CYBER READINESS
INSTITUTE

Cyber Readiness for the Hybrid Workplace – **Demystifying Technology**

Here is the situation small and medium-sized enterprises (SMEs) now face: Employees working from home, the office, and other locations (even outdoors, weather permitting). Employees using company devices and personal devices. Employees accessing or transferring documents from location to location and device to device. Employees sharing documents with other employees and third parties. Hackers systematically probing networks, seeking to take advantage of new vulnerabilities.

The hybrid workplace poses enormous cybersecurity challenges for organizations of all sizes. People need to develop new habits and organizations need to implement policies adapted to the hybrid workplace. Human behavior is the foundation of security in all organizations.

However, organizations also need to consider deploying new technology for the hybrid workplace. As employees move from location to location, they may be using different devices. They are likely using different connections to access your network and data from different locations. Variable access throughout the hybrid workplace creates vulnerabilities and the potential for confusion and chaos.

For SMEs, we recommend thinking about the hybrid workplace in terms of devices, connections, and data. Here are the basic questions you need to answer:

Devices:

1. **What devices are employees using?**
2. **Are they using the same devices regardless of where they are?**

Connection:

1. **How are employees connecting to your network when remote?**
2. **How are employees connecting to your network at the company’s location?**

Data

3. **How are employees accessing data from each device and location?**
4. **What data are they accessing?**
5. **How are employees transferring data from device to device, from location to location, and to other employees or third parties?**
6. **How and where are people storing data?**

There is an enormous amount of technology available to try and reduce cybersecurity risk, including an overwhelming number of hardware and software choices. The challenge for SMEs is to understand what technology investment will significantly reduce cybersecurity risk – and what technology will enable secure employee behavior instead of encouraging workarounds.

Thinking about technology through the lens of devices, connections and data is an effective way to evaluate your options and make decisions. As you think about technology, the number of employees and your budget will, of course, have a huge impact on what is possible. Here are a few considerations to get you started.

Devices:

1. **Company-issued computers and/or tablets:** These will reduce your risk and afford you more control over what software is installed, software updates, doing virus and malware scans, etc. – if you can afford it. An alternative is to consider virtual desktop infrastructure (see below).
2. **Company-issued smartphones:** Depending on your business and how people work, consider these company-issued devices, as well. Individuals conduct much of their personal lives on a smartphone and the vulnerabilities created by social and entertainment apps could provide access to your company network if they are not properly firewalled. Company-issued smartphones can be controversial because individuals don't like to carry two smartphones. As a manager, you need to make the risk management decision that makes sense.

Connections:

1. **Virtual private network (VPN):** A VPN is an important basic protection when people are working remotely. It creates a private, secure "pipeline" between the employee's home and your network.
2. **Segregating the employee's home network:** For employees accessing valuable and confidential information, help them set-up their own wi-fi network at home with a separate password.
3. **Company-issued hot spot:** Some of today's mobile hot spots have a built-in VPN. These hot spots can be a good alternative to having people use shared wi-fi or their personal phone as a hot spot. Also, a company-issued hot spot is a good option for employees who work from multiple remote locations.

Data:

1. **Cloud-based file-sharing:** This file-sharing eliminates many of the security issues with data access, transfer, and storage when people are working from multiple locations because the documents are all stored centrally. However, it does require people to change their behavior and develop new habits, such as: A) An organized approach to document locations; and B) A process for version control. Companies must also make sure employees have strong, secure connections (see above) when they are working remotely to ensure the security of the file-sharing system.
2. **Virtual desktop infrastructure (VDI):** VDI means that the employees' "desktop" is not on their device. It is on a server that they can access from any device and can eliminate the need to provide company-issued devices. Applications and data only exist on the server so they can be centrally managed. This offering is often bundled with cloud services, software, and cybersecurity software.

No matter what approach to technology you choose, remember that human behavior is critical in developing a cyber ready culture at your organization. As you select and deploy new technology, make sure it is practical for people to use given their jobs, that you update your policies as needed, and that you provide training and ongoing support.

Stay tuned as we continue our hybrid workplace series to demystify cybersecurity by providing tips for managers and employees. Take a look at our other guides on helping people develop good cyber readiness habits and implementing practical policies that people will follow.

About the Cyber Readiness Institute

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). Explore the building blocks of good cybersecurity with our Starter Kit or create a cyber readiness culture in your organization with the self-guided, online Cyber Readiness Program. Our Remote Work Resources and Hybrid Workplace Guides offer timely tips for addressing the evolving cyber challenges of today. To find out more, visit www.BeCyberReady.com.