Enhancing Cybersecurity Compliance in Remote Work: Strategies, Challenges, and Behavioural Insights

Merve Pacarizi Kabashi

Nida Santuri Fishekqiu

Elida Hadro

South East European University,
Tetovo, North Macadonia

Received: 14 July 2025 / Accepted: 28 August 2025 / Published: 25 September 2025

Doi: 10.56345/ijrdv12n2s105

Abstract

Organizations now rely heavily on remote working which requires strong cybersecurity compliance measures to address associated risks. The research examines remote workers' adherence to cybersecurity rules and policies by analyzing organizational compliance strategies and the challenges remote workers face while exploring their techniques to minimize cyber risk exposure. The paper analyzes best practices to maintain trust and protect assets while minimizing insider threats and human error which leads to recommendations for improved compliance. Human elements represent the weakest link in cyber and information security (CIS) frameworks around the world even as advanced technical defenses exist. Psychological and theoretical frameworks shape how organizations follow compliance guidelines while also dictating violation patterns. This research utilizes mixed-methods procedures to evaluate remote workers understanding, dedication, and motivation for adhering to cybersecurity standards. Organizations have compliance strategies, but numerous employees still lack awareness and necessary training. The development of cybersecurity behavior frequently results from deterrence systems and policy awareness combined with technological protection measures. Research demonstrates the necessity of stronger organizational governance alongside training initiatives and better security culture to achieve compliance among remote employees. Organizations will enhance their digital asset protection and remote work resilience by addressing existing gaps.

Keywords: *Cybersecurity, Compliance, Remote Work, Information Security, Organizational Policy, Cyber Risk*

1. Introduction

The move to working from home, which is being sped up by global events like the COVID-19 pandemic and digital change, has created new security holes. Although technological defenses have improved, human error and bad behavior are still big problems. Since remote workers don't work in standard office settings, it's harder to make sure they follow company policies and keep an eye on technological compliance for remotework.

This study looks into how following cybersecurity policies affects how people act when they work from home. It highlights the need for unified plans that include rules, teaching, and understanding how people behave to promote safe behavior among employees that operate in different places.

2. Literature Review

2.1 Cybersecurity Risks and Remote Work

Remote work introduces uncontrolled technology, insecure networks, and limited physical oversight, therefore extending the attack surface. Common threats include phishing, malware, unauthorized access, and data leaks. Based on Verizon's Data Breach Investigations Report (2023), the human factor is involved in over 82% of incidents.

2.2 Difficulties with Compliance in Remote Work

Lack of security training:
- Inconsistent device security
- Weak password habit
- Unclear regulations for remote settings
- Limited employee responsibility is some of the main difficulties to compliance.

2.3 The Human Aspect in Cybersecurity

Secure actions are impacted by attitudes, recognized standards, and self-efficacy, as explained by behavioral models like the Protection Motivation Theory (PMT) and the Theory of Planned behavior (TPB). Many employees ignore policies because they believe they are unnecessary or inconvenient.

2.4 Strategies for Organizational Compliance

Organizations use a range of strategies to increase cybersecurity compliance:
- Using technical safeguards (such as VPNs and multi-factor authentication)
- Using incident response simulations
- Using behavior-based monitoring
- Providing security awareness training.

3. Research Objectives

Purpose of this study is to:
- ➢ Identify the most common cybersecurity challenges faced by remote workers.
- ➢ Analyze how organizational strategies is affected by compliance behavior.
- ➢ Explore how behavior and psychology impact adherence to policy.
- ➢ Provide practical recommendations for improving compliance among remote workers.

4. Methodology

4.1 Design of Research

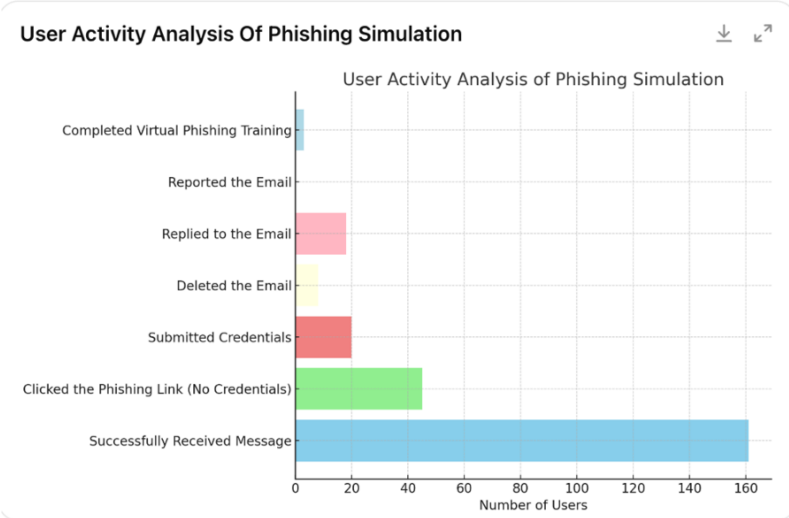
In order for recording both data trends and personal observations, this study employs a combination of methods, combining quantitative surveys and qualitative interviews.

4.2 Participants

The sample includes 240 remote employees from mid-sized to large business in industry of an IT Company.
- Criteria: Every employee including the Management such as (CEO, CFO, COO, CTO) and every employee with technical expertise, and previous experience working remotely must have worked at least six months working remotely.
- The phishing test is conducted by embedding a phishing link in a regular monthly informative email sent to all employees. The email appears as a normal communication, and user interactions (clicks, submissions,

replies) are tracked. Afterward, data is analyzed, and feedback is provided to improve awareness and security practices.

5. Results



5.1 *Phishing Results*

- **Successfully Received Message**: 67.08% (161 out of 240)
- **Clicked the Phishing Link (No Credentials):** 18.75% (45 out of 240)
- **Submitted Credentials:** 8.33% (20 out of 240)
- **Deleted the Email:** 3.33% (8 out of 240)
- **Replied to the Email**: 7.5% (18 out of 240)
- **Reported the Email:** 0% (0 out of 240)
- **Completed Virtual Phishing Training:** 1.25% (3 out of 240)

5.2 *Insights from interview*

High Awareness of Phishing Attempts: Most users (67.08%) were able to successfully receive the phishing message without responding to it. Given that many users chose not to interact with the message, this suggests a high level of awareness regarding phshingattempts.

Interaction with Phishing Links: 18.75% of users clicked on the phishing link but did not enter their login information. This indicates that even though they refrained from disclosing sensitive information, a sizable percentage of users are vulnerable to possible phishing threats. This is a sensitive area where user training needs to be improved. **Risk of Credential Submission:** 8.33% of users sent in their login information, posing a serious risk. By clicking on the phishing link, these users revealed private information. This needs to be addressed right away, perhaps with multi-factor authentication and improved phishing awareness training to lessen the impact.

Email Deletion Behavior: A relatively small percentage of users—just 3.33%—deleted the phishing email. Better instruction on the significance of promptly deleting questionable emails rather than responding to them could change this behavior.

7.5% of users responded to the phishing email. Even though this percentage is lower than the number of people who clicked the link, it nevertheless suggests that there is some misunderstanding or confusion regarding how to respond to phishing emails.

Absence of Reporting: The fact that no users reported the phishing email raises the possibility that either there are weaknesses in the reporting procedures or users lack the confidence to recognize phishing attempts. This emphasizes the necessity of improved reporting procedures and phishing attempt detection training.

Completion of Virtual Phishing Training: Only 1.25 percent of users finished the virtual phishing training, indicating that many employees have not yet benefited from it. The comparatively high number of users who clicked on the phishing link or submitted credentials may be attributed in large part to this low completion rate. Encouraging participation in such training should receive more attention.

6. Discussion

The findings reinforce that technology alone cannot ensure cybersecurity in remote work settings. Behavioral insights are critical. Security culture, motivation, and accountability directly influence adherence to compliance protocols. Policies must be:

- Clear and contextualized for remote environments,
- Communicated frequently and interactively,
- Backed by both incentives and deterrents,

Organizational support, including open communication channels and responsive IT support, fosters a more resilient workforce.

7. Recommendations

1. **Behavioral Training**: Incorporate gamification, simulations, and real-life case studies in training.
2. **Microlearning**: Use short, targeted modules for frequent learning reinforcement.
3. **Policy Personalization**: Tailor policies based on employee roles and risk profiles.
4. **Feedback Loops**: Allow two-way communication on policy challenges and improvements.
5. **Cultural Integration**: Promote security as a shared value, not just an obligation.

7.1 Security and Best Practices

A. Implementing Strong Authentication Measures

The deployment of strong authentication protocols is a critical requirement when it comes to remote work environment security. The implementation of multi-factor authentication (MFA) procedures is necessary to achieve this. MFA is a complex solution that requires users to provide various forms of identity to access systems or sensitive data. "Something you have" (like a mobile device or security token), "something you know" (like a password), and "something you are" (biometric data like fingerprints or facial recognition) are the three guiding concepts of multifactor authentication (MFA). Together, these several authentication components strengthen the security posture and dramatically lower the likelihood of unwanted access, particularly in situations when one factor is compromised. MFA serves as a strong defence against any breaches by requiring the simultaneous verification of multiple credentials. This extra layer of security is essential for safeguarding sensitive data and maintaining the integrity of remote work environments. The implementation of multi-factor authentication (MFA) is becoming a crucial step towards creating a digital workspace that is both secure and robust, as remote work becomes more common.

B. Data Encryption Protocols for Both Rest and Transit Data

When it comes to the security of remote work, the key is careful data protection while it's in transit and at rest. Strong encryption methods are at the forefront, guaranteeing the security of data that is stored and protecting the privacy of communications between distant devices and central systems. Notably, the industry standard for cryptography, Advanced Encryption Standard (AES), leads the way in protecting data when it is at rest. Its reputation for strength comes from its capacity to completely seal off stored data from unwanted access by constructing an unbreakable barrier around it.

The implementation of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols becomes critical during communication as data travels across digital highways. By establishing safe channels that prevent illegal interceptions and eavesdropping, these protocols serve as the watchful guardians of data while it is in transit. SSL and TLS protect sensitive data from potential attacks in the ever-changing world of remote work by ensuring that it stays private during its route. When combined, these encryption techniques create a vital barrier that strengthens the fundamentals of data security in remote work settings and increases an organization's overall resistance to cyber-attacks.

C. Antivirus and Endpoint Protection Solutions:

The importance of Transport Layer Security (TLS) or Secure Sockets Layer (SSL) implementation in the context of remote work cannot be emphasised. When information moves via the complex network of digital communication channels, these protocols become essential security measures. They play a crucial role in creating secure channels by serving as watchful guardians who foil unauthorised interceptions and eavesdropping efforts. This becomes more important given the ever-changing nature of remote work and the possibility for data breaches.

The foundation of data security during transit is formed by SSL and TLS, which guarantee that private data is kept hidden from snoopers. The combination of these encryption methods creates a strong barrier that strengthens the fundamentals of data security in remote work settings. This increases an organization's overall resilience against cyber threats and protects the confidentiality of transmitted data. To put it briefly, SSL and TLS are essential for strengthening the security framework of remote work and helping to create a strong defence against any cyberattacks.

D. Technologies for Secure Remote Access:

Ensuring the security and integrity of remote work environments is crucial in the modern remote work world, when virtual communication transcends the bounds of traditional office buildings. Unquestionably, the introduction of flexible work schedules has made things more convenient than before, but it has also exposed businesses to a wide range of cybersecurity risks. Regular security audits and vulnerability assessments become essential elements of a proactive cybersecurity strategy to strengthen defences and strengthen digital perimeters.

Vulnerability assessments and security audits act as the watchful gatekeepers in the changing world of remote work settings. Regular evaluations serve as more than just checklist items; they are an active defence against ever-changing cyberthreats. These evaluations serve as a thorough health check for the security architecture of an organisation, closely detecting possible weaknesses, assessing the effectiveness of current security measures, and guaranteeing scrupulous adherence to established security rules

Given how flexible and adaptable remote work is, the need of these evaluations is even more apparent. By actively participating in these assessments, organisations may improve their entire security posture and adjust to the constantly shifting threat landscape. Because of their scattered and varied endpoints, remote work environments necessitate a sophisticated security strategy. Frequent evaluations give vital insights into possible weak areas that malicious actors may exploit, helping organisations keep ahead of growing dangers.

Furthermore, these evaluations are essential for ensuring adherence to industry rules and security norms. Organisations must make sure that their remote work policies comply with the most recent security requirements as the legal environment changes. Frequent audits encourage a culture of continuous improvement in security processes by identifying any non-compliance concerns and opening the door for corrective actions.

E. Role-Based (or role-based) access control

Security procedures are now crucial in the ever-changing world of remote work to protect sensitive data and preserve the integrity of digital environments. Role-Based Access Control (RBAC) is a crucial and effective approach among these approaches. RBAC ensures that users may only access resources that are necessary for their given jobs by effectively distributing user permissions based on specified job roles, hence addressing the issues presented by remote work.

The fundamental idea behind RBAC is the mapping of job duties to access entitlements. This strategy adheres to the least privilege principle, which states that people should only be given the minimal amount of access required to carry out their jobs. In addition to streamlining processes, this provides a powerful safeguard against unwanted access. RBAC greatly lowers the possibility of anyone obtaining access to data or systems beyond the purview of their duties by customising access rights to specific positions within an organisation.

RBAC installation becomes especially important when it comes to reducing security threats related to remote work environments. The traditional perimeter-based security approach is less effective when teams are distributed, therefore user-centric security measures become crucial. RBAC offers a sophisticated and flexible approach to security with its job-specific access control, enabling enterprises to strike a delicate balance between control and accessibility.

When there is an unlucky security compromise, RBAC is essential to limiting possible damage. Users' access is allowed according to their job duties, which naturally restricts the extent of a breach. For attackers to be prevented from moving laterally across an organization's digital infrastructure, this containment technique is essential. In addition to limiting unauthorised access, RBAC makes it possible to respond quickly to security issues, reducing their effect and speeding up the recovery process.

RBAC shows up as a key component in creating a secure and regulated digital environment as businesses manage the challenges of remote work. It offers a framework that effortlessly integrates with the dynamic nature of contemporary work environments while providing an adaptable and scalable security solution. RBAC ensures that access to sensitive resources is proportionate to job duties and protects against possible risks by upholding the concept of least privilege. It also fosters a culture of responsibility. To sum up, RBAC is a critical component of the cybersecurity toolkit that helps organisations defend against the changing threats brought about by the remote work model.

F. Frequent Vulnerability Assessments and Security Audits:

It is now crucial to ensure the security of digital environments in the continuously changing world of remote work. Regular security audits and vulnerability assessments are essential to defending virtual perimeters, protecting sensitive data, and preserving the integrity of organisational processes. Regular assessments play a crucial role in pinpointing possible vulnerabilities, assessing the effectiveness of current security protocols, and guaranteeing rigorous compliance with specified security guidelines.

Organisations may strengthen their defences against various cyber threats by thoroughly examining and strengthening them through security audits, which work as a proactive tool. Security audits give a thorough overview of possible vulnerabilities that bad actors may exploit by methodically examining digital infrastructure. Organisations may prioritise and remediate vulnerabilities based on their severity and possible effect by using process to develop a detailed picture of their security landscape.

The ability to assess the efficacy of established security measures is one of the main advantages of conducting frequent security audits. Since the danger environment in the dynamic world of remote work is always changing, it is essential to conduct periodic evaluations to see if the security policies in place are still effective and flexible. Organisations may remain resilient against future threats by identifying areas for improvement and implementing the necessary upgrades by evaluating their present security posture against industry standards and best practices.

Furthermore, security audits play a major role in maintaining regulatory compliance. It is imperative for organisations to verify that their remote work environments comply with pertinent security requirements, given the increasingly rigorous data protection rules. Organisations may prove their compliance with regulatory frameworks through regular evaluations, which helps them avoid legal repercussions and maintain the trust of stakeholders and clients.

As a subset of security audits, vulnerability assessments concentrate on finding and fixing certain flaws in digital infrastructure. In these examinations, prospective cyberattacks are simulated, vulnerabilities that may be exploited are actively sought for, and the response of security measures is assessed. Organisations may maintain a strong defence against developing cyber hazards and keep ahead of prospective attacks by proactively resolving these vulnerabilities.

To sum up, frequent security audits and vulnerability analyses are essential parts of an all-encompassing cybersecurity plan for remote work settings. Organisations are able to improve their security posture, proactively handle emerging risks, and guarantee continuous regulatory compliance thanks to these periodic assessments. Organisations may manage the unpredictable world of remote work with confidence, resilience, and a consistent commitment to protecting their digital assets by adopting a proactive approach to cybersecurity.

7.2 Employee Training and Awereness

A. Security Awareness Programmes Are Important

In remote work situations, it is essential to implement security awareness programmes to inform staff members about possible hazards and vulnerabilities related to working outside of typical office settings. These courses are essential for improving staff members' comprehension of cybersecurity risks, recommended procedures, and the value of upholding a safe remote work environment. Organisations may drastically lower the probability of security incidents like malware attacks, unauthorised access, and data breaches by arming staff members with the knowledge and abilities to recognise and address security risks.

Employees that participate in security awareness programmes are also more likely to have a proactive mentality and be motivated to actively contribute to keeping their workplace safe. This degree of awareness is especially crucial in distant environments where people's decentralised work may make them more susceptible to cyberattack.

B. Educating Staff Members on Phishing Attack Recognition

In remote work contexts, where employees are frequently the subject of fraudulent emails, messages, or websites, phishing assaults continue to pose a significant concern. A vital part of cybersecurity education is teaching staff members how to spot and react to phishing attempts. Workers must be made aware of the telltale symptoms of phishing efforts, which include unexpected attachments, dubious email addresses, and demands for private information.

In order to offer staff members practical experience spotting and responding to phishing attempts, training programmes may incorporate simulated phishing exercises. Organisations might also demonstrate the dangers and repercussions by sharing actual phishing incidence samples.

8. Conclusion

The practice of working remotely has become a permanent fixture in the modern workplace, radically changing conventional organizational frameworks. However, there are serious cybersecurity issues brought on by the growing reliance on digital platforms and decentralized workforces, which drive businesses to completely reevaluate their approaches. Effective cybersecurity in remote work environments depends on a deep comprehension of human behavior supported by organizational culture and psychological concepts. It is not enough to merely rely on technological fixes or standardized compliance procedures because employee attitudes, actions, and motives have a big imapact on security.

As a result, companies need to integrate behavioral insights into their cybersecurity frameworks and actively cultivate a culture of security awareness through ongoing training, transparent communication, and easily accessible support systems. In addition to being technically sound, policies should be inclusive and flexible, taking into consideration the various experiences and emotional reactions of remote workers. Increased ownership, compliance, and resilience can result from promoting active employee involvement in security policy making.

Organizations can create comprehensive and reliable remote work environments by carefully integrating psychological knowledge with technical solutions and inclusive, collaborative policy-making procedures. Furthermore, to successfully reducing cybersecurity threats, these ecosystems will improve overall productivity, employee happiness, and organizational agility, setting up companies for long-term success in a world that is becoming more and more digital.

References

(2019) "How remote working increases cyber security risks," Financial Times, https://www.ft.com/content/f7127666-0c80-11ea-8fb7-8fcec0c3b0f9.

[Online]. Available: https://www.indeed.com/career-advice/career-development/video-conferencing-tools. [Accessed 12 December 2022].

An exploratory study of cybersecurity in working from home: problem or enabler?

Association of Computing Machinery, "ACM Code of Ethics and Professional Conduct," 22 January 2019. [Online]. Available: https://ethics.acm.org/code-of-ethics/. [Accessed 09 December 2022].

CDC, "Centers for Disease Control and Prevention," 26 January 2023. [Online]. Available: https://www.cdc.gov/coronavirus/2019-ncov/index.html. [Accessed 29 January 2023].

CyberRisk&Stats, "Statistics of Cyber Security Risks When Working from Home," 09 January 2021. [Online]. Available: https://www.dbxuk.com/statistics/cyber-security-risks-wfh. [Accessed 2022 October 2022].

E Brynjolfsson, J J Horton, A Ozimek, D Rock, G Sharma, et al. (2020) "COVID-19 and remote work: An early look at US data," National Bureau of Economic Research 27344.

Forbes Editorial Team, "15 Must-Have Features Of A Successful, User-Friendly Mobile App," 12 August 2022. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/20 21/05/24/15-must-have-features of-a-successful-user-friendly-mobile-app/?sh=22d74c8a6a7a. [Accessed 01 January 2023].

https://scholarlypublishingcollective.org/psup/information-policy/article/doi/10.5325/jinfopoli.12.2022.0010/320386/An-Exploratory-Study-of-Cybersecurity-in-Working

Indeed Editorial Team, "Indeed," 02 April 2022.

J. Nurse, N. Williams, E. Collins, N. Panteli, J. Blythe and B. Koppelman, "Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy," Internation Conference on Human Computer Interaction, vol. 1421, pp. 583-590, 2021.

Journal of Information Policy, Volume 12, 2022 This work is licensed under Creative Commons Attribution CC-BY-NC-ND

K Curran (2020) "Cyber security and the remote workforce," Elsevier BV 11-12.

McKinsey & Company (2022) "Is working remotely effective: The research is in," https://www.mckinsey.com/industries/ real-estate/our-insights/americans-are-embracing-flexible-work-and-they-want-more-of-it

NIST, "NIST," 19 June 2022. [Online]. Available: https://csrc.nist.gov/glossary/term/computer_securi ty. [Accessed 2022 20 November].

Owen, Artist, Remote Working Platforms. [Art]. Coderus, 2021.

P Damon (2022) "The Effect of COVID-19 on Remote Work Policies," Journal of Science Policy & Governance 21.

P. Satam, K. Hairiri and S. Hariri, "Anomaly behavior analysis of website vulnerability and security," international Conference of Computer Systems and Applications, vol. 13, pp. 300-314, 2016.

S. J. Bigelow, "Data Privacy (Information Privacy)," 10 August 2022. [Online]. Available: https://www.techtarget.com/searchcio/definition/da ta-privacy-information-privacy. [Accessed 18 November 2022].

Security Risks and Challenges of Remote Working and Learning, Computer Science Department Hampton University

V Soni, D Kukreja, D K Sharma (2020) "Security vs. Flexibility: Striking a Balance in the Pandemic Era," 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS 1-5.

VMware, "What is remote work security?" 19 September 2022. [Online]. Available: