International Journal of Information Security (2025) 24:187
https://doi.org/10.1007/s10207-025-01095-z

REGULAR CONTRIBUTION

Investigating the cybersecurity risks of remote work: a systematic literature review of organizational vulnerabilities and mitigation strategies

Mohammad Nizamuddin[1]

Accepted: 30 June 2025 / Published online: 27 July 2025

Abstract
The rapid adoption of remote work has transformed organizational operations, introducing complex cybersecurity vulnerabilities that demand rigorous scholarly investigation. This systematic literature review (SLR) critically examines cybersecurity risks in remote work environments by synthesizing findings from 20 peer-reviewed studies published between 2010 and 2024. Employing the PRISMA framework for transparency and rigor, the review integrates both qualitative and quantitative evidence using a convergent thematic synthesis approach. The analysis reveals a multifaceted threat landscape encompassing human factors, technical vulnerabilities, and organizational shortcomings. Key risks include phishing, social engineering, device misuse, insecure Wi-Fi and VPN usage, and policy non-compliance. Human behavior emerges as a predominant risk vector, exacerbated by limited training, misuse of remote autonomy, and blurred personal-professional boundaries. Organizational challenges—such as rushed digital transitions, shadow IT practices, and poor communication of cybersecurity protocols—further aggravate the threat matrix. The review also incorporates critical appraisal using MMAT, CASP, and JBI tools to ensure methodological soundness and bias mitigation. Synthesis tables distill findings into thematic clusters, providing actionable insights into risk categories and mitigation strategies. Proposed recommendations emphasize cybersecurity training, device and network hygiene, policy alignment, zero-trust frameworks, and continuous monitoring. This study contributes a comprehensive evidence base for scholars and practitioners navigating remote work cybersecurity. It advocates for adaptive, behavior-aware strategies to strengthen digital resilience, highlighting the need for future research on quantum, AR/VR, and blockchain technologies in remote settings. As remote work persists, cybersecurity must evolve accordingly to safeguard organizational integrity and continuity.

Keywords Remote work · Work from home (WFH) · Cyber risks · Risks of remote working · Organizational cybersecurity

1 Introduction

The shift to remote work has transitioned from a temporary adjustment to a fundamental aspect of modern organizational practices [19]. Accelerated by global events, technological advancements, and evolving workplace dynamics, remote work offers various advantages, including enhanced flexibility, improved work-life balance, and access to a diverse talent pool [10, 11, 31]. However, this paradigm shift has introduced unprecedented challenges, particularly in the domain of cybersecurity, as organizations navigate the complexities of operating in a zero-trust environment [8, 21, 40].

Remote work inherently disperses employees across geographic locations, increasing reliance on digital communication platforms and cloud-based technologies [11]. This distributed model has created new avenues for cyber threats, exacerbating risks that were previously managed within centralized office environments [8]. As noted by Nurse et al. [55], addressing these vulnerabilities is imperative for safeguarding organizational security. Unlike controlled office setups, home environments lack comprehensive IT policies and best practices, rendering remote work setups more susceptible to cyberattacks [21]. Key risks include the use of unsecured Wi-Fi networks and personal devices, delayed software updates, and inadequate cybersecurity measures, all of which

✉ Mohammad Nizamuddin
mohammad.nizamuddin@bcc.cuny.edu

[1] Department of Engineering, Physics and Technology, Bronx Community College, City University of New York, New York, USA

expose organizations to significant threats [4, 8]. Additionally, remote workers face targeted attacks such as phishing and social engineering [77] and may inadvertently use unauthorized software, increasing the likelihood of unauthorized access to sensitive resources [22]. These challenges encompass a range of risks, including technical vulnerabilities, procedural non-compliance, human behavior-related risks, and external threats [6, 69].

The cybersecurity implications of remote work are profound. The remote work environment has become a focal point for cybercriminal activity, as highlighted by Sirineni [69]. For instance, Malwarebytes [47] reported that 20% of organizations experienced a data breach linked to remote work, leading to increased business expenses, with 24% incurring unforeseen costs to mitigate breaches. Furthermore, the IBM Cost of a Data Breach report revealed that breaches involving remote work elevated the average cost of a data breach by over $1 million and extended the containment timeline by 58 days compared to office-based breaches [54, 70]. Similarly, Bitglass found that 60% of remote workers used unsecured personal devices to access work networks, significantly amplifying security risks [28]. The Black Hat USA 2020 Survey highlighted that 72% of CISOs reported an increase in cyber threats since the onset of the pandemic, and IBM Security noted a 20% rise in ransomware attacks due to remote work practices [28].

The dynamic nature of remote work, with employees accessing organizational networks and sensitive data from diverse locations, necessitates robust cybersecurity measures to prevent breaches, unauthorized access, and malicious activities [21]. Failure to address these vulnerabilities can result in severe consequences, including financial losses, reputational damage, and operational disruptions. High-profile cases illustrate the potential risks: Zoom faced incidents of "Zoom-bombing," while SolarWinds and Microsoft suffered data breaches directly linked to remote work environments [15, 34, 50, 61].

This systematic literature review investigates the intersection of remote work and cybersecurity, focusing on the unique risks posed by remote work environments and remote employees. By analyzing existing research, the study aims to identify cybersecurity challenges, propose mitigation strategies, and provide actionable recommendations for enhancing security protocols in remote work settings. As remote work continues to redefine the future of work, comprehensively addressing its cybersecurity implications is vital for maintaining the resilience and integrity of modern organizations.

The primary research question examines the impact of remote work on an organization's cybersecurity posture, specifically exploring how this shift has influenced vulnerabilities and the effectiveness of existing measures. The objectives of this review include analyzing the cybersecurity challenges associated with remote work, identifying best practices for risk mitigation, and developing insights for maintaining robust cybersecurity protocols. Key areas of focus include employee awareness, technological safeguards, and policy development. This review contributes to a nuanced understanding of the interplay between remote work and cybersecurity practices, providing a foundation for informed decision-making in securing remote work environments.

2 Methodology

This section outlines the systematic methodology adopted to ensure the rigor, transparency, and replicability of the literature review. Guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, the study followed a structured and multi-phased approach to identify, select, appraise, and synthesize relevant literature on cybersecurity risks in remote work environments. Each stage of the process—from article identification to quality assessment and thematic synthesis—was designed to ensure comprehensive coverage and methodological integrity. The following subsections detail the specific methods used in executing this review.

2.1 Systematic literature review framework

The systematic literature review (SLR) conducted in this study was guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology, an evidence-based approach for conducting and reporting systematic reviews [49]. PRISMA provides a structured process to ensure the rigorous inclusion of relevant and high-quality research. The study selection process is visually represented in the PRISMA flow diagram (Fig. 1), detailing the four key phases of identification, screening, eligibility, and inclusion [44, 62].

In the identification phase, a total of 1042 records were initially retrieved from major academic databases including IEEE Xplore, Scopus, ScienceDirect, Google Scholar, and ACM Digital Library. After removing 81 duplicate records, 496 articles remained for further consideration. During the screening phase, titles and abstracts of the remaining 415 articles were evaluated based on predefined inclusion and exclusion criteria (see Sect. 2.2). Non-peer-reviewed, non-English, and irrelevant studies were excluded. Screening was performed independently by multiple reviewers, with discrepancies resolved through discussion, resulting in the exclusion of 287 articles. This left 128 studies for the eligibility phase, where full-text analysis was conducted to assess relevance to cybersecurity in remote work. At this stage, 108 articles were excluded for lacking empirical focus or

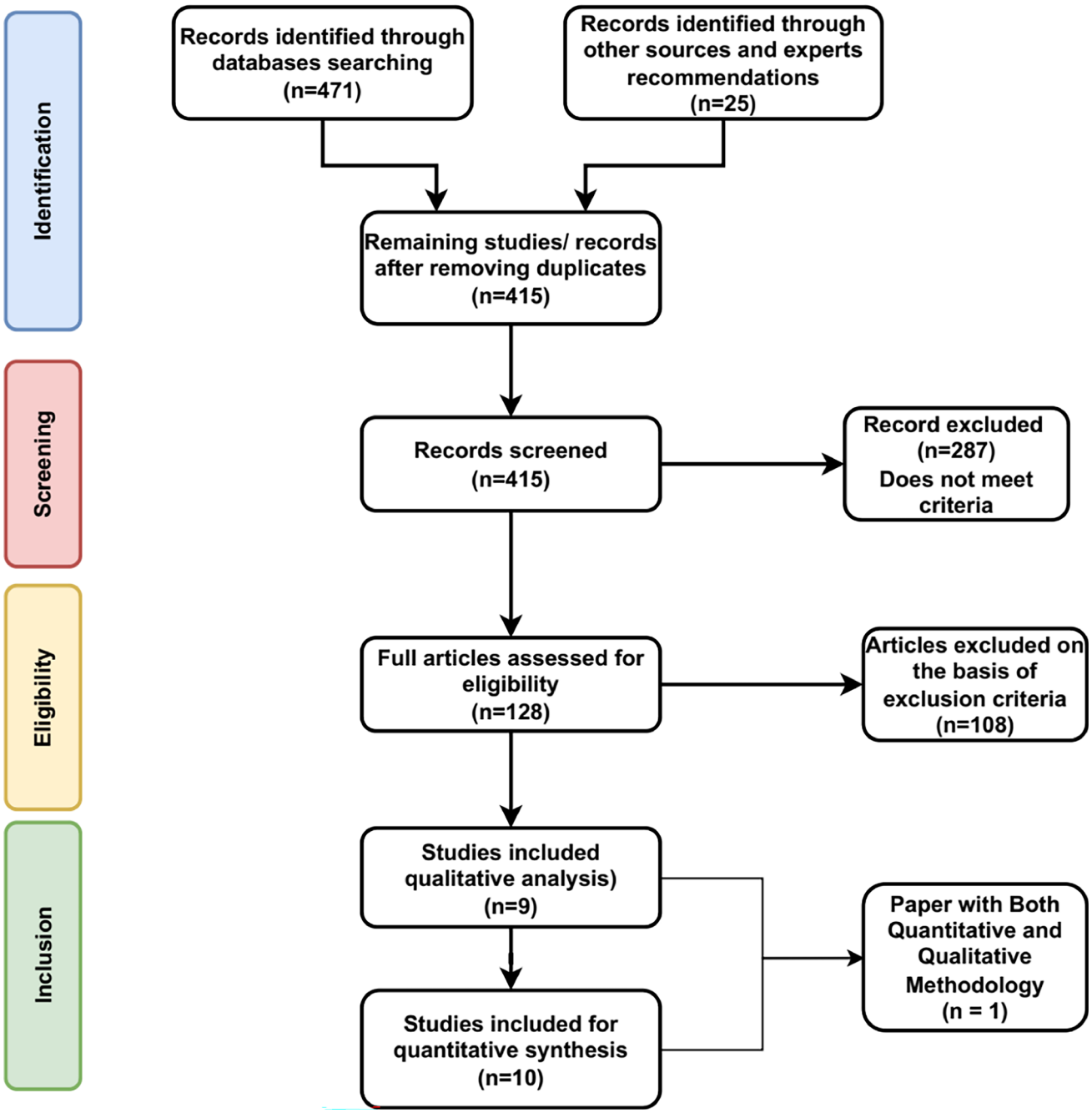

Fig. 1 PRISMA flow chart for the SLR

alignment with the research objectives. Finally, in the inclusion phase, 20 studies were deemed eligible and included in the review: comprising 9 qualitative studies, 10 quantitative studies, and 1 mixed-method study. This rigorous multi-phase process ensured methodological transparency, analytical robustness, and comprehensive coverage of the relevant literature.

It is pertinent to mention that while SLRs often emphasize qualitative synthesis, this review incorporated 10 quantitative studies to enrich the analysis with empirical, statistical insights. Given the complex nature of cybersecurity threats in remote work, quantitative research offers critical data on incident prevalence, employee behavior metrics, and organizational readiness. Following recommendations from Kitchenham et al. [41] and Grant & Booth [29], this mixed

Table 1 Summary of extracted screened records from different research databases

Database	Number of records
Scopus	28
Google Scholar	349
IEEE Explorer	45
ScienceDirect	49
Experts Recommendations	25
Total	496

evidence synthesis enhances both analytical rigor and practical applicability.

2.2 Search strategy and database selection

The comprehensive literature search strategy was meticulously designed to identify relevant academic articles, conference proceedings, and industry reports focusing on the intersection of remote work and cybersecurity across four databases: IEEE Xplore, Scopus, Google Scholar and Science Direct. A diverse set of keywords and phrases were utilized using Boolean operators such as AND, OR, NEAR to combine key terms related to remote work and cyber security. The search string was included ("remote work" OR "telecommut*" OR “telework*” OR "work from home") AND ("cyber*" OR "information security" OR "security risk" OR “cyber risks”) AND ("attack" OR "threat" OR "compliance"). Other search string used were (“impact of cyber security” OR “effect of cyber security”) AND (“remote work” OR “work from home” OR “information security” remote work). The search was based on English languaged and limited to conference proceedings, per-reviewed journal and articales from 2010 to 2024 capturing trends of remote work the cyber security issues and vulnerbilities faced by remoted work or occurred as a result of remote work.

The search strategy was adapted to align with the requirements and search functionalities of prominent databases, including Scopus, Google Scholar, IEEE Xplore, and ScienceDirect, to ensure comprehensive coverage. Table 1 provides a summary of the records retrieved from each database, showcasing the breadth of sources considered in this review.

2.3 Inclusion and exclusion criteria

To maintain the academic rigor and relevance of the review, specific inclusion and exclusion criteria given in Table 2 below were established to guide the selection of literature. These criteria were designed to ensure that only studies directly relevant to cybersecurity within remote work contexts were considered.

Table 2 Inclusion and exclusion criteria for study selection

Inclusion criteria	Exclusion criteria
Peer-reviewed journal articles and conference papers published in English	Non-peer-reviewed sources such as books, blogs, editorials, and magazines
Studies published between 2010 and 2024 to capture the evolving relevance of remote work and cybersecurity	Articles outside the defined publication period
Articles that explicitly examine the impact of remote work on cybersecurity practices	Studies unrelated to cybersecurity in remote work (e.g., studies focused solely on software or unrelated infrastructure)
Studies providing detailed insights into cybersecurity risks, challenges, and mitigation strategies in remote work environments	Review papers, theoretical frameworks, and conceptual-only discussions were excluded
Empirical studies employing qualitative, quantitative, or mixed-method approaches	Duplicate records and studies focusing purely on technical aspects (e.g., protocol-level issues) without reference to the remote work setting were not considered

The timeframe 2010–2024 was selected to capture developments in remote work cybersecurity from early adoption of telework technologies through the rapid transformations induced by the COVID-19 pandemic [32]. The period also includes major post-pandemic shifts toward hybrid/ remote work [65, 73] and long-term cybersecurity planning, ensuring that both legacy risks and modern threats are adequately represented [9, 57].

Furthermore, these inclusion and exclusion criteria helped distill studies that offer actionable insights into the unique cybersecurity challenges posed by remote work environments. The final selection reflects a balance of methodological diversity and thematic relevance, supporting the robust synthesis of findings in the subsequent sections of this paper.

2.4 Quality assessment

To ensure methodological consistency and minimize bias, all 20 included studies were appraised using the Mixed Methods Appraisal Tool (MMAT), with qualitative studies further evaluated using the Critical Appraisal Skills Programme (CASP) checklist. MMAT is well-suited for mixed research designs and systematically evaluates study objectives, methodological alignment, data collection rigor, and the validity of findings [35, 36]. CASP provided an additional layer of assessment specifically for qualitative studies,

focusing on credibility, ethical consideration, and interpretative clarity [46, 68].

Out of the 20 studies assessed, 14 were rated as high quality (MMAT score ≥ 4.5), and 6 were rated as moderate (MMAT score $= 3.5$). High-rated studies demonstrated methodological robustness and clear alignment between research questions, methods, and outcomes. Moderate-rated studies often lacked transparency in sampling, ethical disclosure, or analytical rigor.

For qualitative papers, five studies received a High CASP rating ($\geq$ 8/10), highlighting strong methodological coherence and rich data analysis. Four studies were rated Moderate (6–7/10), primarily due to limited reflexivity and insufficient ethical reporting.

Together, MMAT and CASP offered a dual-framework approach that enhanced the transparency and reliability of the evidence base, aligning with PRISMA standards and reviewer recommendations for rigorous quality appraisal.

2.5 Risk of bais assessment

The Joanna Briggs Institute (JBI) Critical Appraisal Tools were employed to assess the methodological quality and potential risk of bias across the 20 studies included in this review. The JBI bias assessment considered several dimensions, including the appropriateness of the research aim, clarity of methodology, data analysis rigor, researcher influence, outcome transparency, and data integrity [51, 52].

The majority of studies, particularly those employing quantitative designs, demonstrated a low risk of bias due to consistent methodological structure and robust statistical evaluation. However, five qualitative studies exhibited a moderate risk of bias, primarily attributable to unclear ethical declarations and insufficient methodological detail.

These moderately rated studies were retained in the review due to their conceptual relevance and contribution to thematic depth. However, their findings were interpreted with appropriate caution during synthesis to mitigate the influence of potential bias.

2.6 Data extraction and synthesis

To ensure a rigorous and transparent synthesis of the selected studies, a structured data extraction and thematic framework analysis approach was employed. Following the final inclusion of 20 studies, a standardized data extraction form was developed to collect essential information, including study objectives, methodologies, sample characteristics, core findings, and cybersecurity risk themes relevant to remote work environments.

The analysis followed an inductive thematic coding process inspired by Braun and Clarke's [12] six-step framework: (1) familiarization with data, (2) initial coding, (3) searching for themes, (4) reviewing themes, (5) defining and naming themes, and (6) producing the final synthesis. All included studies were carefully read and coded independently using a spreadsheet-based matrix, where codes related to types of cyber threats (e.g., phishing, malware, insecure Wi-Fi), vulnerabilities (e.g., lack of awareness, BYOD practices), and mitigation strategies were identified.

To enhance consistency and reliability, thematic coding was applied uniformly across qualitative, quantitative, and mixed-methods studies. Quantitative findings, such as frequency statistics or compliance survey results, were not treated separately; instead, they were integrated into broader thematic categories alongside qualitative insights. This convergent synthesis approach allowed for the triangulation of qualitative narratives and statistical trends under unified themes, thus enriching the validity of the results [64, 75].

The thematic categories formed the basis of the narrative discussion in Sect. 3 and informed the structured presentation of results in Tables 3 and 4, which respectively synthesize qualitative and quantitative study outcomes. This integrative process ensured that both descriptive richness and empirical evidence were adequately captured to support a comprehensive understanding of cybersecurity risks in remote work environments.

3 Findings from the review

The shift to remote work has redefined organizational dynamics, introducing a complex interplay between digital technologies and cybersecurity. This transformation—particularly accelerated during the COVID-19 pandemic—exposed organizations to a myriad of vulnerabilities and challenges [6]. As businesses adapted to remote operations, the accelerated adoption of technology often outpaced cybersecurity measures, leaving organizations exposed to risks. This section presents a detailed analysis of the cybersecurity challenges arising from remote work and their implications for organizational security practices.

3.1 Cyber risks, threats, and vulnerabilities due to remote work and its impact on organizational cybersecurity

The analysis of the 20 selected studies revealed a wide array of cybersecurity risks stemming from the evolving nature of remote work environments. These risks have been systematically categorized into three overarching dimensions to enable a structured exploration: (1) human factors contributing to cyber threats, (2) technical and infrastructural vulnerabilities, and (3) organizational and cultural weaknesses. This section presents the key findings from the reviewed literature, highlighting how these categories interconnect to shape

Table 3 Synthesis of findings from the qualitative studies in the area of remote work environment

Year and author	Objectives of the study	Core findings	Comparative analysis	Theoretical implications	Managerial implications	Future research directions
Borkovich and Skovira [10]	This study explores the cyber risks and rewards to businesses and individuals when employees work from home and further offers recommendations to curb and mitigate these nefarious cyber influences upon teleworkers and their organizations	Explored the shift in cybersecurity paradigms due to WFH	Focus on paradigm shift complements other studies	Reflects on the adaptability of cybersecurity frameworks	Adapt cybersecurity frameworks to new work paradigms	Adaptability and resilience of cybersecurity frameworks in the corporate world
Eiza et al. [21]	Identify risks of work from home and recommend framework for Securing home network	Presented a comprehensive at @Home cybersecurity framework	Comprehensive approach similar to Sebastian's plan	Framework supports layered security theory	Implement @Home cybersecurity framework proposed by the author	Framework's adaptability to different IT environments
Faisal and Ismail [22]	Examine the effect of work from home and threat of cybercrimes	Highlighted the need for secure devices and robust authentication	Focuses on device security, aligning with Sebastian	Significance of device management and user authentication	Implement policies for secure device usage and authentication	Impact of device security on cybersecurity posture
Jason et al. [40]	Analyzing cybersecurity and privacy concerns raised from remote work	Detailed analysis of evolving cybersecurity threats	Comprehensive threat analysis performed by the authors	Supports the dynamic nature of cybersecurity threat landscape	Update cybersecurity policies to address new threats like APTs, ransomware	Emerging threats in post-COVID remote work must be
Sebastian [66]	Measure the awareness in employees on the proliferation of cyber-attacks, increased by the work from Home Effective methods to proactively detect and mitigate cyber risks are recommended so these attacks do not obstruct the work-from-home environment	Introduced an 8-step WFH cyber-attack mitigation plan	More structured and detailed approach than others mentioned in this research	Illustrates adaptive security model which is theoretically sound	Management/ Professionals have to Adopt 8-step plan as a comprehensive framework to counter the cyber issues resulted from remote work	Effectiveness of this across industries will have to be analyzed

Table 3 (continued)

Year and author	Objectives of the study	Core findings	Comparative analysis	Theoretical implications	Managerial implications	Future research directions
Bispham et al. [8]	Exploring implication of shifting to work from home focusing on cybersecurity concerns	Balanced view on cybersecurity challenges and opportunities	Contrasts with the generally problem-focused literature	Proposes a dual-factor theory of cybersecurity	Leverage cybersecurity as an enabler for remote work with the implementation of cybersecurity measures and best practices	Exploring positive impacts of cybersecurity measures in the context of remote work context
Alotibi and Abdulwahid [4]	Investigate cybersecurity issues and challenges face in Saudi Arabia in remote work and explorer current state of work in COVID pandemic	Insights into region-specific cybersecurity challenges	Adds a geographical dimension to the discussion	Highlights the importance of context in cybersecurity	Tailor cybersecurity strategies to regional characteristics and organization culture	Cross-cultural studies on cybersecurity in remote work are required
Treacy et al. [76]	Explore cybersecurity risk from remote work and mitigation strategies	Emphasized strategic planning in cybersecurity post-pandemic	Strategic focus differentiates from operational emphasis in other studies	Aligns with strategic management theories	Integrate cybersecurity into organizational strategic planning	Long-term strategic cybersecurity planning have to be focused on
Rakha [61]	Exploring the legal implications and international best practices to ensure cyber-security in remote workers	Outlined international legal frameworks and compliance issues	Legal perspective adds a new dimension	Bridges cybersecurity practices with legal compliance	Ensure compliance with international cybersecurity laws and standards	Legal challenges in evolving cybersecurity landscape

the cybersecurity landscape in remote work contexts. Each thematic category is explored in detail to uncover the specific mechanisms through which cyber risks emerge, escalate, and persist in decentralized digital work environments:

3.1.1 Human factors

The first-dimension centers on human factors, which emerged as a dominant contributor to cybersecurity vulnerabilities in remote work settings. These factors encompass behavioral, psychological, and procedural issues that compromise digital security. From a lack of awareness and social engineering susceptibility to the misuse of remote autonomy and poor personal cyber hygiene, human-centered risks were found to be deeply entrenched in the remote work paradigm. The sub-sections below analyze these issues in detail, providing insights into how individual behaviors and cognitive biases shape the overall cyber risk posture of organizations.

3.1.1.1 Social engineering

Social engineering has emerged as a prominent attack vector in remote work environments, leveraging the human factor to exploit organizational vulnerabilities [3, 22]. These attacks manipulate remote employees through deceptive tactics, compelling them to disclose sensitive information or perform actions that compromise organizational security [8, 61, 66].

Research by Basit and Zafar [7] underscores the increasing use of personalized and context-specific social engineering strategies. Cybercriminals exploit publicly available information from social media and professional networks to design highly tailored spear-phishing and pretexting attacks. These methods align closely with the employee's work responsibilities or personal interests, increasing their plausibility and making them more difficult to detect.

The isolated nature of remote work further exacerbates this threat. Hijji and Alam [33] observe that cybercriminals capitalize on the reduced real-time communication between colleagues to create urgent or persuasive scenarios.

Table 4 Synthesis of findings from the quantitative studies in the area of remote work environment

Year and author	Sample	Objectives of the study	Core findings	Comparative analysis	Theoretical implications	Managerial implications	Future research directions
Clear [13]	378 firms including ('Media', 'Logistics', 'Internet Services' and 'Food Processing')	Investigate data security concerns among SMEs with increased electronic mediation in business processes	Found varying practices in data security, policy, and training across sectors and firm sizes, with a general lack of comprehensive security measures	Contrasts with later research like Atstāja et al. [6], showing an evolution in the understanding and implementation of cybersecurity measures in organizations	Indicates an early recognition of the cybersecurity challenges faced by SMEs, contributing to the discourse on organizational cybersecurity maturity	Points to the need for SMEs to adopt more robust and comprehensive data security measures, considering the evolving cyber threat landscape	Future studies might examine the progress in SMEs' cybersecurity practices and the impact of regulatory changes
Sandamali [63]	178 respondents	Investigate the impact of Information Security Policies (ISP) on the productivity of remote-working software professionals	Factors like additional work due to policy compliance, policy complexity, and general awareness about security significantly affect productivity	This study focuses on the intersection of remote work, ISP, and productivity, offering a unique angle compared to broader studies on remote work's impact on organizational culture or performance metrics	Highlights the need for nuanced ISP that consider remote work contexts and their unique challenges and opportunities	Suggests tailoring ISPs to the remote work environment to enhance productivity without compromising security	Conduct focused studies on regions with limited sample access, such as Africa. Explore the impact of ISPs in government/public and semi-government sectors and integrate qualitative research and technical aspects to enhance remote work productivity without compromising security

Table 4 (continued)

Year and author	Sample	Objectives of the study	Core findings	Comparative analysis	Theoretical implications	Managerial implications	Future research directions
Atstāja et al. [6]	313 remotely working respondents	Explore the impact of the COVID-19 pandemic on cybersecurity risks and challenges in remote work	Identified tailored cyber risk management practices among organizations based on industry specifics, information nature, employee skills, and pre-pandemic investments	This study emphasizes tailored risk management strategies, contrasting with literature that often advocates for uniform security measures across industries	Highlights the need for flexible cybersecurity frameworks that account for diverse organizational needs and contexts	Suggests that managerial practices should be adaptive, considering the specific cybersecurity needs and pre-existing conditions of the organization	Further research could explore the effectiveness of tailored versus standardized cybersecurity approaches in various industries
Fritzen [24]	59 participants	Discuss the cybersecurity threats associated with remote work in Ireland, emphasizing IoT device security	Highlighted the need for new security measures and training, particularly for IoT devices, to address vulnerabilities introduced by remote work	Fritzen's focus on IoT devices adds a specific technological angle to the broader discussion on remote work security challenges, similar to studies like Lindroos et al. [45] that examine specific security aspects like WLAN	Reinforces the notion that cybersecurity challenges in remote work extend beyond traditional network security, requiring a focus on IoT and other emerging technologies	Suggests that organizations should develop targeted training and security measures for remote workers, particularly addressing IoT security	Future research could delve into the development and implementation of IoT-specific cybersecurity training for remote workers
Koski [42]	6 interviews from construction, energy, IT, finance, and education departments	Investigate the effects of increased remote work on phishing threats and the role of new technologies	Identified a general increase in phishing attacks with the rise of remote work, exacerbated by new technologies and user confusion	Koski's emphasis on phishing and technology contrasts with studies like Downer and Bhattacharya [20], which focus more on policy and human factors, showcasing the multifaceted nature of cybersecurity challenges	Underscores the evolving nature of cyber threats, particularly phishing, in the context of remote work and technological advancements	Indicates that organizations need to adapt their cybersecurity training to address the specific threats and challenges posed by new technologies and remote work environments	Calls for research into effective anti-phishing strategies and the role of technology in mitigating cyber threats in remote work

Table 4 (continued)

Year and author	Sample	Objectives of the study	Core findings	Comparative analysis	Theoretical implications	Managerial implications	Future research directions
Georgiadou et al. [26]	264 participants from 13 European countries	Evaluate cybersecurity culture readiness of organizations during COVID-19, focusing on teleworking	Found varying levels of information security readiness and resilience among individuals and organizations, leading to specific cybersecurity recommendations	This study's focus on cybersecurity culture complements the technological and policy-focused perspectives in the literature, offering a more holistic view of organizational cybersecurity readiness	Highlights the critical role of cybersecurity culture in enhancing organizational resilience against cyber threats, especially in remote work settings	Emphasizes the need for organizations to develop and promote a strong cybersecurity culture, alongside technological and policy measures	Suggests further exploration into the components and development of effective cybersecurity cultures in diverse organizational contexts
Georgiadou et al. [27]	264 participants from 13 European countries	Assess the cybersecurity culture readiness of organizations during COVID-19	Significant variations in cybersecurity readiness across industries, with many employees lacking proper guidelines	Compared to Sandamali [63], this study broadens the scope to organizational readiness and culture, emphasizing the need for comprehensive guidelines and training in cybersecurity for remote workers	Emphasizes the importance of a robust cybersecurity culture and readiness in the context of the increasing trend of remote work	Highlights the need for enhanced training and clear cybersecurity guidelines for remote workers	Examine security adjustments in various business domains towards a virtual office. Focus on individual security characteristics like behavior, attitude, awareness, and compliance, aiming to quantify these qualitative indicators
Lindroos et al. [45]	7 experiment-based surveys	Analyze the impact of the COVID-19 pandemic on WLAN security in Southwest Finland	Despite a significant increase in WLAN deployment, there was no notable improvement in security, highlighting a lack of awareness	This study's specific focus on WLAN security provides a technological perspective that complements broader discussions on remote work cybersecurity, such as the cultural and policy aspects explored by Georgiadou et al. [26]	Contributes to the understanding of how pandemics and mass shifts to remote work can affect specific aspects of cybersecurity, like WLAN security	Suggests a need for increased awareness and education on WLAN security to prevent cybercrime, particularly in the context of widespread remote work	Future research could investigate the effectiveness of different strategies to raise WLAN security awareness among the general population and within organizations

Table 4 (continued)

Year and author	Sample	Objectives of the study	Core findings	Comparative analysis	Theoretical implications	Managerial implications	Future research directions
Nwankpa and Datta [56]	203 remote workers across the US	To explore the impact of remote work on cybersecurity awareness and precaution-taking among employees using the Peltzman Effect and complacency framework	Remote working is positively associated with cybersecurity awareness and the adoption of security precautions. Information security policy compliance moderates the effect of remote working on cybersecurity awareness	Not directly provided, but the study contributes to the understanding of cybersecurity behaviors in remote work settings	Reinforces and complements current theoretical frameworks on security-precaution behaviors	Highlights the critical role of information security policies in promoting cybersecurity awareness and behaviors among remote workers. Emphasizes the need for organizations to ensure these policies are well communicated and enforced	Investigate the long-term impacts of remote work on cybersecurity behaviors and the effectiveness of various policy interventions in different organizational contexts
Radu et al. [60]	857 participants including managers and non-managers from a large insurance company	Explore the perception of remote work, its effect on work performance, and the moderating role of psychological safety post-pandemic	Remote work sentiment is more favorable in non-sales fields and among employees who work remotely often. Psychological safety strengthens the positive relationship between remote work sentiment and work performance	This research adds to the body of knowledge by integrating psychological safety as a moderating factor, which is less explored in the works of Sandamali [63] and Georgiadou et al. [26, 27]. The focus on post-pandemic insights provides contemporary relevance	Advances understanding of the complex dynamics between remote work sentiment, psychological safety, and work performance	Urges the consideration of employee well-being and psychological safety in remote work policies to boost performance	Investigate specific conditions under which remote work benefits both employees and organizations, focusing on psychological well-being and performance. Explore strategies to enhance psychological safety and support for remote workers

Table 4 (continued)

Year and author	Sample	Objectives of the study	Core findings	Comparative analysis	Theoretical implications	Managerial implications	Future research directions
Senapati and Bharathi [67]	A total of 150 respondents (73% IT employees and 27% non-IT sector). Currently Remote working (59%), Previous remote work experience (41%)	To identify the significant factors impacting cybersecurity compliance among home-based workers during the pandemic, focusing on human internet habits, video conferencing security, and awareness of cyber threats	Human internet habits, secure video conferencing practices, and awareness of cybersecurity best practices positively correlate with compliance to cybersecurity best practices. Organizational guidelines and security policies do not significantly impact cybersecurity compliance	Not directly provided, but the study highlights the significant factors influencing cybersecurity compliance in remote work settings	Suggests a reevaluation of the traditional beliefs regarding the impact of organizational guidelines and security policies on employee cybersecurity compliance	Indicates a need for organizations to focus more on individual employee behaviors and awareness rather than solely on top-down policy enforcement. Urges a shift towards more personalized cybersecurity training and awareness programs	Further exploration into why organizational guidelines and security policies do not significantly impact employee cybersecurity compliance and awareness

For instance, employees may bypass established verification procedures when responding to seemingly legitimate but fraudulent requests, as highlighted by the Australian Cyber Security Centre [2].

Mitigating social engineering risks requires a multifaceted approach, including regular cybersecurity awareness training, simulated phishing exercises, and fostering a culture of skepticism where employees verify requests through established channels before acting on them.

3.1.1.2 Lack of awareness about the risk of remote work

Employee awareness of cybersecurity risks remains a critical weakness in the remote work model. Studies by Fritzen [24] and Nwankpa & Datta [56] indicate that a significant proportion of cyberattacks originate from actions by remote workers who are unaware of the risks associated with their behaviors. These include clicking on malicious links, accessing untrusted websites, and inadvertently sharing sensitive personal or organizational information [8, 40].

The lack of familiarity with secure remote working practices has further exacerbated these risks. Devices infected with malware through home networks are often connected to corporate systems, introducing vulnerabilities that undermine an organization's cybersecurity culture [40]. Atstāja et al. [6] point to the widespread inability of remote workers to identify phishing attempts, comprehend the implications of using unsecured networks, or recognize the risks of unauthorized data sharing. This emphasizes the urgent need for continuous, tailored cybersecurity training programs. Such initiatives should focus on equipping employees with the skills to identify and mitigate potential risks while reinforcing a culture of cybersecurity awareness across the organization.

3.1.1.3 Exploitation of trust in remote environment

The trust placed in employees working remotely has inadvertently introduced significant cybersecurity risks. Remote work environments often include shared spaces with individuals who may not be trusted by the organization, increasing the risk of unauthorized access to sensitive corporate data and systems [6]. Malicious actors exploit this trust to manipulate employees and compromise organizational security [21, 40].

A report by Kroll [48] emphasizes the heightened risks associated with misplaced trust in remote work scenarios. The report highlights cases where employees, untrusted individuals, or even poorly vetted third-party security tools inadvertently created vulnerabilities, enabling malicious actors to gain unauthorized access to corporate networks and sensitive data. This underscores the critical need for robust trust management frameworks, including rigorous access controls and verification mechanisms, to mitigate the exploitation of trust in remote work environments.

3.1.1.4 Misuse of remote work autonomy

The autonomy afforded to remote workers in managing organizational resources introduces significant cybersecurity challenges. Without the immediate oversight present in traditional office settings, employees may misuse corporate data, resources, or services, leading to potential security breaches and compliance violations [8].

Crossland et al. [16] discuss how the lack of direct supervision in remote work environments enables risky behaviors, such as using unsecured networks or installing unauthorized software. These practices expose organizations to data breaches and increase their vulnerability to internal and external threats. The study underscores the importance of implementing effective monitoring mechanisms and establishing clear policies to govern the responsible use of corporate resources. These measures are critical for mitigating the risks associated with remote work autonomy while maintaining a secure operational environment.

3.1.1.5 Bad actors' access to enterprise resources

Remote workers' access points have become a prime target for malicious actors seeking entry into enterprise systems. The shift to remote work has introduced vulnerabilities that attackers exploit, often gaining access to internal systems due to inadequate authentication mechanisms. Mistakes by remote employees, such as weak passwords or insecure Wi-Fi usage, increase the risk of unauthorized access, further exposing critical resources, including networks, databases, and organizational infrastructure [22, 66].

A study by Hadlington [30] highlights the growing sophistication of attacks targeting remote access systems. Many breaches occur due to the absence of robust authentication processes, such as multi-factor authentication (MFA). Hadlington also emphasizes the role of user behavior, noting that simple oversights, such as sharing credentials or using outdated systems, significantly contribute to organizational vulnerabilities. To address these challenges, organizations must prioritize implementing continuous monitoring, MFA, and advanced endpoint protection strategies to detect and mitigate unauthorized access attempts [30, 45].

3.1.1.6 Lack of remote work security training

The rapid transition to remote work necessitated by the COVID-19 pandemic left many organizations unprepared to provide comprehensive cybersecurity training for their remote workforce. This lack of preparation created a significant vulnerability, as employees operating in remote environments without sufficient training became prime targets for cybercriminals [24]. Poor security practices and a lack of awareness about potential threats amplify the risk of cyberattacks, ultimately jeopardizing organizational security [6, 8].

Recent studies underscore the inadequate efforts made to equip remote workers with the knowledge and skills

to mitigate cyber risks effectively. Borkovich and Skovira [10] identified a systemic failure in implementing structured security training programs during the hurried adoption of remote work models. This gap has resulted in a workforce that is unprepared to address the unique cybersecurity challenges associated with remote work. The authors advocate for integrating regular, interactive, and scenario-based training modules to ensure employees remain vigilant against evolving cyber threats [30, 71].

3.1.2 Technical and infrastructural vulnerabilities

In addition to human-centered risks, the review identifies a significant array of technical and infrastructural vulnerabilities that affect the cybersecurity integrity of remote work environments. These risks stem from insecure access points, misconfigured devices, open communication protocols, and under-secured network configurations. Remote work necessitates expanded digital infrastructure, often adopted hastily or without adequate oversight, thereby introducing systemic weaknesses. This section discusses the technical pathways exploited by malicious actors—including phishing, malware, insecure Wi-Fi, RDP exposures, and MITM attacks—and explores mitigation strategies supported by empirical studies.

3.1.2.1 Malware, phishing attacks and distractions Remote work has increased employees' exposure to phishing and malware attacks, largely due to the blurred boundaries between work and personal obligations. Home environments—characterized by informal settings, distractions, and competing priorities—increase susceptibility to such threats [6, 76]. Family responsibilities and the presence of cohabitants contribute to reduced vigilance, making employees more prone to cyberattacks, particularly phishing attempts [8, 40, 66].

Phishing attacks have notably escalated with the rise of remote work, as cybercriminals exploit current events and remote work tools to deceive users. Alkhalil et al. [3] reported a significant increase in phishing campaigns targeting communication platforms like Zoom and Microsoft Teams. These attacks often involve emails containing malicious links or attachments, which can compromise systems when accessed via less secure home networks. The lack of robust IT oversight in home setups exacerbates these vulnerabilities.

The use of personal devices for professional purposes further augments these risks. Personal devices are often less secure and susceptible to malware, particularly when used for both work and personal activities. As highlighted by Din [18], downloading unauthorized applications or visiting non-work-related websites on work-used devices can inadvertently introduce malware into corporate systems. Curran [17] further emphasizes that this dual usage of devices creates pathways for cyber threats, undermining organizational security.

The rapid deployment of remote work technologies also contributes to the problem. Confusion among employees regarding new tools and protocols has been linked to increased phishing susceptibility, as noted by Koski [42]. This, coupled with a lack of sufficient training on identifying phishing attempts, leaves remote workers particularly vulnerable.

Distractions in home environments present an additional layer of risk. Informal settings, such as working from a living room or kitchen, reduce employee focus and vigilance. As highlighted by Jalali et al. [39], divided attention caused by family responsibilities or interruptions increases the likelihood of employees engaging with malicious emails or links. In the absence of a structured work environment, remote employees are less likely to exercise the level of caution typically maintained in office settings.

3.1.2.2 Cross site scripting (XSS) Cross-site scripting (XSS) attacks present a critical cybersecurity threat for remote workers who frequently access organizational websites and portals over the Internet. These attacks involve the injection of malicious scripts into legitimate web applications, enabling attackers to steal user credentials or redirect employees to fraudulent websites masquerading as trusted organizational platforms [61].

The sophistication of XSS attacks has evolved significantly, as noted in the work of Quyen [59]. Attackers increasingly exploit vulnerabilities in web applications used by remote employees, bypassing conventional security measures and executing scripts within users' browsers. Once executed, these scripts grant unauthorized access to sensitive organizational data. Additionally, attackers employ refined social engineering techniques to lure remote workers into accessing compromised websites, deploying XSS payloads covertly.

Given the proliferation of web-based applications in remote work environments, the threat posed by XSS attacks is significant. This necessitates the implementation of advanced security measures, including input validation, content security policies (CSPs), and robust user authentication protocols to mitigate the risks associated with XSS vulnerabilities.

3.1.2.3 DoS and DDoS attack Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks have emerged as significant threats to organizations in remote work environments. DoS attacks overwhelm organizational resources, rendering employees unable to access critical systems. Malicious actors exploit remote systems connected to the organization's network, using them as conduits for launching large-scale DDoS attacks. These attacks flood

target systems with excessive requests, severely impacting resource availability and disrupting business operations [8, 61].

Recent findings by Yoachimik and Pacheco [79] from Cloudflare illustrate a sharp rise in sophisticated botnets employed for DDoS attacks, with remote workers' systems increasingly being leveraged as attack vectors. These incidents frequently exploit the vulnerabilities of home networks, which often lack enterprise-grade security measures. The study highlights the growing need for advanced network security strategies, such as deploying distributed denial-of-service protection services, traffic anomaly detection, and proactive threat mitigation techniques to ensure uninterrupted access to organizational resources.

3.1.2.4 Privileges escalation through open RDP ports The use of Remote Desktop Protocol (RDP) for remote access has become a necessity for organizations; however, it also introduces significant vulnerabilities. Open RDP ports are often exploited by attackers for ransomware campaigns and privilege escalation attacks. When improperly secured, these ports can serve as entry points for cybercriminals to gain unauthorized access to organizational systems [8, 76].

Li [43] underscores the dual nature of RDP as both a critical tool for remote work and a potential cybersecurity risk. The study reveals that attackers often exploit weak authentication mechanisms or misconfigured RDP settings to escalate privileges and execute ransomware attacks. To mitigate these threats, Li recommends the implementation of multi-factor authentication (MFA), the use of strong passwords, and regular monitoring of RDP sessions for anomalous activity. Proactive network segmentation and limiting RDP access to authorized users are also crucial strategies to prevent exploitation.

3.1.2.5 Unsecure wi-fi and internet connection The reliance on home Wi-Fi networks for remote work introduces considerable cybersecurity risks. Many home networks lack the advanced security features found in corporate environments, making them vulnerable to attacks such as eavesdropping, data interception, and unauthorized access [45]. Remote employees' use of unsecured Wi-Fi routers for official tasks further exacerbates the risk of malware infiltration and data breaches [76].

Bispham et al. [8] identify unsecured Wi-Fi connections as a persistent vulnerability in remote work setups. Cybercriminals often exploit weak encryption protocols or default router configurations to gain unauthorized access to devices and sensitive data. Studies by Lindroos et al. [45] and Thankappan et al. [74] advocate the use of virtual private networks (VPNs), stronger encryption protocols such as WPA3, and periodic security audits of home networks as effective countermeasures. Educating employees on secure Wi-Fi practices is equally essential to mitigate these risks.

3.1.2.6 Risks due to the use of personal devices for official work and official devices for personal work The use of personal devices for official tasks and vice versa has introduced significant cybersecurity vulnerabilities in remote work environments. Remote employees often use personal devices to access corporate networks, while employer-provided devices are frequently utilized for personal activities, such as emailing, browsing, and accessing social media platforms [6, 40]. This dual-purpose usage significantly increases the risk of malware infections and unauthorized access, as devices may be exposed to untrusted websites or insecure online content [24].

The practice of interchanging devices between personal and professional use undermines traditional best practices that prohibit personal device usage within corporate networks [22]. The introduction of unverified applications or interactions with malicious content can create entry points for cybercriminals to compromise both individual devices and the broader organizational network. Addressing this challenge necessitates strict policies prohibiting dual-purpose device usage, advanced endpoint security measures, and robust monitoring protocols to prevent unauthorized access and ensure the security of organizational data.

3.1.2.7 Risk of stolen or compromised devices Remote work environments, characterized by less-controlled settings, significantly heighten the risk of device theft or compromise. Unlike office settings, where physical security is enforced, remote work often involves shared or unsecured living spaces that increase the likelihood of device theft [25, 40]. Devices lost or stolen without adequate security measures—such as encryption or remote wiping capabilities—pose a severe risk, as they may grant unauthorized access to sensitive corporate data.

George [25] underscores the vulnerability of devices used in remote work setups, highlighting that unencrypted or inadequately secured devices are prime targets for cybercriminals. To mitigate these risks, organizations must implement comprehensive device security measures, including robust encryption protocols, secure boot processes, and the capability for remote wiping of data in the event of device loss or theft. Additionally, educating employees on secure device handling and reporting protocols is critical to minimizing the likelihood of compromised organizational assets.

3.1.2.8 Man in the middle attack Remote work environments inherently heighten the risk of man-in-the-middle (MITM) attacks due to their reliance on remote connections.

These attacks involve adversaries intercepting communication and data traffic between remote workers and organizational systems, compromising sensitive data and jeopardizing internal security [61].

MITM attacks often exploit insecure Wi-Fi networks, particularly those using outdated encryption protocols or lacking essential security updates [45]. A study by Thankappan et al. [74] reveals that remote employees frequently connect to public or inadequately secured home networks, providing cybercriminals with opportunities to intercept or manipulate communication channels. Such breaches can lead to corporate espionage, data theft, or significant operational disruptions.

Additionally, attackers increasingly target vulnerabilities within virtual private networks (VPNs), widely adopted by remote workers for secure connections. Abbas et al. [1] detail how cybercriminals exploit weaknesses in VPNs, particularly during the handshake process, to intercept encrypted data streams. This demonstrates the evolving sophistication of MITM techniques.

Modern MITM attacks now extend beyond passive data interception to include active manipulation of communication. Attackers may inject malicious payloads or redirect users to fraudulent websites, amplifying the scope and impact of these breaches. This necessitates the adoption of robust mitigation strategies, such as end-to-end encryption, advanced intrusion detection systems, and continuous monitoring of network traffic for anomalies.

3.1.3 Organizational and cultural weaknesses

The final dimension of analysis focuses on organizational and cultural weaknesses that underpin systemic vulnerabilities in remote work cybersecurity. These include inadequate policy implementation, rushed technology adoption, lack of structured security training, and legal non-compliance. Organizational responses to remote work have often lagged behind technological shifts, leading to fragmented governance and shadow IT practices. This section evaluates how weak cybersecurity culture, ambiguous guidelines, and ineffective communication systems contribute to persistent security risks in distributed workforces.

3.1.3.1 Reduced access to information and knowledge The remote work paradigm disrupts the natural flow of information and collaborative problem-solving inherent in traditional office settings. Asynchronous communication channels have replaced face-to-face consultations, delaying employees' ability to seek guidance on security-related decisions. Georgiadou et al. [26, 27] highlight how the COVID-19 pandemic further exacerbated this issue, creating an environment where security lapses occur due to delayed access to timely information and uncertainty about appropriate security practices.

The shift from synchronous, in-person collaboration to asynchronous communication also hinders the dissemination of critical cybersecurity guidance. Studies by Alsharif et al. [5] and Finnell [23] underscore the challenges employees face in accessing timely support, particularly when navigating cybersecurity protocols in remote work settings. To address these challenges, organizations must prioritize developing effective communication strategies and tools that provide immediate and clear guidance, thereby reducing the risks associated with delayed decision-making in security matters.

3.1.3.2 Risks due to rushed technology adoption and shadow IT The urgency of transitioning to remote work during the COVID-19 pandemic compelled organizations to adopt technology solutions rapidly, often without sufficient preparation or technological readiness [40, 42]. This hastened adoption resulted in the deployment of untested or inadequately vetted technologies, introducing vulnerabilities into organizational cybersecurity frameworks [22]. In parallel, shadow IT practices emerged as a significant risk factor, as employees circumvented established security protocols in favor of unsanctioned tools that offered perceived efficiency or convenience [14].

Shadow IT—defined as the use of unauthorized hardware, software, or platforms—has gained prominence in remote work setups, bypassing organizational oversight and increasing the risk of data breaches [22]. These practices undermine cybersecurity measures and compromise the integrity of organizational networks. Mitigating these risks requires comprehensive governance policies, employee training on authorized technology use, and proactive monitoring of shadow IT activities.

3.1.3.3 Legal and compliance challenges Remote work introduces a range of legal challenges for organizations, encompassing privacy breaches, non-compliance with regulatory frameworks, and liability issues. Non-adherence to legal and regulatory requirements such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), and other data protection laws exposes organizations to significant financial penalties, loss of customer trust, and potential legal action [61].

Recent studies underscore the increasing complexity of these legal risks. Data privacy breaches have risen in frequency, often due to unsecured networks, improper handling of sensitive information, or failure to adhere to established data management protocols. As employees operate in decentralized settings, organizations face heightened difficulty in ensuring consistent compliance with data protection mandates [38, 78]. Furthermore, there has been a marked increase in litigation related to remote work, indicating that legal risks

extend beyond regulatory non-compliance to include labor law violations and liability issues for remote workplace incidents.

3.1.3.4 Security issues with remote communication tools

The widespread adoption of remote communication tools such as Zoom and Microsoft Teams has exposed inherent vulnerabilities, creating opportunities for cyber attackers to exploit these platforms [6, 72]. Misconfigurations, outdated software, and inadequate security practices often serve as entry points for malicious actors to target these tools, leading to data breaches and compromised communications [8].

Suciu [72] emphasizes that the rapid expansion of remote communication platforms has outpaced the implementation of robust security measures. For example, cybercriminals have leveraged vulnerabilities in platform configurations and delays in software updates to launch targeted attacks. Misconfigured tools can bypass best cybersecurity practices, exposing sensitive organizational information to unauthorized access. To mitigate these risks, the study underscores the need for regular security audits, consistent updates, and employee awareness of secure usage practices. Such measures are critical to preserving the integrity of organizational cybersecurity amidst widespread reliance on these tools.

While Sect. 3.1 provided a categorized exploration of the specific cyber risks, threats, and vulnerabilities emerging from remote work, the following section delves deeper into the underlying factors that contribute to the manifestation of these risks. This transition from descriptive analysis to causal insight enables a more nuanced understanding of how human, technical, and organizational elements converge to shape cybersecurity outcomes in remote work environments.

3.2 Factors contributing to cyber risks in remote work: insights from review

As the remote work model becomes increasingly entrenched, particularly in response to global disruptions like the COVID-19 pandemic, the critical role of human behaviors, technological factors, and organizational practices in shaping cybersecurity vulnerabilities has gathered significant attention. This section synthesizes insights from a range of quantitative and qualitative studies, shedding light on how these factors collectively contribute to the cyber risks associated with remote work environments.

Atstāja et al. [6] underscore the importance of employee computer skills, coupled with pre-pandemic investments in cybersecurity and digital transformation, as critical determinants of an organization's cyber resilience. Their study demonstrates that deficiencies in these areas can significantly elevate cyber risks, especially in the context of rapid and unplanned transitions to remote work. Similarly, Fritzen [24] highlights the vulnerabilities posed by IoT devices in remote work setups, pointing to the absence of tailored security measures and training as a considerable oversight. This is further corroborated by Sebastian [66], who attributes many cybersecurity risks to a lack of employee awareness and preparedness.

The research by Georgiadou et al. [26, 27] provides a comprehensive perspective on cybersecurity readiness and culture within organizations during the COVID-19 pandemic. Their findings emphasize the interplay between individual and organizational security dimensions, highlighting how human factors influence overall cybersecurity posture. In a similar course, Koski [42] identifies user confusion and insufficient education on phishing threats as critical vulnerabilities arising from the rapid deployment of technology in remote work environments.

Sandamali [63] offers an alternate perspective by examining the implications of complex information security policies on employee productivity. The study reveals that overly intricate compliance requirements can impose additional workloads, detrimentally affecting employee performance and engagement. Complementing this, Georgiadou et al. [26, 27] uncover a concerning gap in employer-provided cybersecurity guidelines for remote workers, leaving employees ill-equipped to navigate evolving cyber threats.

The research by Senapati and Bharathi [67] delves deeper into human factors influencing cybersecurity compliance in remote work environments. Using empirical data from online surveys, the study identifies personal internet habits, video conferencing practices, and awareness of cybersecurity as key factors driving compliance with best practices. The study suggests that organizational guidelines and policies have limited influence on employee compliance or awareness, pointing to potential areas for further exploration and improvement.

Collectively, these studies provide a nuanced understanding of the multifaceted factors contributing to cyber risks in remote work settings, which can be summarized as follows:

Deficiencies in employee computer skills and insufficient pre-pandemic investments in cybersecurity and digital transformation.
Lack of targeted security measures and training for remote workers, particularly concerning IoT devices.
Inadequate cybersecurity readiness and culture within organizations, affecting both organizational and individual security dimensions.
User confusion and lack of education on phishing threats due to rapid technology deployment.
Complexity of information security policies and the additional workload imposed by compliance requirements, negatively impacting employee productivity.
Lack of cybersecurity guidelines provided by employers to remote employees.

Positive influence of personal compliance with security policies on the adoption of cybersecurity precautions.
Impact of personal internet and video conferencing habits, as well as awareness of recent cyberattacks, on cybersecurity compliance.
Poor security configurations in WLANs and VPNs, including weak Wi-Fi encryption protocols and the absence of regular network security audits.
Blurred security boundaries caused by the use of personal devices for official work and vice versa.
Lack of direct supervision, leading to potential misuse of company resources and engagement in unsafe cybersecurity practices.
Exploitation of trust in remote work environments, creating opportunities for malicious actors to breach organizational security.

These identified factors reveal systemic vulnerabilities in remote work practices, ranging from human errors to infrastructural shortcomings. Addressing these challenges is imperative to fortifying organizational cybersecurity and safeguarding critical assets in an era increasingly defined by remote work. Proactive measures, such as targeted training, simplified security policies, and improved network protections, are essential to mitigate these risks and ensure the operational integrity of remote work environments.

The findings presented in Sect. 3 offered a structured and detailed account of the key cybersecurity risks identified across the reviewed studies, categorized into human, technical, and organizational dimensions. These insights revealed the complex interplay between remote work environments and emerging cyber threats, shedding light on specific vulnerabilities, behaviors, and systemic gaps. However, to extract broader meaning and develop a more integrative understanding of the literature, it is essential to move beyond thematic categorization. Section 4 undertakes this task by synthesizing the reviewed studies across methodological types, evaluating the depth and scope of their contributions, and identifying converging insights, contradictions, and research gaps that inform the evolving discourse on remote work cybersecurity.

4 Synthesis of the literature

Synthesizing the extensive body of research on cybersecurity in remote work settings is essential for transforming complex information into actionable insights. The synthesis presented in Tables 3 and 4 contributes significantly to the existing body of knowledge on cybersecurity challenges in remote work environments. By meticulously extracting and consolidating the objectives, core findings, comparative analyses, theoretical and managerial implications, and future research directions from the included studies, this systematic review offers a unique and detailed overview of the domain. This effort facilitates a deeper understanding of the multifaceted risks associated with remote work and provides a robust foundation for developing informed strategies to enhance cybersecurity measures. By bridging the gap between academic research and practical application, the findings deliver critical insights for both scholars and practitioners navigating the complexities of remote work cybersecurity.

Table 3 synthesizes findings from qualitative studies in this domain. The synthesis provides valuable insights into the complexities of remote work-related risks and highlights informed approaches to improving the safety and efficiency of remote work practices.

Table 4 presents a detailed synthesis of quantitative research focused on identifying risks inherent to remote work environments. These studies employ diverse methodologies, including practical survey experiments, in-depth empirical interviews, and the analysis of firsthand data collected from remote work settings. The findings reveal the nature and scope of risks, contributing factors, and underlying causes, as well as potential mitigation strategies that can be employed effectively to address these risks.

The synthesis critically examines the multifaceted risks and strategies related to organizational cybersecurity within remote work contexts. Key observations emphasize the necessity of structured cybersecurity frameworks, the importance of secure device management, and the influence of organizational culture on cybersecurity efficacy. Additionally, the findings underscore the critical role of ensuring legal compliance and the need for organizations to adapt to the rapidly evolving cybersecurity threat landscape. This analysis provides a comprehensive overview for understanding and addressing the complex cybersecurity challenges posed by remote work environments.

The synthesis presented in Sect. 4 provided a comparative evaluation of the reviewed studies, highlighting convergent insights, methodological contributions, and recurring themes across qualitative and quantitative research. These synthesized findings reinforced the multifaceted nature of cybersecurity challenges in remote work environments and underscored systemic vulnerabilities arising from human behaviors, technological gaps, and organizational misalignments. However, identifying risks alone is insufficient in addressing the growing cyber threat landscape. The next section builds upon these insights to propose a structured set of cybersecurity strategies tailored to remote and hybrid work settings. It offers a forward-looking framework grounded in empirical evidence and theoretical implications, aimed at guiding organizations toward more secure, resilient, and adaptable remote work practices.

5 Strategizing cyber security in remote work or work from home environments: a way forward

The systematic review of the literature has highlighted a significant increase in remote work during the COVID-19 pandemic and the years after it, which necessitated a swift and unplanned transition to remote work environments. This transition underscored the urgency of secure implementation and cyber resilience measures [4, 6, 10, 40, 66, 77]. However, the rapid adoption of remote work practices led to a rise in cyberattacks, forcing organizations to confront challenges distinct from those encountered in planned remote work setups [28].

The cybersecurity risks associated with remote work include phishing emails, malware, compromised systems, and human factors such as negligence, digital skills gaps, lack of awareness, social engineering, use of personal devices, and unsecured private networks. These risks not only undermine organizational cybersecurity practices but also create legal consequences that further complicate the management of cyber risks.

Effectively addressing the extensive cybersecurity risks inherent in remote work environments necessitates the adoption of a multifaceted strategy. To foster a secure work-from-home ecosystem, the following strategies are being proposed:

- *Robust Cybersecurity Frameworks*: Organizations must implement structured frameworks for remote work that encompass policy development, risk identification, advanced cybersecurity controls (e.g., strong encryption protocols, secure WLANs and VPNs), and continuous monitoring. These frameworks are critical to maintaining a resilient cybersecurity posture [8, 21].
- *Comprehensive Training and Digital Literacy*: Enhancing employee digital literacy and cybersecurity awareness through targeted training programs is essential. Training should focus on key areas such as IoT device security, social engineering tactics, and phishing threat identification, thereby addressing risks associated with rapid technological deployment [6, 24, 42].
- *Policy Formulation, Compliance and Best Practices*: Developing well-structured information security policies that address compliance requirements while remaining actionable in day-to-day operations is vital. Ensuring these policies are balanced and practical can improve employee adherence and reduce the burden of compliance [56, 63].
- *Personal Behavior and Compliance*: Encouraging employees to adopt responsible internet and video conferencing habits, alongside a strong awareness of cybersecurity threats, reinforces best practices for cybersecurity compliance [67].
- *Enhancing Personal Cyber Hygiene*: Promoting secure use of personal and work devices is critical to mitigating risks. This includes emphasizing secure device configurations and responsible online behavior to protect organizational resources [67].
- *Consistent Security Across Environments*: Adopting hybrid work models with uniform cybersecurity practices across remote and office settings, including the application of a Zero Trust approach, minimizes security risks [8].
- *Cultivating an Inclusive WFH Culture*: Fostering a secure and supportive remote work culture can prevent exploitation and misuse of company resources. Strategies to maintain employee engagement, direct supervision, and trust are critical to enhancing compliance with cybersecurity policies [10].
- *Guidelines for Personal and Official Device Use*: Organizations must establish clear policies regarding the use of personal devices for official work and vice versa. These policies should include strict monitoring and security controls to maintain clear boundaries and prevent security breaches [24].
- *Remote Monitoring and Incident Management*: Deploying advanced network scanning, DoS protection services, and Security Information and Event Management (SIEM) technologies enables real-time detection and response to cybersecurity incidents [66].
- *Backups, BIA-Recovery Plans, and Data Encryption*: Comprehensive disaster recovery plans, including encrypted backups and business impact assessments, are essential to ensuring data integrity and facilitating swift recovery following cybersecurity incidents [66].
- *Vendor Security Controls and SOC Audits*: Establishing stringent security controls for vendors, along with regular SOC-2 audits, ensures that third-party providers meet high cybersecurity standards [66].
- *Regular Security Assessments and Audits*: Conducting frequent network security assessments and audits helps identify and address vulnerabilities, fostering continuous improvement in cybersecurity measures [45, 66, 72].

Recognizing that no singular strategy can provide complete protection against cyber threats, a multifaceted approach is essential. The strategies outlined above address both technical and human-centric challenges, emphasizing the need for continuous adaptation to an evolving cybersecurity threat landscape. Future research should focus on the integration of artificial intelligence and machine learning into cybersecurity frameworks to proactively identify and mitigate emerging threats. These advancements will be critical in addressing the implications of remote work on organizational security.

6 Conclusion, limitations and future work

This systematic literature review critically examined the cybersecurity challenges introduced by the widespread adoption of remote work, particularly in the context of post-pandemic workplace transformations. Drawing on 20 rigorously selected peer-reviewed studies and guided by the PRISMA methodology, the review synthesized both qualitative and quantitative evidence using a convergent thematic approach. It identified a complex web of organizational vulnerabilities stemming from technical, human, and procedural factors that have emerged or intensified in remote work environments.

Key findings underscore the prevalence of threats such as phishing, malware, misconfigured remote access protocols, insecure personal device usage, and legal compliance gaps. These risks are magnified by human behavior-related factors—including lack of awareness, autonomy misuse, and social engineering susceptibility—as well as infrastructural challenges like open RDP ports and weak home network configurations. The review also revealed how rushed technology adoption, inadequate training, and blurred organizational policies contribute to systemic weaknesses in remote work security. A major contribution of this study lies in its multi-pronged synthesis framework, which not only categorizes cyber risks but integrates quality appraisal using MMAT, CASP, and JBI tools—thereby enhancing the transparency and credibility of its findings.

From a practical standpoint, this research provides targeted, evidence-based recommendations for strengthening cybersecurity in distributed work settings, including robust zero-trust frameworks, remote device hygiene, compliance monitoring, and the cultivation of cyber-aware organizational cultures. These insights offer value for security professionals, policy-makers, and organizational leaders navigating the complex intersection of digital transformation and workforce decentralization.

While this review employed a rigorous and systematic methodology guided by PRISMA standards, several limitations must be acknowledged. First, the study relied exclusively on peer-reviewed articles published in English, potentially excluding relevant research in other languages or from grey literature sources such as industry white papers, technical reports, and conference proceedings. Second, the search was limited to five major academic databases, which, despite their breadth, may not capture all relevant interdisciplinary studies on cybersecurity and remote work. Third, the review did not involve empirical validation, such as expert interviews or field data collection, due to the nature of a literature-based approach. Finally, while the inclusion of both qualitative and quantitative studies enhances thematic richness, the synthesis process may still be influenced by the inherent methodological heterogeneity and reporting styles of the included studies. These limitations suggest that future work could benefit from expanding the scope of evidence and incorporating primary data to triangulate findings and validate emerging themes.

Looking ahead, future research should investigate the implications of emerging technologies that are poised to reshape cybersecurity in remote work contexts. Quantum computing, for example, poses a dual challenge—potentially compromising traditional encryption protocols while also offering accelerated threat detection through quantum-enhanced computation [37]. Similarly, immersive technologies such as augmented and virtual reality (AR/VR) demand new security paradigms to address risks like identity spoofing, data interception, and unauthorized access in virtual spaces [58]. In parallel, blockchain-based architectures offer promise for decentralized identity and data management in remote ecosystems, though their practical applicability and vulnerabilities require further empirical validation [53].

The evolving nature of remote work underscores the need for adaptive, layered cybersecurity models that can accommodate emerging technologies and workforce behavior trends. Ongoing research, policy refinement, and cross-disciplinary collaboration will be essential to building resilient digital infrastructures that safeguard organizational integrity in a permanently hybrid work environment.

Acknowledgements The author would like to express gratitude to the anonymous reviewers for their insightful comments and constructive feedback.

Author contributions This paper is solely the work of the author, Dr. Mohammad Nizamuddin, who carried out all aspects of the research, analysis, and writing independently.

Funding This research did not receive funding from any external source.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Abbas, H., Emmanuel, N., Amjad, M.F., Yaqoob, T., Atiquzzaman, M.: Security assessment and evaluation of VPNs: a comprehensive survey. ACM Comput. Surv. (2023). https://doi.org/10.1145/3579162
2. ACSC.: ASD Cyber threat report 2022–2023. Australian Cyber Security Center (ACSC). (2023).https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023
3. Alkhalil, Z., Hewage, C., Nawaf, L., Khan, I.: Phishing attacks: a recent comprehensive study and a new anatomy. Front. Comput. Sci. (2021). https://doi.org/10.3389/fcomp.2021.563060

4. Alotibi, G.N., Abdulwahid, A.A.: An investigation of cybersecurity issues of remote work during the COVID-19 pandemic in Saudi Arabia. Int. J. Adv. Comput. Sci. Appl.Comput. Sci. Appl. (2023). https://doi.org/10.14569/ijacsa.2023.0140106
5. Alsharif, M., Mishra, S., AlShehri, M.: Impact of human vulnerabilities on cybersecurity. Comput. Syst. Sci. Eng. **40**(3), 1153–1166 (2022). https://doi.org/10.32604/csse.2022.019938
6. Atstāja, L., Rūtītis, D., Deruma, S., Aksjoņenko, E.: Cyber security risks and challenges in remote work under the covid-19 pandemic. Eur. Proc. Social Behav. Sci. (2021). https://doi.org/10.15405/epsbs.2021.12.04.2
7. Basit, A., Zafar, M., Liu, X., Javed, A.R., Jalil, Z., Kifayat, K.: A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommun. Syst. **76**(1), 139 (2020). https://doi.org/10.1007/s11235-020-00733-2
8. Bispham, M., Creese, S., Dutton, W.H., Esteve-González, P., Goldsmith, M.: An exploratory study of cybersecurity in working from home: problem or enabler? J. Inf. Policy **12**, 353–386 (2022). https://doi.org/10.5325/jinfopoli.12.2022.0010
9. Booth, A., Papaioannou, D., Sutton, A.: Systematic approaches to a successful literature review. Sage (2012)
10. Borkovich, D., Skovira, R.: Working from home: cybersecurity in the age of Covid-19. Issues Inf. Syst. (2020). https://doi.org/10.48009/4_iis_2020_234-246
11. Braesemann, F., Stephany, F., Teutloff, O., Kässi, O.: The global polarisation of remote work. PLoS ONE **17**(10), e0274630 (2022). https://doi.org/10.1371/journal.pone.0274630
12. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qual. Res. Psychol. **3**(2), 77–101 (2006). https://doi.org/10.1191/1478088706qp063oa
13. Clear, F.: SMEs, electronically-mediated working and data security: cause for concern? Int. J. Bus. Sci. Appl. Manag.Manag. **2**(2), 1–20 (2007)
14. Cask.: Shadow IT: Understanding, managing, and mitigating risks. Cask. (2023). https://casknx.com/resources/shadow-it/
15. Chin, K.: Biggest data breaches in US history. UpGuard. (2022). https://www.upguard.com/blog/biggest-data-breaches-us
16. Crossland, G., Michaelides, N., Ertan, A.: Remote working and cyber security: literature review. Research Institute for Sociotechnical Cyber Security (RISCS). (2021)
17. Curran, K.: Cyber security and the remote workforce. Comput. Fraud Secur. **2020**(6), 11–12 (2020). https://doi.org/10.1016/s1361-3723(20)30063-4
18. Din, A.: Most common remote work security risks and best practices. Heimdal Security Blog. (2023). https://heimdalsecurity.com/blog/remote-work-security/
19. Dowling, B., Goldstein, D., Park, M., Price, H.: Hybrid work: Making it fit with your diversity, equity, and inclusion strategy. McKinsey. (2022). https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/hybrid-work-making-it-fit-with-your-diversity-equity-and-inclusion-strategy
20. Downer, K., Bhattacharya, M.: BYOD Security: A Study of Human Dimensions. Info. **9**(1) (2022). https://doi.org/10.3390/informatics9010016
21. Eiza, M., Okeke, R.I., Dempsey, J., Ta, V.-T.: Keep calm and carry on with cybersecurity @Home: a framework for securing home-working IT environment. Int. J. Cyber Situational Awar. **5**, 1–25 (2021). https://doi.org/10.22619/ijcsa.2020.100131
22. Faisal, S.H.S., Ismail, F.: Cybersecurity threats and best practices of working from home. J. Techno-Social **13**(2), 1–5 (2021)
23. Finnell, K.: Rethinking asynchronous communication in remote work. (2022). https://www.techtarget.com/searchunifiedcommunications/feature/Rethinking-asynchronous-communication-in-remote-work
24. Fritzen, M. P.: Remote working and cyber security threats in ireland. Challenges and prospective solutions. (2021). https://norma.ncirl.ie/5108/
25. George, T.: Lost and stolen devices: a gateway to data breaches and leaks. securityWeek. (2023). https://www.securityweek.com/lost-and-stolen-devices-a-gateway-to-data-breaches-and-leaks/
26. Georgiadou, A., Mouzakitis, S., Askounis, D.: Designing a cybersecurity culture assessment survey targeting critical infrastructures during Covid-19 crisis. Int. J. Netw. Secur. Appl. **13**(1), 33–50 (2021). https://doi.org/10.5121/ijnsa.2021.13103
27. Georgiadou, A., Mouzakitis, S., Askounis, D.: Working from home during COVID-19 crisis: a cyber security culture assessment survey. Secur. J. (2021). https://doi.org/10.1057/s41284-021-00286-2
28. Gitnux.: Remote work cybersecurity statistics and trends in 2023. (2023). https://blog.gitnux.com/remote-work-cybersecurity-statistics/
29. Grant, M.J., Booth, A.: A typology of reviews: an analysis of 14 review types and associated methodologies. Health Inf. Libr. J. **26**(2), 91–108 (2009). https://doi.org/10.1111/j.1471-1842.2009.00848.x
30. Hadlington, L.: The "human factor" in cybersecurity: exploring the accidental insider. Res. Anthol. Artif. Intell. Appl. Secur. (2021). https://doi.org/10.4018/978-1-7998-7705-9.ch087
31. Hamingson, N.: Communication technology and inclusion will shape the future of remote work. Business News Daily. (2020). https://www.businessnewsdaily.com/8156-future-of-remote-work.html
32. Harter, J. The post-pandemic workplace: the experiment continues. Gallup. (2025). https://www.gallup.com/workplace/657629/post-pandemic-workplace-experiment-continues.aspx
33. Hijji, M., Alam, G.: A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. IEEE Access **9**, 7152–7169 (2021). https://doi.org/10.1109/access.2020.3048839
34. Hill, M., Swinhoe, D. The 15 biggest data breaches of the 21st century. (2022). https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html
35. Hong, Q.N., Fàbregues, S., Bartlett, G., Boardman, F., Cargo, M., Dagenais, P., Gagnon, M.-P., Griffiths, F., Nicolau, B., O'Cathain, A., Rousseau, M.-C., Vedel, I., Pluye, P.: The mixed methods appraisal tool (MMAT) version 2018 for information professionals and researchers. Educ. Inf. **34**(4), 285–291 (2018). https://doi.org/10.3233/EFI-180221
36. Hong, Q.N., Gonzalez-Reyes, A., Pluye, P.: Improving the usefulness of a tool for appraising the quality of qualitative, quantitative and mixed methods studies, the Mixed Methods Appraisal Tool (MMAT). J. Eval. Clin. Pract. **24**(3), 459–467 (2018)
37. Hossain Faruk, M.J., Tahora, S., Tasnim, M., Shahriar, H., Sakib, N. A review of quantum cybersecurity: threats, risks and opportunities. In: 2022 1st International conference on AI in cybersecurity (ICAIC). (2022). https://doi.org/10.1109/icaic53980.2022.9896970
38. Irwin, L.: GDPR: The implications of working from home or on the road. (2020). https://www.itgovernance.eu/blog/en/gdpr-the-implications-of-working-from-home-or-on-the-road
39. Jalali, M.S., Bruckes, M., Westmattelmann, D., Schewe, G.: Why employees (still) click on phishing links: an investigation in hospitals. J. Med. Internet Res. **22**(1), e16775 (2020). https://doi.org/10.2196/16775
40. Jason, W.N., Collins, E., Panteli, N., Blythe, J., Koppelman, B.: Remote working pre- and post-covid-19: An analysis of new threats and risks to security and privacy. (2021). https://arxiv.org/abs/2107.03907. https://doi.org/10.1007/978-3-030-78645-8_74
41. Kitchenham, B., Brereton, O.P., Budgen, D., Turner, M., Bailey, J., Linkman, S.: Systematic literature reviews in software engineering

– a systematic literature review. Inf. Softw. Technol. **51**(1), 7–15 (2009)
42. Koski, T.: Increase in remote work: effects on phishing. (2021). https://jyx.jyu.fi/handle/123456789/76341
43. Li, A.: An analysis of the recent ransomware families. (2021). https://www.cs.purdue.edu/homes/li3944/blog/Project%20report_Adrian%20Li.pdf
44. Liberati, A., Altman, D.G., Tetzlaff, J., Mulrow, C., Gøtzsche, P.C., John-Clarke, M., Kleijnen, J., Moher, D.: The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. PLoS Med. Med. **6**, e1000100 (2009). https://doi.org/10.1371/journal.pmed.1000100
45. Lindroos, S., Hakkala, A., Virtanen, S.: The COVID-19 pandemic and remote working did not improve WLAN security. Procedia Comput. Sci. **201**, 158–165 (2022). https://doi.org/10.1016/j.procs.2022.03.023
46. Long, H.A., French, D.P., Brooks, J.M.: Optimising the value of the Critical Appraisal Skills Programme (CASP) tool for quality appraisal in qualitative evidence synthesis. Res. Methods Med. Health Sci. **1**(1), 31–42 (2020). https://doi.org/10.1177/2632084320947559
47. Malwarebytes: 20 percent of organizations experienced breach due to remote worker, Labs report reveals. Malwarebytes Labs. Malwarebytes. (2020). https://www.malwarebytes.com/blog/news/2020/08/20-percent-of-organizations-experienced-breach-due-to-remote-worker-labs-report-reveals
48. McLeary, J.: 2023 State of cyber defense: the false-positive of trust. Kroll. (2023). https://www.kroll.com/en/insights/publications/cyber/2023-state-cyber-defense
49. Moher, D., Liberati, A., Tetzlaff, J.: Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. BMJ **339**, b2535–b2535 (2009). https://doi.org/10.1136/bmj.b2535
50. Muhammad, Z.: Remote work caused data breaches for 62% of organizations. (2023). https://www.digitalinformationworld.com/2023/03/remote-work-caused-data-breaches-for-62.html
51. Munn, Z., Aromataris, E., Tufanaru, C., Stern, C., Porritt, K., Farrow, J., Lockwood, C., Stephenson, M., Moola, S., Lizarondo, L., McArthur, A., Peters, M., Pearson, A., Jordan, Z.: The development of software to support multiple systematic review types. Int. J. Evid.-Based Healthc. **17**(1), 1 (2018). https://doi.org/10.1097/xeb.0000000000000152
52. Munn, Z., Barker, T.H., Moola, S., Tufanaru, C., Stern, C., McArthur, A., Stephenson, M., Aromataris, E.: Methodological quality of case series studies. JBI Database Syst. Rev. Implement. Rep. **18**(10), 1 (2020)
53. Narayanan, U., Paul, V., Joseph, S.: Decentralized blockchain based authentication for secure data sharing in Cloud-IoT. J. Ambient. Intell. Humaniz. Comput. (2021). https://doi.org/10.1007/s12652-021-02929-z
54. Nicoletti, P.: Remote work security statistics in 2022. CyberTalk. (2022). https://www.cybertalk.org/2022/03/31/remote-work-security-statistics-in-2022/
55. Nurse, J.R.C., Williams, N., Collins, E., Panteli, N., Blythe, J., Koppelman, B.: Remote working pre- and post-COVID-19: An analysis of new threats and risks to security and privacy. In: Stephanidis, C., Antona, M., Ntoa, S. (eds) HCI International 2021 - Posters. HCII 2021. Communications in Computer and Information Science, vol. 1421, pp. 583–590 (2021). https://doi.org/10.1007/978-3-030-78645-8_74
56. Nwankpa, J.K., Datta, P.: Remote vigilance: the roles of cyber awareness and cybersecurity policies among remote workers. Comput. Secur. **130**, 103266–103266 (2023). https://doi.org/10.1016/j.cose.2023.103266
57. Petticrew, M., Roberts, H.: Systematic Reviews in the Social Sciences (M. Petticrew & H. Roberts, Eds.). Blackwell Publishing Ltd. (2006). https://doi.org/10.1002/9780470754887
58. Pidel, C., Ackermann, P.: Collaboration in virtual and augmented reality: a systematic overview. Lect. Notes Comput. Sci.Comput. Sci. (2020). https://doi.org/10.1007/978-3-030-58465-8_10
59. Quyen, N.V.: Hands-on training for mitigating web application. (2023). https://dspace02.jaist.ac.jp/dspace/bitstream/10119/18734/5/paper.pdf
60. Radu, C., Deaconu, A., Kis, I.-A., Jansen, A., Mișu, S.I.: New ways to perform: employees' perspective on remote work and psychological security in the post-pandemic era. Sustainability **15**(7), 5952 (2023). https://doi.org/10.3390/su15075952
61. Rakha, N. A.: Ensuring cyber-security in remote workforce: Legal implications and international best practices. Int. J. Law Policy. (2023). https://irshadjournals.com/index.php/ijlp/article/download/43/30
62. Rethlefsen, M.L., Kirtley, S., Waffenschmidt, S., Ayala, A.P., Moher, D., Page, M.J., Koffel, J.B.: PRISMA-S: an extension to the PRISMA statement for reporting literature searches in systematic reviews. Syst. Rev. (2021). https://doi.org/10.1186/s13643-020-01542-z
63. Sandamali, A.A.D.: Effective information security policies for efficient remote working: Software professionals' perspective. (2019). http://dl.lib.uom.lk/handle/123/16362
64. Sandelowski, M., Voils, C.I., Barroso, J.: Comparability work and the management of difference in research synthesis studies. Soc Sci Med **64**(1), 236–247 (2007). https://doi.org/10.1016/j.socscimed.2006.08.041
65. Santos, R. de S., Grillo, W., Cabral, D., de Castro, C., Albuquerque, N., França, C. Post-pandemic hybrid work in software companies: findings from an industrial case study. (2024). https://doi.org/10.48550/arXiv.2401.08922
66. Sebastian, G.:A descriptive study on cybersecurity challenges of working from home during COVID-19 pandemic and a proposed 8 step WFH cyber-attack mitigation plan. Communications of the IBIMA, 1–7. (2021). https://doi.org/10.5171/2021.589235
67. Senapati, S., Bharathi, S.V.: An Empirical study on the information security threats due to remote working environments. In: International conference on information science and applications (ICISA), 19–37. (2024). https://doi.org/10.1007/978-981-99-6984-5_2
68. Shaheen, N., Shaheen, A., Ramadan, A., Hefnawy, M.T., Ramadan, A., Ibrahim, I., Hassanein, M., Ashour, M.E., Flouty, O.: Appraising systematic reviews: a comprehensive guide to ensuring validity and reliability. Front. Res. Metr. Analy. (2023). https://doi.org/10.3389/frma.2023.1268045
69. Sirineni, G.: Council Post: remote work has led to a cybercrime boom—here's how to stop it. Forbes. (2022). https://www.forbes.com/sites/forbesbusinesscouncil/2022/03/07/remote-work-has-led-to-a-cybercrime-boom-heres-how-to-stop-it/?sh=74f52a8c2f6a
70. Sjouwerman, S.: Data breach costs increase by $1 million when remote workers are involved. (2022). https://blog.knowbe4.com/data-breach-costs-increase-by-1-million-when-remote-workers-are-involved
71. Specops: Survey reveals the UK business sectors most lacking in cyber security training. (2020). https://specopssoft.com/blog/uk-business-sectors-lacking-cyber-security-training/
72. Suciu, P.: Security remains a real concern with real-time communication tools. (2023). https://www.forbes.com/sites/petersuciu/2023/11/29/security-remains-a-real-concern-with-real-time-communication-tools/?sh=1823fd4615c9
73. Tahlyan, D., Mahmassani, H., Stathopoulos, A., Said, M., Shaheen, S., Walker, J., Johnson, B.: In-Person, hybrid or remote? Employers' perspectives on the future of work post-pandemic. (2024). https://doi.org/10.48550/arXiv.2402.18459

74. Thankappan, M., Rifà-Pous, H., Garrigues, C.: Multi-channel man-in-the-middle attacks against protected Wi-fi networks: a state of the art review. Expert Syst. Appl. (2022). https://doi.org/10.1016/j.eswa.2022.118401
75. Thomas, J., Harden, A.: Methods for the thematic synthesis of qualitative research in systematic reviews. BMC Med. Res. Methodol.Methodol. **8**(1), 1–10 (2008). https://doi.org/10.1186/1471-2288-8-45
76. Treacy, S., Sabu, A., Bond, T., O'Sullivan, J., Sullivan, J., Sylvester, P.: Organizational cybersecurity post the pandemic: an exploration of remote working risks and mitigation strategies. Int. Conf. Cyber Warfare Secur. **18**, 394–401 (2023). https://doi.org/10.34190/iccws.18.1.973
77. Venkatesha, S., Reddy, K.R., Chandavarkar, B.R.: Social engineering attacks during the COVID-19 pandemic. SN Comput. Sci. (2021). https://doi.org/10.1007/s42979-020-00443-1
78. Walters, P.: How Does Remote Work Affect CCPA Compliance? (2021). https://www.truevault.com/blog/how-does-remote-work-affect-ccpa-compliance
79. Yoachimik, O., Pacheco, J.: DDoS threat report for 2023 Q2. (2023). https://blog.cloudflare.com/ddos-threat-report-2023-q2