IJECBE (2025), **3**, **1**, 117–141
Received (16 April 2025) / Revised (29 April 2025)
Accepted (30 April 2025) / Published (30 May 2025)
https://doi.org/10.62146/ijecbe.v3i1.113
https://ijecbe.ui.ac.id
ISSN 3026-5258

International Journal of Electrical, Computer and Biomedical Engineering

RESEARCH ARTICLE

Cybersecurity Of Work From Anywhere Model For Government : A Systematic Literature Review

Muhammad Fahreza Asyrofi* and I Gde Dharma Nugraha

Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia
*Corresponding author. Email: mufahreza7@gmail.com

Abstract

Presidential Regulation No. 21 of 2023 grants Indonesian civil servants (ASN) location flexibility, creating cybersecurity challenges that institutions and authorities have yet to fully address. Existing frameworks such as ISO 27001 and NIST provide only general remote work guidelines, lacking specific recommendations for the Work From Anywhere (WFA) model. This gap poses significant risks to data security and government operations, particularly as cyber incidents reported by the National Cyber and Crypto Agency of Indonesia (BSSN) continue to rise. The 2023 Indonesian Cybersecurity Landscape report recorded 347 suspected cyber incidents, including data breaches and the exposure of over 1.6 million records on the darknet, affecting numerous stakeholders. This study employs a Systematic Literature Review (SLR) to identify cybersecurity threats associated with remote work and explore effective mitigation techniques. The findings reveal five primary threats classified into two categories: human-centric threats (social engineering attacks, insider threats, and human errors) and technology-centric threats (malware-based and network attacks). To address these threats, the study identifies four key best practice themes: Awareness and Education, Phishing Protection, Technical Countermeasures, and Management and Audit. These themes provide a structured approach to enhancing cybersecurity in WFA environments. The results of this study serve as valuable input for formulating policy and technical guidelines to implement WFA in government settings. Future research should explore supply chain security, integration of WFA with on-site operations, cultural factors in security compliance, and governance frameworks to enhance cybersecurity resilience in government WFA environments.

Keywords: Work From Anywhere (WFA), Cybersecurity Best Practices, Remote Work Policy

1. Introduction

Indonesian Presidential Regulation No. 21 of 2023 not only introduces flexible working arrangements for civil servants (ASN), as outlined in Article 8, but also extends its provisions, through Article 10, to government institutions and employees funded by the State or Regional Budget [1]. This reflects an effort to modernize work policies across a broad spectrum of public institutions. However, as stated in Article 11, these provisions exclude specific entities, such as the military, police, and diplomatic representatives abroad, recognizing their unique operational demands [1]. This regulation highlights the government's intent to adopt flexible work systems while balancing the distinct needs of critical sectors, but it also underscores the need for clear cybersecurity frameworks to address emerging risks in the implementation of such policies. As flexible working hours are granted to employees with limited technical expertise, there is an increased opportunity for attackers to exploit security vulnerabilities. This is due to a lack of understanding of cybersecurity risks among non-technical staff, who may be more susceptible to social engineering attacks like phishing. Furthermore, the shift to remote work increases the exposure of government systems to cyber threats, especially when employees access work resources from personal or unsecured devices and from public networks.

Based on IBM Reports 2024, for the second consecutive year, phishing and stolen or compromised credentials were identified as the most common attack vectors, and they were also among the top four most expensive types of breaches [2]. Based on the 2023 Cybersecurity Landscape report by BSSN, the government sector has become a major target for cyberattacks, with the highest percentage of data exposures—39.78% of the total [3]. This trend highlights the increasing vulnerability of government agencies to cyber threats, which may include data breaches, credential theft, and other forms of cybercrime.

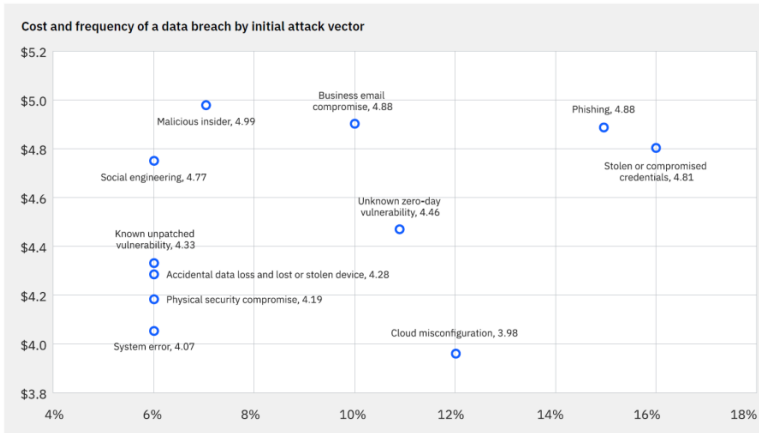

Figure 1. Top Initial Attack Vectors and Breach Costs (USD) in 2024 – IBM Report [2]

Currently, government institutions are required to interpret the provisions for flexible working hours and locations as outlined in Presidential Regulation No. 21

of 2023. However, there is no official open access guideline specifically addressing remote work security for ASN issued by any government agency. Some ministries have introduced general frameworks for remote work. For example, the Indonesian Ministry of Finance addressed the implementation of Flexible Working Space (FWS). Article Six of this decree mandates that employees ensure the availability of supporting infrastructure, including the security of data, information networks, technology, and communication systems used during FWS implementation [4]. Despite this initiative, such guidelines remain broad and do not provide detailed measures to address the growing risks of cybersecurity threats in flexible working environments.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Core, as outlined in NIST CSWP 29 Appendix A [5] and ISO 27001 Annex A.6.2.2 [6] are widely recognized standards that provide structured, high-level guidance for managing cybersecurity risks. However, both frameworks tend to remain conceptual and generalized, offering limited operational detail for specific scenarios such as WFA. In practice, these standards often require significant interpretation to address the unique challenges of remote work environments. Moreover, their recommendations are not always backed by empirical implementation evidence, particularly in the context of public sector operations or distributed workforces. Without a foundation in scenario-based validation or field-tested practices, the applicability of these frameworks in dynamic WFA settings remains largely assumed rather than demonstrably proven.

Based on the previously described context, this paper aims to identify the key components of cybersecurity in the context of remote work or WFA. The objective is to understand how cybersecurity aspects should be addressed when governments plan to implement WFA, by formulating the following research question:

1. RQ1: What cybersecurity threats are commonly associated with remote work in a work-from-anywhere model?
2. RQ2: What best practices are currently recommended for securing data and communication in a WFA environment?

This research will leverage a Systematic Literature Review (SLR) methodology to examine cybersecurity key components tailored to the WFA model. The SLR will focus on identifying and synthesizing cybersecurity risk and recommendations documented in peer-reviewed journal articles for securing remote work environments. The results will be analyzed comprehensively, followed by a discussion and conclusion. This paper is organized as follows: Sections 1 and 2 offer an overview by summarizing the WFA model and its cybersecurity challenges both in the government context and more broadly, while also reviewing related works. Section 3 details the methodological approach used in this study. Section 4 presents the findings from the systematic literature review. Lastly, Section 5 provides a discussion and conclusion.

2. Literature Study

2.1 WFA Model and Security Issues

The WFA model is an evolution of the traditional Work From Home (WFH) approach. While WFH primarily emphasizes flexibility in work schedules, WFA extends this

flexibility to include the geographical location of work. According to Choudhury et al. [7], WFA allows employees to choose where they work, removing the geographical constraints typically associated with office-based or home-based work setups. One closely related concept to WFA is telework. The International Labor Organization (ILO) [8] defines telework as work conducted entirely or partially from alternative locations outside the primary workplace, utilizing electronic devices for communication and task completion. NIST further elaborates on telework, emphasizing its application not just to employees but also to contractors, business partners, and vendors [9]. NIST defines telework as the capability to work from locations outside the organization's facilities, often leveraging third-party networks [9]. However, this flexibility comes with increased risks. Devices operating on third-party networks face higher exposure to potential compromises, and their communications are more susceptible to being monitored. This insight is particularly relevant to the WFA model, where individuals work from diverse locations such as cafes, coworking spaces, or even international destinations, thus heightening the importance of robust cybersecurity measures.

The WFA model presents several cybersecurity challenges, particularly due to reliance on unsecured external networks. Public Wi-Fi and third-party networks often lack encryption, exposing telework devices to eavesdropping and direct internet access vulnerabilities [9]. Additionally, the absence of physical security controls makes devices prone to theft or loss, increasing the risk of sensitive data compromise. Other significant concerns include malware infection from Bring Your Own Device (BYOD) or third-party devices spreading to internal networks and increased risks from external access to internal resources. Unsecured networks also face threats like eavesdropping and man-in-the-middle (MITM) attacks [10]. These issues highlight the critical need for robust security measures, such as VPNs, regular updates, and strict access controls, to protect WFA environments effectively

The WFA model and challenges shown in Figure 2 consist of four main components: employees, devices and software, connectivity networks, and the organization [11]. Each component plays a critical role in enabling flexible work environments while introducing unique challenges, particularly in the realm of cybersecurity.

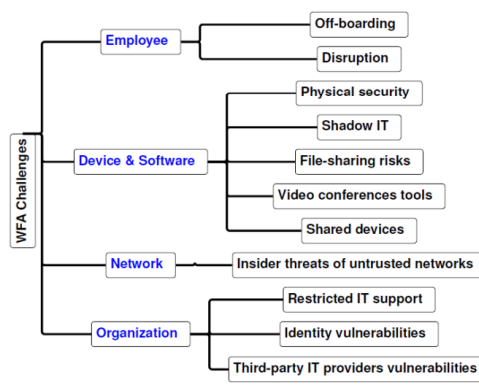

Figure 2. WFA Model Challenges [11]

ASN plays a crucial role in securing WFA systems. However, many ASNs mistakenly believe cybersecurity is solely the responsibility of IT staff, emphasizing the need for proper training. ASNs use various devices like laptops, computers, and mobile phones, often with self-installed applications, relying on tools such as VPNs and video conferencing. These devices face vulnerabilities that require regular updates and secure configurations. ASNs access government servers through networks like home Wi-Fi, mobile hotspots, or public connections, which pose risks like eavesdropping and unauthorized access. While VPNs and encryption help, full end-to-end security remains challenging. The government, as the responsible organization, must secure networks, devices, and applications while training employees and ensuring secure connections. Proactive cybersecurity practices are essential to prevent operational and security breaches [11]. NIST highlights key teleworking risks [10]:

a) Lack of Physical Security: Organizations cannot fully control how employees handle their devices outside the office.
b) Unsecured Networks: Employees may use unsafe internet connections, so organizations must enforce security policies.
c) Infected Devices: Organizations cannot guarantee that employees' devices are malware-free. If infected, these devices can spread malware to internal networks.
d) Unauthorized Access: Remote access increases the risk of unverified devices or networks being compromised by malware.

2.2 Related Works

Given these challenges, addressing the security issues in government WFA models requires a deeper understanding of best practices and effective mitigation strategies. Various studies have examined this topic from different perspectives. For instance, Klint (2023) [12] investigates best practices for ensuring cybersecurity in home-office settings post-COVID, using a combination of structured literature review and semi-structured interviews with industry professionals. The study underscores the need for updated best practices that consider the distinct threat landscape of home-office setups and suggests future work to assess the long-term effectiveness of its recommendations. Similarly, Galajda (2023) [13] examines how the rapid shift to teleworking during the pandemic impacted employees' information security awareness (ISA). Through a quantitative survey and hypothesis testing, the study offers valuable insights into the relationship between knowledge, attitude, and behavior in teleworking security, while emphasizing the need for balanced awareness of both risks and recommendations. The study from Gumilang et. al. (2023) [14] addresses the increased reliance on teleworking during the COVID-19 pandemic, particularly within government sectors. Using a qualitative, literature-based methodology, the research identifies key risks associated with teleworking, such as data classification, internet network vulnerabilities, and inadequate data protection. It leverages theories from cybersecurity, network security, authentication, and non-repudiation to propose a robust framework for mitigating these risks. The recent study, Mahyoub et. al. (2024) [11] examines the cybersecurity challenges posed by the rapid shift to the WFA model during the COVID-19 pandemic. The research combines a detailed analysis of WFA-related cybersecurity issues with data from an online user study involving 45 participants from diverse sectors, including

universities, government, private organizations, and nonprofits. The study emphasizes enhancing employee behavior, awareness, and compliance through tailored security training programs. Additionally, it outlines best practices and recommendations for organizations to strengthen their resilience against cybercrime and fraud. These related works contribute valuable knowledge to understanding and improving the method to examine security of WFA models, particularly in government contexts.

3. Research Methodology

Several steps were undertaken to reach the conclusions of this study, including identifying the problem, conducting a literature study, designing the research methodology, and performing a SLR. The research methodology was selected based on the research objectives, the nature of the research question, and the depth of understanding required to address the problem.

SLR is consistently defined in various sources as a method for identifying, evaluating, and interpreting research relevant to a specific question, topic, or phenomenon. SLR as a way to evaluate and interpret available research on a particular area [15], while emphasizing its role in systematically assessing and synthesizing studies to address a research question or topic [16]. To enhance the systematic process further, this study incorporates its methods [17] into the PRISMA flow diagram. The PRISMA protocol consists of three stages: planning, conducting the review, and reporting and dissemination. In the planning stage, research objectives, questions, and inclusion/exclusion criteria are defined. The review stage involves identifying and evaluating relevant articles, while the reporting stage synthesizes and presents the findings. This study focuses on cybersecurity risks within the WFA model in government environments, guiding the SLR to explore strategies for safeguarding data and communication in remote work settings. A multi-database strategy was employed to address the limited availability of relevant publications. Search strings with carefully selected keywords were created, followed by title screening, abstract reviews, and detailed information extraction. A quality assessment of each article was conducted to ensure methodological rigor and relevance to the RQ's.

Table 1. Database selection

Databases	Website's URL
IEEE – Institute of Electrical and Electronics Engineers	https://ieeexplore.ieee.org/Xplore/home.jsp
Scopus	https://www.scopus.com/
ACM Digital Library	https://dl.acm.org/
Taylor and Francis Online	https://www.tandfonline.com/

Table 2. Inclusion and Exclusion Criteria

Inclusion	Exclusion
Articles must be written in English to ensure clarity and comprehension.	Studies focused on topics unrelated to information security in remote work (e.g., electric vehicles, IoT, control systems).
Articles must be fully accessible.	Studies that focus on traditional office environments or work-from-home (WFH) scenarios instead of WFA.
Articles should discuss best practices for cybersecurity in the context of remote work or telework within the WFA model.	Studies that address general administrative aspects of WFA, rather than focusing on cybersecurity practices.

Table 3. Keyword and Search Strings

Keywords	Search Strings
"remote-work", "telework", "work from anywhere", "internet cafe", "best practices", "guide" "cybersecurity", "cyber security", "information security"	("remote-work" OR "telework" OR "work from anywhere" OR "internet cafe") AND ("best practices" OR "guide") AND ("cybersecurity" OR "cyber security" OR "information security")

The PRISMA Flow Diagram was used to visually represent the systematic selection process, illustrating stages such as literature identification, screening, and eligibility assessment to ensure transparency and rigor. These structured steps aimed to provide a strong foundation for analyzing and synthesizing findings, offering valuable insights into cybersecurity best practices for the WFA model. Forward and backward snowballing iterations were performed until no additional papers meeting the inclusion criteria were identified. Forward snowballing involves identifying new papers by examining those that cite the paper under review, while backward snowballing focuses on discovering additional papers through the references listed in the examined paper [18].

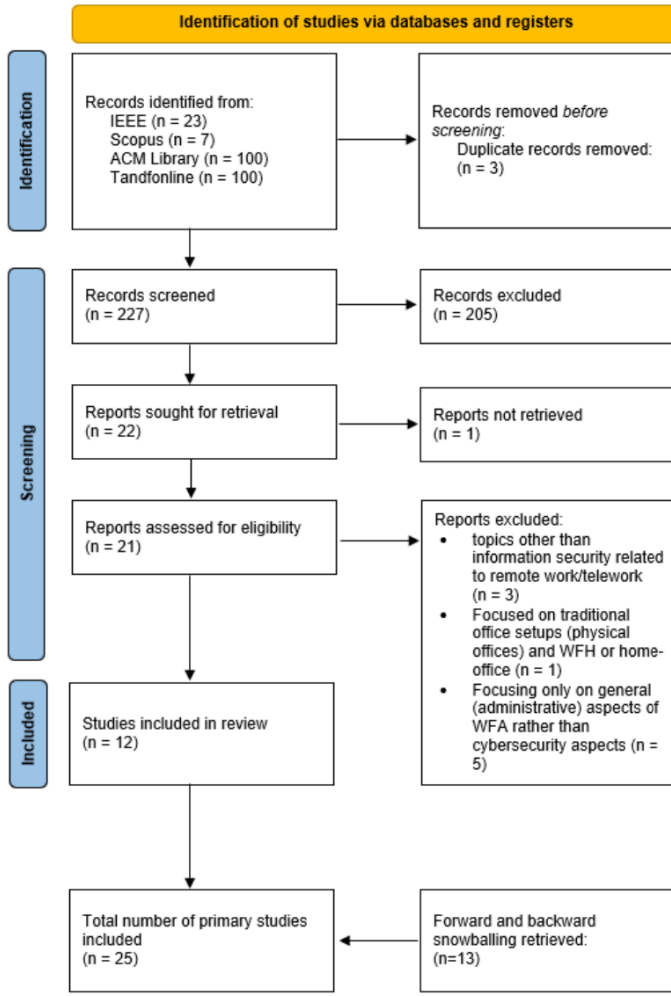

Figure 3. SLR and Snowball Processing

4. Findings

All papers that successfully passed the quality assessment underwent data extraction to evaluate the completeness of the information and ensure the accuracy of the recorded data within them organized into matrix analyses. Summary of information extracted from 25 selected articles will be shown in Table IV, identified common threats in Table V, and cybersecurity for WFA recommendations in Table VI. Following "concept-centric" approach [19], this research used a concept matrix to organize and categorize these concepts into themes. This approach was applied to each research question to facilitate understanding and the identification of information.

Table 4. Summary of information extracted from 25 selected articles

Author and year	Goals
(Naidoo, 2020) [20]	Understand how cybercriminals use the COVID-19 pandemic to carry out scams. It looks at how they choose victims, impersonate trusted sources, and use social tricks to steal information. The study offers advice to help people and organizations protect themselves from these threats.
(Abukari et al.,2020) [21]	Help teleworkers stay safe from cyberattacks during the COVID-19 pandemic and beyond. It provides simple guidelines for education, training, and security policies to protect against online threats, especially social engineering attacks. The aim is to improve cybersecurity for individuals, organizations, and government agencies.
(Palanisamy et al.,2021) [22]	Identify BYOD (Bring Your Own Device) security risks in public sector organizations and suggest ways to reduce them. It focuses on risks caused by employees not following security rules. The study offers solutions like better security training, clear policies, management support, and technical tools to improve BYOD security
(Othman et al., 2021) [23]	Identify mobile device security risks in organizations using BYOD (Bring Your Own Device). It explores how IS (Information System) audits can check mobile security and policy compliance. The study provides strategies to manage risks and improve mobile security practices to protect organizational data
(Mihailovic et al.,2021) [24]	Understand how teleworking during and after COVID-19 affects employee views on efficiency and cybersecurity. It looks at the risks of remote work, increases in cyberattacks, and how well organizations handle these threats. The study aims to help improve cybersecurity awareness and support effective remote work
(Atstāja et al., 2021) [25]	Analyze the cyber risks and challenges faced by companies and organizations due to the sudden shift to remote work during the COVID-19 pandemic.
(Nurse et al., 2021) [26]	Identify security and privacy risks from remote working before and after COVID-19. It focuses on new threats like cyberattacks, lack of security training, and privacy issues caused by workplace monitoring. The study aims to help organizations protect their data while respecting employee privacy.
(Bicakci et al., 2021) [27]	Create a secure USB device to protect remote workers from cyber threats. It aims to address risks like data theft, unauthorized access, and system tampering using Zero Trust principles. Overall, the research aims to provide a simple, secure, and cost-effective solution for safe remote work.
(Gogri, 2022) [28]	Identify the new cyber threats caused by the shift to remote work during the pandemic and suggest ways to protect against them. It focuses on issues like phishing, ransomware, and insecure networks.

(Atstāja et al., 2021) [25]	Analyze the cyber risks and challenges faced by companies and organizations due to the sudden shift to remote work during the COVID-19 pandemic.
(Georgiadou et al.,2022) [29]	Use a cybersecurity culture framework to detect insider threats. It focuses on how human behavior and security practices can lead to accidental or intentional breaches. The study connects types of insider threats with specific behaviors to help organizations better identify and prevent these risks.
(Khantamonth on et al.,) 2022 [30]	Understand how ransomware attacks target weak VPN security. Through real case studies, it shows how these attacks happen and offers practical advice for system administrators to detect and prevent them
(Pedapudi et al., 2022) [31]	Improve network security for Virtual Private Networks (VPNs). It focuses on identifying risks, suggesting protective measures, and providing strategies like firewall use, security policies, and threat management tools. The aim is to help organizations create secure and reliable VPN environments
(Kaur et al., 2022) [32]	Understand how system administrators adapted their work during the COVID-19 pandemic. The study identifies challenges, highlights lessons learned, and provides recommendations to improve how sysadmins and organizations handle future disruptions.
(Plachkinova et al., 2023)[33]	Compare how employees in New Zealand, the USA, and Vietnam follow information security practices. It focuses on how cultural differences affect handling sensitive information and reporting security incidents. The aim is to help organizations improve security training and policies to better fit the needs of a global workforce.
(Keshvadi, 2023) [34]	Improve cybersecurity in Western organizations by educating non-technical employees. It focuses on reducing security risks caused by a lack of cybersecurity awareness. The study proposes a training program to give non-technical staff the knowledge to help protect their organizations and support cybersecurity efforts
(AlSayfi, 2023) [35]	Understand how remote work affects corporate security. It identifies common cybersecurity risks and highlights best practices to reduce these threats. The study aims to help companies improve security by using strategies like strong passwords, two-factor authentication, VPNs, and employee security training.
(Soubhagyala kshmi et al., 2023) [36]	Identify security risks in Bring Your Own Device (BYOD) use at workplaces. It aims to find issues like data breaches, unauthorized access, and privacy concerns. The study offers simple guidelines, security policies, and technical solutions to help organizations protect their data while allowing employees to use their own devices.
(Muthuswam y, 2023) [37]	Identify cybersecurity challenges for employees in Saudi Arabia's digital workplaces. It focuses on issues like lack of training, insider threats, social engineering, weak passwords, and BYOD risks. The study offers recommendations to help organizations improve security training, policies, and protection measures

(Nwankpa, 2023) [38]	Understand how remote working affects employees' cybersecurity awareness and security practices. It looks at how remote work, combined with security policies, influences how well employees follow security measures. The study aims to help organizations boost cybersecurity awareness and improve security practices among remote workers
(Mohan etal., 2024) [39]	Protect email systems from insider threats. It introduces the Cached-N-Proxy algorithm, which acts as a middle layer to intercept and analyze emails in real time. This approach aims to prevent data breaches, unauthorized access, and email-based attacks by insiders
(Raghav et al., 2024) [40]	Understand and prevent masquerade attacks in online meetings. It looks at how these attacks happen, their effects, and ways to detect and stop them. The study helps organizations improve security in virtual meetings and protect sensitive information.
(Fikry et al., 2024) [41]	Explain what cyber hygiene is and why it's important. It focuses on how good cyber hygiene can protect personal information, prevent cyberattacks, and keep online activities safe. The study encourages people and organizations to make cyber hygiene part of their daily routine to stay secure online.
(Palanisamy et al., 2024) [42]	Identify what makes public sector employees follow BYOD (Bring Your Own Device) security policies. It focuses on key factors like clear rules, employee confidence, IT support, and a sense of ownership. The study suggests improving security training, setting clear policies, and offering IT support to boost compliance and protect organizational data.
(Falade et al., 2024) [43]	Understand privacy risks in mobile apps used to monitor remote employees. It examines how these apps affect employee privacy and employer trust. The study helps organizations and developers balance tracking productivity while protecting employee privacy
(Ozer et al., 2024) [44]	Understand how remote work during the COVID-19 pandemic affected data breaches and cybersecurity. By comparing breaches before and after remote work started, the study identifies new risks and best practices. The findings help organizations improve their security and protect against cyber threats in remote work settings

Table 5. Matrix analysis of identified common threats

Common Threats / Author and year	Social Engineering Attack	Malware-based Attack	Insider Threat	Network Attack	Human Error
(Naidoo, 2020) [20]	✓	✓			
(Abukari et al., 2020) [21]	✓				
(Palanisamy et al., 2021) [22]		✓	✓	✓	✓
(Othman et al., 2021) [23]		✓		✓	✓
(Mihailovic et al.,2021) [24]	✓	✓	✓	✓	✓
(Atstāja et al., 2021) [25]	✓	✓		✓	✓
(Nurse et al., 2021) [26]	✓	✓	✓	✓	✓
(Bicakci et al., 2021) [27]	✓	✓		✓	
(Gogri, 2022) [28]	✓	✓		✓	
(Georgiadou et al., 2022) [29]			✓		✓
(Khantamonthon et al., 2022) [30]		✓		✓	✓
(Pedapudi et al., 2022) [31]	✓	✓		✓	
(Kaur et al., 2022) [32]	✓		✓		✓
(Plachkinova et al., 2023) [33]					✓
(Keshvadi, 2023) [34]					✓
(AlSayfi, 2023) [35]	✓	✓		✓	✓
(Soubhagyalakshmi et al., 2023) [36]		✓		✓	✓
(Muthuswamy, 2023) [37]	✓	✓	✓		✓
(Nwankpa, 2023) [38]	✓	✓		✓	✓
(Mohan et al., 2024) [39]	✓	✓	✓		✓
(Raghav et al., 2024) [40]	✓		✓	✓	✓
(Fikry et al., 2024) [41]	✓	✓		✓	✓
(Palanisamy et al., 2024) [42]		✓		✓	✓
(Falade et al., 2024) [43]				✓	✓
(Ozer et al., 2024) [44]	✓	✓	✓	✓	✓

Table 6. Matrix analysis of cybersecurity for WFA recommendations identified

Common Threats / Author and year	Awareness and Education	Phishing Protection	Technical Countermeasures	Management and Audit
(Naidoo, 2020) [20]	✓	✓		
(Abukari et al., 2020) [21]	✓			✓
(Palanisamy et al., 2021) [22]	✓		✓	✓
(Othman et al., 2021) [23]				✓
(Mihailovic et al.,2021) [24]	✓		✓	✓
(Atstāja et al., 2021) [25]	✓		✓	✓
(Nurse et al., 2021) [26]	✓		✓	✓
(Bicakci et al., 2021) [27]			✓	✓
(Gogri, 2022) [28]	✓		✓	
(Georgiadou et al., 2022) [29]				✓
(Khantamonthon et al., 2022) [30]			✓	✓
(Pedapudi et al., 2022) [31]			✓	✓
(Kaur et al., 2022) [32]	✓		✓	✓
(Plachkinova et al., 2023) [33]	✓			✓
(Keshvadi, 2023) [34]	✓			
(AlSayfi, 2023) [35]	✓		✓	✓
(Soubhagyalakshmi et al., 2023) [36]	✓		✓	✓
(Muthuswamy, 2023) [37]	✓		✓	✓
(Nwankpa, 2023) [38]	✓			✓
(Mohan et al., 2024) [39]	✓	✓	✓	✓
(Raghav et al., 2024) [40]			✓	✓
(Fikry et al., 2024) [41]	✓		✓	✓
(Palanisamy et al., 2024) [42]	✓			✓
(Falade et al., 2024) [43]			✓	✓
(Ozer et al., 2024) [44]	✓		✓	✓

4.1 Common Cybersecurity Threats in WFA Environments

This section presents an in-depth discussion aimed at addressing the research questions that have been formulated.

RQ1: What cybersecurity threats are commonly associated with remote work in a work-from-anywhere model?

The study of cybersecurity threats in remote work is not a novel area, as numerous researchers have already explored the risks and challenges associated with teleworking environments. Previous studies have primarily focused on identifying the common and current threats that emerge in remote work or telework models, providing

insights into the vulnerabilities faced by users in flexible work settings. The purpose of employing a systematic evaluation is to leverage the understanding of these threats and apply this knowledge to develop effective strategies aimed at mitigating the risks associated with telework environments. Based on the data extracted in Section 4, a matrix analysis was conducted to categorize the findings, presenting a list of studies along the horizontal axis and the identified common threats along the vertical axis (Table V). The analysis identified four primary threats associated with remote work environments, classified into two categories: human-centric and technology-centric threats. The human-centric category encompasses social engineering attacks, insider threats, and human errors, while the technology-centric category includes malware-based and network attacks. This classification underscores the distinction between threats originating from human actions and those arising from technical vulnerabilities or exploitation.

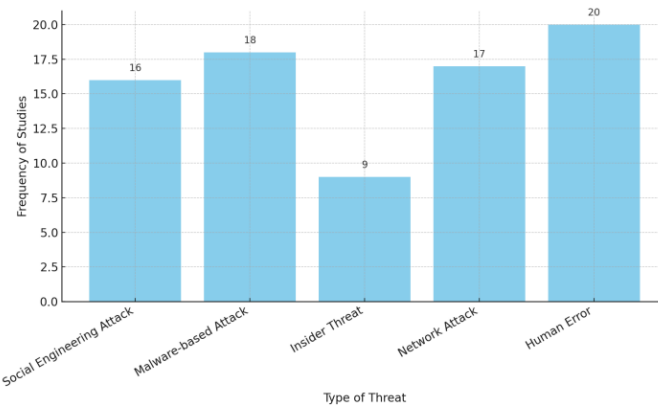

Figure 4. Frequency of Common Threats Identified in SLR

This section discusses these identified threats in detail, as outlined in the objectives.

4.1.1 Social Engineering Attack

The second most commonly discussed threat in studies related to cybersecurity in remote working environments is social engineering attacks. Frequent examples of social engineering include phishing, malware, spear phishing, pretexting, and baiting [45]. While social engineering attacks may differ in execution, they follow a similar pattern. The first step involves collecting target information, followed by engaging with the target. The attacker then uses the gathered information to carry out the attack, and ultimately, they leave no trace of their actions [46][47]. The study explains how cybercriminals exploit global crises like the COVID-19 pandemic by leveraging situational factors such as uncertainty to target vulnerable individuals, organizations, and technologies [20]. It highlights various victimization targets, including impersonation of trusted entities, and the use of crimeware like malware and phishing kits to execute attacks.

4.1.2 Malware-based Attack

Malware, defined as harmful software, infiltrates systems to disrupt operating systems or networks, often resulting in issues such as data exfiltration [48]. A key challenge in remote work settings is that employees' operating systems are typically not managed by the company's IT department, making it difficult to maintain system security. For example, these systems may become vulnerable to viruses or other malicious software [28].

4.1.3 Insider Threat

Insider threat is considered a major security risk for private companies, institutions, and government organizations by both scientists and security experts [29]. Unintentional insider threats can arise from negligence or accidental actions. Negligent insiders, aware of security policies, create risks by ignoring them, such as allowing unauthorized access or failing to apply security updates. In contrast, accidental threats occur through unintentional mistakes like sending sensitive emails to the wrong recipient, clicking malicious links, or mishandling confidential documents [49]. Furthermore, insider threats can involve malicious actions by individuals within an organization's IT department who seek unauthorized access to employee emails. The attacker may craft convincing spear-phishing emails and target specific employees. These emails contain links to fraudulent login pages designed to closely mimic the company's legitimate email gateway, serving as the initial step of the attack [39].

Another common threat in remote work is the use of personal devices (BYOD). Studies highlight several security risks, especially in the public sector. Employees often ignore security policies when using personal devices, increasing the risk of data breaches and unauthorized access [23]. The other study explored mobile security risks in BYOD environments and emphasized the need for audits to check security and policy compliance [24]. Common BYOD issues are data leaks, unauthorized access, and privacy concerns [36]. The study also shows that certain factors influence how well employees follow BYOD security policies. Clear rules, employee confidence in security, IT support, and a sense of responsibility help improve compliance [42].

4.1.4 Network Attack

Network attacks, on the other hand, aim to bypass security defenses by exploiting vulnerabilities, thereby disrupting normal network operations. Such attacks can lead to device malfunctions, network overloads, service denial for legitimate users, reduced throughput, and malicious scanning activities [50]. Common tools used in network attacks include password cracking, sniffing, spoofing, reconnaissance, scanning, trojan horses, denial of service, and SQL injection, all of which target the integrity of computer networking infrastructure [31].

4.1.5 Human Error

Human error remains the most commonly identified threat in studies of remote working environments. Despite deploying robust security systems and processes, human factors continue to be the weakest link in cybersecurity [51]. The expanded threat surface and limited control over employees' personal networks and devices

significantly heighten risks, particularly in managing information and reporting security incidents [33]. The lack of cybersecurity awareness among non-technical employees not only increases the risk of security breaches and data leaks but also places a burden on dedicated cybersecurity teams [34].

4.2 Cybersecurity Recommendations for WFA Models

This section presents a summary of the answers to the research question below.

RQ2: What best practices are currently recommended for securing data and communication in a WFA environment?

The rapid shift towards remote work has brought forth a need for adaptable and robust cybersecurity strategies to protect sensitive information and ensure secure communication channels. As organizations continue to embrace flexible work models, the reviewed studies highlight various practices that address the unique challenges posed by WFA environments. In the discussion of best practices for securing data and communication in a WFA environment, it is essential to address the four key themes identified in the literature: Awareness and Education [R1], Phishing Protection [R2], Technical Countermeasures [R3], and Management and Audit [R4]. Using the data extracted in Section 4, a matrix analysis was performed to organize the findings. This analysis presents a list of studies along the horizontal axis and the identified cybersecurity for WFA recommendations along the vertical axis (Table VI).

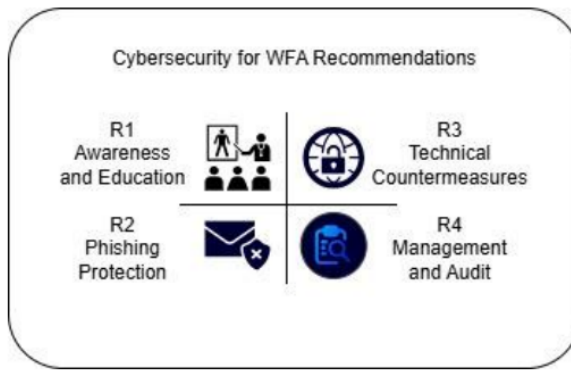

Figure 5. Cybersecurity for WFA Recommendations

This section discusses these identified cybersecurity for WFA recommendations in detail.

4.2.1 Awareness and Education [R1]

A multi-level cybersecurity training approach can enhance ASN competency in handling cyber threats, particularly in remote work settings [20]. Training should cover key areas such as phishing awareness, secure password management, insider threat, and incident reporting, as government employees often work with classified information that could be targeted by cybercriminals [35][38][39]. Additionally, digital literacy gaps among some civil servants necessitate continuous education on

internet ethics, social engineering risks, and safe teleworking behaviors to prevent inadvertent security breaches [21][24]. To foster a strong security culture, government agencies must integrate Security Education, Training, and Awareness (SETA) programs tailored to the cultural and operational contexts of different institutions [23][33][42]. These programs should emphasize effective cybersecurity reporting mechanisms to ensure that employees feel responsible for maintaining security and promptly reporting suspicious activities [34].

Given the hierarchical structure of many government institutions, structured security competency development and assessment programs are essential to reinforce awareness at all levels, from administrative staff to senior officials [23]. Regular phishing simulations and crisis-response exercises can also improve preparedness, reducing the risk of cyber incidents caused by human error [20][34]. The growing reliance on Bring Your Own Device (BYOD) policies in government agencies further underscores the need for BYOD security awareness programs that educate employees on the risks of using personal devices for official tasks [36].

Beyond general employee training, system administrators play a vital role in securing WFA environments within government agencies. Their responsibilities include ensuring stable and secure remote access, endpoint protection, and compliance with cybersecurity policies [32]. As remote work becomes more structured in government institutions, IT teams should receive specialized training in secure network configuration, remote monitoring, and endpoint protection strategies to safeguard both centralized and distributed IT infrastructures [34]. Additionally, regular cyber hygiene training for all ASN employees is critical to minimize security breaches caused by human error [41]. To support secure remote work, agencies should provide IT support hotlines and digital helpdesks that assist employees in maintaining secure configurations and resolving security concerns promptly [42].

By institutionalizing cybersecurity awareness as part of the national digital transformation agenda, government agencies can mitigate risks associated with remote work, protect sensitive public-sector data, and ensure operational efficiency in a flexible work environment [37][38]. Ultimately, a well-trained and security-aware ASN workforce is essential to strengthening the cybersecurity resilience of government institutions in the era of remote and digital governance.

Based on the key recommendations identified in previous studies, the following practical steps can be applied to improve cybersecurity awareness among non-technical ASN in a realistic and sustainable manner. To improve cybersecurity awareness among non-technical ASN, government agencies need to provide training that is simple, practical, and easy to understand. Key topics should include how to recognize phishing, create strong passwords, spot insider threats, and report incidents. This training should use formats like short videos, infographics, and real-life examples to keep employees engaged. Continuous learning is also important, especially to help staff understand safe internet use, social engineering tricks, and how to work securely from home.

Awareness programs should be adjusted to fit different job roles and organizational cultures. Agencies should also make it easy for employees to report suspicious activity and ensure they feel supported when doing so. Because many government offices have strict hierarchies, training should be given at every level — from junior staff to

top officials. Regular phishing tests and security drills can help reinforce learning. As more employees use personal devices for work, training should also cover how to keep those devices secure. Lastly, helpdesks and IT support must be available to guide employees in keeping their systems safe. These simple steps can build strong security habits among all staff, even those without technical backgrounds.

4.2.2 Phishing Protection [R2]

Remote work increases the risk of phishing attacks targeting government employees, making it essential for IT departments in government agencies to implement advanced email filtering mechanisms that detect and block phishing emails before they reach employees' inboxes [20]. These protections should be designed to identify misleading subject lines—such as urgent government updates or health alerts—that cybercriminals often use to exploit public sector workers [20]. Additionally, IT teams should optimize government email security infrastructures using techniques like Cached-N-Proxy, which enhances email filtering, reduces server load, improves response times, and mitigates insider threats that could originate from compromised or negligent government employees [39]. By integrating email security measures, strict access policies, and advanced filtering techniques, government institutions can reduce the risk of phishing attacks, protect classified information, and ensure secure remote communication for ASN in a WFA environment.

4.2.3 Technical Countermeasures [R3]

Government agencies must enforce endpoint protection tools like VPNs and ZTA to ensure secure remote access to government networks and classified systems [22][27]. Given the risks of unauthorized access, Multi-Factor Authentication (MFA), risk-based authentication (RBA), and role-based access controls (RBAC) should be mandatory, especially for high-privilege government accounts [28][36][40]. To mitigate ransomware and advanced persistent threats (APT), government institutions should secure VPN infrastructures using MFA, network segmentation, and endpoint protection tools such as Endpoint Detection and Response (EDR) and Next-Generation Antivirus (NGAV) [30]. Agencies must also deploy firewalls at VPN gateways, main offices, and branch networks, ensuring strict traffic segmentation between government, public, and confidential services [31].

Additionally, digital forensic readiness, including forensic logging and incident response planning, is essential for analyzing cyber incidents and strengthening national cybersecurity resilience [41]. Government IT teams should implement router-level security, VLAN segmentation, strong encryption, and secure cloud services to protect classified government communications and public service data [35][43]. To counter social engineering threats, email filtering, anti-phishing software, and endpoint security policies must be enforced across government agencies [37]. By integrating all recommendations above, the government can fortify remote work environments for ASN.

4.2.4 Management and Audit [R4]

Establishing clear IT security policies ensures compliance, defines personnel behavior, and enforces preventive measures against cyber threats [21]. Regular security audits, vulnerability assessments, and log analysis help identify and mitigate risks in remote work settings [30][35][43]. To strengthen cybersecurity culture, leadership must set a "tone at the top" by promoting security awareness and accountability across government institutions [23]. Continuous monitoring of remote access logs, user behavior, and network activity enhances threat detection [31][40][44], while RBA and privileged access management (PAM) provide additional layers of security [28][39]. Mobile Device Management (MDM) can be used to secure government-issued and BYOD devices, ensuring controlled access to sensitive data [36].

Government agencies must also implement non-punitive incident reporting mechanisms [33], compliance frameworks aligned with privacy regulations [43], and AI-driven behavioral analytics to detect anomalies [40]. By integrating governance, continuous auditing, and proactive monitoring, public institutions can build a resilient security culture that protects classified data, prevents insider threats, and ensures a secure and efficient remote work environment for ASN [38][29].

5. Disscussion and Conclusion

5.1 Case Study: Technical and Policy Approaches to Secure WFA in Government

To demonstrate how cybersecurity controls can be effectively implemented in a public sector setting, the following case example illustrates the approach taken by Government Agency A:

Government Agency A, operating in public services such as weather forecasting, earthquake alerts, and air quality monitoring, has adopted a secure WFA model. The agency runs a centralized data center receiving real-time data from sensors and branch offices via a secure tunnel. Employees can access these systems both from the internal network and remotely through SSL-VPN, protected by SSO and MFA. To support BYOD, the agency mandates EDR software on all employee devices. Internally, the data center is protected by a Next-Generation Firewall (NGFW), while external-facing services are secured using a Web Application Firewall (WAF). Periodic vulnerability scans and penetration testing are conducted to identify technical risks. On the human side, the agency regularly sends cybersecurity awareness emails and conducts phishing simulations. It also performs security audits and incident management on vulnerable hosts. This case demonstrates how WFA cybersecurity can be effectively managed in the public sector by combining technical controls with employee awareness, reflecting the four key themes identified in this study: Awareness and Education, Phishing Protection, Technical Countermeasures, and Management and Audit.

Government Agency A has integrated cybersecurity into its policies and daily operations. Remote access is allowed only through SSL-VPN, which is mandatory for accessing central systems from outside the headquarters. The agency's BYOD policy sets clear device requirements, including the installation of EDR, and outlines employee responsibilities for securing personal devices. Cybersecurity awareness programs are part of internal regulations, requiring participation in phishing simulations and

ongoing training, with activities tracked and tied to performance metrics. Incident response protocols are included in the agency's standard operating procedures (SOP), so employees know how to respond to security events. To improve this approach, the agency could add more practical steps to its WFA policy, such as clearer SOPs on remote work security measures. Additionally, sharing best practices through group discussions or social media could make it easier for employees to stay informed and engaged with cybersecurity practices, helping integrate security into everyday remote work.

5.2 Discussion : Challenges and Opportunities for Underexplored Areas

The WFA model offers significant benefits in enhancing the efficiency of business processes within the government sector. A common concern is that strict cybersecurity measures might hinder flexibility and innovation. While this concern is valid if the approach is disproportionate, the opposite is often true: flexible work can only be safe and sustainable if it is supported by appropriate and adaptive security controls. Without adequate protection, organizations are vulnerable to cyber incidents which could ultimately lead to access restrictions, operational disruptions, or even the suspension of flexible work policies. Therefore, cybersecurity should be seen not as a barrier, but as a fundamental enabler of flexibility. Adopting a risk-based approach allows security controls to be tailored to the user context, data sensitivity, and device conditions. For example, SSO technology simplifies authentication by allowing employees to securely access multiple systems with a single login. This reduces password fatigue and minimizes security risks, making the user experience more efficient while maintaining a strong security posture [52]. Rather than impeding innovation, smart and proportionate cybersecurity strategies create a safer and more flexible environment for remote work.

Some may argue that the productivity and efficiency gained from flexible work arrangements justify the risks associated with cybersecurity vulnerabilities. While this viewpoint highlights the tangible benefits of WFA, it overlooks the potential long-term consequences of insufficient security—such as data breaches, reputational damage, and disruption of critical government services [53]. Cybersecurity is not a barrier to productivity, but a foundational element that sustains it. Without secure systems, the very flexibility that enables productivity could be revoked in response to incidents.

However, WFA also introduces various security vulnerabilities, many of which have been discussed in prior studies. While general mitigation strategies for securing WFA environments have been explored, this study highlights certain threats that remain underexamined in existing literature. Furthermore, specific recommendations tailored to government institutions for mitigating cyber threats in WFA settings are still lacking. These gaps point to two key areas for further research: (1) deeper investigation into supply chain and third-party threats, and (2) development of cybersecurity frameworks and cultural assessments to strengthen WFA security in the public sector.

Although several common WFA threats have been addressed previously, emerging threats such as supply chain attacks and third-party risks have received limited attention. Supply chain security is particularly critical, as government procurement

processes often lack stringent cybersecurity oversight—creating exploitable vulnerabilities. Additionally, hybrid work environments, where on-site operations intersect with remote access, expose systems to risks, especially when third-party vendors or maintenance personnel access government infrastructure.

While general mitigation strategies for WFA security have been explored in the literature, these approaches are often broad and not directly applicable to the unique context of government institutions. The government sector, with its regulatory obligations, sensitivity of information, and hierarchical structures, presents distinct challenges that require tailored approaches. Governance and policy frameworks for WFA security must be reevaluated, as existing policies may not sufficiently address the complexities of remote work—especially regarding classified information and regulatory compliance. Moreover, cultural factors significantly impact cybersecurity resilience. Employee behavior, low awareness levels, and resistance to security protocols can impede the effective implementation of security measures. Cultural factors play a key role in improving security compliance among employees in flexible work settings. A strong security culture helps employees understand the importance of cybersecurity and encourages them to follow security rules, even when working remotely. Leadership is crucial in setting a good example by prioritizing security and encouraging staff to do the same. When employees see that security is a priority, they are more likely to follow the rules. Additionally, when security is part of the company culture, employees are more likely to report issues and work together to keep things secure, creating a safer environment for everyone.

To address these challenges, future research should focus on developing a cybersecurity framework specifically designed for WFA in the government sector. This includes strengthening supply chain security, managing third-party risks, and conducting cultural assessments to improve compliance and resilience. By addressing these gaps, particularly in supply chain security, third-party risk management, and cultural integration, future work can help establish cybersecurity frameworks that not only safeguard sensitive government data but also support the broader adoption of flexible work policies in the public sector.

6. Conclusion

Research on cybersecurity in WFA environments is not a new topic in academic literature. Various journals have explored this issue from different perspectives. However, challenges in identifying cyber threats and formulating best practices for WFA environments present opportunities for researchers to gain a deeper understanding of existing threats and develop effective mitigation strategies for the future. For policymakers in the government sector, this study also holds the potential to serve as an academic reference in formulating policies that support the implementation of WFA for ASN. By establishing clear, research-based guidelines, the adoption of WFA among government employees can be carried out securely, efficiently, and in a comprehensive manner that strengthens existing cybersecurity standards. Currently, there is little research focused specifically on cybersecurity in WFA environments within the government sector. While the government is part of the broader public sector, its unique challenges require more targeted research. This gap presents an

opportunity for future studies to explore government-specific cybersecurity needs in WFA settings, helping to develop more tailored and effective security strategies.

Cybersecurity in WFA environments, particularly within the government sector, remains an open area for further research. While many technical threats have been studied, several critical aspects require deeper exploration. Key topics for future research include supply chain security, focusing on vulnerabilities in government procurement processes and the need for stronger vendor risk management. Another important area is the integration of WFA with on-site operations, where hybrid work models create security gaps, especially when third-party vendors access government systems. Additionally, governance and policy frameworks need further evaluation to ensure cybersecurity policies remain enforceable and adaptive to remote work challenges. Lastly, cultural factors in security compliance should be studied to understand employee behavior, address resistance to security measures, and foster a security-first mindset. By addressing these gaps, future research can provide valuable insights to strengthen cybersecurity strategies for WFA in government institutions.

Future Research should examine how supply chain attacks impact government WFA environments and propose stronger vendor assessments, compliance enforcement, and regulatory controls. Future studies should explore secure access management strategies, including privileged access controls and network segmentation, while ensuring security measures do not disrupt operational efficiency. Research should assess current policies, identify enforcement gaps, and propose adaptive governance models that align with evolving cybersecurity threats. Future research should identify barriers to compliance and explore strategies for fostering a security-first culture through targeted training, leadership-driven initiatives, and incentive-based compliance programs.

Acknowledgement

The author expresses gratitude to the Meteorology, Climatology, and Geophysics Agency (BMKG) of the Republic of Indonesia for their support through the domestic Master's scholarship program, enabling this research to be conducted.

References

[1] Republik Indonesia. *Peraturan Presiden Republik Indonesia Nomor 21 Tahun 2023 Tentang Hari Kerja Dan Jam Kerja Instansi Pemerintah Dan Pegawai Aparatur Sipil Negara*. Peraturan Presiden Republik Indonesia. 2023.

[2] International Business Machines (IBM). *Cost of a Data Breach Report 2024*. IBM Security. 2024.

[3] Badan Siber dan Sandi Negara (BSSN). *Lanskap Keamanan Siber Indonesia 2023*. Id-SIRTII/CC–BSSN. 2023.

[4] Kementerian Keuangan Republik Indonesia. *Keputusan Menteri Keuangan Republik Indonesia Nomor 223/KMK.01/2020 Tahun 2020 Tentang Implementasi Fleksibilitas Tempat Bekerja (Flexible Working Space) Di Lingkungan Kementerian Keuangan*. Kementerian Keuangan Republik Indonesia. 2020.

[5] National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2.0*. Tech. rep. Gaithersburg, MD: National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.CSWP.29.

[6] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Standard. 2022.

[7] Prithwiraj Choudhury, Camelia Foroughi, and Barbara Larson. "Work From Anywhere: The Productivity Effects of Geographic Flexibility". In: *Strategic Management Journal* 42.4 (Apr. 2021), pp. 655–683.

[8] Eurofound and International Labour Organization. *Working Anytime, Anywhere: The Effects on the World of Work*. Geneva, CH and Luxembourg: Publications Office of the European Union, 2017.

[9] National Institute of Standards and Technology (NIST). *User's Guide to Telework and Bring Your Own Device (BYOD) Security*. Tech. rep. Gaithersburg, MD: National Institute of Standards and Technology, 2016. DOI: 10.6028/NIST.SP.800-114r1.

[10] National Institute of Standards and Technology (NIST). *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*. Tech. rep. Gaithersburg, MD: National Institute of Standards and Technology, 2016. DOI: 10.6028/NIST.SP.800-46r2.

[11] M. Mahyoub et al. *Cybersecurity Challenge Analysis of Work-from-Anywhere (WFA) and Recommendations guided by a User Study*. arXiv preprint arXiv:2409.07567. 2024.

[12] R. Klint. "Cybersecurity in home-office environments: An examination of security best practices post Covid". MA thesis. Sweden: University of Skövde, 2023.

[13] L. Galajda. "A study of information security awareness on teleworking security risks and recommendations since Covid19 pandemic". MA thesis. Sweden: Luleå University of Technology, 2023.

[14] S. Gumilang, R. Sutanto, and A. G. Dohamid. "Security Standard Recommendation of Teleworking in Government". In: *International Journal Of Humanities Education And Social Sciences (IJHESS)* 2.6 (2023), pp. 2070–2077.

[15] B. Kitchenham. *Procedures for Performing Systematic Reviews*. Tech. rep. Keele, UK: Keele University, 2004.

[16] J. Jesson, L. Matheson, and F. M. Lacey. *Doing Your Literature Review: Traditional and Systematic Techniques*. London, UK: SAGE Publications Ltd, 2011.

[17] M. J. Page et al. "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews". In: *BMJ* 372 (2021), n71. DOI: 10.1136/bmj.n71.

[18] C. Wohlin. "Guidelines for snowballing in systematic literature studies and a replication in software engineering". In: *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering (EASE 2014)*. 2014, p. 110.

[19] R. T. Watson and J. Webster. "Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0". In: *Journal of Decision Systems* 29.3 (2020), pp. 129–147.

[20] R. Naidoo. "A multi-level influence model of COVID-19 themed cybercrime". In: *European Journal of Information Systems (EJIS)* 29.3 (2020), pp. 306–321.

[21] A. M. Abukari and E. K. Bankas. "Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond". In: *International Journal of Scientific and Engineering Research (IJSER)* 11.4 (2020), pp. 1401–1407.

[22] R. Palanisamy, A. A. Norman, and M. L. Mat Kiah. "BYOD Security Risks and Mitigation Strategies: Insights from IT Security Experts". In: *Journal of Organizational Computing and Electronic Commerce* 31.4 (2021), pp. 320–342.

[23] N. A. A. Othman, A. A. Norman, and M. L. Mat Kiah. "Information System Audit for Mobile Device Security Assessment". In: *3rd International Cyber Resilience Conference (CRC)*. IEEE Access, 2021.

[24] A. Mihailovic et al. "COVID-19 and Beyond: Employee Perceptions of the Efficiency of Teleworking and Its Cybersecurity Implications". In: *Sustainability* 13 (2021), p. 6750.

[25] L. Astaja et al. "Cyber Security Risks and Challenges in Remote Work Under The COVID-19 Pandemic". In: *16th International Strategic Management Conference (ISMC)*. European Proceedings of Social and Behavioural Sciences. 2021, pp. 12–22.

[26] J. R. C. Nurse et al. "Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy". In: *HCI International 2021 - Posters*. Ed. by C. Stephanidis, M. Antona, and S. Ntoa. Vol. 1421. Communications in Computer and Information Science. Springer, 2021, pp. 583–590.

[27] K. Bicakci, Y. Uzunay, and M. Khan. "Towards Zero Trust: The Design and Implementation of a Secure End-Point Device for Remote Working". In: *International Conference on Information Security and Cryptology (ISCTURKEY)*. IEEE Access, 2021.

[28] D. Gogri. "Threats and Mitigation Strategies in Remote Work Scenarios: A Cybersecurity Perspective Post - COVID-19". In: *International Journal of Science and Research (IJSR)* 11.1 (2022), pp. 1687–1694.

[29] A. Georgiadou, S. Mouzakitis, and D. Askounis. "Detecting Insider Threat via a Cyber-Security Culture Framework". In: *Journal of Computer Information Systems* 62.4 (2022), pp. 706–716.

[30] N. Khantamonthon and K. Chimmanee. "Digital Forensic Analysis of Ransomware Attacks on Virtual Private Networks: A Case Study in Factories". In: *6th International Conference on Information Technology (InCIT)*. IEEE Access, 2022.

[31] S. M. Pedapudi and N. Vadlamani. "A Comprehensive Network Security Management in Virtual Private Network Environment". In: *International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*. IEEE Access, 2022.

[32] M. Kaur, S. Parkin, and M. Janssen. "I needed to solve their overwhelmness: How System Administration Work was Affected by COVID-19". In: *Proceedings of the ACM on Human-Computer Interaction* 6.CSCW2 (2022), p. 390.

[33] M. Plachkinova and L. Janczewski. "Comparing Information Security Compliance Between New Zealand, USA, and Vietnam". In: *Journal of Computer Information Systems* (2023), pp. 1–16.

[34] S. Keshvadi. "Enhancing Western Organizational Cybersecurity Resilience through Tailored Education for Non-Technical Employees". In: *International Humanitarian Technology Conference (IHTC)*. IEEE Access, 2023.

[35] Q. Alsayfi and A. Alsirhani. "The Impact of Remote Work on Corporate Security". In: *3rd International Conference on Computing and Information Technology (ICCIT)*. IEEE Access, 2023.

[36] P. Soubhagyalakshmi and K. S. Reddy. "An efficient security analysis of bring your own device". In: *IAES International Journal of Artificial Intelligence (IJ-AI)* 12.2 (2023), pp. 696–703.

[37] V. V. Muthuswamy. "Cyber Security Challenges Faced by Employees in the Digital Workplace of Saudi Arabia's Digital Nature Organization". In: *International Journal of Cyber Criminology* 17.1 (2023), pp. 40–53.

[38] J. K. Nwankpa and P. M. Datta. "Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers". In: *Computers & Security* 130 (2023).

[39] L. R. Mohan, R. K. Sambandam, and R. Gokulapriya. "Cached-N-Proxy: An Intelligent Proxy Algorithm for Preventing Insider Email Threats to Mail Servers". In: *International Conference on Contemporary Computing and Communications (InC4)*. IEEE Access, 2024.

[40] B. V. Raghav, N. S. Sree, and S. Pamitha. "A Comprehensive Analysis on Online Masquerade Attacks". In: *3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*. IEEE Access, 2024.

[41] A. Fikry et al. "Defining the Beauty of Cyber Hygiene: A Retrospective Look". In: *IEEE Engineering Management Review* 52.2 (2024).

[42] R. Palanisamy, A. A. Norman, and M. L. Mat Kiah. "Employees' BYOD Security Policy Compliance in the Public Sector". In: *Journal of Computer Information Systems* 64.1 (2024), pp. 62–77.

[43] P. V. Falade and P. O. Momoh. "Evaluating the Permissions of Monitoring Mobile Applications for Remote Employees: Analysing the Impact on Employer Trust and Employee Privacy Concerns". In: *International Journal of Scientific Research in Computer Science and Engineering* 12.1 (2024), pp. 42–52.

[44] M. Ozer et al. "The Shifting Landscape of Cybersecurity: The Impact of Remote Work and COVID-19 on Data Breach Trends". In: *Computer Science, Computer Engineering, Applied Computing (CSCE)*. IEEE Access, 2024.

[45] R. B. Permadi and K. Ramli. "Analysis of Measuring Information Security Awareness for Employees at Institution XYZ". In: *MALCOM: Indonesian Journal of Machine Learning and Computer Science* 4 (2024), pp. 1330–1338.

[46] F. Mouton, L. Leenen, and H. S. Venter. "Social engineering attack examples, templates and scenarios". In: *Computers & Security* 59 (2016), pp. 186–209.

[47] H. Abroshan et al. "Phishing Happens beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process". In: *IEEE Access* 9 (2021), pp. 44928–44949.

[48] J. Ferdous et al. "A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms". In: *IEEE Access* 11 (2023), pp. 12118–121141.

[49] Cybersecurity & Infrastructure Security Agency (CISA). *Defining Insider Threats*. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats. Accessed: 2025-05-11. 2024.

[50] N. Hoque et al. "Network attacks: Taxonomy, tools and systems". In: *Journal of Network and Computer Applications* 40 (2014), pp. 307–324.

[51] E. P. Subagyo and K. Ramli. "Analyzing the Impact of Information Security Awareness Training to the Employees of Telco Company XYZ". In: *Budapest International Research and Critics Institute (BIRCI-Journal)* 5 (2022), pp. 8799–8808.

[52] IQPC. *Finding the balance: Remote work flexibility vs. cybersecurity risks*. https://www.iqpc.net.au/finding-the-balance-remote-work-flexibility-vs-cybersecurity-risks/. Accessed: 2025-05-11. 2025.

[53] European Union Agency for Cybersecurity (ENISA). *Remote Working – Cybersecurity Advice for Employers*. https://www.enisa.europa.eu/publications. Accessed: 2025-05-11. 2021.