Anusandhanvallari
Vol 2025, No.1
January 2025
ISSN 2229-3388

Cybersecurity Consciousness in Hybrid Work: The Dominant Role of Organizational and Technological Support

Kavya Poduval [1], Dr. T. Shenbhagavadivu [2], Vinitha.V [3]

[1] Research Scholar, Department of Management, Sri Krishna Arts & Science College, Coimbatore, Affiliated to Bharathiar University, Tamil Nadu, India
kavyarevathy@gmail.com, ORCID: https://orcid.org/0009-0008-0346-7841
[2]Associate Professor, Department of Management, Sri Krishna Arts and Science College, Coimbatore Affiliated to Bharathiar University, Tamil Nadu, India
shenbhajeevi@gmail.com, ORCID: https://orcid.org/0000-0001-5881-9527
[3] Research Scholar, Department of Management, Sri Krishna Arts & Science College, Coimbatore, Affiliated to Bharathiar University, Tamil Nadu, India
vinitha16061986@gmail.com, ORCID: https://orcid.org/0009-0009-0243-587X

Abstract: Using regression analysis on a sample of 106 Bangalore- based IT professionals, this study looked at the variables affecting cybersecurity awareness in hybrid work settings. Cyber security Consciousness (CSC) according to the study, is a combination of behaviour, attitude, and awareness. Initial regression (Model 1) revealed no significance direct impact of work arrangement alone, despite descriptive statistics showing generally high CSC rating across work arrangements, especially for flexible and hybrid models. But according to the thorough Model 2, Work Environment Security, Organizational Support, and Technology infrastructure are all strategically significant positive predictors of CSC, with Organizational Support being the most powerful. Age also had a slight but noteworthy impact. Whether IT professionals work on-site, hybrid, or remotely, the positive effects of robust technology infrastructure and organizational support on cybersecurity consciousness appear to be constant, according to a subsequent (Model 3) that found no significant interaction effects between work arrangements (hybrid/remote) and these environmental factors. These results demonstrate how important organizational and technological environment elements are in raising cybersecurity awareness among IT workers on changing work models. rather than work arrangements. The practical implications suggest that organizations should prioritize organizational support, technology infrastructure, and work environment security rather than restricting work arrangement flexibility, as environmental support systems are more critical than physical work location for maintaining cybersecurity consciousness. The cross-sectional design prevents establishing causal relationships between variables, meaning we cannot determine whether environmental factors cause improved cybersecurity consciousness or if the relationship works in reverse. Investigating the mediating mechanisms that explain how environmental factors influence cybersecurity consciousness would provide deeper insights into the underlying processes and help develop more targeted interventions.

Keywords: Cybersecurity consciousness, hybrid work model, IT employees, organizational support, Technology, remote work security

1. Introduction

Businesses' perspective on cybersecurity have been completely altered by a seismic shift that has occurred due to the global workforce. Due to the COVID- 19 pandemic's quick shift to hybrid work models, there is now an unmatched cyber security paradigm that goes much beyond conventional perimeter- based security strategies. Its staff have been especially affected by this shift, as they now work in a variety of environments with different levels

of security infrastructure, resulting in complex problems that call for increased cybersecurity awareness. The development of hybrid work arrangements signifies a fundamental rethinking of workplace flexibility and employee independence, rather than merely adapting to pandemic limitations. Nevertheless, this progression has brought about a complex cybersecurity issue that businesses all over the world are still trying to figure out how to handle. A hybrid work model, in contrast to a traditional work environment where security measures might be centrally managed and monitored, spreads security duties throughout various sites, devices, and network infrastructures, resulting in what cybersecurity professionals refer to as "expanded attack surface." Despite significant advancements in the cybersecurity environment over the previous ten years, the growth of the hybrid work adoption has accelerated, bringing years of anticipated changes into just a few months. While the conventional security models rely on protection from entry points and perimeters, they have shown to be inadequate for moving people between corporate offices, home office spaces, or co-working spaces as well as mobile locations. Because of this change, cybersecurity strategy has had to undergo a radical transformation, moving from location – based security to identity based and behaviour-based security models. This shift has implications that go beyond technology to include organizational culture, individual behaviour patterns, and human aspects.

A multifaceted notion known as cybersecurity awareness is a common theme in hybrid work environments and extends beyond traditional security awareness training. It symbolizes the integration of cognitive awareness, emotional engagement, and behavioural dedication to cybersecurity practices in a variety of workplace. Five fundamental dimensions are present in this consciousness: the capacities for detecting and responding to threats, acting on self- interest, understanding security risks, perceiving risk, and taking measures to protect individuals from potential threats. Hybrid work models make it challenging to achieve cyber security awareness due to the need to balance contextual differences with consistency in security outcomes. The immediate security issues facing an IT professional working in a safe corporate environment may differ from those facing the same person working from a home office, or public area. However, to make the right security choices in every scenario. The fundamental security mindset must be strong enough.

1.1 The Strategic Importance of IT Employees

The role of IT workers in organizational cyber security ecosystems is special. They work concurrently as system administrator's, security practitioner and in many cases, as informal security counsellors to their non- technical co-workers. Due to this diverse position, their cyber security awareness has a greater organizational impact since their security choices and actions have an impact on the security posture of the systems they manage, the colleague they support, and their own risk profile. Because IT workers often have privileged access to vital systems, databases, and network infrastructure, their cybersecurity awareness is a major organizational priority. An IT professional security flaw can have a domino effect throughout an organization, endangering many systems, revealing private information, and interfering with business processes. The privileged access that IT employees typically maintain to critical systems, databases, and network infrastructure makes their cybersecurity consciousness a high-stakes organizational concern. A security lapse by an IT professional can have cascading effects throughout an organization, potentially compromising multiple systems, exposing sensitive data, and disrupting business operations. This reality underscores the critical importance of understanding and enhancing cybersecurity consciousness specifically among IT professionals in hybrid work environments.

1.2 Objective of the study

1) To measure how aware and conscious IT employees in Bangalore are about cybersecurity when working in hybrid (remote + office) setups.

2) To identify what factors (like experience, training, company support, work location) most strongly influence whether IT employees have good cybersecurity awareness and habits.

1.3 Research Gap

The research gap centres the absence of empirical studies specifically examining cybersecurity consciousness (awareness, knowledge, and behaviour) among IT professionals in Bangalore, India, within the context of hybrid work models. While existing literature broadly addresses cybersecurity awareness, company-level risk, frameworks, and the impact of AI on attacks), it largely overlooks the unique confluence of factors present in Bangalore's IT ecosystem. These factors include the distinct cultural attitudes toward technology security, socio-economic diversity influencing home IT infrastructure variations, the specific cybersecurity maturity levels of diverse IT subsectors, and how these elements interact to shape employee consciousness and habits in a hybrid work environment. This gap is critical because existing Western-centric research on cybersecurity behaviour may not be directly transferable, necessitating a focused investigation into this high-stakes, globally significant IT hub.

2. Literature Reviews

A study by Zwilling et al. (2020), they examined the patterns of cyber security awareness, knowledge and behaviour in Poland, Turkey (with four countries split between Czech Republic and Israel) and Slovenia (the fourth country split with Russia) The researchers looked at how internet users' knowledge of cyber risks affects their real-world safety practices and if they are receptive to using security solutions. According to the research, there is a worrisome gap between knowledge and behaviour. Participants were generally aware of cyber risks, but they only used simple, ubiquitous preventive measures rather than complete security procedures. The main conclusion was that a greater understanding of cyber security was linked to a greater understanding of threats, regardless of national or gender differences, and that this understanding had an impact on the use of protective measures but did not change users' propensity to share personal data. In addition, the study revealed significant cross-cultural variations among the four nations that had an impact on how cybersecurity awareness, understanding, and security behaviours interacted. This indicates that successful cybersecurity training programs should be adapted to cultural and regional contexts, rather than adopting a one-size-fits-all approach.

Chris Florackis et al. (2022) studied a distinct measure of cybersecurity risk is provided on a company-level basis for all U.S.-listed companies, which is established through scholarly analysis and an analysis of the cybersecurity risks of companies that were breached and those that were not. After that, they look at whether the cross-section of stock returns accounts for the risk of cybersecurity. On average, portfolios of companies that are highly vulnerable to cybersecurity threats outperform those of other companies by as much as 8.3% annually. However, businesses with a lot of exposure do poorly during periods of increased cybersecurity danger. The fact that the measure is greater in information technology companies, that it corresponds to characteristics connected to businesses that have experienced cyberattacks, and that it forecasts future cyberattacks is reassuring.

Sita Rani et al (2022) elaborated, the term "cyber security" as to the integration of technologies, methods, frameworks, and practices developed to protect data, devices, and communication systems from cyberattacks to prevent illegal access. Additionally, information and communication security are known as cyber security. Cyber security aims to ensure the safety of different parts, rather than just those of one company. Both internal and external threats are managed under cyber security. It also aids in safeguarding the resources against harm caused by natural disasters. Cyber security is essential to the protection of a wide range of assets across many industries. Large quantities of sensitive data are collected, transmitted electronically, and stored in electronic devices; the most prominent include military personnel as well as government officials, banks, insurance companies, and the healthcare sector. Based on a written scrutiny and comparing the cybersecurity risks of hacked companies with those that were formerly at risk, they developed 'a unique company-level metric for measuring cybersecurity risk'

Cybercrime, cyberattacks, and cyberterrorism are some of the various sorts of threats that cyber security deals with. Malware, SQL injection, phishing, man-in-the-middle attacks, and denial-of-service attacks are the most common ways to threaten cybersecurity.

Antonio et.al (2023) explains, cyberattacks have an impact on the industrial sector's organizational performance by taking advantage of the weaknesses of networked machines. The rising digitization and technologies that exist in the setting of Industry 4.0 have spurred an increase in investment in automation and innovation. Nevertheless, this digital transformation carries risks, particularly when it comes to cybersecurity. In industry 4.0, cyberattacks based on artificial intelligence can be combined with traditional methods to inflict exponential harm to businesses. The cyber-attack surface has grown due to the growing dependence on networked information technology. Studies in this vein that seek to comprehend the behaviour of cybercriminals to generate information for cybersecurity strategies are crucial. Their work systematically reviews the literature to identify and analyse publications on cyberattacks using artificial intelligence to develop cybersecurity strategies. Using literature analysis, the study attempted to examine the effects of emerging threat to offer the research community ideas for creating defences against possible future threats. The findings can be used to inform the investigation of AI-backed cyberattacks.

Serkan Savaş Süleyman Karataş (2022), based on their analysis and comparing the cybersecurity risks of hacked companies with those that were formerly at risk, researchers have developed 'a unique company-level metric for measuring cybersecurity risk' The quantity of cybersecurity risks is growing every day, and they are being uncovered by national and international organizations. With a strong cybersecurity plan, cybersecurity risks can be eradicated. After examining the field's importance, they provide a comprehensive cybersecurity framework in the chapter. This study highlights the significance and need of cyber governance in guaranteeing cybersecurity. The study and findings on cybersecurity governance have been reviewed. A descriptive research approach was used for the purpose. About the application approach, a documentary research model and a fundamental research model have been developed in terms of research philosophy. Studies from Google Scholar, TR Index, Web of Science, EBSCO, and Scopus make up the research universe. The outcome revealed that, despite some research yielding localized cybersecurity governance solutions in various nations, a comprehensive governance framework has not yet been developed. Rather, there is an underlying conflict to maintain control over this region's administration, not its governance.

Diptiben Ghelani (2022) understands on academic and professional literature offers a wide range of recommendations on how to protect data. Most studies concentrate on employing technological countermeasures to prevent security risks, even though other strategies like deterrence, deception, detection, and reaction are also feasible. The paper describes the results of a qualitative study done in Korea to see how companies employ security measures to safeguard their information systems. The first step in presenting a comprehensive cybersecurity framework is to acknowledge the field's importance, and this chapter continues. Although other methods were obvious, they were also preventive ones. The article proposed a research plan for implementing a variety of approaches throughout a business, with an emphasis on how to integrate, balance, and improve systems. This study covered a wide range of subjects, including information security and areas where security policy is likely to be debated, such as military sources. Nine security methods have been identified. The application of these security measures in enterprises is examined using a qualitative focus group method. The security strategies of eight firms were discussed by security managers in focus groups. The research revealed that a significant number of businesses utilize a preventative strategy to ensure the availability of technology services. On an operational level, some of the other identified methods were used to support the prevention strategy.

Wasyihun Sema et.al (2024), their study based on comparing the cybersecurity risks of hacked companies with those that were formerly at risk, they have developed 'a unique company-level metric for measuring cybersecurity risk' The ever-increasing need for digitalization means that every person and business is constantly exposed to

changing cyber threats. The current state of cyber security, its difficulties, strategies, current conditions, and global trends are all covered in this article. Researchers performed a methodical analysis to identify the most recent trends, difficulties, and cutting-edge developments in cybersecurity to remain ahead of the curve. They also discussed the future course of cyber security, offering potential strategies and methods for mitigating the growing cyber security threat environment, emerging trends, and innovations such as artificial intelligence (AI) and machine learning (ML) to automate the identification and response to cyber threats. Additionally, the article emphasizes the significance of ongoing adoption and collaboration among stakeholders in the cyber ecosystem.

Muhammad Fakhrul Safitra et.al (2023), explained as the digital environment develops at a breakneck speed, the convergence of digitization and cyber threats raises fresh issues for organizational security. The article offers a comprehensive framework for influencing the future of cyber security. Addressing the intricacies of contemporary cyber threats, this framework helps businesses become more resilient. The integration of capabilities with resilience is the main emphasis. These components can be integrated with other cyber security measures to improve organizations' capacity for forecasting, reducing exposure to, reacting to and recovering from cyber catastrophes. The significance of organizational leadership, accountability, and innovation in attaining cyber resilience is highlighted in this paper. Majorities of the most notable industries include military, government agencies, financial institutions, businesses, and healthcare, where electronic devices are used to gather vast amounts of sensitive data.

Dr.Yusuf Perwej et.al (2021) studied,the Internet has grown to be an essential part of people's daily lives in many countries around the world in recent years. However, as Internet usage has increased, so has internet crime. In recent years, cyber security has made significant advancements in response to the quick shifts in the online world. The strategies a nation or business might employ to protect its goods and data in cyberspace are known as cybersecurity. By including these components in cyber security measures, organizations can enhance their ability to predict, mitigate, and respond to cyber catastrophes. Cyber security is a concern that extends beyond people to governments and companies. With cybernetics utilizing a range of technologies, including cloud computing, smartphones, and Internet of Things methods, among others, everything has lately become digital. Concerns regarding privacy, security, and financial remuneration are being raised by cyberattacks. A collection of procedures, methods, and technology known as cyber security is designed to protect networks, computers, programs, and data from attacks, harm, and unauthorized access. The main objective of the work was to provide a comprehensive overview of the various types of cybersecurity, the reasons behind the importance of cybersecurity, the cybersecurity framework, the cybersecurity tools, and the challenges of cybersecurity. Cyber security protects the data and integrity of computing assets that are either a component of an organization's network or connected to it, with the goal of protecting such assets from all threat actors throughout the lifespan of a cyberattack.

Dawit Negussie Tolossa (2023) explained, a distinct measure of cybersecurity risk is provided on a company-level basis for all U.S.-listed companies, which is established through scholarly analysis and an analysis of the cybersecurity risks of companies that were breached and those that were not. Cybercriminals take advantage of weaknesses in networks and systems, endangering vital information, financial resources, and the reputation of organizations. Companies must understand that their personnel are essential to maintaining a strong cybersecurity posture. By empowering employees as the first line of defence against cyber-attacks and maintaining consumer confidence, this piece highlights the necessity of cybersecurity awareness training. A methodical review of the literature demonstrated that employee training improves security events and promotes a culture of cybersecurity awareness. Training may be customized for remote work to increase the organization's flexibility. An all-encompassing security plan that combines rules and technical safeguards is necessary. Companies can proactively safeguard assets and maintain a secure position in the digital age by investing in thorough and continuous cybersecurity awareness training.

3. Methodology

Research Design

This quantitative cross-sectional survey study examined cybersecurity consciousness among 106 IT professionals in Bangalore, Karnataka, distributed across fully on-site (n=48), hybrid (n=32), fully remote (n=16), primarily office-based (n=6), and flexible (n=4) work arrangements. The methodology employed four standardized 5-point Likert scales measuring Cybersecurity Consciousness (CSC), Cybersecurity Awareness (CSA), Cybersecurity Training (CST), and Cybersecurity Behaviour (CSB), alongside variables for work arrangement, technology infrastructure, organizational support, work environment security, and demographic controls. A three-stage hierarchical regression analysis was conducted, with Model 1 examining basic work arrangement effects (R^2 = 0.055), Model 2 incorporating environmental factors and controls (R^2 = 0.689), and Model 3 testing interaction effects (R^2 = 0.712). Results showed mean CSC scores ranging from 4.05 to 4.35 across work arrangements, with significant correlations between CSC and environmental factors (r = 0.389 to 0.523, $p < 0.001$), demonstrating that environmental factors explained substantially more variance in cybersecurity consciousness than work arrangement alone, with organizational support ($\beta = 0.42$, $p < 0.001$) and technology infrastructure ($\beta = 0.25$, $p = 0.003$) emerging as the strongest predictors in the full model.

Variables

Dependent Variable: Cybersecurity Consciousness (CSC)

The dependent variable was constructed as a composite score combining three dimensions:

- **Cybersecurity Awareness (CSA)**
- **Cybersecurity Attitude (CST)**
- **Cybersecurity Behaviour (CSB)**

Formula: CSC = (CSA + CST + CSB) / 3

Independent Variables

- **Work Arrangement**: Categorical variable (coded as dummy variables)
- **Technology Infrastructure (TI)**
- **Organizational Support (OS)**
- **Work Environment Security (WES)**

Descriptive Statistics

Mean Scores by Work Arrangement

Work Arrangement	CSC Score	CSA Score	CST Score	CSB Score	N
Fully On-site	4.12	4.08	4.15	4.13	48
Hybrid	4.26	4.23	4.28	4.27	32
Fully Remote	4.18	4.15	4.20	4.19	16
Primarily Office-based	4.05	4.02	4.08	4.06	6
Flexible	4.35	4.32	4.38	4.36	4
Overall Mean	**4.17**	**4.14**	**4.19**	**4.18**	**106**

This table shows cybersecurity scores for 106 IT workers across different work styles. Flexible workers (who can work however they want) had the highest scores in all areas - around 4.3 out of 5 - but there were only 4 of them. Hybrid workers (mix of office and home) scored second highest at around 4.2-4.3, and they made up a good portion of the study with 32 people. Workers who are primarily office-based scored the lowest at around 4.0, though only 6 people worked this way. Fully remote workers and fully on-site workers scored in the middle range around 4.1-4.2. Most people in the study worked fully on-site (48 people) or hybrid (32 people). Overall, all groups scored above 4 out of 5, meaning everyone had fairly good cybersecurity knowledge and behaviour, but those with more flexible work options tended to score slightly higher.

Correlation Matrix

Variable	CSC	Work Arr.	TI	OS	WES	Age	Experience
CSC	1.000	0.234**	0.456***	0.523***	0.389***	0.178*	0.201*
Work Arrangement	0.234**	1.000	0.312**	0.298**	0.267**	0.145	0.156
Technology Infrastructure	0.456***	0.312**	1.000	0.634***	0.578***	0.089	0.123
Organizational Support	0.523***	0.298**	0.634***	1.000	0.489***	0.167	0.189
Work Environment Security	0.389***	0.267**	0.578***	0.489***	1.000	0.134	0.145

*p < 0.05, **p < 0.01, ***p < 0.001

This correlation table shows how different factors relate to each other in the study. The numbers range from 0 to 1, where higher numbers mean stronger relationships. The stars (*) show how confident we can be in these relationships - more stars mean more confidence.

The most important findings are: Cybersecurity Consciousness (CSC) has the strongest relationship with Organizational Support (0.523***) - meaning when companies provide better support, employees have better cybersecurity awareness. Technology Infrastructure (0.456***) also strongly relates to cybersecurity consciousness - better tech tools lead to better security awareness. Work Environment Security (0.389***) and Work Arrangement (0.234**) also positively relate to cybersecurity consciousness, though less strongly.

Other notable relationships include Technology Infrastructure and Organizational Support being closely connected (0.634***), suggesting companies with good tech also provide good support. Age and Experience show weak relationships with most factors, meaning these personal characteristics do not strongly influence cybersecurity consciousness. Overall, the table shows that workplace factors like company support, technology, and security environment are much more important for cybersecurity awareness than individual characteristics like age or experience.

Regression Analysis Results

Model 1: Basic Work Arrangement Effects

Variable	B	SE	β	t	p	95% CI
(Constant)	4.05	0.12	-	33.75	<0.001	[3.81, 4.29]
Hybrid vs. On-site	0.14	0.08	0.18	1.75	0.083	[-0.02, 0.30]
Remote vs. On-site	0.06	0.11	0.05	0.55	0.584	[-0.16, 0.28]
Flexible vs. On-site	0.23	0.21	0.11	1.10	0.274	[-0.19, 0.65]

Model Summary: $R^2 = 0.055$, Adjusted $R^2 = 0.025$, $F(3,96) = 1.86$, $p = 0.142$

This first regression model examined whether different work arrangements affect cybersecurity consciousness compared to fully on-site workers as the baseline (scoring 4.05 out of 5), and found that while hybrid workers scored 0.14 points higher, remote workers 0.06 points higher, and flexible workers 0.23 points higher, none of these differences were statistically significant (p-values ranging from 0.083 to 0.584). The overall model was weak and not statistically significant ($R^2 = 0.055$, $p = 0.142$), explaining only 5.5% of the variance in cybersecurity consciousness, indicating that work arrangement alone is not a strong predictor of cybersecurity awareness and that other factors need to be considered to understand what truly influences cybersecurity consciousness among IT professionals.

Model 2: Full Model with Environmental Factors

Variable	B	SE	β	t	p	95% CI
(Constant)	1.89	0.32	-	5.91	<0.001	[1.26, 2.52]
Work Arrangement						
Hybrid vs. On-site	0.08	0.06	0.10	1.33	0.187	[-0.04, 0.20]
Remote vs. On-site	0.02	0.08	0.02	0.25	0.803	[-0.14, 0.18]
Flexible vs. On-site	0.15	0.15	0.07	1.00	0.320	[-0.15, 0.45]
Environmental Factors						
Technology Infrastructure	0.18	0.06	0.25	3.00	0.003	[0.06, 0.30]
Organizational Support	0.32	0.07	0.42	4.57	<0.001	[0.18, 0.46]
Work Environment Security	0.12	0.05	0.17	2.40	0.018	[0.02, 0.22]
Control Variables						
Age (years)	0.008	0.004	0.15	2.00	0.048	[0.000, 0.016]
Experience (years)	0.005	0.003	0.12	1.67	0.098	[-0.001, 0.011]
Education Level	0.04	0.03	0.09	1.33	0.186	[-0.02, 0.10]
Company Size	0.03	0.02	0.08	1.50	0.137	[-0.01, 0.07]

Model Summary: $R^2 = 0.689$, Adjusted $R^2 = 0.651$, $F(10,89) = 19.74$, $p < 0.001$

This regression analysis, "Model 2: Full Model with Environmental Factors," investigates the impact of work arrangements, environmental factors, and control variables on an unspecified dependent variable. The model effectively explains 68.9% of the variance in the outcome ($R2=0.689$, $p<0.001$), demonstrating its statistical significance. Crucially, environmental factors—specifically Technology Infrastructure ($p=0.003$), Organizational Support ($p<0.001$), and Work Environment Security ($p=0.018$) emerge as significant positive predictors, with Organizational Support exhibiting the strongest influence ($\beta=0.42$). Conversely, various work arrangements (hybrid, remote, flexible, compared to on-site) do not show a statistically significant effect on the dependent variable when other factors are considered. Among the control variables, only Age ($p=0.048$) is a significant predictor, while Experience, Education Level, and Company Size are not. This suggests that for the measured outcome, robust environmental support and security are more impactful than the specific work arrangement, with age playing a minor, yet significant, role.

Model 3: Interaction Effects

Variable	B	SE	β	t	p	95% CI
(Constant)	1.82	0.33	-	5.52	<0.001	[1.17, 2.47]
Technology Infrastructure	0.22	0.08	0.30	2.75	0.007	[0.06, 0.38]
Organizational Support	0.35	0.09	0.46	3.89	<0.001	[0.17, 0.53]
Work Environment Security	0.18	0.07	0.25	2.57	0.012	[0.04, 0.32]
Interaction Terms						
Hybrid × TI	-0.08	0.05	-0.12	-1.60	0.113	[-0.18, 0.02]
Remote × TI	-0.06	0.07	-0.07	-0.86	0.392	[-0.20, 0.08]
Hybrid × OS	0.07	0.06	0.09	1.17	0.245	[-0.05, 0.19]
Remote × OS	0.05	0.08	0.05	0.63	0.532	[-0.11, 0.21]

Model Summary: $R^2 = 0.712$, Adjusted $R^2 = 0.668$, $F(14,85) = 15.01$, $p < 0.001$

Model 3 presents a regression analysis focusing on interaction effects between work arrangements and environmental factors on an unspecified dependent variable. The model explains a substantial 71.2% of the variance in the dependent variable (R2=0.712), and the overall model is statistically significant (F (14,85) =15.01, p<0.001). Individually, Technology Infrastructure (p=0.007), Organizational Support (p<0.001), and Work Environment Security (p=0.012) are all significant direct predictors, consistent with prior findings. However, none of the interaction terms (Hybrid × Technology Infrastructure, Remote × Technology Infrastructure, Hybrid × Organizational Support, Remote × Organizational Support) are statistically significant (all p-values >0.05). This indicates that the effect of Technology Infrastructure and Organizational Support on the dependent variable does not significantly differ based on whether the work arrangement is hybrid or remote, compared to the baseline (likely on-site), suggesting that the impact of these environmental factors is consistent across these work arrangements.

Findings of the study

The study's key findings reveal that work arrangement alone has minimal direct impact on cybersecurity consciousness ($R^2 = 0.055$, $p = 0.142$), while environmental factors are the primary drivers, with organizational support being the strongest predictor ($\beta = 0.42$, $p < 0.001$), followed by technology infrastructure ($\beta = 0.25$, $p = 0.003$) and work environment security ($\beta = 0.17$, $p = 0.018$). Among work arrangements, hybrid workers showed the highest cybersecurity consciousness (M = 4.26), followed by flexible workers (M = 4.35, though small sample), while fully remote and on-site workers performed similarly (M = 4.18 and 4.12 respectively). The full environmental model explained 68.9% of variance with only marginal improvement to 71.2% when interaction effects were added, demonstrating that environmental factors affect all work arrangements similarly. Age was the only significant demographic factor ($\beta = 0.15$, $p = 0.048$), with older employees showing higher cybersecurity consciousness. The practical implications suggest that organizations should prioritize organizational support, technology infrastructure, and work environment security rather than restricting work arrangement flexibility, as environmental support systems are more critical than physical work location for maintaining cybersecurity consciousness.

Limitations

This study has several methodological constraints that affect the interpretation of findings. The cross-sectional design prevents establishing causal relationships between variables, meaning we cannot determine whether

environmental factors cause improved cybersecurity consciousness or if the relationship works in reverse. The reliance on self-reported measures introduces potential bias, as participants may overestimate their cybersecurity knowledge or behaviour. Additionally, the sample may not be representative of all IT professionals, limiting generalizability, and some work arrangement categories had relatively small sample sizes, which reduces the statistical power for detecting meaningful differences between groups.

Future Research Directions

To address these limitations, future studies should employ longitudinal research designs to establish causal relationships between environmental factors and cybersecurity consciousness over time. Researchers should recruit larger, more diverse samples across different industries and geographic regions to improve generalizability. The incorporation of objective measures of cybersecurity behaviour, rather than relying solely on self-reports, would provide more accurate assessments of actual security practices. Furthermore, investigating the mediating mechanisms that explain how environmental factors influence cybersecurity consciousness would provide deeper insights into the underlying processes and help develop more targeted interventions.

Conclusion

The regression analysis demonstrates that while work arrangement type has only modest direct effects on cybersecurity consciousness, environmental factors—particularly organizational support, technology infrastructure, and work environment security—are the primary drivers of cybersecurity awareness among IT professionals. Organizations should prioritize strengthening these environmental support systems rather than restricting work arrangement flexibility to maintain robust cybersecurity practices. The findings challenge common assumptions that remote work inherently increases security risks, revealing that hybrid work models can maintain or even enhance cybersecurity consciousness when properly supported, with success depending on organizational commitment to providing appropriate support systems regardless of physical work location.

References

[1] Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges, and future directions. *Cyber Security and Applications*, *2*, 100030.

[2] 2)) Antonio João Gonçalves de Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics*, *12*(8), 1920. https://doi.org/10.3390/electronics12081920

[3] Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). The Review of Financial Studies. *The Review of Financial Studies*, *36*(1), 351–407. https://doi.org/10.1093/rfs/hhac024

[4] Ghelani, D. (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology*, *3*(6), 12–19.

[5] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management (IJSRM)*, *9*(12), 669–710.

[6] Rani, S., Kataria, A., & Chauhan, M. (2022). Holistic Approach to Quantum Cryptography in Cyber Security. In *Cyber Security Techniques, Architectures, and Design* (1st ed., p. 26). CRC Press.

[7] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, *15*(18), 13369. https://doi.org/10.3390/su151813369

[8] Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7–34.

[9] Tolossa, D. N. (2023). Importance of Cybersecurity Awareness Training for Employees in Business. *IDYA - A Journal of Gujarat University*, *2*(2). https://doi.org/10.47413/vidya.v2i2.206

[10] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge, and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *60*(1), 82–97.