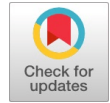


Enhancing Cybersecurity for Remote Work: Identifying the Gaps and Design Considerations for A Robust Security Tool

Om Madat, Mayank Poriya, Srivaramangai R



Abstract: Traditional office-based security systems cannot cope with the increased cybersecurity threats that have resulted from the change to remote work. The paper discusses the most prevalent security vulnerabilities in remote working, focusing on data security and protection. This by its nature exposes businesses to risks through vulnerable home networks, personal devices from different setups, and behavior from other users, including advanced persistent attacks, access without authorization, and data breaches. The research highlights the weaknesses of the existing security procedures being put in place such as the detection and prevention capabilities, plans for endpoint security, and data protection processes. The recommendations will highlight the need for an all-inclusive tool in the remote working environment. This solution brings together strong user access control, real-time threat detection and response mechanisms, along with advanced cryptography approaches. The proposed approach is also a user-centered design that can be easily adapted to different technical contexts and organizational structures. The study is based on a multilayered methodology that includes case studies of previous cybersecurity issues associated with remote working, literature-based analysis of the security framework, and iterative design techniques. Important conclusions emphasize the need for adaptable security solutions that can adapt to not only the current threats but also to the mounting demands of preventing new threats in the context of remote work. The improvement that this study brings into the information security and protection domains through practical suggestions and an applied strategy for organizational resilience provides a basis to maintain confidentiality and improve endpoint security for a more secure and long-lasting environment for the remote worker.

Keywords: Network Security, Cryptographic Solutions, Threat Detection, Access Control, Incident Response Framework, Data Security and Protection, Endpoint Protection Strategies, Cybersecurity for Remote Work, Adaptive Security Solutions, and Cyber Risk Management.

Abbreviations:

MDMS: Mobile Device Management Solutions
APT: Advanced Persistent Threats
IIoT: Industrial Internet of Things

Manuscript received on 07 December 2024 | First Revised Manuscript received on 15 December 2024 | Second Revised Manuscript received on 19 March 2025 | Manuscript Accepted on 15 April 2025 | Manuscript published on 30 April 2025.

*Correspondence Author(s)

Om Madat, Department of Information Technology, University of Mumbai, Mumbai (M. H.), India. Email: ommadat2002@gmail.com.

Mayank Poriya, Department of Information Technology, University of Mumbai, Mumbai (M. H.), India. Email: mayankporiya27@gmail.com.

Srivaramangai R*, Head, Department of Information Technology, University of Mumbai, Mumbai (M. H.), India. Email: rsrimangai@gmail.com, ORCID ID: [0000-0003-2723-6067](https://orcid.org/0000-0003-2723-6067).

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

I. INTRODUCTION

The practice of staff working from home or other locations other than a traditional office is very common nowadays. As much as this flexibility brings many advantages, new security challenges open up that companies should address. This is different from office environments where security measures could be tightly controlled; remote work in ensuring security presents different risks since employees use different devices and networks, normally from home environments that are not as secure. Allowing employees to work from home means they connect to the company's systems from other places, which might be their homes or another public place, using personal devices such as laptops or smartphones. A device or a network like this may not have similar security to that in an office. These come with several possible open gaps in security, including data breaches, unauthorized access, and exposure to different types of cyberattacks. These new kinds of threats are not easily handled by traditional security tools and practices built for an office environment. The solution to these issues involves developing a security tool specifically for the remote work environment. This would need a tool that can handle challenges that are peculiar to remote working, such as data security across multiple devices and location-specific access. This research paper, therefore, explains these security gaps and design considerations to enable the development of an integrated security tool to guard the remote work environments efficiently. This paper will label the risks and propose solutions against them and help the organizations take necessary precautions to better secure the remote settings where their crucial information is processed.

II. LITERATURE REVIEW

The network environment of the organization has been hugely transformative because most of its vulnerabilities and threats have surfaced due to a shift to remote working. This change in security is clearly articulated in the literature concerning the technology-related and human-centric challenges posed by safeguarding corporate networks and individual devices. According to Solanki et al. [1], remote working environments have increased corporate network vulnerability, personal devices, as well as communication systems. According to them, the traditional defense mechanism solutions are no longer viable enough to fight the new attacks by ransomware and botnets that have hitherto used VPN for accessing a remote network. Mandadi stresses Croatia's un-proactive position before increased cyber threats posed during the



Enhancing Cybersecurity for Remote Work: Identifying the Gaps and Design Considerations for A Robust Security Tool

COVID-19 pandemic [2]. According to the author, no warnings or guidelines for cyber-security were released by the government with the swift transition into remote work by businesses, leaving the latter on its own to take measures to counter such risks. Ogungbemi et al [3]. developed the CAT framework for assessing and developing employee cybersecurity skills, especially for home workers. The authors believed that the structured three-level framework - beginner, medium, and advanced - reduces increased risk from remote work. Alromaih et al [4]. concluded information security awareness gained at work translates into the home environment. The study provides an avenue to expand organizational security programs to the home setting and create a total security culture. Kim et al [5]. suggest that 95% of the people in their study believe there is a need for sophisticated security systems within homes, a need for intelligent security systems primarily for working parents who are concerned with child supervision. Gannon et al [6]. analyze the risks of BYOD to remote work; they suggest robust policies and Mobile Device Management Solutions (MDMS) for the security of organizational data. They believe that if BYOD is not well-managed, it poses significant security risks. Kılıç et al [7]. discovered a great demand for increased awareness about security and privacy risks related to BYOD on higher education campuses in Malaysia. Even though BYOD is increasingly becoming prevalent, students are not enlightened enough about the risks associated with it. Olawale et al [8]. discuss the kinds of attacks on BYOD which have been developed, Advanced Persistent Threats, (APT), and malware in particular. They then advance solutions tailored for the X.800 security architecture to mitigate these threats. Rakha et al [9]. gave recommendations for adaptive security strategies applicable to the remote work environment. They emphasize having strong authentication and encryption as well as conducting periodic vulnerability assessments. Anil et al [10]. were discussing the successful implementation of an Endpoint Security System at CWPRS, Pune. Critical scientific data and devices involved there were protected from external threats. They advise endpoint security as one of the required defense mechanisms. Singh et al [11]. identify a mechanism to bind endpoint validation for the server with remote at-testation using TCG quoting, eliminating relay attacks by using platform-dependent endpoint certificates. The scalability of endpoint security in remote environments is enhanced, as well. Andras et al [12]. obviate VPN-based security limitations for remote access. They develop a secure scheme of remote access that reduces such vulnerabilities. Hijji and Alam believe that endpoint security systems will be taken to a higher level if advanced technologies such as machine learning are implanted into them [13]. For instance, they suggested multi-layered security against ransomware and botnets especially when one is focusing on remote workers. Specific security requirements for Zero Trust-based cloud services by Posa et al [14]. will have to be studied in great detail against commercial cloud platforms, which would be constantly up-to-date and encrypted. Hammi et al [15]. discuss security behaviors at work by considering informal communication and experience design to ensure the security of the team. Han et al. present a new multi-user and multi-configuration endpoint for Globus Compute, thus enhancing security and management for shared high-performance computing clusters in remote work environments. Smith et al. developed a parallel

version of ClamAV using OpenMP that reduced the malware detection time by 62%. They have emphasized the need for efficient antivirus solutions to cope with the increasing complexity of malware in remote environments. Brenna et al [16]. in their work focused on setting up a zero-trust security mechanism for remote work environment. They have discussed the current vulnerabilities which are faced in remote work places and have recommended few steps like strong authentication, endpoint security, and cloud-based solutions. The study also emphasizes on encryption and multi-factor authentication as a preventive measure of threats. Rządowska et al [17]. in his research has actually shown the practical implementation of zero-trust frameworks as suggested in the previous work. In his study, he analyzes the current case studies and suggest the best practices to be followed while setting up the infrastructure for remote work. Bispham et al [18]. demonstrated that the unified communication tools, such as Microsoft Teams, make the physically deficiently separated from virtual workspaces, increase productivity, and reduce e-mail, and in-person meetings dependency. Battisti et al [19]. identified major challenges that IT professionals encounter while working remotely. The two primary challenges highlighted include cybersecurity risk and team cohesion. They emphasize the aspects of trust, effective communication, and robust cyber security policies. Employee self-efficacy and compliance intentions are lower with remote employees than with their in-office counterparts, conclude Wu et al. [20]. More situational support and cybersecurity training for remote workers would be in order, the authors recommend. Georgiadou et al [21]. emphasize the need for better solutions in PKI to meet the steep rise in demand for working from home in the wake of the COVID-19 pandemic. They stress the adoption of ownership of PKI by organizations and rigorous training of employees to secure remote networks. Ilag et al [22]. do a careful review of smart home security along with vulnerabilities and proposed countermeasures. These authors emphasize safe access controls along with encryption as countermeasures against the risks identified. Grim et al [23]. introduced an educational virtual cybersecurity lab, that was pretty appealing to the students, and it presented high satisfaction and high effectiveness for improving cybersecurity skills. Bodsberg et al [24]. provide a discussion regarding the addition of new vulnerabilities and risks that the remote operation introduces for oil and gas installations, including difficulties in crisis management from a distance and situational awareness. The paper emphasizes the need for effective collaboration between the operators and suppliers to mitigate risk in such settings. According to Li et al [25]., Identity and Access Management plays a paramount role in protecting sensitive data as well as systems in an organization. The paper emphasizes automating access permissions, capturing user identities, and controlling permissions to boost data security in the remote working environment. Rosu et al [26]. believe that smart home security system design gives minimal consideration to user experience on the aspects of privacy and security features. The authors lay a charge on an improvement in the collaboration between security experts and designers as an avenue to meet these challenges. Pohl et al [27]. posit that information



security behaviors at home differ from those found in organizational settings as they have different contextual factors unique to the particular setting. They outline a research agenda that explores such behavioral differences for making security strategies better for home users who often perform their work in less controllable environments.

Sabin et al [28]. suggest a VPN-based network architecture solution for geographically dispersed enterprises. The authors provide guidelines on the configuration of open-source software, Nagios, which should be used by an enterprise network to monitor it generally but now including virtual development projects. Atstāja et al [29]. assess the performance of VPNs during the COVID-19 pandemic and discuss that VPNs made flexible working from remote locations possible. The study shows how IT companies scaled VPN infrastructure for an increase in the number of remote users while simultaneously maintaining business continuity and security. Malecki et al [30]. have compared the performance of OpenVPN and IPsec in Industrial Internet of Things (IIoT) scenarios. The results showed that IPsec has higher throughput and efficiency in key exchange as compared to openVPN, which makes it a perfect fit for scalable architectures of IIoT remote access. Buldakova et al [31]. is a comprehensive review of popular forms of cybersecurity threats in remote work settings. In this paper, details of the analysis of phishing attack awareness and security guidelines reveal that there are tremendous discrepancies in terms of user awareness about phishing via URLs as compared to email scams. Johnston et al [32]. explore how individual remote workers develop coping strategies for dealing with challenges posed by working remotely. The authors envision the necessity of developing an environment of visibility management, social support infrastructures, and adaptations in work rhythms to reduce the isolation and other time zone drawbacks that telecommuters face. Gomez et al [33]. do a review of the literature on the psychosomatic and cognitive effects of telework. Furthermore, this research gives evidence that though the majority of studies emphasize the social and professional consequences of telecommuting, one should conduct more research on the cognitive and health impacts as well concerning long-term remote operations. Chalhoub et al [34]. introduce TFHEs - A library that uses the combination of Fully Homomorphic Encryption and Intel SGX to extend security for remote computing. The study demonstrates that this hybrid encryption model is practical and improves performance, with stronger security guarantees than either FHE or SGX would supply on its own. Goldman et al [35]. argue for creating a cybersecurity-aware organizational culture as a means of safeguarding data in remote workspaces. The authors believe that all this needs to happen at the organizational level to cultivate such an attitude toward secure employee behavior. Škiljić et al [36]. refer to the new cybersecurity threat produced by an abrupt shift in the work environment due to COVID-19. According to the authors, on top of the strategies companies must utilize to minimize such risks include multi-factor authentication, VPNs, and updates. Organizational Security Challenges Facing Organizations During the Transition Period to Remote Work: Can They Be Addressed? Talib et al [37]. provide an analysis of security challenges that organizations faced during the pandemic when transitioning to a remote work environment. The paper emphasizes the necessity of enhancing PKI solutions and employee training as the backbone that helps

preserve network integrity in remote work environments. Chitnis et al [38]. discuss organizational security readiness in light of the COVID-19 situation, which caused remote work to become necessary. Pointing out that most of the employees were not given security guidelines while working, and a majority of the employees use personal devices with minimal strict security policies. Singh et al [39]. highlight the various risks of cyberattacks in the pandemic era and advise firms to take necessary steps to safeguard their data and networks. The primary suggestions include proper backup and recovery plans, employee education, and protocols in response to cyberattacks. Aguboshim et al [40]. talk about the long-term consequences of working from home and the cybersecurity issues experienced during the period of the pandemic. The paper concludes with a future research agenda in terms of further empirical studies to determine how workforce behaviors and digital skills influence cybersecurity risks. In the empirical study by Singh et al [41]., the authors found that firms that had implemented work-from-home policies before the COVID-19 pandemic experienced a higher number of cyber events. Over the course of the pandemic, however, this relationship greatly diminished because the diffusion of work-from-home policies and an organization-wide spread of cybersecurity awareness might have acted as a form of natural immunity that reduced their negative impact. Forain et al [42]. identify the positive and negative implications of teleworking as given by the COVID-19 period. This paper focuses on the occupational health service providers who take roles to enable employees to ensure their health is well protected in a teleworking work situation. Chalhoub et al [43]. conclude that the effects of the COVID-19 pandemic shoot up the cybersecurity risks that accompany changes in work habits and skills in digital. The authors bring out employer-led risk management practices brought about in response to the particular needs of each kind of industry. Patrick et al., [44] examine the economic-financial effects of working remotely. They point out that the use of high technology and increased utilities have made workers compromise. Psychological factors, including job satisfaction and technostress, made the workers want to continue working from home. Charalampous et al. [45] pointed out that remote work increases vulnerabilities of the environment to phishing attacks and data breaches [46]. The paper holds it necessary for better security of cybersecurity in the context of work from anywhere with an alert workforce, proper training programs, and advanced technologies [47]. This study not only highlights the demand for achieving a balance between a secure digital environment and the demand for flexibility and productivity within an emerging paradigm of remote work [48]. There should be proper comments of the reviewers for acceptance/ rejection. There should be a minimum 01-to-02-week time window for it.

III. SECURITY GAPS IN REMOTE WORK ENVIRONMENTS

As working from home emerged as the mainstream operation model globally, it has also opened up several operational and security gaps that threaten sensitive data security and employee



Enhancing Cybersecurity for Remote Work: Identifying the Gaps and Design Considerations for A Robust Security Tool

productivity. Therefore, this section presents a few key security gaps witnessed in work-from-home settings and identifies specific threats regarding weak authentication methods, unsecured home networks, insider threats, phishing, and poor data encryption and backup strategies. Additional discussion will also be done on how these vulnerabilities might affect company data and productivity.

A. Weak Authentication Methods

The work-from-home settings make a remote environment highly vulnerable to weak authentication practices, mostly supported by passwords that become targets for brute force and account takeover. This might lead to employees using weak and easily guessed passwords. In the absence of robust password policies and MFA/biometric authentication, companies remain in a jeopardy position for credential theft, unauthorized access, and ultimately account takeovers. Stolen credentials may allow an attacker to steal sensitive information and perform further attacks. Employees face frequent disruptions, including password resets and account lockouts, that lower productivity and raise frustration.

B. Insecure Home Networks

Most working-from-home scenarios of employee-employer engagements are based on employees connecting via unsecured home networks that lack some of the sophisticated security features found on corporate systems. Generally, such networks are the playing grounds for cybercriminals since they are supposedly protected by very poor router passwords, probably with outdated firmware. They are also used simultaneously by a large number of users, further complicating the possibility of malware infection. Unsecured networks risk man-in-the-middle attacks or network breaches, thus exposing sensitive corporate data, leading to data breaches, regulatory fines, and erosion of confidence. Employees are victims of network-based attacks that reduce Internet performance, disrupt resource access, and require IT intervention at the cost of efficiency.

C. Insider Threats from Personal Devices

Personal devices, increasingly used due to remote work, have turned out to be a very serious security concern. The corporate data can be accessed by employees without proper security controls, making them an easy target for an attacker. Accidental or intentional insider threats result in a data breach, intellectual property theft, and financial loss. The risks are more difficult to manage in a remote environment regarding personal device monitoring and control. The resultant security incidents take away IT remediation; which means a lack of productivity and longer response times. Therefore, strict security measures become paramount in remote working environments.

D. Phishing and Social Engineering Attacks

Remote work observes an uptick in phishing and social engineering attacks because employees tend to show less skepticism toward suspicious messages from colleagues or supervisors. Such isolation is then taken advantage of through well-structured emails, SMSs, or voice calls, where employees are tricked into sharing sensitive information or malicious file access. The aftermath of phishing attacks includes stolen credentials, penetration into unauthorized systems, and malware/ransomware attacks. Furthermore, phishing leads to a

chain reaction wherein more employees or systems become vulnerable to another attack, leading to a loss of productivity.

E. Poor Data Encryption and Backup Strategy

The remote work environment mostly comprises poor encryption of data and backup strategy for the same, thus sensitive data are prone to interception. Workers working from their devices are not compliant with encryption regarding the files stored on the local device, hence more cases of data theft. Similarly, there is a lack of consistent backup solutions to increase the risk of data loss due to hardware failure, ransomware, or just simple accidental deletion. Without proper backups, critical data recovery may cause more time for operational impacts in these organizations. Non-availability of encryption and backup strategies results in legal liabilities, compliance violations, and damage to the reputation of the organizations, while employees suffer from substantial losses of productivity due to data loss with significant downtime and loss of deadlines.

F. Impact of Security Gaps on Company Data and Employee Productivity

The security gaps in the remote work environment are substantially affecting the organizational data integrity and the productivity of the employees. Weak authentication, unsecured networks, and insider threats increase the risk of unauthorized access and data breaches, which always result in financial losses and regulatory penalties, damaging one's reputation. The list is enhanced by phishing attacks and poor encryption. All these force employees to waste their precious time resolving security problems rather than working on the core tasks, which consequently results in constant workflow interruptions. Data loss in case of either poor backup or a breach-causes project delays, reduces individual productivity and increases missed deadlines. It therefore means that addressing these gaps in security protects the data of the company, continuity of operations, and employee productivity.

IV. DESIGN CONSIDERATIONS FOR A COMPREHENSIVE SECURITY TOOL

For the enterprise remote work solution deployment in a secure way requires painstaking planning of various security features. The following considerations are among the very important design considerations that provide a robust and secure system for employees and organizational data.

A. Secure Network Infrastructure and Connectivity

The most critical issues about data security relate to intercepting information and unauthorized access. Some of the key components comprise a secure network infrastructure:

VPN: It will provide a channel of encryption in the communication between the remote workers and the organizational network so that data will not be intercepted by other people.

B. Firewalls and Intrusion Detection/Prevention Systems

Firewalls and intrusion detection/prevention systems filter and monitor network traffic. Intrusion detection and prevention systems



provide added security by the detection of suspect behavior, which is then stopped before it becomes a threat to the network.

Segmentation: Segmentation of sensitive areas of the network into differentiated zones limits the amount of exposure during a breach and does not let an attacker move laterally within the system with so much ease.

Reliability in Connectivity: The employees are guaranteed reliable and secure access to the internet. Limiting the risks from non-secured networks can be done through the provision of guidelines on how to set up secured home networks using protocols for encryption, such as WPA2 or WPA3.

C. Secure Access and Authentication to Employees

In other words, with the gained secured access to corporate systems from remote employees, unauthorized access to data or data breaches can be avoided.

Strong Password Policy: Complex password policies must be in place, which would enforce strong, unique passwords; frequent updates thereof; and prohibition of password reuse. Such policies must be supported with enabling tools such as password managers for easy compliance by employees.

MFA: MFA stands for Multi-factor Authentication. This means that there is an added layer of verification, something like one-time code verification or biometric scanning, which enhances the security manifold times since attempts by unauthorized users are hard and hence less likely to happen even in those cases where the password may be compromised.

RBAC: This should be role-based; for example, the employee needs to have minimum access depending on his requirement for work speedily and effectively. This will reduce the impact when any account gets compromised.

Encryption of Remote Desktop Protocols: The encryption of remote desktop protocols like RDP or VNC can make the data secure while transmitting it from a remote device to a corporate server. Mobile Device Management solutions have gained immense importance due to the rapid proliferation in the number of mobile devices employees are using for working remotely. These will facilitate your organization in enforcing its security policies regarding devices and ensure monitoring and remote wiping of sensitive data in case of loss/stolen of a mobile device.

D. Encryption and Data Loss Prevention Strategies

Data protection becomes a highly critical concern within the setting of remote work, especially when it has to be transferred across probably insecure networks.

Encryption of Data: Data encryption both at rest and in transit ensures that even in case such sensitive information gets intercepted, its contents can't be readable. Uniform end-to-end encryption should be applied in communication channels and file transfers.

Secure File Sharing: With secure file-sharing tools, encryption, and access controls, such as password protection and file expiration, ensure that files are shared only with authorized personnel.

Data Loss Prevention-DLP: The DLP tools monitor the flow of sensitive data. Besides that, they block unauthorized sharing or storage. Such software helps an organization avoid any accidental or intentional leakage of data and maintain its integrity.

Perform regular backups that can reduce the chances of losing critical data. Testing regular backup processes helps to ensure the recoverability of data in cases of system crashes or being attacked via cyber-attacks.

The policies regarding data privacy of employees should, therefore, be developed, and adherence to relevant data protection laws, such as General Data Protection Regulations and the California Consumer Privacy Act, will help build confidence and avoid litigations.

Cloud Security: An organization that leverages the cloud should collaborate with service providers that offer comprehensive encryption, access control, and segregation of data. Frequent audits and periodic security reviews are performed of the cloud environments to make sure that the cloud service providers are maintaining high standards of security.

E. Device and Remote Access Point Hardening

The most vulnerable points in a remote working environment constitute the endpoints, personal devices, and home networks. Effective endpoint security strategies become a must.

Endpoint Protection Software: Antivirus, anti-malware, and firewall software are to be installed on the remote devices to keep them safe from any kind of cyber-attack. Most importantly, it is very important to enable auto-update features so that all the recent security patches will apply themselves.

Patch Management: You significantly reduce the likelihood of exploitation of any known vulnerabilities by regularly patching operating systems and applications. You can use a patch management system to push regular updates to all remote devices.

Wi-Fi Connections: Workers shall connect to the available Wi-Fi in a secure and encrypted way, preferably using WPA2/WPA3. Networks that are public or open should not be used because they are susceptible to certain types of attacks.

Mobile Device Security: Mobile devices are some of the most accessible devices to work remotely, and these have to be set up with strong passcodes or biometric authentication. Moreover, there must be the ability to allow remote wipes of stored information or encryption.

Remote Access Policies: To begin with, employees working from home should have policies regarding the use of devices and remote access, along with good security behavior. Updates and reminders will need to be regularly passed on.

F. Raising Cybersecurity Awareness Among Employees

This is an important area in which, for a winning security strategy, employees should be abreast of best practices concerning cybersecurity. Awareness and training have prominent roles to play in ensuring a security-savvy remote workforce.

Cybersecurity Awareness Programs: Such robust training in security-related remote work, phishing awareness, and social engineering prevention makes them more aware of the risks to which they are vulnerable.

Regular Training Sessions: Updating the employees periodically about recent threats and security best practices will make them

Enhancing Cybersecurity for Remote Work: Identifying the Gaps and Design Considerations for A Robust Security Tool

more vigilant in handling any potential security incident.

Simulated Phishing Exercises: Frequent phishing simulation exercises are good to run to test employee awareness of recognizing malicious communications. Feedback will reinforce good habits.

Security Policy and Guidelines: The policies and guidelines related to security while working remotely are communicated to help employees understand how they can play a role in maintaining security.

Continuous Reminders through Communications: Emails and newsletters reinforce "key" practices, making the employee remember that security matters.

Co-operation with IT Support: Creating a line of communication with IT teams aids in quicker reporting by employees of potential issues; this helps employees walk through security measures.

Recognition/Incentives: Being able to recognize those employees who are showing exemplary behavior in cyber-security within their daily responsibilities might inspire others to do just as well.

These design considerations, once integrated into the security tool, will help an organization progress toward a wholesome and effective solution to secure its remote work environment. This minimizes risks in virtual access while keeping sensitive data safe, building up a security-conscious corporate culture in the process, and damaging to reputation of the organizations, while employees suffer from substantial losses of productivity due to data loss with significant downtime and loss of deadlines.

V. CONCLUSION

This study found several security gaps around which interventions in remote work environments should be crafted: weak authentication, unsecured home network, insider threats, phishing, and social engineering attacks, and poor data encryption and backup. These are proposed to be the causes of major breaches in sensitive company data and the cramping of employee productivity. The security tool will provide a solution to these gaps with features such as real-time network monitoring, strong authentications, device security scans, and threat detections. Additionally, the tool would implement user-friendly training modules and offer actionable remediation suggestions for an organization to reduce its risks and work on enhancing its security posture in a remote environment. Such security tools need to be updated and refined throughout because the threats are continually changing the way they act. It must integrate machine learning and AI-driven threat detection, automatically update, and integrate well with cloud services to remain current and functional. Future research efforts should focus on the most recent technologies in the domain of advanced threat detection, the investigation of truly secure collaboration tools, and the newly opened vulnerabilities in remote work infrastructure. Security tools require sustained improvement and innovation at a higher pace to keep up with the changing landscape of cyber threats.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.

- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it has been conducted without any external sway.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Pratap Singh Solanki, Ajay Singh, Shaneel Sao, N.D. Atkekar "Protection of Research Data and Devices from Malware Attacks Using Endpoint Security System in Network." International Journal of Scientific Research in Network Security and Communication 12.3 (2024): 15-18., DOI: <https://doi.org/10.26438/ijnsrsc>
2. S. Mandadi, S. P. Gochhayat, V. Torremocha, and J. Kethar, "Cybersecurity risks in remote work and learning environments and methods of combating them," J. Student Res., vol. 13, no. 2, 2024, DOI: <https://doi.org/10.47611/jsrshs.v13i2.6808>
3. O. S. Ogungbemi, F. A. Ezeugwa, O. O. Olaniyi, O. I. Akinola, and O. B. Oladoyinbo, "Overcoming remote workforce cyber threats: A comprehensive ransomware and botnet defense strategy utilizing VPN networks," J. Eng. Res. Rep., vol. 26, no. 8, 2024., DOI: <https://doi.org/10.9734/jerr/2024/v26i81237>.
4. Alromaih, Sarah, Ivan Flechais, and George Chalhoub. "Beyond the Office Walls: Understanding Security and Shadow Security Behaviours in a Remote Work Context." In Twentieth Symposium on Usable Privacy and Security (SOUPS 2024), pp. 507-525. 2024., DOI: <https://www.usenix.org/system/files/soups2024-alromaih.pdf>.
5. H. Kim, Y. Kim, and S. Kim, "A study on the security requirements analysis to build a zero trust-based remote work environment," 2024, DOI: <https://doi.org/10.48550/arXiv.2401.03675>.
6. Gannon, D., Bramley, R., Fox, G. et al. Programming the Grid: Distributed Software Components, P2P, and Grid Web Services for Scientific Applications. Cluster Computing 5, 325–336 (2002). DOI: <https://doi.org/10.1023/A:1015633507128>.
7. C. Kılıç, İ. B. Uzun, A. T. Ardoğan, W. Saleem, and A. Sezen, "Security Issues of Remote Work Environments and Alternative Solution Approaches", IJMSIT, vol. 8, no. 1, pp. 46–51, 2024., <https://dergipark.org.tr/en/pub/ijmsit/issue/85925/1509706>.
8. Olawale, Olufunke, Funmilayo Aribidesi Ajayi, Chioma Ann Udeh, and Opeyemi Abayomi Odejide. "Risk management and HR practices in supply chains: Preparing for the Future." Magna Scientia Advanced Research and Reviews 10, no. 02 (2024): 238-255., DOI: <https://doi.org/10.30574/msarr.2024.10.2.0065>.
9. N. A. Rakha, "Ensuring cyber-security in the remote workforce: Legal implications and international best practices," Int. J. Law Policy, vol. 1, no. 3, 2023., DOI: <https://doi.org/10.59022/ijlp.43>
10. A. K. Anil, S. A. I. Parambil, and T. N. Santhosh, "Ensuring robust security in remote work environments: Addressing challenges and implementing strategic solutions," ResearchGate, 2023, DOI: [10.13140/RG.2.2.13692.51847](https://doi.org/10.13140/RG.2.2.13692.51847).
11. Singh, Chetanpal, Rahul Thakkar, and Jatinder Warraich. "IAM identity Access Management—importance in maintaining security systems within organizations." European Journal of Engineering and Technology Research 8, no. 4 (2023): 30-38, DOI: <https://doi.org/10.24018/ejeng.2023.8.4.3074>.
12. P. Andras et al., "Trusting Intelligent Machines: Deepening Trust Within Socio-Technical Systems," in IEEE Technology and Society Magazine, vol. 37, no. 4, pp. 76-83, Dec. 2018., DOI: <https://doi.org/10.1109/MTS.2018.2876107>.
13. M. Hijji and G. Alam, "Cybersecurity awareness and training (CAT) framework for remote working employees," Multidiscip. Digit. Publ. Inst., 2022., DOI: <https://doi.org/10.3390/s22228663>.
14. Pósa, Tibor, and Jens Grossklags. 2022. "Work Experience as a Factor in Cyber-Security Risk Awareness: A Survey Study with University Students" Journal of



- Cybersecurity and Privacy 2, no. 3: 490-515. DOI: <https://doi.org/10.3390/jcp2030025>.
15. Badis Hammi, Sherali Zeadally, Rida Khatoun, Jamel Nebhen, "Survey on smart homes: Vulnerabilities, risks, and countermeasures", Computers & Security, Volume 117, 2022, 102677, ISSN 0167-4048, DOI: <https://doi.org/10.1016/j.cose.2022.102677>.
 16. Lars Brenna, Isak Sunde Singh, Håvard Dagenborg Johansen, Dag Johansen, "TFHE-rs: A library for safe and secure remote computing using fully homomorphic encryption and trusted execution environments", Array, Volume 13, 2022, 100118, ISSN 2590-0056, DOI: <https://doi.org/10.1016/j.array.2021.100118>.
 17. Sidor-Rzadkowska, Małgorzata. "Human-the weakest or the strongest link? The role of organizational culture in ensuring security of remote work." Journal of Modern Science 49, no. 2 (2022): 608-620., DOI: <https://doi.org/10.13166/jms/156776>.
 18. Bispham, Mary and Creese, Sadie and Dutton, William H. and Esteve-González, Patricia and Goldsmith, Michael, "Cybersecurity in Working from Home: An Exploratory Study", TPRC49: The 49th Research Conference on Communication, Information and Internet Policy, August 1, 2021, DOI: <http://dx.doi.org/10.2139/ssrn.3897380>.
 19. Enrico Battisti, Simona Alfiero, Erasmia Leonidou, "Remote working and digital transformation during the COVID-19 pandemic: Economic-financial impacts and psychological drivers for employees", Journal of Business Research, Volume 150, 2022, Pages 38-50, ISSN 0148-2963, DOI: <https://doi.org/10.1016/j.jbusres.2022.06.010>.
 20. Wu, Qingman and Yoon, Kyunghye and No, Won Gyun, "The Effect of Remote Workforce on Firms' Cybersecurity Risk Disclosures and Incidents" July 15, 2022, SSRN, DOI: <http://dx.doi.org/10.2139/ssrn.4342761>.
 21. Georgiadou, A., Mouzakitis, S. & Askounis, D. "Working from home during COVID-19 crisis: a cyber security culture assessment survey", Secur J 35, 486-505 (2022). DOI: <https://doi.org/10.1057/s41284-021-00286-2>.
 22. Ilag, Balu N. "Tools and technology for effective remote work." International Journal of Computer Applications 174, no. 21 (2021): 13-16., DOI: <https://doi.org/10.5120/ijca2021921109>.
 23. Grimm, R., Bershad, B.N. (1999). "Providing Policy-Neutral and Transparent Access Control in Extensible Systems". In: Vitek, J., Jensen, C.D. (eds) Secure Internet Programming. Lecture Notes in Computer Science, vol 1603. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-48749-2_15.
 24. L. Bodsberg, T. O. Grøtan, M. G. Jaatun and I. Wærø, "HSE and Cyber Security in Remote Work," 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 2021, pp. 1-8, DOI: <https://doi.org/10.1109/CyberSA52016.2021.9478249>.
 25. Li, Ying and Siponen, Mikko, "A Call For Research On Home Users' Information Security Behaviour" (2011). PACIS 2011 Proceedings. 112. <https://aisel.aisnet.org/pacis2011/112>.
 26. S. M. Roşu and G. Drăgoi, "Virtual enterprise network general architecture," 2010 8th International Conference on Communications, Bucharest, Romania, 2010, pp. 313-316, DOI: <https://doi.org/10.1109/ICCOMM.2010.5509052>.
 27. Pohl, F., Schotten, H.D. (2017). "Secure and Scalable Remote Access Tunnels for the IIoT: An Assessment of openVPN and IPsec Performance." In: De Paoli, F., Schulte, S., Broch Johnsen, E. (eds) Service-Oriented and Cloud Computing. ESOC 2017. Lecture Notes in Computer Science(), vol 10465. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-67262-5_7.
 28. Jason Sabin, "The future of security in a remote-work environment", Network Security, Elsevier, Volume 2021, Issue 10, 2021, Pages 15-17, ISSN 1353-4858, DOI: [https://doi.org/10.1016/S1353-4858\(21\)00118-5](https://doi.org/10.1016/S1353-4858(21)00118-5).
 29. L. Atštāja, D. Rūtišis, S. Deruma, and E. Aksjončenko, "Cyber Security Risks and Challenges in Remote Work under the Covid-19 Pandemic", European Proceedings of Social and Behavioural Sciences EpSBS, 2021, e-ISSN: 2357-1330, DOI: <https://doi.org/10.15405/epsbs.2021.12.04.2>.
 30. F. Malecki, "Overcoming the security risks of remote working", Computer Fraud & Security, Vol. 2020, No. 7, 2021, DOI: [https://doi.org/10.1016/S1361-3723\(20\)30074-9](https://doi.org/10.1016/S1361-3723(20)30074-9).
 31. T. I. Buldakova and A. V. Sokolova, "Structuring Information about the State of the Cyber-Physical System Operator," 2020 V International Conference on Information Technologies in Engineering Education (Inforino), Moscow, Russia, 2020, pp. 1-5, DOI: <https://doi.org/10.1109/Inforino48376.2020.9111654>.
 32. Johnston, Allen C.; Wech, Barbara; Jack, Eric; and Beavers, Micah, "Reigning in the Remote Employee: Applying Social Learning Theory to Explain Information Security Policy Compliance Attitudes" (2010). AMCIS 2010 Proceedings. 493. <https://aisel.aisnet.org/amcis2010/493>.
 33. Robles-Gómez, Antonio, Llanos Tobarra, Rafael Pastor-Vargas, Roberto Hernández, and Jesús Cano. 2020. "Emulating and Evaluating Virtual Remote Laboratories for Cybersecurity" Sensors 20, no. 11: 3011. DOI: <https://doi.org/10.3390/s20113011>.
 34. Chalhoub, George, and Andrew Martin. "But is it exploitable? Exploring how router vendors manage and patch security vulnerabilities in consumer-grade routers." In Proceedings of the 2023 European Symposium on Usable Security, pp. 277-295. 2023., DOI: <https://doi.org/10.1145/3617072.3617110>.
 35. K. Goldman, R. Perez, and R. Sailer, "Linking remote attestation to secure tunnel endpoints," IBM Research Report, RC23982 (W0606-099), 2020., DOI: <https://doi.org/10.1145/1179474.117948>.
 36. A. Škiljić, "Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats," Int. Cybersecurity Law Rev., vol. 1, 2020., DOI: <https://doi.org/10.1365/s43439-020-00014-3>.
 37. S. Talib, N. L. Clarke, and S. M. Furnell, "An analysis of information security awareness within home and work environments," in Proc. Int. Conf. Availability, Reliability Security (ARES), 2020., DOI: <https://doi.org/10.1109/ARES.2010.27>.
 38. Chitnis, Sudhir, Neha Deshpande, and Arvind Shaligram. "An investigative study for smart home security: Issues, challenges and countermeasures." Wireless Sensor Network 8, no. 4 (2016): 61-68. DOI: <https://doi.org/10.4236/wsn.2016.84006>.
 39. Singh, Manmeet Mahinderjit, Chen Wai Chan, and Zakiah Zulkefli. "Security and privacy risks awareness for bring your own device (BYOD) paradigm." International Journal of Advanced Computer Science and Applications 8, no. 2 (2017)., DOI: <https://doi.org/10.14569/IJACSA.2017.080208>.
 40. F. C. Aguboshim and J. I. Udobi, "Security issues with mobile IT: A narrative review of bring your device (BYOD)," J. Inform. Eng. Appl., vol. 9, no. 1, 2019. <https://core.ac.uk/download/pdf/234677445.pdf>.
 41. Singh, Manmeet Mahinderjit, Soh Sin Siang, Oh Ying San, Nurul Hashimah, Ahamed Hassain Malim, and Azizul Rahman Mohd Shariff. "Security attacks taxonomy on bring your own devices (BYOD) model." International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol 4 (2014): 1-17. https://eprints.usm.my/47317/1/SECURITY_ATTACKS_TAXONOMY_ON_BRING_YOUR.pdf.
 42. I. Forain, R. de Oliveira Albuquerque and R. T. de Sousa Júnior, "Towards System Security: What a Comparison of National Vulnerability Databases Reveals," 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), Madrid, Spain, 2022, pp. 1-6, DOI: <https://doi.org/10.23919/CISTI54924.2022.9820232>.
 43. Chalhoub, George, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. "Factoring user experience into the security and privacy design of smart home devices: A case study." In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1-9. 2020., DOI: <https://doi.org/10.1145/3334480.3382850>.
 44. Patrick C. Shih, Kyungsik Han, and John M. Carroll. 2015. Using social multimedia content to inform emergency planning of recurring and cyclical events in local communities. Journal of Homeland Security and Emergency Management, Vol. 12, Issue. 3 (Sep. 2015), pp. 627-652. DOI: <https://doi.org/10.1515/jhsem-2014-0071>.
 45. Charalampous, Maria, Christine A. Grant, Carlo Tramontano, and Evie Michailidis. "Systematically reviewing remote e-workers' well-being at work: A multidimensional approach." European journal of work and organizational psychology 28, no. 1 (2019): 51-73., DOI: <https://doi.org/10.1080/1359432X.2018.1541886>.
 46. M. Nalini, Anvesh Chakram, Digital Risk Management for Data Attacks against State Evaluation. (2019). In International Journal of Innovative Technology and Exploring Engineering (Vol. 8, Issue 9S4, pp. 197-201). DOI: <https://doi.org/10.35940/ijitee.i1130.0789s419>.
 47. Sharma, K., Bhasin, S., & Nalini, P. B. (2019). A Worldwide Analysis of Cyber Security And Cyber Crime using Twitter. In International Journal of Engineering and Advanced Technology (Vol. 8, Issue 6S3, pp. 1051-1056). DOI: <https://doi.org/10.35940/ijeat.f1333.0986s319>.
 48. Yadav, A. K., Garg, D. M. L., & Dr Riitika. (2019). Cryptographic Solutions for Cloud-Based Storage System. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 2, pp. 2079-2084). DOI: <https://doi.org/10.35940/ijrte.b2298.078219>

Enhancing Cybersecurity for Remote Work: Identifying the Gaps and Design Considerations for A Robust Security Tool

AUTHOR'S PROFILE



Om Madat is a research scholar in the Department of Information Technology, University of Mumbai, Mumbai, India. He has published his work in a Springer journal and filed a patent for an innovative three-factor authentication system developed in collaboration with the Tata Institute of Fundamental Research (TIFR).

Their academic journey reflects on the focus of cybersecurity research, where projects have touched upon topics such as predictive mental health using machine learning and secure access control. He has further sharpened his research acumen from Google, and IBM certifications, as well as specialized training in penetration testing and digital forensics. Their deep interest in cybersecurity principles and hands-on research experience puts them in a forward-thinking scholar position who can advance cybersecurity through impactful studies and practical solutions.



Mayank Poriya is a research scholar in the Department of Information Technology, University of Mumbai, Mumbai, India. Mayank Poriya is a professional in Cybersecurity with a Bachelor of Computer Application (BCA) degree from KPB Hinduja College of Commerce, affiliated with Yashwantrao Chavan Maharashtra Open University, Nasik.

He is currently pursuing a Master of Science (MSc) in Cybersecurity at the Department of Information Technology, Mumbai University. He has been identified by CERT-IN for his efforts in discovering critical vulnerabilities in government websites. His area of expertise includes digital forensics, vulnerability analysis, and penetration testing. He is credited with having numerous achievements, including NCiIPC acknowledgment, and has made key contributions to several landmark investigations while working as a Cybercrime and Digital Forensic Investigator.



Srivaramangai R is currently the head of the department of IT, University of Mumbai, and is a Ph.D. guide and referee for Ph.D. viva voce. She is also a peer reviewer in many leading journals and conferences. Her expertise includes computational sciences, data analytics, cloud computing, and cybersecurity. Dr. Srivaramangai R's research spans cybersecurity, data mining, and big data analytics. Notably, she developed the Link-Guard algorithm to detect spear-phishing attacks by analyzing URLs and domain identities. In healthcare informatics, she explored data mining techniques like Naïve Bayes and Support Vector Machines to predict and manage child health issues. Her work also includes big data applications in semiconductor manufacturing, focusing on anomaly detection and predictive maintenance using frameworks like Hadoop.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

