Cybersecurity Threats Targeting Remote Workers: A Review

Ngomani Fundiswa and Noluntu Mpekoa
University of Johannesburg, South Africa

ngomani.fundiswa@outlook.com
noluntum@uj.ac.za

Abstract: Remote workers encounter numerous cybersecurity risks that differ significantly from those faced in traditional office settings. These threats can range from cybersecurity risks, such as phishing attacks and data breaches, to challenges like feelings of isolation and work-life balance issues. The widespread use of insecure home networks further exacerbates these risks, as many employees connect their devices to Wi-Fi networks that lack essential security measures like strong passwords and encryption. As remote employees operate beyond the protective perimeter of an organisation's secure systems, businesses are increasingly dependent on robust cybersecurity frameworks, best practices, and comprehensive policies to protect their data and assets. The primary objective of this paper is to tackle the urgent issues related to cybersecurity management in remote work settings. This study presents a systematic review of research on cybersecurity risks targeting remote workers, following the PRISMA framework. A total of 20 studies published between 2019 and 2025 were reviewed from Scopus and Google Scholar. The results showed that phishing, malware, ransomware, insecure networks and human factors such as the lack of cybersecurity awareness training are among the most frequently reported threats. The most common mitigation strategies include employee training and awareness, VPNs, multifactor authentication (MFA) and the adoption of the zero-trust framework. Recommendations include offering relevant, current, and personalised cybersecurity awareness training for remote workers, as well as implementing and training on security tools such as multi-factor authentication (MFA) and the use of strong passwords.

Keywords: Cybersecurity threats, Security training, Remote working, MFA

1. Introduction

Remote work is defined as the organisation's work operations that are being performed outside the organisation's space (Olson, 1983). Following the COVID-19 pandemic, organisations introduced the work-from-home (remote work) and hybrid work models. Even though the model does offer some benefits, it also introduces some challenges (Newbold et al, 2021). Cybersecurity is defined as a practice that is concerned with safeguarding the integrity of the organisation's systems from manipulation and unauthorised access (Schiliro, 2023). With employees operating in different geographic areas, away from the organisation's secured and private networks, organisations are required to rely on cybersecurity best practices and policies. Remote workers often rely on personal devices, cloud-based collaboration tools, home networks and sometimes public networks in coffee shops and other establishments (Bispham et al, 2021). The lack of proper and robust security protocols, such as those in corporate environments, makes them particularly susceptible to cyber threats and attacks. This shift has also simultaneously expanded the cybersecurity attack surface, introducing newer, sophisticated cybersecurity vulnerabilities for both workers and employers. To effectively identify and implement viable solutions, organisations must first gain a thorough understanding of the diverse threats faced by remote workers (Sokolic, 2022). It is essential to identify specific vulnerabilities, such as unsecured home networks and inadequate communication tools.

This comprehensive insight will allow organisations to devise tailored strategies and relevant solutions for each identified threat, ensuring that remote workers receive the support and protection they need in their work environment (Sanusi, 2025). Recent studies have highlighted the surge in cybersecurity attacks targeting remote workers, including phishing attacks, social engineering and ransomware attacks, to name a few (Admass, Munaye and Diro, 2024). The COVID-19 pandemic in 2020 accelerated the remote work trend by forcing organisations to move their work operations and rapidly adopt and implement remote work strategies, in some cases without any comprehensive security measures. This has exposed the gap in employee cybersecurity awareness, organisations' IT and cybersecurity policies, underscoring the need for a systematic understanding of the threats that are facing remote working individuals (Nwankpa and Datta, 2023). The objective of this review is to identify, evaluate and synthesise existing research on cybersecurity threats targeting remote workers. By analysing peer-reviewed studies published between the years 2019 and 2025, this review seeks to answer the following questions:

- What are the main cybersecurity challenges that affect remote workers and;
- What mitigation strategies have been proposed?

This review also aims to create categories of threats based on their types and severity, highlight the patterns and trends across different studies, and to identify gaps in the current research that require further investigations. Understanding the cybersecurity challenges that are being faced by remote workers is a critical step for organisations aiming to safeguard their company assets and sensitive information, maintain operational continuity and foster a secure remote working environment. This review provides insights into the most prevalent threats and offers guidance for both researchers and organisations seeking to enhance their cybersecurity practices in the era of a distributed workforce. This paper is sectioned as follows: Sections 2 present the study background, Section 3 is the research methodology, Section 4 follows with findings, Section 5 is the discussion and Section 6 is the conclusion.

2. Cybersecurity Threats and Mitigation Strategies

The shift to remote work has transformed the modern workplace, offering flexibility but also introducing a new set of security risks. Understanding these risks is crucial, as traditional organisational security measures often fail to address vulnerabilities specific to home and remote environments. This section provides context for the current gaps in the literature and highlights the need for a systematic review of threats targeting remote workers, together with the available mitigation strategies. While existing literature addresses organisational cybersecurity policies, there is limited focus on threats that specifically target remote workers (Mihailović et al, 2021). Empirical studies often overlook the risks associated with personal devices, home networks and informal working environments (Ferdousi, 2022). These shortcomings make it challenging to develop effective mitigation strategies that are tailored to the remote work setting. Mahboubi et al (2024) note that traditional threat models do not adequately account for vulnerabilities introduced by the remote working technologies, while Nwankpa and Datta (2023) emphasise that security awareness programs rarely address behavioural risks that target remote workers specifically. Zakki et al (2025) highlight that challenges such as technical, human and organisational nature do exist in the remote work environment, and these are challenges when it comes to delivering resource allocations to remote workers. Furthermore, the global survey by Gibson (2022) found that organisations that allow workers to bring personal devices to work often fail to implement comprehensive remote access policy protections. These studies reveal the lack of comprehensive reviews targeting remote workers addressing specific questions i) What are the main cybersecurity challenges that affect remote workers? and (ii) What mitigation strategies have been proposed?

This paper aims to bridge the identified gaps by conducting a systematic review of cybersecurity threats targeting remote workers. The review synthesises findings from various studies to provide a comprehensive understanding of the primary challenges and the effectiveness of proposed mitigation strategies. By addressing the research questions, this study contributes to both academic literature and practical applications in enhancing cybersecurity for remote work environments.

3. Research Methodology

The main objective of this paper was to tackle the urgent issues related to cybersecurity management in remote work settings. This systematic literature review followed PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), a framework that ensures a rigorous and transparent methodology of synthesising research. The review process involved several steps, including identifying relevant studies, applying predefined inclusion and exclusion criteria, systematic data extraction and finally the synthesis of findings. Each step was conducted in accordance with PRISMA guidelines to ensure reproducibility and to minimise bias (Page et al., 2021).

3.1 Search Strategy

A comprehensive search of electronic databases was conducted, where the relevant literature was identified. The following databases were used: Google Scholar and Scopus. The search terms that were used were developed using the study's objectives and included the combination of keywords, "remote work AND cybersecurity", "hybrid AND cyber threats", "work from home AND security vulnerabilities", and "remote workers AND information security". Some Boolean operators, such as (AND, OR), were used to refine the search results and the retrieval of relevant studies. A total of 333 studies from Google Scholar and 4 from Scopus were returned in the initial search. After screening for the inclusion and exclusion criteria, a total of 20 studies were included in this systematic review.

3.2 Inclusion and Exclusion Criteria

The inclusion and exclusion criteria applied in the selection review of the studies are outlined as follows: studies published between 2019 and 2025, including peer-reviewed works such as journal articles, conference proceedings, and peer-reviewed book chapters, must be in English and specifically address cybersecurity in the context of remote work. The exclusion criteria encompass opinions, blogs, and non-peer-reviewed materials, as well as studies that focus on general cybersecurity topics or are not available in full-text format. These criteria were assessed against a total of 337 papers prior to the final selection process.

3.3 Screening and Selection Process

The initial search yielded 337 articles, some of which were duplicates, some sources were not available in full text and only abstracts were available. After removing duplicates, 238 unique records remained. Screening abstracts reduced this to 118 studies for full-text review. Following full text assessment based on predefined inclusion criteria namely, relevance to the research objectives, empirical evaluation and alignment with the study scope, 20 studies were selected for this study.

3.4 Data Extraction

From each chosen source of the 20 papers, key information was systematically extracted and organised into a table that includes Authors and the year of publishing, the study's key findings, the cybersecurity threats addressed and the mitigation strategies.

3.5 Synthesis and Findings

The extracted data from the 20 papers were thematically analysed by the most common cybersecurity threats targeting remote workers, a common pattern among the studies and the gaps in literature. The findings were then organised into key themes, including social engineering and phishing, malware and ransomware, VPN and remote access, insider threat and human error. The mitigation strategies were summarised according to human and technical approaches. This methodology ensured a comprehensive and replicable review of the current literature on cybersecurity threats facing remote workers.

4. Findings

The systematic review of 20 peer-reviewed studies specifically addressing cybersecurity threats targeting remote workers and their mitigation strategies revealed several recurring threats. The studies differ in scope, methodology, and focus, but they highlighted the same threats, such as phishing, malware, ransomware, and insecure networks, which were the most frequently reported threats (Cuyugan and Rey, 2024; Mandadi et al, 2024; Pranggono & Arabo, 2021; Nwankpa et al, 2022). Human factors, such as employee behaviour, awareness, and attitudes, also play a significant role (Rakha, 2023; Qollakaj et al, 2025). Phishing attacks were reported in 15 studies, malware and ransomware in 12 studies, insecure networks and VPNs in 8 studies, and human factors such as the lack of security awareness in 7 studies. Table 1 below presents some of the major threat types together with the key findings of the studies.

Table 1: Major threats and mitigation strategies

Author (s)	Threat type	Mitigation strategy	Key findings
Mandadi et al (2024)	Spyware, Trojan horse, phishing, and insecure Wi-Fi	VPNs, strong passwords, endpoint management, training	Employee awareness and training is the most critical mitigation strategy
Cuyugan & Rey (2024)	Malware infections, Phishing	Policies, strong cybersecurity culture, and MFA deployment	Importance of multi-factor authentication and Zero Trust Network Access, MFA
Pranggono & Arabo (2021)	Phishing, Ransomware, DDoS, malware	Policies, employee education, VPNs, MFA, segmentation	Zero Trust approach is emphasised; remote work raises cybersecurity risks
Atstāja et al (2023), Georgiadou et al (2021)	Human factors, security awareness, phishing, and insecure networks	Cybersecurity training, CAT frameworks, and individual security focus	Human behaviour is key to information security; precaution-taking is critical
Nwankpa et al (2022); Milson & Altan (2023)	Confidentiality, data integrity, phishing, social	Cybersecurity training, MFA, VPNs, and patch management	Remote work increases risk; fostering cybersecurity best practices mitigates threats

Author (s)	Threat type	Mitigation strategy	Key findings
	engineering, and insecure home networks		
Hasan & Elweskiöld (2021); Qollakaj et al (2025)	Isolation, phishing, delayed support, invisible IT presence	Tailored phishing simulations, training and support	Remote work diminishes information flow; isolation increases phishing susceptibility
Cremer et al (2022); Alawida et al (2023); Rakha (2023)	Ransomware, malware, DDoS, phishing, hacking	Proactive cybersecurity, policies, guidelines, cyberattack detection & response	Proactive measures and legal compliance improve security in remote work
Bispham et al. (2021); Mahyoub et al. (2024)	Zoom bombing, ransomware, malware, phishing, Denial of service attacks (DDoS), physical device security	Policies, developing an incident response plan, VPNs, avoiding public WiFi, anti-Virus Software	The need for a zero-trust approach is emphasized, organisations should prioritize promoting security behaviour
Whitty, Moustafa and Marthie (2024); Nurse et al. (2021); Ozer et al. (2024)	Spear phishing, financial fraud, DDoS, insecure WiFi networks, VPNs, social engineering scams	Avoiding a one-size-fits-all approach, cybersecurity training, applying zero trust framework, regular updates on emerging threats	Remote work requires additional cybersecurity practices, the tension between workers wanting privacy and employer's goal to monitor workers, organizations to remain vigilant and adapt their cybersecurity strategies as the remote work trend increases
Khatri, Cherukuri and Kamalov (2023), Hiji and Alam (2022); Jerotirmay (2020)	Identity theft, DDoS, hacking, phishing, digital stalking, social engineering, lack of cybersecurity awareness, malware, data breaches, unsecure home networks	Regular cybersecurity awareness training, using VPNs, DNS security, data loss prevention, zero trust architecture	The study highlights the urgent need to improve cybersecurity hygiene practices and secure cyber infrastructure to mitigate future threats. Organisations must implement CAT framework to train and provide awareness to their employees regarding cyber threats. Traditional cybersecurity measures are no longer effective to protect organisations data.

As indicated in Table 1 above, several commonly recommended mitigation strategies encompass employee training and awareness programs, the use of Virtual Private Networks (VPNs) (Mandadi et al, 2024; Nwankpa et al, 2022; Milson & Altan, 2023), multi-factor authentication, the implementation of robust policies and guidelines (Pranggono & Arabo, 2021; Milson & Altan, 2023; Alawida et al, 2023), effective endpoint management, and the adoption of a zero-trust framework Atstāja et al, 2023; Georgiadou et al, 2021; Alawida et al, 2023). Numerous studies highlight the importance of employee education and proactive security measures, particularly in remote work environments (Alawida et al, 2023; Rakha, 2023). Specifically, 16 studies advocate for the utilisation of VPNs, while secure network configurations are endorsed by 10 studies. Additionally, 8 studies emphasise strategies such as multi-factor authentication and endpoint management, with 6 studies recommending the establishment of comprehensive policies and frameworks. Overall, the findings indicate that while technical solutions like VPNs and antivirus software play a crucial role, human-centric approaches and organisational policies are essential for achieving effective cybersecurity in remote work settings.

5. Discussion

The findings of this systematic review illuminate the urgent and multifaceted cybersecurity challenges encountered by remote workers, specifically highlighting ransomware, insecure networks, malware, and phishing as the most prominent threats in this realm. This observation aligns with previous research, including the comprehensive study conducted by Qollakaj et al. (2025), which reveals that the transition to remote work not only heightens the risk landscape but also exposes organisations to a diverse array of technical vulnerabilities and human-centric threats. A particularly critical aspect of this issue is the human factor, where deficiencies in

cybersecurity awareness among employees significantly compromise the safeguarding of digital assets. Research indicates that employees often lack a fundamental understanding of best practices in online security, making them potential targets for social engineering attacks. While implementing robust technical measures—such as leveraging Virtual Private Networks (VPNs) for secure data transmission, effective endpoint management to ensure devices are protected, and Multi-Factor Authentication (MFA) to add layers of security—are indeed essential for enhancing an organisation's cyber defences, literature consistently underscores the necessity of comprehensive training and awareness programs tailored for employees.

These educational initiatives have emerged as some of the most effective strategies to mitigate cybersecurity risks, emphasising the importance of cultivating a culture of security awareness within organisations. Successful cybersecurity frameworks, therefore, should seamlessly integrate both behavioural aspects, such as employee training and prompt reporting mechanisms for suspicious activities, alongside technological approaches to establish a formidable defence strategy. Moreover, this review highlights that organisations adopting a zero-trust security framework—which operates on the principle of never assuming trust, regardless of the user's location—coupled with well-defined policies and guidelines, are significantly better positioned to tackle the unique risks associated with remote work environments. By prioritising both sophisticated technical safeguards and ongoing employee education and engagement, companies can not only enhance their cybersecurity posture but also foster a resilient and adaptive cybersecurity culture that effectively addresses emerging threats in an increasingly digital landscape.

Numerous studies have identified significant challenges in the implementation of security measures for remote work, including resistance to change among employees, concerns surrounding privacy, and the varying nature of home office environments. These findings indicate a pressing need for flexible security policies that can be customised to address the diverse requirements of different remote work settings. While much of the existing research has concentrated on well-known threats such as malware and phishing, there is a noticeable gap in the literature regarding emerging threats, particularly social engineering attacks that target collaboration platforms and cloud-based applications. This oversight presents valuable opportunities for future research endeavours aimed at investigating advanced threat detection methodologies, the development of proactive employee monitoring systems, and organisational tactics designed to mitigate risks associated with remote work.

The ongoing discussion underscores the importance of a multifaceted approach that integrates policy frameworks, human-centred interventions, and robust technical safeguards as integral components for ensuring the security of remote work environments. Organisations must remain committed to evolving their cybersecurity strategies, not only to confront both emerging and existing threats but also to prioritise the continuous training and awareness of employees. This emphasis on ongoing education is crucial in fostering a culture of security awareness, ultimately reducing vulnerabilities in an increasingly digital and remote workforce.

6. Future Work

While the reviewed studies offer valuable insights into cybersecurity, several critical gaps persist that warrant further examination:

- Longitudinal Studies: A limited number of studies have explored the long-term effectiveness of various training programs and technical interventions. Understanding the sustained impact of these initiatives is essential for developing enduring cybersecurity strategies that can adapt to evolving threats over time.
- Focus on Small and Medium Enterprises (SMEs): The majority of existing research tends to concentrate on large organisations, leaving a notable deficit in studies that address the unique challenges faced by small to medium enterprises. SMEs often have distinct resource constraints and risk profiles, and targeted research in this area could lead to more effective and scalable cybersecurity solutions for these entities.
- Investigating Emerging Threats: The landscape of cybersecurity threats is continually shifting, particularly with the rise of new technologies such as collaboration platforms and the Internet of Things (IoT). However, there is a need for more comprehensive research into the vulnerabilities associated with these emerging technologies, as they pose unique risks that require tailored responses.

Addressing these gaps is crucial for organisations aiming to develop more agile and effective cybersecurity frameworks that cater specifically to the needs of remote workers. Furthermore, it will guide future research efforts in this essential field, ultimately enhancing overall cybersecurity resilience.

7. Conclusion

The systematic review was aimed at examining the main cybersecurity challenges facing remote workers and their mitigation strategies proposed in recent literature. The findings revealed that phishing, malware, ransomware and insecure networks remain the most persistent threats, while human factors such as the lack of cybersecurity awareness and training further amplify the risks in the remote work environments. Overall, by consolidating the findings across 20 studies, this paper contributes to the growing body of knowledge on remote work cybersecurity and identifies areas where research remains limited, particularly around emerging threats in collaboration tools and cloud platforms. Future research should investigate the advanced detection mechanisms, training models and long-term effectiveness of the zero-trust architecture in the remote work setting.

Ethics Declaration: Ethical clearance was not required for this research, as it was based solely on a systematic review of published academic and industry literature. No human participants or sensitive data were involved in the study.

AI Declarations: Grammarly was utilised to aid in the preparation of this paper. AI was engaged to assist with refining the language and editing the structure. The author maintained complete responsibility for reviewing, verifying, summarising, and interpreting all outputs, thereby ensuring the accuracy and integrity of the final document.

References

Admass, W.S., Munaye, Y.Y. and Diro, A.A. (2024). Cyber security: State of the art, Challenges and Future Directions. Cyber Security and Applications doi:https://doi.org/10.1016/j.csa.2023.100031.

Alawida, M., Omolara, A.E., Abiodun, O.I. and Al-Rajab, M. (2022). A Deeper Look into Cybersecurity Issues in the Wake of Covid-19: a Survey. Journal of King Saud University - Computer and Information Sciences, 34(10), pp.8176–8206. doi:https://doi.org/10.1016/j.jksuci.2022.08.003.

Aslan, Ö., Aktuğ, S.S., Okay, M.O., Yilmaz, A.A. and Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 12(6), pp.1–42. doi:https://doi.org/10.3390/electronics12061333.

Atstāja, L., Rūtītis, D., Deruma, S. and Aksjoņenko, E. (2021). Cyber Security Risks and Challenges in Remote Work under the Covid-19 Pandemic. European Proceedings of Social and Behavioural Sciences, 121. doi:https://doi.org/10.15405/epsbs.2021.12.04.2.

Bispham, M., Creese, S., Dutton, W.H., Esteve-Gonzalez, P. and Goldsmith, M. (2021). Cybersecurity in Working from Home: an Exploratory Study. SSRN Electronic Journal. doi:https://doi.org/10.2139/ssrn.3897380.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3), pp.698–736. doi:https://doi.org/10.1057/s41288-022-00266-6.

Cuyugan, M.J.R. and Rey, W.P. (2024). Beyond the Firewall: Strategies in Securing Remote Work Environment. 2024 14th International Conference on Software Technology and Engineering (ICSTE), pp.94–101. doi:https://doi.org/10.1109/icste63875.2024.00024.

Georgiadou, A., Mouzakitis, S. and Askounis, D. (2021). Working from Home during COVID-19 crisis: a Cyber Security Culture Assessment Survey. Security Journal, 35(35). doi:https://doi.org/10.1057/s41284-021-00286-2.

Gibson, K. (2022). Remote Work Creates a Gap in Security Practices - IT-Online. [online] IT-Online. Available at: https://it-online.co.za/2022/02/03/remote-work-creates-a-gap-in-security-practices [Accessed 29 Sep. 2025].

Hijji, M. and Alam, G. (2022) Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors, 22, Article No. 8663. https://doi.org/10.3390/s22228663

Hasan, R., Elweskiöld, M. and Mutimukwe, C. (n.d.). Phishing in Remote Work: an Understanding of Factors That Enhance Employee Susceptibility to Phishing Attacks a Qualitative Study Degree Project at the Bachelor Level Computer and System Sciences Spring Term 2025. Available at: https://su.diva-portal.org/smash/get/diva2%3A1980971/FULLTEXT01.pdf? [Accessed 11 Sep. 2025].

Jerotirmay, J. (2020). View of Adapting to Remote Work: Emerging Cyber Risks and How to Safeguard Your Organization. Turcomat.org. Available at: https://turcomat.org/index.php/turkbilmat/article/view/15190/10904.

Khatri, S., Cherukuri, A.K. and Kamalov, F. (2023). Global Pandemics Influence on Cyber Security and Cyber Crimes. doi:https://doi.org/10.48550/arxiv.2302.12462.

Mahyoub, A., Luong, K., Aboutorab, H., Bui, H.T., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B. and Gately, H. (2024). Evolving Techniques in Cyber Threat hunting: a Systematic Review. Journal of Network and Computer Applications, 232, pp.104004–104004. doi:https://doi.org/10.1016/j.jnca.2024.104004.

Mandadi, S., Gochhayat, S.P., Torremocha, V. and Kethar, J. (2024). Cybersecurity Risks in Remote Work and Learning Environments and Methods of Combating Them. Journal of Student Research, 13(2). doi:https://doi.org/10.47611/jsrhs.v13i2.6808.

Mihailović, A., Cerović Smolović, J., Radević, I., Rašović, N. and Martinović, N. (2021). COVID-19 and Beyond: Employee Perceptions of the Efficiency of Teleworking and Its Cybersecurity Implications. Sustainability, 13(12), p.6750. doi:https://doi.org/10.3390/su13126750.

Milson, S. and Altan, B. (2023). Cybersecurity in Remote Work Environments: Challenges and Best Practices. easychair.org. Available at: https://easychair.org/publications/preprint/9lj5.

Newbold, J.W., Rudnicka, A., Cook, D., Cecchinato, M., Gould, S. and Cox, A.L. (2021). The new normals of work: a framework for understanding responses to disruptions created by new futures of work. Human–Computer Interaction, 37(6), pp.1–24. doi:https://doi.org/10.1080/07370024.2021.1982391.

Nurse, Jason R. C., Williams, Nikki, Collins, Emily, Panteli, Niki, Blythe, John and Koppelman, Ben (2021) Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy. In: 23rd International Conference on Human-Computer Interaction.

Nwankpa, J.K. and Datta, P. (2023). Remote Vigilance: the Roles of Cyber Awareness and Cybersecurity Policies among Remote Workers. Computers & Security, 130(1), pp.103266–103266. doi:https://doi.org/10.1016/j.cose.2023.103266.

Olson, M.H. (1983). Remote Office work: Changing Work Patterns in Space and Time. Communications of the ACM, 26(3), pp.182–187. doi:https://doi.org/10.1145/358061.358068.

Ozer, M., Kose, Y., Bastug, M., Kucukkaya, G. and Varlioglu, E.R. (2024). The Shifting Landscape of Cybersecurity: The Impact of Remote Work and COVID-19 on Data Breach Trends. arXiv (Cornell University). doi:https://doi.org/10.48550/arxiv.2402.06650.

Pranggono, B. and Arabo, A. (2020). COVID-19 Pandemic Cybersecurity Issues. Internet Technology Letters, 4(2). doi:https://doi.org/10.1002/itl2.247.

Qollakaj, K., Larsson, L.E. and Memeti, S. (2025). Cybersecurity of Remote Work migration: a Study on the VPN Security Landscape Post Covid-19 Outbreak. Array, 27, p.100437. doi:https://doi.org/10.1016/j.array.2025.100437.

Rakha, N.A. (2023). Ensuring Cyber-security in Remote Workforce: Legal Implications and International Best Practices. International Journal of Law and Policy, 1(3). doi:https://doi.org/10.59022/ijlp.43.

Sabin, J. (2021). The Future of Security in a remote-work Environment. Network Security, 2021(10), pp.15–17. doi:https://doi.org/10.1016/S1353-4858(21)00118-5.

Sanusi, M. (2025). Cybersecurity Challenges in Remote Work Environments: Common Threats and Mitigation Strategies. Available at: https://www.diva-portal.org/smash/get/diva2:1995670/FULLTEXT01.pdf [Accessed 28 Sep. 2025].

Schiliro, F. (2023). Towards a Contemporary Definition of Cybersecurity. Towards a Contemporary Definition of Cybersecurity. doi:https://doi.org/10.48550/arxiv.2302.02274.

Sokolic, D. (2022). Remote Work And Hybrid Work Organizations. [online] ResearchGate. Available at: https://www.researchgate.net/publication/359056200_Remote_Work_And_Hybrid_Work_Organizations.

Vivekananth, P. (2022). Cybersecurity Risks in Remote Working Environment and Strategies to Mitigate Them. International Journal of Engineering and Management Research, 12(1), pp.108–111. doi:https://doi.org/10.31033/ijemr.12.1.13.

Whitty, M.T., Moustafa, N. and Marthie Grobler (2024). Cybersecurity When Working from Home during COVID-19: considering the Human Factors. Journal of Cybersecurity, 10(1). doi:https://doi.org/10.1093/cybsec/tyae001.

Williams, J., Collins, N., Panteli, E., Blythe, N. and Koppelman, J. (2021). Remote Working Pre-and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy. Communications in Computer and Information Science. doi:https://doi.org/10.1007/978-3-030-78645-8.

Zakki, M.N., Iftikhar, N., Khan, S.S.U., Nishat, F. and Arshi, O. (2025). Overcoming Challenges and Implementing Effective Information Security Policies for Remote Work Environments. Information Systems Engineering and Management, pp.135–151. doi:https://doi.org/10.1007/978-3-031-81481-5_10.