THE USE OF VIRTUAL PRIVATE NETWORK IN THE CONTEXT OF "BRING YOUR OWN DEVICE" IN THE POST COVID-19 REMOTE WORKPLACE

Ali RAH

USA

ABSTRACT

Using a Virtual Private Network (VPN) for remote work provides an added layer of security by encrypting the internet connection. It helps protect sensitive data and prevents unauthorized access. With a VPN, employees can securely access company resources and files from anywhere in the world. This allows for greater flexibility in work arrangements and enables employees to collaborate seamlessly. Implementing a VPN as a remote workplace solution can lead to cost savings for businesses. It eliminates the need for physical office space and reduces expenses associated with commuting and travel.

While VPNs offer numerous benefits for remote work, it is crucial for organizations to implement proper security measures and educate employees on best practices to realize this technology's full potential. This article explores the change in the use of VPNs during and after the Covid-19 pandemic era. A short literature review precedes the opinion of the information security community about the usage and role of VPNs in efficiently securing information and information systems.

KEYWORDS

VPN, Remote Workplace, InfoSec, Information, Security

1. INTRODUCTION

In 2020, the global pandemic caused a significant shift from on-site to remote work, primarily from home, significantly changing many people's work dynamics without a clear boundary between home and work [1]. This sudden change, occurring over a brief period without warning, amplified security threats to all organizations' assets [2]. This new work environment is now a permanent fixture, as many organizations discovered that they could maintain productivity levels without the overhead of managing on-site personnel and the associated costs. Moreover, more than a third of surveyed employees preferred to continue working from home after the pandemic [3].

There are many lasting changes to expect in the workplace culture. The need to maintain business operations during the pandemic led to these changes and improved communication channels, such as video conferencing and virtual events [4]. Remote work has become the new standard, either entirely or in a hybrid form, with video calls supplanting traditional phone calls as the norm [5]. Employees' preference for remote work also stems from a desire to relocate from major cities to more affordable locations while preserving a similar income [6].

Before the pandemic, most organizations had their employees working on-site, with no more than 6% working remotely, part-time or full-time, or while traveling. However, during the pandemic,

DOI: 10.5121/ijcsitce.2024.11201

this percentage surged to over 70% [7]. Organizations' information systems were mainly accessed internally, except for traveling employees who used work devices with various protective measures to connect to the organization's information system. Following the sudden shift to remote work, organizations had to swiftly implement remote access, Identification, authentication, and authorization [8]. Employees primarily utilized their home internet connection, cellular data, and freely available Wi-Fi to connect to the organization's information system [9]. Organizations did not provide employees with dedicated work devices, resulting in using personal computers, phones, or other personal devices for work purposes [10]. Furthermore, employers did not provide employees with security training on remote work best practices and potential pitfalls [11]. To hastily secure remote access, organizations widely implemented Virtual Private Networks (VPN), leading to a 124% increase during the two weeks between March 8 and March 22, 2020 [12].

2. Literature Review

Information security involves evaluating organizations' assets, identifying vulnerabilities and threats, implementing controls, and reducing the attack surface [13]. Connecting to organizations' information systems using personal devices and public networks elevates security risks, including session hijacking, man-in-the-middle attacks, data interception, impersonation, and data breaches [14]. Using personal devices for work and personal activities without proper separation can create a pathway for unauthorized access to trusted networks from public networks, leading to similar security issues [15]. The lack of awareness and security training heightens the susceptibility of employees to falling prey to social engineering attacks, raising concerns about privacy and compliance with data protection regulations [16].

A survey by SANS revealed that 42% of the U.S. workforce works remotely, with 80% of company leaders planning to continue allowing remote work part-time and 47% planning to permit it full-time in the long run. Additionally, the survey found that 20% of businesses experienced security breaches due to remote work in the preceding year [17]. Security professionals have suggested various methods for securing remote work, including Secure Access Service Edge (SASE), Zero-Trust Network Architecture (ZTNA), Software-Defined Wide Area Networks (SD-WAN), and Software-Defined Perimeters (SDP). Prior to the pandemic, VPN usage was primarily limited to corporate computers accessing trusted networks while employees were traveling or for certain C-suite members. However, with the shift to remote work and the significant increase in Bring Your Own Device (BYOD) practices, many organizations hastily adopted VPN solutions to bolster security in the new remote work environment. While some providers offered turnkey VPN solutions, these options often proved costly. They did not necessarily align with the specific needs of organizations [18].

As remote and hybrid work became the norm due to the pandemic, the surge in BYOD practices brought VPNs into the spotlight, resulting in extensive coverage in articles, papers, vendor publications, and limited research studies. However, most of these sources either recommended using VPNs without delving into specifics regarding the type of VPNs to use or proper usage guidelines or cautioned against their use without thoroughly addressing the associated risks. Consequently, the prevailing trend leans towards recommending their usage.

Shortly after the World Health Organization declared COVID-19 a global pandemic, Haber [19] reported that countries were implementing stay-at-home measures to combat the virus. The author added that this shift to remote work clarified that corporate VPNs should not be installed on personal computers used in BYOD setups, as using a VPN on personal devices has never been a best practice. The exponential growth of BYOD introduces the risk of widespread malware infections, system corruption, and data breaches.

The author outlined numerous reasons why VPNs should not be used on personal devices, including users operating devices with administrative privileges, outdated, unsupported operating systems, lack of regular software updates, and the potential for multiple users within a household to compromise organizational information security. Moreover, the lack of authority to manage an individual's home computer, even with employee approval and legal protection, poses significant challenges in ensuring the security of the organization's network.

To mitigate these risks, the author recommended providing corporate devices to remote employees and implementing modern, well-architected remote access solutions that do not rely on complex environments or VPNs. These solutions could be based on cloud-based architecture, utilizing a web browser without the need for VPNs, dedicated applications, or tunneling.

Abhijith & Senthilvadivu [20] explained that VPNs leverage various technologies, including firewalls, authentication, Encryption, and tunneling, to secure connections to trusted networks. They emphasized that VPNs without firewalls are ineffective and expose organizations to cybersecurity risks.

The authors have outlined several VPN solutions offered by vendors, including traditional and cloud-based options, along with the features of each solution. They also noted that the onset of the pandemic caught many organizations off guard. Those who had never utilized VPNs in the past hastily adopted this solution, with some even resorting to free VPN versions. Meanwhile, organizations already using VPNs before the pandemic encountered challenges as their user base surged ten to twenty times. The overarching issue was that no one was fully prepared to navigate this new landscape. The primary hurdle for organizations during the pandemic was the need to scale up to accommodate the influx of VPN users rapidly. Nevertheless, the authors proposed that VPNs will become indispensable in the new era of remote work and are poised to regain momentum swiftly.

In a study conducted by Bansode & Girdhar [21], a qualitative research methodology using surveys was employed to identify the vulnerabilities of VPNs and propose mitigation policies. The research was prompted by the sharp increase in VPN usage during the COVID-19 pandemic, where internet traffic surged by up to 90%, with organizations relying heavily on VPNs for remote access to their intranet.

The researchers recognized the security challenges associated with VPN usage, noting that twenty-eight Common Vulnerabilities and Exposures (CVE) were added in the first eight months of 2020, with the majority related to hardware issues. The latest identified CVEs were associated with VPN hardware, software, configurations, and implementations. They emphasized the importance of security checks at every data processing stage. They suggested the hybrid version of VPN-Firewall as the Next-Gen Firewall. Additionally, they recommended various mitigation tools such as updating hardware firmware, security patches, and client software, implementing multi-factor authentication, Encryption, and monitoring while also advocating for using Machine Learning and Artificial Intelligence for handling incidents and mitigating Zero-day attacks in future studies.

Furthermore, Statista [12] reported a significant increase in VPN usage in countries affected by the coronavirus, reflecting the adoption of VPNs as the primary means of securing connections between organizations and remote employees. However, Venkat's article on Zscaler's [22] VPN

Report revealed that 97% of surveyed enterprises expressed concerns about the susceptibility of VPNs to cyberattacks. The report also highlighted the intention of 80% of companies to transition to a Zero-trust architecture to mitigate risks associated with VPN usage.

Even organizations with prior experience implementing BYOD policies, whether on-premises or remote, found themselves inundated by the exponential surge in devices accessing their networks via untrusted internet connections. For instance, using VPNs to secure devices accessing corporate networks garners significant professional consensus. However, opinions diverge when it comes to implementing a corporate VPN on a personal device, with some professionals staunchly opposed and others viewing it as the key to securing remote access for BYOD.

Several security measures, including strong passwords or passwordless solutions, multi-factor authentication, and VPNs, have been recommended by various sources [23]. Nevertheless, certain factors have raised concerns among professionals, such as home internet connections, shared usage of devices among family members, and using devices for purposes other than professional ones. These issues have transformed the devices into threat vectors for the organization's information systems.

3. Research Method

The research employed a quantitative approach, focusing on the security controls identified in the literature review, which included Identification and authentication, VPN, Antivirus and antimalware, Encryption, Updates and patches, and Device Management. Survey Monkey™ was utilized to enable IT professionals responsible for information system security to evaluate these controls. The objective was to affirm the significance of these security measures while eliminating any controls deemed non-crucial or less critical and incorporating any newly identified crucial security measures.

4. Results and Analysis

4.1. Mandatory Security Controls

The primary security controls frequently cited in the literature as integral to addressing security challenges are Updates and patches, MDM, Antivirus/Antimalware, Encryption, VPN, and Identification/Authentication.

A survey was done using SurveyMonkey in early 2023, targeting information security professionals and asking them about different means used to secure information systems, the ones actually used, and the ones they recommend for better protection. VPN was one of the primary means identified and confirmed as crucial for such security. Hereafter are some results of this survey.

The survey findings indicate that approximately 93% of respondents strongly agree, slightly agree, or agree that these security controls are essential for safeguarding BYOD, as shown in Figure 1.

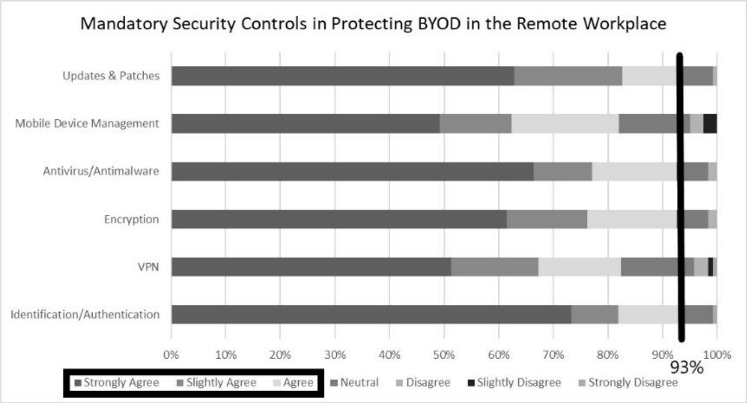

Figure 1 Security Controls Identified from the literature

Although two categories (MDM and VPN) exhibited a lower score, they still demonstrated over 80% agreement on the essentiality of implementing these security controls. To validate the organizations' practical usage of these security controls, respondents were individually queried about them.

4.2. Virtual Private Network (VPN)

The study findings revealed that 55% of organizations provided their remotely working employees with a corporate VPN. Despite the significance of this figure, it is essential to note that 15% of organizations do not utilize a VPN for their employees when accessing trusted networks. Additionally, 12% of respondents indicated using a free VPN, while another 18% reported using a paid VPN for remote work. This brings the total percentage of organizations where employees either use no VPN or a VPN unknown to the organization when connecting to the secure network to 45%, as depicted in Figure 2 and Table 1.

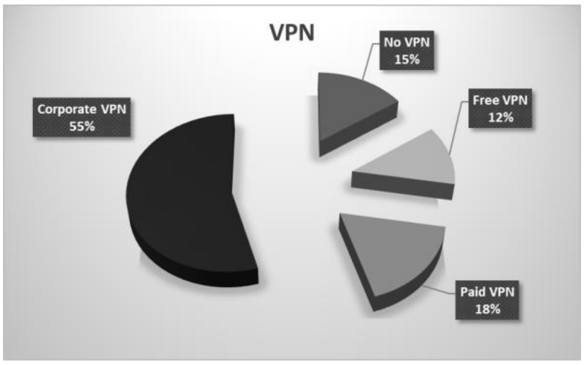

Figure 2 VPN Types Used by Organizations

Table 1 VPN Types Used by Organizations

VPN	Responses	
No VPN	15.38%	20
Free VPN	12.31%	16
Paid VPN	17.69%	23
Corporate VPN	54.62%	71

4.3. Minimum Acceptable Level of Protection for BYOD in the Remote Workplace

At the survey's conclusion, respondents were tasked with selecting security measures to guarantee a minimum acceptable level of security for BYOD usage by employees during remote work. The majority of the identified security measures from the literature, including Encryption (62%), Identification/Authentication (57%), virus/malware protection (57%), and VPN (52%), were prominently featured, as depicted in Figure 5.

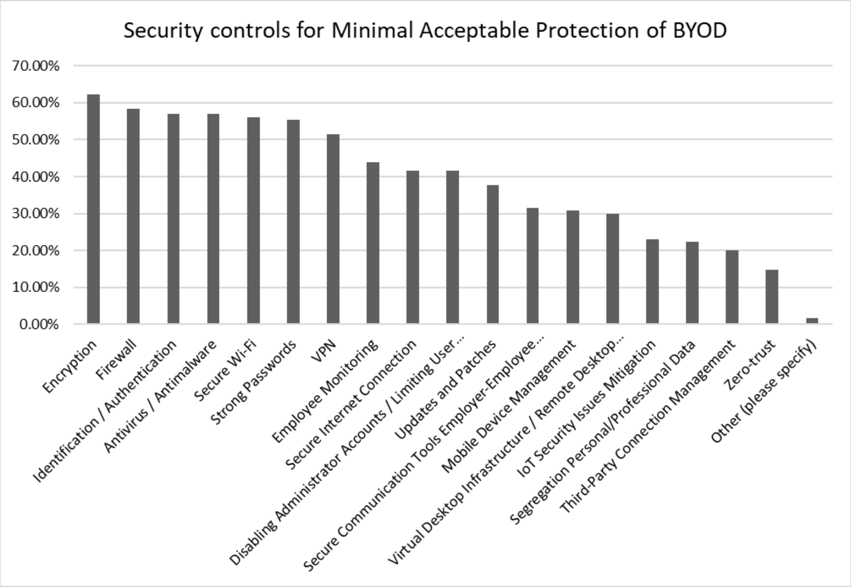

Figure 5 Minimum Acceptable Level of Protection for BYOD in the Remote Workplace

Note: This chart shows the security controls IT professionals consider for the minimum acceptable protection of BYOD. The security controls identified from the literature are all on the left side of the chart, along with Firewalls. MDM is left behind and shows on the right side. Zero-trust shows on the extreme right, confirming that these security controls are not currently used.

Specific security controls, such as MDM, received lower scores (31%), whereas others, like firewalls, garnered higher scores (58%). Additionally, some security controls, such as Zero-trust, received a lower importance score of less than 15%.

Concerning VPN suitability for organizations, 55% of respondents indicated that VPNs meet their security needs, mainly through corporate VPNs for devices used in the context of BYOD for remote employees. Moreover, approximately 18% of employees utilize paid VPNs to connect their devices in remote workplaces.

Several concerns highlighted in the participants' responses from the survey pertain to the lack of significant implementation of specific security controls by organizations. Additionally, some organizations utilize only parts of a security control rather than implementing it comprehensively. These concerns encompass:

- 17% of organizations do not utilize any encryption.
- 14% of organizations solely use passwords for their Identification and authentication process.
- 15% of organizations do not employ VPNs.
- 12% of respondents reported using a free VPN.

5. CONCLUSION

Even though some professionals are against the use of VPNs in securing information systems in the context of the post-pandemic remote workplace, VPNs remain one of the crucial means for the better protection of these systems. Information Security professionals should, however, enforce corporate VPN use in conjunction with better password policy, Encryption, improvement of Zero-Trust use, and better Mobile Device Management.

REFERENCES

[1] Varner, K., & Schmidt, K. (2022). Employment-at-Will in the United States and the Challenges of Remote Work in the Time of COVID-19. Laws, 11(2), 29. https://doi.org/10.3390/laws11020029

[2] Sheridan, K. (2020, March 11). COVID-19 Drives Rush to Remote Work. Is Your Security Team Ready? Retrieved from https://www.darkreading.com/operations/covid-19-drives-rush-to-remote-work-is-your-security-team-ready-

[3] Willis, A. (2021, August 17). Facing a Distributed Future: The Role of Remote Work Post-COVID. Retrieved from: https://blogs.blackberry.com/en/2021/08/facing-a-distributed-future-the-role-of-remote-work-post-covid

[4] ILR School. (2020, October 16). Enhancing Workplace Communication during the Pandemic and Beyond. Retrieved from_____https://www.ilr.cornell.edu/work-and-coronavirus/student-voices/enhancing-workplace-communication-during-pandemic-and-beyond

[5] Dave, A. (2021, April 20). Video calling needed more than a pandemic to finally take off. Will it last? Retrieved from_https://www.sciencenews.org/article/video-call-zoom-pandemic-popularity-phone-tech-history

[6] Stahl, A. (2021, February 1). 5 Lasting Changes to Expect in The Workplace Post-Covid. Retrieved from:_____https://www.forbes.com/sites/ashleystahl/2021/02/01/5-lasting-changes-to-expect-in-the-workplace-post-covid/?sh=13242f3c213d

[7] Horowitz, J. M., Minkin, R., & Parker, K. (2020, December 9). How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work. Retrieved from https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/

[8] Guidotti, A. (2020, April 17). Authentication and Identification, essentials for secure remote working. Retrieved from_https://www.vintegris.com/blog/authentication-identification-essentials-secure-remote-working-during-covid-19/

[9] Chen, B. X. (2020, March 18). The Tech Headaches of Working from Home and How to Remedy Them. The New York Times. Retrieved from https://www.nytimes.com/2020/03/18/technology/personaltech/working-from-home-problems-solutions.html

[10] Ready, F. (2020, July 15). Companies May Be Refreshing 'Bring Your Own Device' Policies During COVID-19. Retrieved from https://www.law.com/2020/07/15/companies-may-be-refreshing-bring-your-own-device-policies-during-covid-19/?slreturn=20220417203258

[11] Al-Habaibeh, A., Watkins, M., Waried, K., & Javareshk, M. B. (2021). Challenges and opportunities of remotely working from home during Covid-19 pandemic. Global Transitions, 3, 99-108.

[12] Statista. (2022, July 7). COVID-19 and VPN usage increase in selected countries as of March 2020. Retrieved from https://www.statista.com/statistics/1106137/vpn-usage-coronavirus/

[13] Computer Security Resource Center. (n.d.). Infosec - glossary. CSRC. Retrieved from https://csrc.nist.gov/glossary/term/INFOSEC

[14] Johnson, I. (2021, September 14). Top 8 cyber security risks of working from home. Retrieved from https://e2etechnologies.co.uk/blog/top-8-cyber-security-risks-of-working-from-home/#:~:text=Unfortunately%2C%20one%20of%20the%20most,their%20devices%20or%20company%20files.

[15] Miradore. (2021, October 28). Separating work and personal data on iPhones and iPads. Miradore. Retrieved from https://www.miradore.com/knowledge/ios/separating-work-and-personal-data-on-ios-devices/

[16] N-able. (2021). The Top 7 Risks of Bring Your Own Device (BYOD) MSPs Should Remember. Retrieved from https://www.n-able.com/blog/the-top-7-risks-of-bring-your-own-device-msps-should-remember

[17] SANS. (n.d.). Work from Home: Precautions, Risks, and Potential Outcomes. Retrieved from: https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit/

[18] Crossland, G., & Ertan, A. (2021). Remote Working and (In) Security. Retrieved from https://www.riscs.org.uk/wp-content/uploads/2021/07/RemoteWorking.pdf

[19] Haber, M. J. (2020, March 30). Is Your Workforce Going Remote? – Why VPNs and Personal Computers (BYOD) Should Never Mix. Retrieved from https://www.beyondtrust.com/blog/entry/is-your-workforce-going-remote-why-vpns-and-personal-computers-byod-should-never-mix

[20] Abhijith, M., & Senthilvadivu, K. (2020). Impact Of VPN Technology On IT Industry During Covid-19 Pandemic. In IJEAST. Retrieved from https://www.ijeast.com/papers/152-157,Tesma505,IJEAST.pdf

[21] Bansode, R., & Girdhar, A. (2021). Common Vulnerabilities Exposed in VPN–A Survey. In Journal of Physics: Conference Series (Vol. 1714, No. 1, p. 012045). IOP Publishing. Retrieved from https://iopscience.iop.org/article/10.1088/1742-6596/1714/1/012045/pdf

[22] Venkat, A. (2022, September 26). 97% of enterprises say VPNs are prone to cyberattacks: Study. Retrieved from https://www.csoonline.com/article/3674793/97-of-enterprises-say-vpns-are-prone-to-cyberattacks-study.html

[23] Wilkinson, J. (n.d.). COVID Access: The Importance of Multi-factor Authentication During Remote Learning. Retrieved from https://www.skyward.com/discover/insider/november-2020/covid-access-the-importance-of-multifactor-authent

AUTHOR

Dr. Ali Rah has over 30 years of experience in different fields related to security (Physical, Building, Staff, Electronic, Information, Access control, Law enforcement, Legal policies, …). He holds a Master in Cybersecurity and a Doctorate in Information Assurance. He also holds different security certifications including CISSP, CompTia Security +, and AWS Cloud Foundations.