INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 8, (2024) E-ISSN: 2222-6990

Software Security Readiness Index for Remote Working Employee in Public Organization: Preliminary Study

Raihana Syahirah Abdullah, Halimaton Hakimi, Massila Kamalrudin

Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka
Corresponding Author Email: halimaton.saadiah@apu.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i8/22773 DOI:10.6007/IJARBSS/v14-i8/22773

Published Date: 31 August 2024

Abstract

The COVID-19 pandemic necessitated a rapid shift to remote working, compelling employees in public organizations to rely heavily on software facilitated by the Internet. This sudden transition, combined with limited guidance, exposed organizations to heightened software security risks, potentially affecting their overall performance. In response, this preliminary study investigates the software security readiness of remote working employees in public organizations. Through a systematic literature review, common security challenges faced by remote workers were identified, along with key factors influencing software security. However, to ensure the relevance and applicability of these factors, a survey was conducted to empirically validate them. The survey targeted remote working employees in public organizations, aiming to uncover current challenges and evaluate the significance of the identified software security factors. The findings from the survey offer critical insights into the prevalent security issues and the effectiveness of the factors in mitigating these risks. This research contributes to the understanding of software security readiness in remote working environments, providing a foundational framework for public organizations to enhance their software security posture. The results emphasize the importance of proactive security measures and awareness among employees to safeguard organizational assets in the evolving landscape of remote work.

Keywords: Software Security, Public Organization, Preliminary Study, COVID-19, Readiness Model.

Introduction

The outbreak of the COVID-19 pandemic in early 2020 prompted an unprecedented global shift in work practices, with remote working becoming the new norm for millions of employees across both the private and public sectors. Public organizations, traditionally characterized by structured work environments with stringent protocols, found themselves abruptly transitioning to decentralized, home-based work settings. This shift, driven by the need for social distancing, introduced a new set of challenges, particularly in the realm of software security. As employees began working remotely, often using personal devices and unsecured networks, public organizations became increasingly vulnerable to cyber threats, which could potentially compromise sensitive data and disrupt critical public services.

The rapid adoption of remote work, while essential for maintaining operations during the pandemic, exposed significant gaps in the software security preparedness of many public organizations. The reliance on software applications and internet-based tools, many of which were hastily implemented without thorough security assessments, created new vulnerabilities. Cybercriminals, recognizing these weaknesses, quickly adapted their tactics, leading to a surge in cyberattacks targeting remote workers. Public organizations, which often handle sensitive information and provide essential services, were particularly at risk, underscoring the urgent need to address these software security challenges.

Software security readiness, which encompasses the awareness, preparedness, and ability of employees to secure software systems, became a critical focal point in this new work environment. Ensuring that remote working employees in public organizations are equipped to manage and mitigate software security risks is essential for safeguarding organizational assets and maintaining the integrity of public services. However, despite the growing recognition of these challenges, there is a lack of comprehensive research specifically focused on the software security readiness of remote workers within the public sector. This gap in the literature highlights the need for a targeted investigation into the software security challenges faced by public sector employees and the factors that influence their readiness to address these challenges.

The primary objective of this study is to explore and empirically validate the factors that contribute to software security readiness among remote working employees in public organizations. By conducting a systematic literature review and subsequent survey, this research aims to identify the common security challenges faced by remote workers and assess the significance of key factors in enhancing software security. The findings from this study will provide valuable insights into the current state of software security readiness in public organizations and offer practical recommendations for improving security practices in the context of remote work.

Given the critical role that public organizations play in society, ensuring their software security is not only a matter of organizational integrity but also a public concern. A breach in security could have far-reaching consequences, affecting not just the organization but also the citizens who rely on its services. As such, this research is motivated by the need to support public organizations in strengthening their software security frameworks and ensuring that their employees are adequately prepared to navigate the complexities of remote work in a secure manner.

This paper is structured as follows: The next section provides a detailed literature review, examining existing studies on software security and remote working, and identifying the key factors influencing software security readiness. The methodology section outlines the research design, including the survey used to collect empirical data. The results section presents the findings from the survey, highlighting the current challenges and the significance of the identified factors. Finally, the discussion and conclusion sections reflect on the implications of these findings for public organizations and offer recommendations for enhancing software security readiness in remote working environments.

Research Background and Motivation

The COVID-19 pandemic catalyzed one of the most significant shifts in modern work practices, compelling organizations worldwide to adapt to remote working. For many public sector organizations, the transition was abrupt, and the move to a predominantly online work environment posed unprecedented challenges, particularly in software security. As employees started working from home with limited preparation, the reliance on software applications and internet-based tools intensified, exposing these organizations to heightened risks of cyber threats and vulnerabilities. The urgency of these challenges underscored the need for public sector organizations to assess their readiness in ensuring software security for remote working employees.

Remote working, while not a new concept, was rapidly normalized during the COVID-19 pandemic. Public organizations, which typically have stringent protocols and controlled environments for information security, were suddenly forced to operate in a decentralized manner. Employees, now working from home, had to rely on personal devices, insecure networks, and unfamiliar software platforms, many of which were hastily implemented to facilitate remote work. This shift created a fertile ground for cybercriminals, who quickly adapted their strategies to exploit the vulnerabilities inherent in this new work environment.

Software security threats such as phishing attacks, ransomware, and data breaches became more prevalent during the pandemic, targeting both private and public sectors (Rao & Kope, 2021). Public organizations, which often handle sensitive information, were particularly at risk. The existing security frameworks were not designed to accommodate such a large-scale and rapid transition to remote working, leaving many organizations scrambling to implement measures that could mitigate these new risks. As a result, the software security landscape for remote work became a critical area of concern, necessitating immediate attention and action from both organizational leaders and policymakers.

The Need for Software Security Readiness

Software security readiness is crucial in safeguarding public organizations against the myriad of cyber threats that have proliferated with the rise of remote working. Ensuring that employees are not only aware of these threats but also equipped with the necessary tools and knowledge to combat them is essential for maintaining organizational security. However, the transition to remote work revealed significant gaps in the preparedness of many public organizations, particularly in terms of software security.

Studies have shown that remote working employees often lack the necessary training and awareness to effectively manage software security risks (Kotulic & Clark, 2020). This lack of preparedness is compounded by the fact that many public organizations rely on legacy systems that are not designed for remote access, making them more vulnerable to attacks. Furthermore, the rapid deployment of new software solutions during the pandemic, often without thorough security vetting, exacerbated these vulnerabilities. This situation highlighted the urgent need for public organizations to reassess their software security frameworks and to ensure that their employees are prepared to operate securely in a remote working environment.

Theoretical Underpinnings and Literature Review

The concept of software security readiness can be understood through various theoretical lenses. One approach is the Technology-Organization-Environment (TOE) framework, which posits that the successful implementation of technological solutions, including software security measures, depends on the interplay between technology, organizational structure, and the external environment (Tornatzky & Fleischer, 1990). In the context of remote work, this framework suggests that the effectiveness of software security measures is influenced not only by the technology itself but also by the organization's policies, culture, and the broader external threats that it faces. Another relevant theoretical perspective is the Protection Motivation Theory (PMT), which emphasizes the role of perceived threats and coping strategies in motivating protective behaviors (Rogers, 1975). In the context of software security, PMT suggests that employees are more likely to adopt secure practices if they perceive a high level of threat and believe that they have the capability to mitigate these risks through appropriate actions. This theory underscores the importance of awareness and training in fostering a culture of security within organizations.

Empirical research in the field has identified several factors that influence software security readiness in remote work settings. For instance, Kotulic and Clark (2020) highlight the importance of employee awareness and training in reducing software security risks. Their study found that organizations that invested in regular software security training for their employees were better able to manage the risks associated with remote work. Additionally, Rao and Kope (2021) emphasize the role of organizational policies in shaping employee behavior, noting that clear and enforced policies regarding software use and data protection are crucial for maintaining security in a remote working environment.

Research Motivation

The motivation for this research arises from the critical need to address the software security challenges faced by public organizations in the wake of the COVID-19 pandemic. While much of the existing literature has focused on software security in general, there is a lack of comprehensive studies that specifically examine software security readiness in the context of remote work within the public sector. This research seeks to fill that gap by exploring the specific challenges faced by public sector employees and identifying the key factors that contribute to effective software security in a remote working environment. Given the sensitivity of the information handled by public organizations, the implications of a security breach can be severe, ranging from compromised citizen data to disruptions in essential services. As such, it is imperative to understand how well-prepared public organizations are in terms of software security and to identify areas where improvements can be made. This research is driven by the need to provide actionable insights that can guide public organizations in enhancing their software security frameworks, ensuring that they are better equipped to manage the risks associated with remote working.

Furthermore, the findings from this research will contribute to the broader body of knowledge on software security, offering valuable insights into how organizations can adapt their security practices to meet the challenges posed by remote work. By empirically validating the factors that influence software security readiness, this study aims to provide a robust framework that public organizations can use to assess and improve their software security posture.

Methodology

This study employed a mixed-method approach, combining quantitative and qualitative research methods to investigate the research problems related to software security readiness for remote working employees in public organizations. Two preliminary studies were conducted: a user study through a survey and semi-structured interviews. The combination of these methods allowed for a comprehensive understanding of the issues at hand, providing both statistical data and in-depth insights into the experiences and perspectives of the participants. The primary method of data collection was an online survey, which targeted individuals working in public universities in Malaysia, specifically those with experience using software systems as remote workers during the COVID-19 pandemic. The survey aimed to explore their involvement with software security, identify their experiences with remote access, and uncover the main challenges they faced in software security preparedness.

A total of 108 respondents participated in the survey, comprising lecturers and administrative officers from various public universities in Malaysia. These participants were selected based on their roles in higher education institutions, where they had substantial experience with software systems and remote working. The survey was conducted online, ensuring that all participants were treated anonymously to protect their privacy and encourage honest responses. Participation in the survey was voluntary, and the respondents were informed that their involvement was not mandatory, they would not be evaluated on their performance, and the data collected would be used solely for research purposes. This approach aligns with ethical research practices, ensuring the participants' rights and confidentiality were upheld (Creswell & Creswell, 2018).

The survey was designed to collect quantitative data on the participants' experiences and perceptions regarding software security in a remote working environment. The questions were structured to assess their level of involvement in software security, their experience with remote access during work-from-home scenarios, and the challenges they encountered in ensuring secure remote working practices. The survey also sought to identify any factors that influenced their software security readiness, such as organizational policies, training, and the availability of secure software tools.

Data were collected through an online survey platform, which allowed for easy distribution and response collection. The responses were automatically recorded and compiled into a database for analysis. The quantitative data were analyzed using statistical methods, including descriptive statistics to summarize the demographic details of the participants and inferential statistics to identify significant factors influencing software security readiness. The results of this analysis provided a broad overview of the challenges faced by remote workers in public universities and the factors that impacted their ability to maintain secure work practices

The demographic details of the participants are summarized in Table 1. The table provides an overview of the number of participants, their roles, their working experience in public universities in Malaysia, and the purpose of the study. This information is crucial for contextualizing the findings and ensuring that the results are representative of the population under study

Table 1
The demography details of the participants

Demography	Details of Participants
Number of Participants	108
Level of Experience	Lecturer and Administrative
Working Experience	Working experience in public university in Malaysia
Purpose of the Study	(1) To explore the involvement of using software security (2) To identify the experience of lecturer using remote access during work from home. (3) To identify the main current problem that face in preparedness software security in facilitating secure remote working. (4) To identify any factors that influence to software security.

Finding

The analysis of respondents' backgrounds revealed a significant gender imbalance among the participants. As illustrated in Figure 1, a substantial majority of the respondents were female, comprising 89% of the sample, while only 11% were male. This disproportionate representation highlights a noteworthy trend within the context of the study, particularly in relation to the professions of the respondents, who were largely lecturers and administrative officers in public universities. This gender disparity aligns with broader societal beliefs and practices that encourage the entry of women into certain professions, such as teaching. According to Nair (2017), teaching is often perceived as a suitable profession for women due to its perceived lower demands and shorter working hours compared to other occupations. This perception, combined with societal values and government policies that support women in education, has contributed to a gender ratio in the teaching profession that is considerably skewed toward women.

The findings from this study are consistent with existing literature, which suggests that the teaching profession, particularly in public sector institutions, is dominated by women. This gender distribution may have implications for the study's outcomes, particularly in understanding the experiences and challenges faced by female employees in the context of remote working and software security. Given that the majority of respondents were female, their perspectives and experiences are likely to be reflected more prominently in the results, potentially highlighting gender-specific challenges or needs in relation to software security preparedness in remote work settings. This gender imbalance underscores the importance of considering gender dynamics in the analysis and interpretation of the study's findings. The predominance of female respondents may influence the study's conclusions, particularly in areas where gender-specific experiences play a role in shaping attitudes toward software security and remote work. Further research could explore these dynamics in more detail, examining whether similar patterns emerge in other public sector contexts and how they might impact overall software security readiness in remote working environments**.**

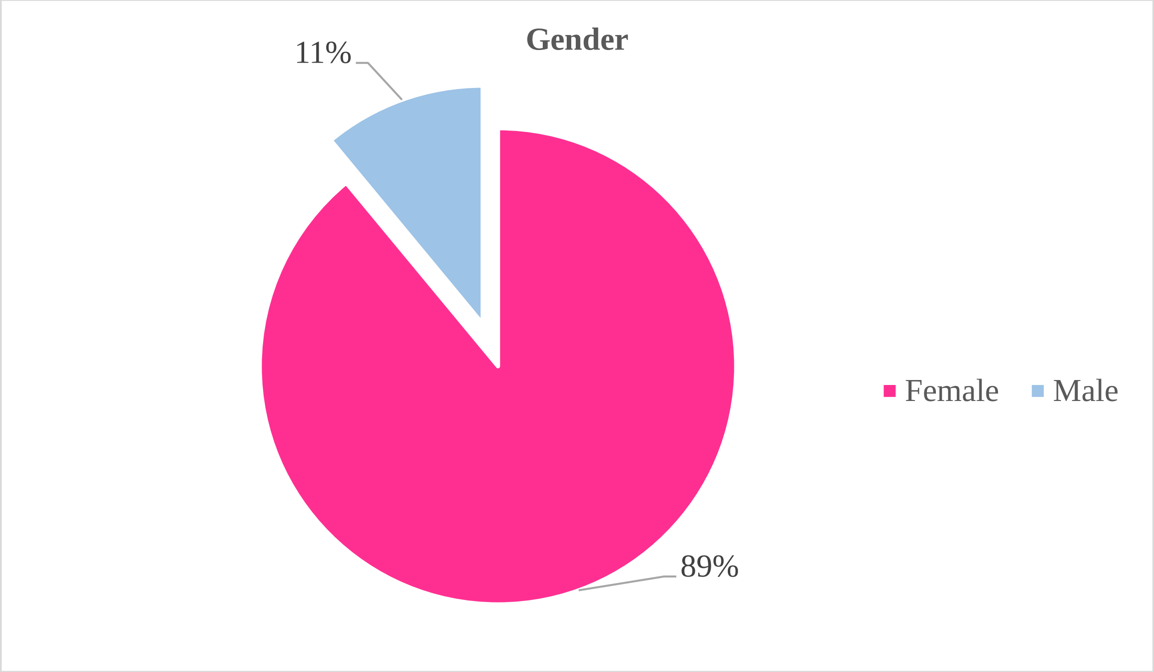


Figure 1: Percentage of respondent’s gender

Figure 2 shows the age of respondents responded the survey, based on three categories, which are 21-30 years, 31-40 years and 41-50 years. The highest percentage, that is 81% responded to the survey are those in the group of 31-40 years old. The percentage of respondents in group 21-30 years old are 11% and the least group that respond the survey are the group 41 years old and over, which is 8%. It can be implied that the young generation are the frequently for remote working.

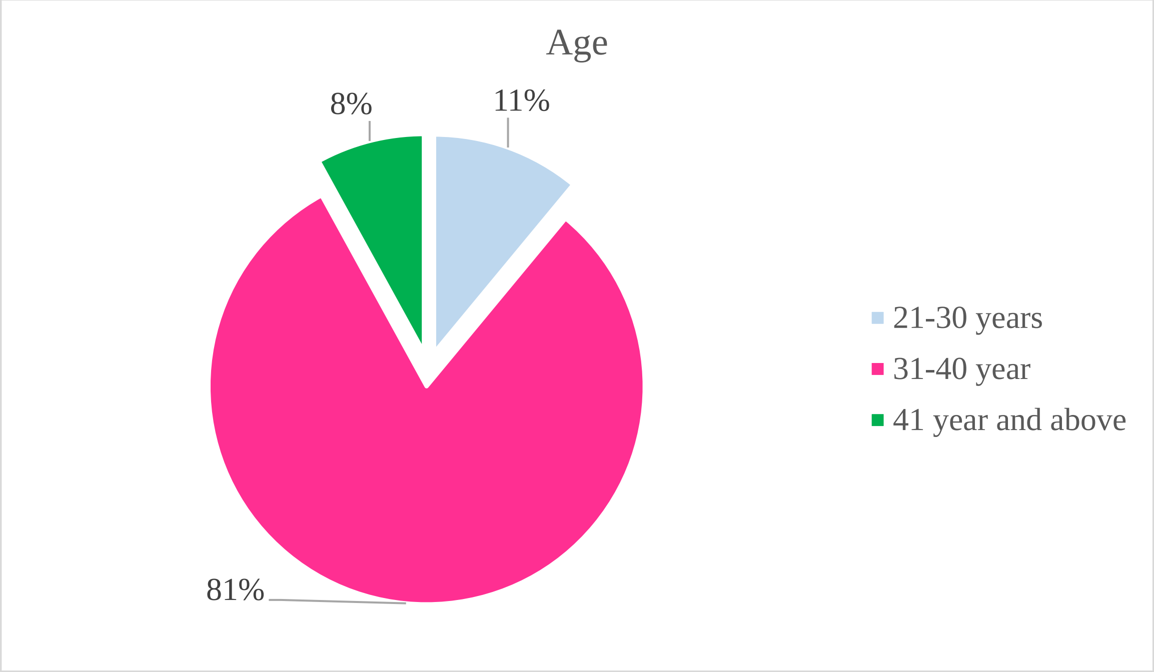


Figure 2: Percentage of respondents' age

According to the findings presented in Table 2, all respondents affirmed that their organizations had embraced remote work or working from home. A significant majority, comprising 90.3% of respondents, verified that their organizations had provided them with the necessary computing tools to facilitate remote work. Regarding whether their organizations conducted assessments on their computing devices (whether personally owned or provided by the organization) to ascertain the security configuration and compliance with security policies for remote work, only 25.8% of respondents agreed with this statement, while 74.2% opposed it.

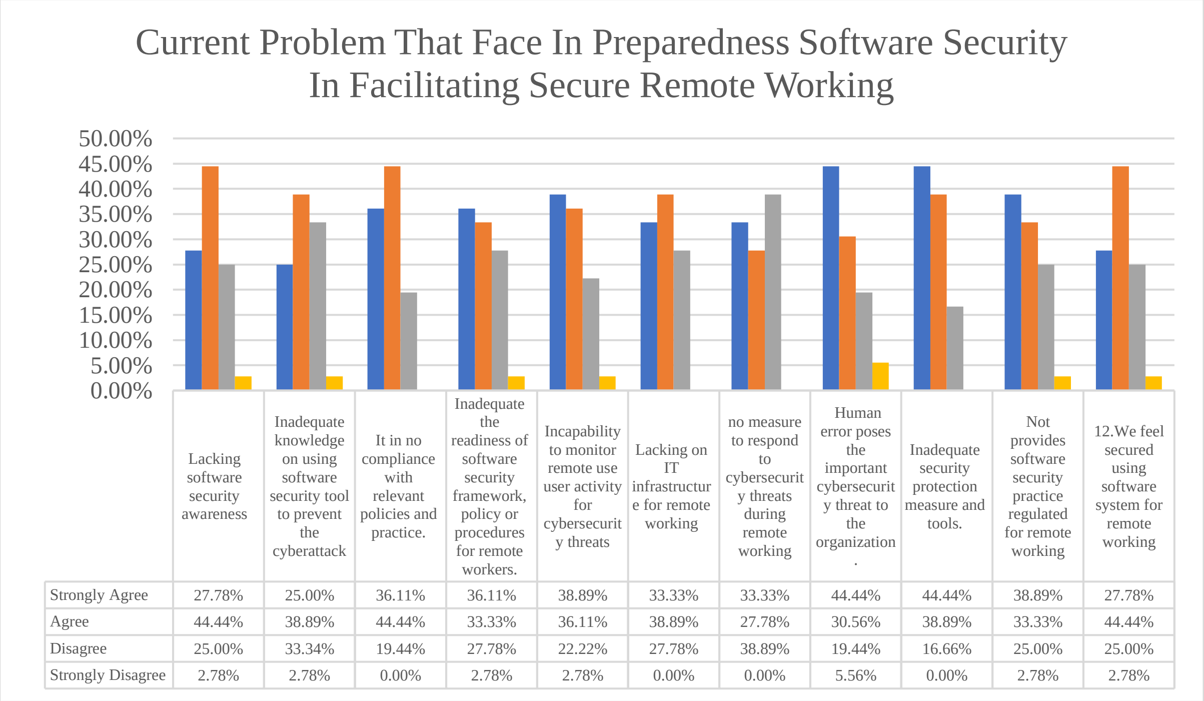
The majority of respondents, totalling 91.9%, confirmed that they were permitted to use their computing devices for personal purposes while working remotely. Lastly, 74.2% of respondents reported that they were able to access all ICT resources needed for their work as if they were physically present in the office.

Table 2
Remote working experience

Question	Yes	No
Did your organization adopt remote working or working from home?	100%	0%
Were you facilitated with the requisite computing tools such example laptop to enable you to work remotely?	90.3%	9.7%
If your answer is (No) above, does your organisation allow you to use you own device to work from home?	100%	0%
Does your organization assess your computing device (personally owned or provided by your organization) to determine the security configuration and compliance level to security policies place for remote working?	25.8%	74.2%
Do you use your computing device for personal use while working remotely	91.9%	8.1%
When working from home, are you able to access all ICT resources required to do your work as though you were physically present at the office?	74.2%	25.8

Discussion

The results from the preliminary study provide valuable insights into the challenges faced by respondents in ensuring software security for remote working environments. Figure 3 illustrates the key issues identified by the participants, highlighting several critical areas of concern.



	Lacking software security awareness	Inadequate knowledge on using software security tool to prevent the cyberattack	It in no compliance with relevant policies and practice.	Inadequate the readiness of software security framework, policy or procedures for remote workers.	Incapability to monitor remote use user activity for cybersecurity threats	Lacking on IT infrastructure for remote working	no measure to respond to cybersecurity threats during remote working	Human error poses the important cybersecurity threat to the organization.	Inadequate security protection measure and tools.	Not provides software security practice regulated for remote working	12.We feel secured using software system for remote working
Strongly Agree	27.78%	25.00%	36.11%	36.11%	38.89%	33.33%	33.33%	44.44%	44.44%	38.89%	27.78%
Agree	44.44%	38.89%	44.44%	33.33%	36.11%	38.89%	27.78%	30.56%	38.89%	33.33%	44.44%
Disagree	25.00%	33.34%	19.44%	27.78%	22.22%	27.78%	38.89%	19.44%	16.66%	25.00%	25.00%
Strongly Disagree	2.78%	2.78%	0.00%	2.78%	2.78%	0.00%	0.00%	5.56%	0.00%	2.78%	2.78%

Figure 3: Current Problem

Based Figure 3 shows the current problem face in preparedness software security when facilitating secure remote working in public organization such as

Lack of Software Security Awareness and Knowledge

A predominant issue reported by respondents is a lack of software security awareness and inadequate knowledge regarding the use of software security tools. This finding underscores a significant gap in the preparedness of remote workers to handle cybersecurity threats. Many participants indicated that they were not sufficiently informed about the best practices for securing software and the tools available to prevent cyberattacks. This lack of awareness can severely undermine the effectiveness of cybersecurity measures and leave remote workers vulnerable to various types of cyber threats.

Insufficient Organizational Compliance and Readiness

Another major concern highlighted by the respondents is the insufficient compliance of organizations with relevant policies related to remote working. Many participants noted that their organizations did not provide adequate support or adhere to established policies for remote work security. This lack of compliance is critical, as it suggests that organizations may not have implemented or enforced effective security frameworks, policies, or procedures tailored to remote working conditions. Without proper guidelines and compliance measures, remote workers are left with limited support and resources to manage cybersecurity risks effectively.

Ineffective Monitoring and Response Measures

Respondents also expressed concerns about their organizations' ability to monitor remote work activities and respond to cybersecurity threats. The majority of participants agreed that their organizations were incapable of effectively monitoring the use of cybersecurity tools by remote workers and lacked efficient measures to respond to cyber threats. This inadequacy in monitoring and response could result in delayed identification and mitigation of security incidents, exacerbating potential damage and compromising organizational data integrity.

The findings of this study reveal critical weaknesses in the current approach to managing software security in remote working environments. The combination of inadequate security awareness among employees, insufficient organizational policies, and ineffective monitoring and response measures highlights a need for comprehensive improvements in cybersecurity practices. Organizations must prioritize enhancing software security awareness through training programs, ensuring compliance with remote work policies, and implementing robust monitoring and response frameworks.

Factors Influencing Software Security Readiness

In the preliminary study, respondents were asked to identify factors influencing software security readiness, with the option to select multiple factors they deemed relevant to remote working environments. Figure 4, presents the factors identified by the respondents, highlighting their views on what contributes to effective software security.

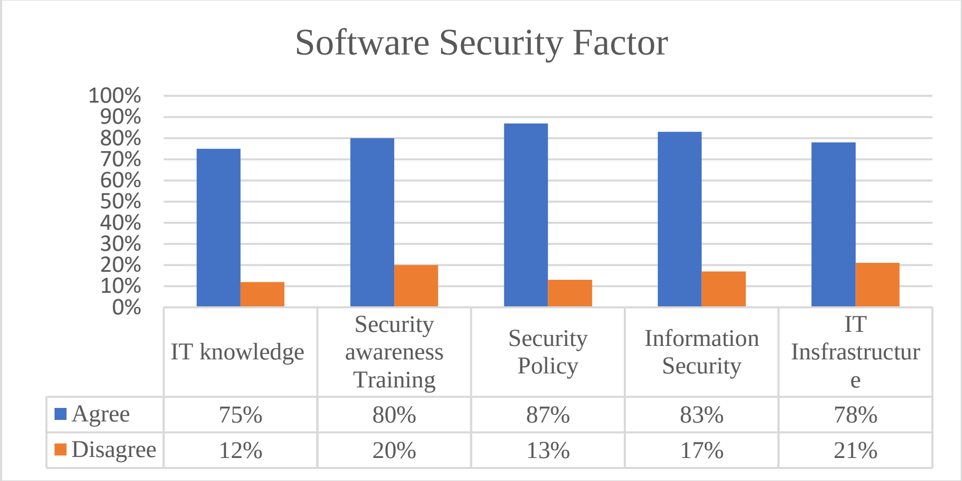


Figure 4: Factor of software security readiness for remote working

Based on Figure 4, Respondents universally agreed that IT knowledge is a crucial factor influencing software security readiness. A strong understanding of information technology and its applications is essential for remote workers to effectively manage and mitigate cybersecurity risks. Proficiency in IT enables employees to use security tools correctly and adhere to best practices for safeguarding sensitive information. Security awareness training emerged as another critical factor. Respondents highlighted that regular training sessions are necessary to keep remote workers informed about the latest cybersecurity threats, vulnerabilities, and protective measures. Such training helps in building a security-conscious culture within the organization and equips employees with the knowledge to recognize and respond to potential threats. The presence and enforcement of a comprehensive security policy were also deemed significant. A well-defined security policy provides clear guidelines and procedures for remote working, ensuring that employees understand their roles and responsibilities in maintaining software security. Effective policies help standardize security practices and ensure consistent protection across the organization. Information security was recognized as a fundamental factor influencing software security readiness. This encompasses measures to protect data from unauthorized access, breaches, and other security threats. Ensuring that information security protocols are in place and adhered to is vital for safeguarding the integrity and confidentiality of organizational data. The adequacy of IT infrastructure was highlighted as another important factor. Robust IT infrastructure, including reliable hardware and secure networks, is essential for supporting secure remote work. An effective infrastructure ensures that remote workers have the tools and resources needed to perform their duties securely and efficiently.

In addition to the established factors, respondents suggested two new factors that could influence software security readiness:

- **Trust:** Building trust between remote workers and their organization is seen as a crucial element. Trust can impact how employees engage with security practices and tools. When employees trust that their organization is committed to their security and well-being, they are more likely to follow security protocols diligently.
- **Technology Reliability:** The reliability of technology used for remote working is another factor suggested by respondents. Reliable technology ensures that security measures function correctly and consistently, reducing the risk of vulnerabilities caused by technical failures or issues.

Conclusion and Future Work

In conclusion, this study provides valuable insights into the factors influencing software security readiness for remote working employees in public organizations. Key factors identified include IT knowledge, security awareness training, security policies, information security, and IT infrastructure. Additionally, trust and technology reliability emerged as important factors that can enhance software security in remote settings. These findings highlight the necessity for organizations to adopt a comprehensive approach to address software security challenges, combining traditional measures with newer considerations to effectively support remote workers and mitigate cybersecurity risks.

However, the study has several limitations. The sample size was relatively small and predominantly consisted of lecturers and administrative officers from public universities, which may not fully represent the broader spectrum of remote workers across different sectors. The reliance on self-reported data introduces potential biases and inaccuracies that could affect the reliability of the findings. Additionally, the study's cross-sectional nature provides only a snapshot of current practices and perceptions, without accounting for changes over time. The scope of factors examined was also limited, and other relevant factors may not have been captured.

Future research should aim to address these limitations by including a more diverse sample of remote workers from various industries to enhance the generalizability of the findings. Longitudinal studies could provide insights into how software security practices evolve over time and track the impact of different interventions. Additionally, exploring other potential factors influencing software security readiness and employing mixed-methods approaches could offer a more comprehensive understanding of the challenges and solutions. Evaluating the effectiveness of specific interventions, such as targeted training programs and technological upgrades, will further aid in developing robust security practices tailored to remote working environments.

References

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Kamalrudin, M., Hakimi, H., Abdollah, M. F., & Hardi, R. (2022, November). SSRINDEX tool: An automated tool to measure level of software security readiness index for remote working during Covid-19 pandemic. In AIP Conference Proceedings (Vol. 2658, No. 1). AIP Publishing.

Nair, R. (2017). Teaching as a Suitable Profession for Women. *Journal of Gender Studies, 26*(1), 89-105.