5 Misconceptions About Home Network Security

Key Concepts Organizations Need to Get Right to Secure the Hybrid Workforce

Change is a fact of life in IT security. Technologies change, security best practices evolve, and enterprise attacks shift and grow. Now, many of these changes are driven by the challenges and opportunities of a hybrid workforce that allows employees to connect, create and collaborate in new ways. While this shift from the office to the home offers many benefits for both employers and employees, the nature of remote work introduces a new generation of security challenges for IT teams. As employees generate and access more data remotely through home networks, the number of security blind spots also balloons. Sensitive and proprietary data that was once confined to secure corporate offices is now susceptible to vulnerable home environments.

With the home now functioning as the new branch office for one, it needs the same level of network security as traditional branch offices. Deploying a robust home network security solution for your work-from-home (WFH) employees will help identify risks, eliminate security gaps, and stop attacks at the home network edge. In this guide, we will identify and correct five of the most common misconceptions about home network security to help organizations plan, implement, and optimize network security strategies for at-home employees.

1 Home networks are too insignificant to be at risk of a cyberattack

REALITY

Easy-to-attack or high-value targets attract cybercriminals

The business of cybercrime is similar to a legitimate business model. Hackers offer differentiated products and services, have integrated marketing campaigns, provide customer support, conduct risk and reward analysis, and even invest in research and development. These easily accessible services and hacker toolkits—like ransomware-as-a-service and phishing-as-a-service—are appealing for lower-skilled threat actors who are happy to rake in hundreds to thousands of dollars with minimal effort. These cybercriminals aim to maximize their gain with the least effort, which often means that vulnerable home networks are prime targets.

Because WFH employees have a persistent and predictable nature, home networks are also susceptible to targeted and sophisticated attacks. Once the home IP address is identified (often via phishing), threat actors can conduct reconnaissance and attempt repeated attacks over a long period with multiple attack vectors. If the home network is breached, cybercriminals can then intercept communications, disrupt availability, or steal sensitive information, particularly from high-value executives or those with access to valuable data.

Insight:
C-level executives are 12 times more likely to be targeted in cyber attacks than other employees in their organization.[1] Most cyber attacks against business leaders stem from financial motivations that include ransomware extortion or the selling of employee data, company trade secrets, or intellectual property.

Tip:
To prevent outsiders from easily accessing home networks, employees should avoid publicizing the SSID. Changing the SSID to something unique and unrelated to their identity or location is ideal. Using the manufacturer's default identifier could allow a potential attacker to pinpoint the type of router and exploit any vulnerabilities.

2

Most home routers are “secure enough” out of the box

REALITY

Consumer routers are fraught with vulnerabilities

Home routers are often targeted by attackers seeking control over a user’s gateway to the Internet. Router misconfigurations (e.g., default credentials, open admin interfaces, etc.) and the lack of security precautions (e.g., software/firmware updates) can make home routers susceptible to exploitation. Unfortunately, many routers do not automatically check for updates like critical patches and security fixes. And, since integrating newly updated firmware can be expensive for manufacturers, the operating system can also be outdated. These potential security holes compound and expand the possible surface area of attack.

Many home routers also come out-of-the-box with overly permissive factory-default configurations, which are intended to reduce customer service troubleshooting time and make them user-friendly. Unfortunately, default configurations are not geared toward security and may open the door to cybercriminals. Once an attacker gains a foothold to a compromised router or an unsecured connected device, they can steal sensitive information from a user’s computer or perform other nefarious activities.

Insight:
In a recent IT security evaluation, nine of the leading consumer routers—including Asus, Netgear, Linksys, and D-Link—had underwhelming results[2] with a total of 226 potential security vulnerabilities found.

Tip:
A large number of manufacturers use default passwords like “admin”, which in many cases can be read in plain text. Employees should change their passwords and enable automatic updates as a security best practice.

3

A corporate VPN will prevent sensitive data exposure

REALITY

VPN alone is insufficient for modern threats

Most organizations have a VPN which encrypts connections at the sending and receiving ends while also blocking unencrypted traffic—allowing secure connections to the corporate network when outside the office. While securing remote work has long been the domain of VPN technology and is an important component of secure remote access, it may not always be enough to limit all the risks that are present in homes. Some of these risks include, but are not limited to:

1. The inability to extend protections to agentless devices without an OS—like printers, hardware prototypes, and VoIP phones. This complicates home office enablement and inhibits reliable corporate controls.

2. Employees who turn off their VPNs to improve performance, connect with printers, or to perform non-work related activities can prevent IT visibility. The moment an employee turns off their VPN, they risk exposing sensitive company data to threat actors.

Insight:
Only 47% of those with a VPN installed always have it on. One in five never use it or only use it when they have no other option.[3] These findings reinforce the position that remote security defenses are often at the mercy of user behavior.

Tip:
Organizations need to complement a robust VPN with an always-on home network security solution that elevates security from the endpoint to the network-layer.

4 Insecure personal devices pose minimal risk

REALITY

Cybercriminals are increasingly targeting personal lives in order to target the company

Employees today expect the flexibility to be able to work wherever and whenever they want. However, using personal devices to access corporate data creates an opportunity for cybercriminals to steal personal information, company data, or breach the home network. If a single home network blends traffic with both corporate-issued and personal devices, there is risk for cross-contamination and lateral movement.

The exchange of information between home and work systems via email or removable media can also put work systems at an increased risk of compromise. Ideally, employees should only use company-issued equipment and accounts to conduct work while at home—but with the lines between personal and professional digital lives being blurred, it's possible that poor employee training, desire for flexibility, and human error can result in sensitive data exposure.

Insight:
Cybercriminals can steal employee information from hacked personal devices, as well as mass scraping of public profiles on social media platforms, recruiter tools, and publicly available background checks. This information can then be leveraged to execute "vishing" campaigns or other social engineering scams that aim to obtain corporate credentials.

Tip:
Network segmentation of personal WiFi from corporate WiFi is an effective strategy to mitigate the risk of lateral attacks from insecure personal devices.

5 A corporate network (at home) will violate employee privacy

REALITY

Robust home network security enhances personal privacy

Any employee's personal privacy is at risk when using insecure consumer routers. If an attacker accesses a home router, they can access an employee's entire Internet life, including personal private information. Everything from web browsing to mobile devices to IoT security cameras has the potential to erode personal privacy. A first step to protecting employees' personal privacy from outside threats is improving home network security with a secure, enterprise-grade router.

Any company-issued router that extends enterprise security into employees' homes will provide visibility and remote management for IT staff. The corporate WiFi network and any connected devices—like work-issued laptops and printers—are subject to the employer's privacy policies. It's important to note that any personal device connected to the corporate network or personal activities on company equipment may be subject to the employer and is not regarded as a violation of employee privacy.

Insight:
Cybercriminals can perform Man-in-The-Middle (MiTM) attacks in order to eavesdrop on personal activities and steal private data, as well as manipulate traffic in a way that sends users to malicious websites. They can also access information sent through WiFi like emails, financial information, and account credentials.

Tip:
Employees should always set up a separate WiFi network for their personal devices. With a VLAN (virtual local area network), employees can ensure their personal devices are on one network and corporate devices are on another. Network segmentation will remove the risk of commingling personal and corporate traffic—which may be visible to employers via company-issued routers.

Summary

We've seen profound change in the way people work. Large factories first attracted workers from rural areas to cities, gradually getting replaced by big offices as economies became more service-sector driven. How we worked, however, remained the same: employees left their home for a place of work and then returned home. But, during the COVID-19 pandemic, we developed a newly persistent work model for the first time since the Industrial Revolution: work from home.

The cybersecurity implications of this paradigm shift are everywhere. A remote hybrid workforce comes with a myriad of risks, ranging from reliance on employees' BYO-Routers to lack of IT visibility and control. The most obvious risk is that all employees' tasks are now conducted on vulnerable home networks with many possible entry points, increasing the attack surface and exposure to cyber attacks.

Okyo Garde Enterprise Edition is a WiFi 6 mesh-enabled router that extends secure access service edge (SASE) to your employees' home networks. It inspects all traffic across all ports with industry-leading threat intelligence. Okyo Garde Enterprise Edition then adds another layer of protection and prevents lateral attacks by segmenting corporate WiFi from personal WiFi. Designed with a Zero Trust model, it provides the same peace of mind while working from home as your employees would in the office.

To learn more about Okyo Garde Enterprise, visit our website or contact your Palo Alto Networks representative.

[1] Verizon Data Breach Investigations Report, 2019

[2] https://www.iot-inspector.com/blog/router-security-check-2021/

[3] Verizon Mobile Security Index 2021 Report