Sycurio.

Home space: the new workplace.

Best practice recommendations for securing the extended enterprise – and keeping remote workers in the healthcare industry safe

Executive summary.

Post pandemic, remote and hybrid workforce models have become the new norm. However, this wholescale shift to remote work is providing low hanging fruit for hackers intent on taking advantage of vulnerabilities created when organizations rush to virtually connect remote workers to the workplace.

Unfortunately, when it comes to securing remote access to sensitive corporate data and applications in the healthcare industry, the traditional method for remote connectivity, virtual private networks (VPNs), lack the inherently strong security measures and safeguards needed to prevent attackers from compromising the remote user and hence potentially the enterprise network. In part, because remote employees will be dependent on home office equipment such as own-procured and managed printers and routers that are far less secure than enterprise office-based networks and IT assets.

> **It's an issue that is becoming a priority for any healthcare provider looking to unlock the operational cost and flexibility benefits to be gained from putting remote workforce models on a permanent footing.**

This paper explores the drivers behind the shift to remote working, examines the security challenges involved and takes a detailed dive into why today's extended enterprise perimeters represent a tempting target for cybercriminals.

Setting out the key security issues that need to be addressed, this paper looks at why it is important to go beyond simply just securing local sensitive data and highlights why it is necessary to lock the back door and not allow fraudsters entry to the corporate network from the home network.

Introduction.

The COVID-19 pandemic has wrought fundamental changes to the way that modern work is undertaken. No longer an optional nice-to-have, remote working with no geographic restrictions is now a core business necessity.

The rapid shift to anytime/anywhere working during government mandated lockdowns saw organizations rapidly rollout architecture and technology upgrades to facilitate work-from-home at scale.

While it remains to be seen if firms will again revert to a predominant office-based environment, current indications suggest that work-from-home or hybrid working (where employees move between home and office) is here to stay.

One advantage of moving agents to home-based environments is the potential cost savings - a reduction in operating costs can be made just through lower utility bills and less upkeep of a physical office space! These significant savings are nudging businesses of all shapes and sizes, and across all industry sectors, to permanently adopt remote operational models. Indeed, a recent report revealed U.S. businesses could save almost $11,000 per employee per year if workers telecommuted an average of 2 ½ days per week.

To accommodate the rising demand for remote access to corporate networks, systems and data sources, IT architectures are becoming ever more complex as network perimeters extend. Keeping pace with these changes is challenging enough for IT teams. A distributed workforce creates more endpoints on the corporate network that can be vulnerable to security breaches. Addressing these risks means security practices must, by necessity, also evolve.

Rethinking security strategies with remote working in mind

Research shows that IT departments are having a difficult time protecting today's significantly wider organizational perimeter.

Historically, protecting the enterprise perimeter has always been a challenge and many organizations have been slow to make the move from perimeter-based protection approaches to more advanced Zero Trust-type security models[1] that radically improve the security posture of the enterprise.

However, in response to the growing number of high-profile security breaches, particularly in the healthcare sector[2], implementing a Zero Trust architecture should be viewed as a mission-critical priority for a number of reasons:

1 The number of **employees working beyond office walls** has increased exponentially and organizations now have to consider how best to minimize the security risks associated with the home networks and personal devices used by workers.

2 In the wake of COVID-19, organizations are increasingly dependent on remote **cloud-based business services** that can be accessed by employees from anywhere.

3 The importance of protecting the IoT (Internet of Things) within the home-network is growing[3] as IoT malware detections surge by 60%[4].

4 The **average cost for ransomware recovery** has skyrocketed from $761,106 in 2020 to $1.85 million in 2021[5]. IoT breaches are even more out of control with Kaspersky[6] reporting 1.5 billion breaches of IoT devices during the first six months of 2021 alone compared with only 639 million for all of 2020.

[1] https://www.hindawi.com/journals/scn/2021/9947347/
[2] Healthcare Data Breach Statistics - Latest Data for 2022 (hipaajournal.com)
[3] https://www.infosecurity-magazine.com/news-features/cybersecurity-home-working-one-year/
[4] https://www.infosecurity-magazine.com/news-features/cybersecurity-home-working-one-year/
[5] www.infosecurity-magazine.com/news/ransomware-iot-malware-detections/ical-smes
[6] https://realbusiness.co.uk/putting-cyber-security-first-latest-trends-make-critical-smes

Scoping the scale of the challenge

Traditionally, IT teams paid little attention to the security status of home networks and personal devices used by staff. In the past, most employees worked from the office using corporate issued (and managed) devices, with remote working a 'nice to have' for a select subset of staff.

Today, it's a different story. All staff home networks, Internet access mechanisms, and any portable networking device - such as personal desktops, laptops, tablets, printers and phone - used to access corporate systems now are in scope of an IT department's purview.

Securing all these previously unknown devices is vital to ensure staff can remain functional and effective when working remotely and that enterprise data assets remain protected. That's because every employee who works from home presents a new gateway into the company's network.

For IT departments, identifying what staff-owned devices are being used - let alone protecting these previously unknown devices - is in itself a significant challenge. Yet as workplace environments evolve beyond BYOD (Bring Your Own Device) to BYOND (Bring Your Own Networks and Devices), deploying appropriate security protocols is of paramount importance for protecting any corporate information accessed from home networks.

The very nature of home network environments means 'difficult to predict' security hurdles must be surmounted. Home networks can be highly complex and interconnected structures; for example, neighbors sharing Internet connections, house shares, apartment complexes with shared IT infrastructure etc.

Added to which, it is often not appreciated by organizations that many staff will use their own devices – such as their personal devices and mobile phones – to receive Multi-Factor Authentication (MFA) tokens via SMS or email. As a result, these personal devices are rarely in scope of an organization's security purview[7] but within the chain of trust and thus should be considered as sensitive assets.

The very nature of home network environments means 'difficult to predict' security hurdles must be surmounted.

[7] https://www.cisco.com/c/en_uk/products/security/ciso-benchmark-report-2020.htm

Attackers focus on the weakest link.

Home office / personal devices typically have weaker security features than corporate assets. This makes them a top attack target for malicious threat actors looking to commit fraud, harvest sensitive information to sell on to criminal underground networks, or to perpetrate ransomware-type attacks.

Key findings revealed in HP Wolf Security's recent home working survey[8] should serve as a wake-up call for IT and information security teams in every organization:

76% of office workers surveyed say working from home during COVID-19 has blurred the lines between their personal and professional lives

27% of office workers surveyed say they know they are not meant to share work devices but felt they 'had no choice'

50% of office workers say they now see their work devices as a personal device

[8] https://threatresearch.ext.hp.com/hp-wolf-security-blurred-lines-blindspots-report-risky-remote-working/

The research also reveals how remote working environments have stimulated a significant associated jump in cyberattack levels:

54% of IT decision makers (ITDMs) saw an increase in phishing

56% of ITDMs identified an increase in web browser related infections

44% of ITDMs saw compromised devices being used to infect the wider business

45% saw an increase in compromised printers being used as an attack point

Even more concerning was the finding from KuppingerCole, an international, independent analyst firm that contributed to HP's report, which showed a 238% increase in global cyberattack volumes during the pandemic.

The message for businesses is clear. Home networks and personal user devices represent a significant weak link in the organization's security defenses - and are absolutely being targeted by cyber criminals. Yet these very networks and devices are being enabled to access the innermost sensitive corporate assets from home!

238%

increase in global cyberattack volumes during the pandemic

The impact of home working on breach costs.

Findings from IBM's 2021 Data Breach Report[9] show that the number of days it takes to identify and contain a security breach increases by 22.5% for organizations with over 50% of their staff working remotely. Not only is it taking longer for these organizations to detect breaches, the cost associated with each breach is also more significant.

IBM's research found that breach costs increased by 38% for organizations deploying more than 80% remote workers. Where remote workers were a factor in the breach event itself, the average cost per breach increased by a staggering $1.07M.

It is stating the obvious that a data breach is highly undesirable for multiple reasons. Depending on the type of data involved, the consequences can include the destruction of databases, the leaking of confidential information, the theft of intellectual property, reputational and customer trust loss, significant regulatory fines, and financial penalties.

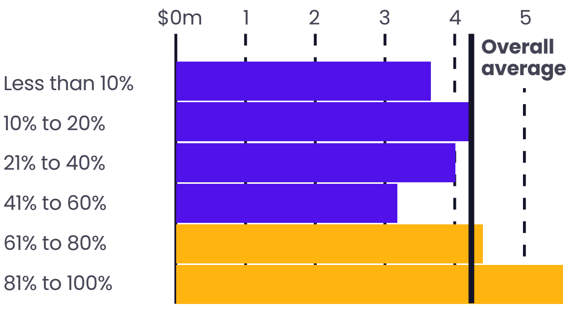
Which is why taking action to protect sensitive data and minimize the risk of data breaches should be considered a necessity.

No. of days taken to identify/ contain a breach increases by 22.5% where firms have 50%+ remote workers

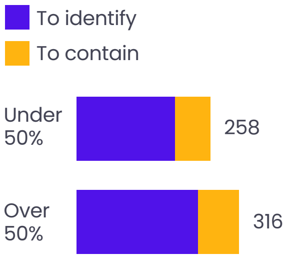
Breach costs increased by 38% for firms deploying > 80% remote workers.

Average cost per breach increased by $1.07M if remote workers were a factor

Average cost of a breach by share of employees working remotely



Average number of days to identify and contain a breach, by level of remote work adoption



Survey of breaches from May 2020 to March 2021.
Source: IBM Securiity Cost of a Data Breach Report 2021

[9] https://www.transpere.com/blog/ibm-data-breach-report-2021/

Potential solutions.

The following high-level recommendations will help organizations minimize their risk of data breaches:

- **Identify all assets, especially BYOND**. This is a non-trivial task that requires continuous effort. To coin a phrase, how do you protect something if you have no idea of its whereabouts or even existence? The importance of this recommendation is significant.
- **Protect BYOND using defensive controls such as firewalls (Network / Web Application Firewalls)** or End Point Protection (EPP) technology. This is a difficult task in non-corporate, home network environments. Additionally, deploying EPP agents on home workers devices often meets with resistance due to users citing privacy and performance issues.
- **Invest in "Human Firewall" or information security awareness training.** It is vital that all employees understand what constitutes 'good' and 'risky' digital behaviors and are appropriately trained on how to spot phishing and other attack approaches.
- **Remote access via VPN with multi-factor authentication (MFA)** is a step in the right direction but again, if the BYOND is compromised, this is susceptible to subversion and would facilitate direct access for an attacker to the corporate network and sensitive data assets. In a recent article, Manuel Reischl[10] highlights some important issues and concerns relating to the suitability of VPNs for protecting access to corporate assets from the home network.

It is vital that all employees understand what constitutes 'good' and 'risky' digital behaviors and are appropriately trained

While organizations can choose from multiple point security solutions, these are often difficult to implement on non-corporate owned networks and private IT assets such as mobile phones, tablets and desktops or laptops. Which is why Zero Trust is emerging as the preferred remedy for addressing work from home and other remote work security challenges.

[10] https://www.cpomagazine.com/cyber-security/everyone-loves-remote-work-especially-hackers/

Zero Trust for working at home.

Part of the Zero Trust approach is to presume that the hacker is already in the network. So how can we protect corporate information that is exposed to workers in the home environment, if that home environment has been breached? There are several security controls that can be adopted, two of which are discussed below:

- Ensure all sensitive corporate data accessed, collected, and exposed to the home network is secure and rendered valueless to cybercriminals
- Enforce a perimeter defense on the home worker's IT asset accessing the corporate network and environment

Let's expand each of these in turn:

Valueless privacy data

Replacing sensitive data with tokens is a long-standing security control practice that in effect substitutes sensitive data with valueless identifiers. Sophisticated techniques such as Dual-Tone Multi-Frequency (DTMF) tone masking that enables customers to securely use their telephone keypad to make credit/debit card payments also prevents exposing this sensitive data to the organization's contact center or agents – no data ever enters or is stored in the company's systems, instead it is sent direct to the payment service provider (PSP) for processing.

Vendors such as Sycurio, who are the pioneers of DTMF tone masking and hold a patent for their secure payment method have a suite of powerful solutions that enable organizations to take secure and PCI DSS compliant payments while delivering a seamless experience for customers. Using Sycurio.Voice for securing payment transactions means that sensitive data completely bypasses the network, is not visible to agents, and cannot be breached.

Client perimeter defense

Even when minimizing the exposure of sensitive data to the home network, it is critically important to secure the permitted home working access to the corporate network and controls must be deployed to mitigate subversion of this legitimate access. Fortunately, solutions like Sycurio's Secure Browser provides an additional layer of application-level defenses.

Secure Browser holds all sensitive corporate data encrypted in memory as opposed to traditional browsers that do not encrypt such data in memory. Sensitive data is only decrypted when visualized.

To protect this decrypted data, Secure Browser also protects all frame images in such a way that any hacker in the network - or even on the endpoint itself - cannot extract visualized images nor dump and extract the contents of memory, as everything is encrypted.

Plus, solutions such as Secure Browser mitigate any risk of memory resident malware on the endpoint itself and also protect against the exfiltration of sensitive data via man-in-the-middle attacks (such as proxy or DNS), and screen-scraping etc.

Conclusion.

Home working is accelerating the need for Zero Trust security architectures and additional Zero Trust defenses will be required for the home network and devices. Any business looking to rapid adoption and commit to home working will need to embrace new Zero Trust techniques for securing the home environment of their remote workforces.

About the Author

Andrew Henwood is a 26-year veteran of the cyber security industry, with 17 of those years being focused on Payment Card Industry (PCI) security, compliance and digital forensics & incident response. In this time, Andrew has been involved in responding to many of the world's largest data breaches where he (and his teams) delivered triage, root cause analysis and communication of findings to regulatory authorities.

He has grown multiple businesses into global companies with 8-figure revenues. During his tenure as CEO, Andrew's last venture was awarded the Queen's Award for Enterprise (receiving this in person at Buckingham Palace), the highest award for UK business.

He is an entrepreneur, investor, frequent public speaker and pre-COVID traveled the world speaking at global conferences. He now enjoys doing similar activities, typically from the comforts of home in Cape Town.

Currently Andrew is the founder and director of several businesses, the primary focus being BlckRhino, a global strategic cyber security services and software solutions provider that cares.

Contact us for more information.

/ +1 888-267-5723

/ nasales@sycurio.com

/ sycurio.com

Sycurio.