HR’s Critical Role in Remote-Work Security

AS COMPANIES EMBRACE REMOTE AND HYBRID WORK, they face a broader range of cybersecurity threats. Employee home networks — many inadequately secured — are accessing corporate data, and every improperly configured connection provides a fresh opportunity for cyberthieves.

IT and security teams are struggling to deal with this new environment. Though they may not realize it, they have a powerful ally who can help: their own human resources departments. By driving security policy awareness among employees, delivering state-of-the-art training, and influencing important decisions about the technologies necessary to secure remote work, HR professionals are uniquely positioned to play a critical role in improving an organization’s cybersecurity profile.

Employees Adrift Amid Threats

Cybercriminals, who are well aware of home network vulnerabilities, have made remote employees a favorite target. According to the National Institute of Standards and Technology, “Organizations should assume that malicious parties will gain control of telework client devices and attempt to recover sensitive data from them or leverage the devices to gain access to the enterprise network.”

Too many have already succeeded. In the Verizon 2022 Mobile Security Index (MSI), 79% of surveyed organizations said remote working had adversely affected their cybersecurity and increased the burden on security teams. Nearly half said they had recently experienced mobile-related compromise — almost twice as many as in the previous year’s survey — and 73% described that compromise as “major.”

Organizations have shifted much of the burden of recognizing and avoiding these attacks to employees, but many don’t provide sufficient training or resources to enable workers to meet the standards they are expected to uphold. Only 47% of the companies in the Verizon MSI survey issue guidance on maintaining privacy when working remotely. Over half fail to provide security training when employees change their working arrangements, such as moving to a remote or hybrid position.

Working together, HR and security teams can help turn situation around, making security awareness second nature for employees and preventing even sophisticated threats from breaching corporate systems.

Creating a Strong Policy and Regular Training

Employees are the organization's first line of defense against cyberthreats, yet many lack the practical knowledge and tools needed to make sound decisions. In the Verizon survey, 48% of companies admitted they don't have a written acceptable use policy that clearly outlines how employees are expected to use company-issued devices and the internet when working remotely.

A robust policy can greatly reduce risks, especially if employees are required to sign a document saying they understand and accept its terms. Every choice a remote employee makes — from ignoring security settings and updates for their consumer-grade modems, to clicking suspicious email links, to downloading unsanctioned consumer applications — can, and should, be influenced by an acceptable use policy developed jointly by HR and IT.

HR teams, with their expertise in developing job skill and career development courses, should advocate for comprehensive security training as a requirement for promotion — or for even getting hired. Because cyberthreats constantly evolve, training should be provided regularly. Remote workers should also have information at their fingertips about when and how to contact security if they encounter a suspicious incident or suspect a breach.

Providing the Right Tools

HR leaders can further contribute to security improvements by pushing for a strong set of standardized tools and technologies for remote employees. Deploying the right technologies can enhance security while saving employees time and allowing them to focus on the tasks they were hired to do. Some of the most important technologies include:

- Wireless network security, including data encryption to help protect sensitive information, and multifactor authentication to ensure that device users are who they say they are. These controls help keep hackers out before their ruses reach employees' eyes.
- Company-issued routers with standardized, built-in protections and remote router management for visibility and control. Home routers often lack even the most basic controls.
- A single online portal that enables IT teams to monitor the health, availability, and performance of company-issued routers and modems — and push required configuration updates consistently across the remote enterprise.
- Mobile device management software to support devices throughout their life cycles. Remote management removes the burden of installing updates on phones, tablets, and computers from busy employees, who create dangerous security gaps when they fall behind. It also makes management easier for IT staff who deal with a large number of devices, makes, and models.
- A videoconferencing platform with extensive security and privacy controls, such as BlueJeans Meetings, which can restrict attendance to legitimate users and comes with AES-256 GCM encryption to keep company information private and secure.
- Virtual 24/7 tech support for employees. Remote workers are not accustomed to managing their own technology. If they can't get their questions answered right away, they may make bad decisions that go unnoticed by IT — until they cause a security incident.

> Organizations should assume that **malicious parties will gain control of telework client devices** and attempt to recover sensitive data from them or **leverage the devices to gain access to the enterprise network**.

Building a Safer Organization

As HR departments know, allowing remote work is essential for attracting and retaining talent. But without adequate security precautions, it can create serious problems. By collaborating with IT to develop a robust security policy and regular training, providing informed advice about the tools employees need to keep corporate systems safe as they work, and advocating for standardized routers and modems for all remote employees, HR leaders can play a key role in improving cybersecurity throughout the organization.

To learn more about how to enhance security in the remote work environment, visit **Verizon Remote Work Solutions**.