A Better Way to Manage Employee Home Internet

NO MATTER WHAT BRING YOUR OWN DEVICE (BYOD) POLICIES COMPANIES USED BEFORE 2020, the ongoing popularity of remote work during and since the pandemic has thrown the old playbook out the window. Today's employees are not only connecting on their own devices — they're also using their home routers to engage in bandwidth-intensive video calls and routinely send and receive sensitive corporate information.

Using home internet connectivity for work creates efficiency and productivity challenges for both employees and company administrators. It also raises serious concerns about cybersecurity, which is anything but a given in home systems.

79%

of organizations said **remote working had adversely affected their cybersecurity** and **increased the burden on security teams**.

Closing your eyes to these problems won't make them go away, just as it didn't stop the BYOD movement. But by facing the problems strategically and proactively, and working with employees to implement a solution, companies can improve productivity and security throughout the organization.

PROBLEM 1: **Administrative Burdens**

Accounting for remote employee internet usage imposes significant administrative burdens. Legal obligations for reimbursing employees for all or a portion of internet connectivity vary by state. As of January 2023, 11 states and Washington, D.C., required expense reimbursement for remote work technology, including internet and mobile data usage. In addition, federal law forbids employers from mandating remote work expenses, such as buying a new computer or upgrading home internet, if doing so reduces an employee's earnings below the required federal minimum wage.

Expense calculations must be done individually. Different carriers have different plans; separating work and private usage can be tricky. These are time-consuming, tedious tasks, especially for companies operating in several states. "Digital nomad" employees who move from state to state further complicate management. Companies that allow employees to use their own plans and routers must familiarize themselves with local laws and stay on top of them as they evolve.

CIO

SPONSORED BY verizon

PROBLEM 2: **Employee Productivity**

Working from home eliminates tiring commutes and allows employees to complete their tasks in a comfortable environment. But home workers often share a router with others. If two or more users are videoconferencing, gaming, or streaming, speeds can slow to a crawl.

In addition, modern homes are filling up with connected devices like voice assistants, smart lighting systems, and robotic vacuums. Employees may not realize it, but each of these devices has its own IP address and operates on the same Wi-Fi network they use for work. Most home routers were not built to accommodate the devices nor traffic they generate, and they don't prioritize work tasks over, say, carpet cleaning.

Taken together, these issues impinge on employee productivity and morale.

PROBLEM 3: **Security**

When improperly configured, consumer-grade routers can increase cybersecurity risk. Many come with simple pre-installed passwords that are difficult or impossible for users to change — and easy for hackers to guess.

While manufacturers provide periodic firmware updates to address security issues and bugs, they aren't always done automatically on home routers. The burden then falls to employees, who may have difficulty finding the updates and following installation instructions — assuming they take time away from work to do so. A 2022 Proofpoint study found that 82% of users had never updated their router's software or firmware, and 80% had never changed their router's password.

Even users who diligently maintain their routers can't solve every problem. Consumer-grade routers introduce the risk of unpatched security flaws, and even fully updated routers will likely contain undetected vulnerabilities that could have been avoided.

These problems come at a time when companies are increasing employee access to the kind of information hackers want to steal. In the Verizon 2022 Mobile Security Index, 53% of organizations said that employee mobile devices have more access to sensitive company data than they did a year ago. Entrusting corporate security to busy employees and technology not meant for professional use is a recipe for trouble. In the Verizon survey, 79% of organizations said remote working had adversely affected their cybersecurity and increased the burden on security teams.

PROBLEM 4: **Lack of IT Visibility and Control**

Allowing remote employees to supply their own connectivity means IT teams have little or no visibility into the health, availability, and performance of those routers. Without a centralized management portal that enables IT teams to monitor router status — or even push simple updates to devices to ensure workers can get the job done — bring your own device can quickly become bring your own disaster.

A Single Solution: Business-Grade Routers for Employees Working from Home

Companies can address all the challenges created by remote internet use by making a strategic decision to issue employees business-grade routers dedicated solely to work.

Upgrading to business-grade routers eliminates the administrative burden of managing reimbursements, especially if companies use a single billing system from a nationwide internet provider. Business-grade routers also solve performance issues, since they are not shared with other family members who may be playing games, streaming video, or doing work for a different employer. With a centralized management portal, companies can also ensure greater visibility into, and control over, remote workers' modems and routers. And companies can configure business-grade routers to apply their own security controls across all remotely connected employee hardware, creating a much safer environment and allowing IT and security staff to focus on the big picture, instead of constantly dealing with individual problems.

To learn more about improving security and productivity with nationwide wireless internet connectivity and business-grade routers, visit **Verizon Remote Work Solutions**.