated 4.6% boost in productivity.[2]

This transition has proven advantageous for smaller businesses, reducing costs and improving mental health and work-life balance. Given that employees report being more satisfied with their jobs, eating better, sleeping better, and overall, being healthier, there are many advantages to changing to or continuing with a hybrid or fully remote work model.[3]

With the unlikelihood of fully returning to traditional office setups and the continuation of hybrid or remote work models, however, concerns about protecting physical and digital business assets against breaches, ransomware, and threats have become paramount.

Employees in the legal and IT industries, among others, were considered essential workers, and many employers in these fields continued with the in-person-only model even during the lockdown. For them, the idea of relinquishing control permanently over parts of their businesses such as the computer network, in-house servers, and backups and the ability to keep a close watch on employees can be intimidating.

In this article, I focus on six essential aspects of protecting your workforce and data, regardless of where employees work: control, digital security, equipment, education, physical security, and collaboration.

James Pearson owns the Computer Center, Janesville. He is a Microsoft Certified Professional and a frequent author and speaker on cybersecurity and safety topics. Access the digital article at www.wisbar.org/wl.

james.pearson@computercenter.com

www.thelawyersgeek.com

Control

Embracing a more mobile workforce requires adapting to the reality that employees will operate in diverse situations and environments over which individuals have seemingly little control. This challenge involves ensuring staff have the necessary equipment, technology, and resources. Beyond the technological aspects, it is crucial to cultivate a positive attitude toward remote work culture.

From an IT perspective, the focus is maintaining as much control over the environment, wherever that may be, to secure devices and data from threats. When a workforce is dispersed and working from home, the challenges and techniques required differ from those used when all devices are housed under one roof.

Ask questions such as the following: Can someone else access the computer and, therefore, client information? Are other computers on the network, especially in a home or public location? Are the router and networking equipment properly configured?

Managing productivity and fostering a positive work culture pose significant social challenges. Some clients have shown interest in employee computer monitoring software, but the software is expensive, rendering it financially impractical for small firms. Ethically, these monitoring tools are often likened to malware, such as keyloggers that capture every keystroke, infringing on privacy. For remote workers engaged in data entry, tracking keystrokes might be relevant, but most businesses prefer alternative key performance indicators (KPIs) such as billable hours for monitoring and evaluation.

When dealing with a mobile workforce, control what you can to protect your staff and your confidential data from ransomware attacks, technical and software failures, and other cybersecurity threats while maintaining a balance between ease of use and productivity.

Digital Security

Comprehensive digital security measures are essential for both in-office and remote scenarios to protect employees from online threats and to secure people and data. This entails safeguarding data, devices, and users irrespective of their work environment by prioritizing robust technological defenses that function seamlessly regardless of location.

To significantly enhance workplace security, consider doing the following. First, set up a virtual private network (VPN) connection to provide a secure method for remote data access. Second, create a dedicated network exclusively for work purposes in an employee's home.

VPNs create a secure link between one device and others, encrypting the connection to protect data over the internet. Typically, this is achieved through software applications, like those offered by companies such as Nord. Using a VPN shields a user's internet traffic from prying eyes, enhancing online security regardless of the Wi-Fi connection.

Treat employee home networks as you would public hotspots unless you are certain that a staff member's home network is properly configured. Requiring employees to always connect to the internet through VPN software, even at home, helps protect the employer's data and communications.

Another approach to digital security is furnishing employees with pre-configured equipment in their homes that they connect to, creating distinct secure and guest networks similar to those found in businesses. This strategy safeguards employees' devices from potential threats lurking in their household networks, such as family members and visitors using the same connection as the employee's business devices. However, this requires an investment in hardware and equipment, which is discussed in the next section.

This can also be achieved by having a professional IT company review employees' home networks and make any necessary configuration changes. At the very least, having someone versed in cybersecurity review employees' home networks might reveal security issues that must be dealt with, and the person can make recommendations for protecting your staff members and your business interests.

Equipment

Whether employees work in an office or remotely, allowing employees to use their personal devices for professional work (bring your own device or BYOD) is common for most small companies. This appears to be a cost savings. However, concerns can arise about device usage, data storage, and security. Some employees may resist having company information and even multifactor-authentication apps on personal devices.

Despite these issues, providing company-controlled and monitored devices, from computers to tablets, and even providing standardized and pre-configured networking equipment, is one of the surest ways to maintain control over data and how it is accessed. Doing so also allows you to set significantly more stringent security protocols than can typically be done if an employee is using their own device for both work and home.

Supplying mobile equipment to employees allows the employer to standardize devices, ensuring a safe and monitored environment across platforms like Apple, Android, Windows, and Mac. Choosing between allowing personal devices or providing company equipment involves balancing control and costs, including insurance and device retrieval when employees leave. Investing in equipment for employees can be justified by cost-saving measures such as downsizing office spaces.

Businesses can use Microsoft 365 to manage devices with a variety of security features. For example, I cannot send or even copy certain documents using my mobile devices without following proper procedures. A company needs a Business Premium license to access these features, but it is worth the investment.

A technology consultant can help review hardware options, including laptops and tablets, and recommend devices suited to a business's needs. In-house IT professionals can make suggestions for device security features that best fit the company's budget.

While home networks can be configured for security, many default settings lack proper protection, emphasizing the need for standardized work-from-home packages with professionally configured equipment. Providing essential equipment to employees upfront offers benefits like control, security, and peace of mind. The initial cost outlay for equipment can be offset by reduced office expenses.

Whether adopting BYOD policies or providing company devices, prioritizing security and controlled access to data is essential. Finding a balance between cost efficiency and data protection remains crucial in business operations, especially amid shifts toward remote or hybrid work models.

Education

In my journey through the tech industry, my focus has shifted from enhancing productivity with technology to educating others on how to avoid tech mishaps and combat cybercrime. Despite technological advancements, complete security remains an elusive goal. This is largely due to the nature of cybercriminals, who prey on human vulnerability.

Consider these statistics that highlight people's attitudes toward email security:

• 44% think an email is safe if it has familiar branding, even though, for example, 30 million malicious emails were sent in 2022 with Microsoft branding.

• 21% don't know that an email can come from someone other than the sender.

• 63% don't know that email link text might not match the website.

• 62% believe that internal emails are always safe.

• 68% believe that their company can block all malicious emails.[4]

Formal education and training programs are important, even in solo practices and small firms. First, no technological solution can provide foolproof protection, making it imperative to educate individuals on recognizing evolving scams. Second, cybercriminals are adept at outsmarting security measures, necessitating continuous vigilance to safeguard against breaches.

Implementing a documented cybersecurity training program not only demonstrates due diligence and builds a culture of cybersecurity awareness to protect your firm but is now a common requirement for acquiring cyber liability insurance or reducing premiums.

When implementing technological security such as email filtering or encryption, current and new staff and clients should be taught about the technology to ensure that it is properly applied. For instance, employees must understand the limitations of email encryption to prevent inadvertent disclosure of sensitive information, such as how and when emails are encrypted and whether there is a manual process an employee must follow, such as pressing an "encrypt" button or using a keyword in the subject. Further, despite encryption software, personally identifiable information should never be included in the "to," "from," "CC," and subject lines and file name attachments because these can never be encrypted.

Education plays a pivotal role in ensuring operational security. An honest mistake that results from a lack of awareness can have catastrophic consequences, leading to data breaches or malware attacks. Therefore, investing in regular education is not merely beneficial but essential for protecting your organization in the digital age.

Physical Security

When safeguarding data and maintaining confidentiality for a mobile workforce, internet incursions are not the only threat to consider. Physical security is often overlooked. This involves remotely protecting computers, tablets, and other devices connected to your network or office.

Concerns about unauthorized access to devices, particularly in home environments where boundaries are often blurred, are increasing. Allowing children to use work devices, for instance, can lead to the installation of malware or viruses and potential data breaches.

Employees might inadvertently leave sensitive information exposed on desks or tablets or write down passwords in easily visible places.

Employees should be encouraged to secure devices as they would sensitive office items like papers and documents, including by doing the following: 1) ensure that devices are stored away from curious kids or visitors; and 2) address situations when outsiders might be present, like friends or servicepersons, and secure documents and devices as one would in the office. This shift to personal responsibility emphasizes the human element in maintaining security.

Employers should establish clear policies and guidelines to address these physical security risks effectively. This includes discouraging the habit of jotting down passwords in physical notebooks, which can be easily viewed, lost, or stolen. Despite their popularity on Amazon, password notebooks are not a secure solution. Instead, investing in a password manager for employees to securely store and share this information with trusted individuals is highly recommended. Additionally, incorporating device theft prevention into overall security strategy is essential.

All physical devices that employees use to access or store business information, including USB drives, should be encrypted. This ensures compliance with Wis. Stat. section 134.98(1)(b), under which entities that possess personal information need not provide notice of unauthorized acquisition of such personal information to the subjects of the personal information if the information is encrypted.

Educating employees plays a key role, alongside implementing encryption, passwords, and automatic device locking. These practices, which mimic office security, are crucial when devices are used remotely.

Collaboration

Sharing documents and files with employees who work remotely or other people has become second nature and is integral to conducting business. Securing files is paramount, regardless of whether employees work from home or in an office. Without a standardized platform and clear procedures on what can and cannot be shared and how to share files, employees might turn to unauthorized file-sharing methods, risking data breaches and creating issues in controlling, backing up, and securing the data. To mitigate such risks, it is essential to establish robust standards and procedures for secure file sharing. This involves restricting external file sharing and consulting with an IT provider on best practices.

Leveraging technologies like Microsoft Teams with appropriate access controls for file sharing within organizations can facilitate effective collaboration. Beyond file sharing, Teams' communication tools, videoconferencing, and chat applications have created an all-in-one system for communicating within and outside organizations.

Managing file-sharing permissions diligently is advisable, particularly for users with a Microsoft 365 license. Leveraging SharePoint and Microsoft OneDrive for Business, for example, enables external file sharing through designated sites while ensuring the security of other documents if configured properly. For example, on my phone I have secure access to a variety of internal documents and information but am restricted as to which I can share externally from that device and the method I can use. This makes the process more challenging but also significantly more secure, protecting me from accidentally sharing information that should not be shared and making me very conscious of what I am sharing.

Employers should use a standard file-sharing platform for seamless internal and client communication by uploading files and sharing secure links. Implementing best practices like setting expiration dates for shared files helps to mitigate prolonged-access risks. Employers can enhance data protection by incorporating additional security measures such as passwords or two-factor authentication and leveraging tools like Microsoft 365 to authenticate recipients before granting access to shared files.

Conclusion

Embracing the efficiency and benefits of a mobile workforce while maintaining security and control over data and employees is a balancing act between convenience, ease of use, and security.

Standardizing equipment and security protocols, regardless of an employee's location, along with providing comprehensive training to ensure adherence to best practices, can significantly enhance productivity and job satisfaction. Knowing that you've diligently protected your staff, clients, and physical and digital assets can provide peace of mind.

The Computer Center has created a free resource center on this topic, available at https://info.computer-center.com/gatewayguard. **WL**

ENDNOTES

[1] Danielle Kaeding, *Wisconsin Makes $100M Available for Broadband Expansion and More Federal Money Is on the Way*, Wis. Pub. Radio, www.wpr.org/economy/wisconsin-makes-100m-available-broadband-expansion-and-more-federal-money-way (Nov. 9, 2021).

[2] Steve Maas, *Work from Home Likely to Remain Elevated Post Pandemic*, Nat'l Bureau Econ. Rsch., www.nber.org/digest/202106/work-home-likely-remain-elevated-post-pandemic (June 1, 2021).

[3] Gleb Tsipursky, *The Surprising Health Benefits of Hybrid Work*, Psych. Today, www.psychologytoday.com/intl/blog/intentional-insights/202304/the-surprising-health-benefits-of-hybrid-work (May 2, 2023).

[4] Proofpoint, *2020 State of the Phish: An In-depth Look at User Awareness, Vulnerability and Resilience* (Dec. 2019), https://go.proofpoint.com/rs/309-RHV-619/images/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf. **WL**