Copyright © 2023 International Journal of Cyber Criminology – ISSN: 0974–2891
July – December 2023. Vol. 17(2): 1–19. DOI: 10.5281/zenodo.4766701
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Cybersecurity Determinants in Iraq's Digital Workplace: Attitude, Policy, and Compliance Roles

Suhaba Nizar Nazem[1]*
Al-Noor University College, Iraq

Majeed M. Abid[2]
Al-Hadi University College, Iraq

Salah Hasan Gdheeb[3]
Mazaya University College, Iraq

Haady Abdilnibi Altememy[4]
The Islamic university in Najaf, Iraq

Isra Shakir Hassan Al Jouani[5]
Al-Esraa University, Iraq

Karrar Shareef Mohsen[6]
Al-Ayen University, Iraq

Alaa Hussein Abdulaal[7]
Ashur University College, Iraq

Abdulnaser Khalid Hamzah[8]
AL-Nisour University College, Iraq

Mustafa Asaad Rasol[9]
National University of Science and Technology, Iraq

[1] Department of Law, Al-Noor University College, Bartella, Iraq.
Email: suhaba.nazar@alnoor.edu.iq
[2] Department of Media/ Al-Hadi University College, Baghdad, 10011, Iraq.
[3] Department of Media/ Mazaya university college Iraq.
[4] College of Islamic Sciences/ The Islamic university in Najaf, Iraq.
Email: haady.altememy@gmail.com
[5] College of Arts, Department of Media/ Al-Esraa University, Baghdad/ Iraq.
Email: isramasar@gmail.com
[6] Information and Communication Technology Research Group, Scientific Research Center, Al-Ayen University, Thi-Qar, Iraq.
[7] Medical device engineering/ Ashur University College/Baghdad/ Iraq.
email: alaa.hussein@au.edu.iq
[8] Department of Medical Laboratories Technology, / AL-Nisour University College/ Baghdad/ Iraq.
Email: abdulniser.kh.eng@nuc.edu.iq
[9] National University of Science and Technology, Dhi Qar, Iraq. Email: mustafa.a.rasol@nust.edu.iq
* Corressponding Author Email: suhaba.nazar@alnoor.edu.iq

Abstract

Technology and digital advancement have produced several advantages to mankind, but it has also created a new field to focus on and monitor, which is cybersecurity for the prevention of cybercrimes. Countries like Iraq have embraced these innovations without any proper prelude measures and are facing different challenges to combat cyber issues. In this context, this study has empirically evaluated the influence of organizational cybersecurity on the digital workplace performance of employees. Some of the external factors, i.e., policy compliance of the organization and attitudes of employees towards cybersecurity, have been investigated as mediators. This study has used a quantitative survey questionnaire approach for the data collection and has analyzed the collected data through primary research software's SPSS and Amos. The results have revealed the significance of organizational cybersecurity in the digital workplace, yet the mediators have reflected the insignificant impact on the digital workplace. This study has discussed its theoretical and practical implications and limitations for policymakers and future researchers as well.

Keywords: cybersecurity, digital workplace, policy compliance, attitude towards cybersecurity.

1. Introduction

Organizational cyberculture relates to people's understandings, opinions, views, beliefs, assumptions, conventions, and principles related to cybersecurity and the way they show up in how they use technological devices. Information security issues should be incorporated into an employee's routine behavior, work routines, and behavior as part of organizational cyberculture (Remac, 2017). Although cybersecurity policies are universal across firms, employees may regard them as recommendations instead of rules because most data intrusions within organizations are caused by human actors.

Similarly to this, enterprises cannot be protected by technology if they are not properly incorporated and used. The rising use of technological advances in routine operations has made cybersecurity a major challenge. Like in all other sectors, business organizations were given a plethora of chances to improve the services they deliver to their clients due to digital transformations (Gull et al., 2023). Nevertheless, this has made it harder for the organization to safeguard its technology infrastructure from unauthorized access. Most firms have made major expenditures to safeguard their electronic infrastructure, either by creating specialized divisions or outsourcing their security activities. Nevertheless, cyberattacks have risen substantially, and cyber criminals are developing new strategies to target businesses and steal valuable data (Saeed, 2023).

Everybody in the organization, from the highest levels to staff members, must use technology to perform daily duties as tools utilized by organizational users, especially those established for security objectives; technology directly affects the level of cybersecurity in the organization. How risks are handled as they arise is a basic yet essential organizational factor that affects the success of designing a cybersecurity attitude (Poehlmann et al., 2021). Nations adopt a variety of precautions to safeguard their infrastructure from malware, which is referred to as cybersecurity. Many industrialized and even emerging economies have started to set up top authorities and councils focused on cybersecurity. Because of Iraq's lack of rapid technological capabilities and the country's robust entry into cyberspace, particularly after 2003, when the utilization of smart cellphones and computers increased, cybersecurity in Iraq has been irreversibly compromised (Jarjees Al-Tae, Al-Dhalimi, & Jabbar Al-Shaibani, 2020). The idea of the digital workplace has become the centerpiece for modernizing business procedures in Iraq as organizations increasingly adopt digital transformation. The risks to these organizations' cybersecurity, nevertheless, are further raised by their increasing reliance on digital technologies. Understanding how organizational cybersecurity factors affect the digital workplace in Iraq in this setting is essential for protecting sensitive data, guaranteeing business continuity, and sustaining trust among stakeholders. The aim of this study is to examine the impact of organizational cybersecurity determinants on the digital workplace in Iraq with an emphasis on the impact of cybersecurity policy and compliance as well as attitude towards cybersecurity. The objectives of this study are:

1. To assess the impact of organizational cybersecurity determinants on the digital workplace in Iraq
2. To assess the management and employee perspectives on cybersecurity in Iraqi organizations operating in the digital workplace
3. To evaluate the impact of policy and compliance on organizations' general cybersecurity anticipation in Iraq's digital workplace.

Understanding the function of organizational cybersecurity determinants is essential for guaranteeing the protection of sensitive data and digital assets in Iraq as the use of the digital workplace grows. The findings of the research can assist businesses in determining where their cybersecurity defenses need to be strengthened and in implementing those changes into practice. The study can help improve organizational resilience against cyber threats by examining the roles played by attitudes toward cybersecurity, policy, and compliance. The development of plans to strengthen response capabilities and minimize the potential impact of cyber incidents might result from the identification of gaps and difficulties in cybersecurity practices.

2. Literature Review

2.1 Theoretical Framework

Researchers have used different theories in the literature as the foundation base of concepts targeted in this study. The best-fit theory for the designed framework was the dynamic system theory. This theory is centered mainly on the process of change and development (Thelen, Ulrich, & Wolff, 1991); this theory has emerged in the business dimension with the name of dynamic system approach [DSA] to influence the psychology of the conceptualization of change in organizations (Golenia et al., 2017). Many researchers have used this approach in addressing different problems related to business management, the demand for change, innovation, and the maintenance of sustainable performance, etc. A past study has underlined this approach, examined cybersecurity from a business, social, and information technology perspective (Tisdale, 2015), and provided several solutions to prevent the loss from cybersecurity violations.

Another study has raised the importance of the dynamic system approach, and they designed a methodology and approach based on the dynamic system approach to calculate the risk associated with the cybersecurity investments of SMEs (Armenia et al., 2021), and they have utilized it as an efficient system for dynamic organizational complexity, cyber risk, and unpredicted dynamics over time.

2.2 The impact of cybersecurity determinants on the digital workplace

The emergence and adoption of the internet in daily life activities from the start of the 21st century have benefited man in several aspects, but it also comes with risks and security concerns about the sites and data available on the internet (Gordon & Loeb, 2006). These risks create a need for the maintenance and proper control of the internet, which is named cybersecurity, the investigation of risk in the information networks of all sorts, and the reduction of these risks with technical means (Gordon & Loeb, 2002). The determinants related to organizational cybersecurity have been addressed as the lack of focus on the root cause analysis, alerts and vulnerabilities, communication gap, human errors, and prioritization issues (Wiens, 2022).

The association between organizational cybersecurity determinants and digital workplace performance has been discussed in the literature in different dimensions. A systematic review has analyzed past studies related to cyber workforce development and cyber education (Dawson & Thomson, 2018); they highlighted six components for organizations to focus; on team working ability in employees, morale improvement for devoted learning, effective communication, need for systemic thinkers, a thought of civic duty, and focus on the progress of both technical and social skills. The digital workplace has gained more popularity in covid-19, and organizations have provided remote working facilities to the employees to improve their efficiency; the dynamic organizational ability of the employees with improved cybersecurity factors improves the employees' work-life balance, and it has been analyzed to stimulate the digital workplace performance. A systematic review has elaborated on the concept of cybersecurity policy awareness of companies on the employee's cybersecurity behavior; they have manifested in their results when the company has good communication, provides good awareness about the cybersecurity policies, and employees positively contribute to the compliance behavior of the company (Li et al., 2019). Along with it, organizational information security positively regulates the employees coping appraisal strategies and employees' threat appraisal. Iraq entered the digitalization advancement in 2003, but still, they have weak legislative systems, expansion of cybercrimes has reflected the vulnerable cybersecurity systems and lack of preventive measures for the improvement of cybersecurity components that can boost the digital workplace performance (Al Duhaidahawi et al., 2020).

Cybersecurity has been raised as a critical factor defining digital workplace effectiveness. Muthuswamy (2023) has recently investigated this assumption. Their results have reflected the importance of cybersecurity components, i.e., critical infrastructure and cloud security, for digital workplace performance, and this association gained more speed and firmness with cybersecurity awareness and support. The literature has highlighted the importance of cybersecurity and its factors for the digital workplace, and it provided a concept to the researcher for investigation in Iraqi companies and organizations. By taking these-view as a foundation, the following hypothesis has been designed:

H1: *The organizational cybersecurity determinants significantly positively impact digital workplace performance.*

2.3 Mediation of attitudes towards cybersecurity in the digital workplace

Several studies have attempted to explain the influence of different personality traits on the intentions to use new cybersecurity applications and practices. The attitudes and behaviors have several dimensions that trigger or nullify the willingness for cybersecurity practices (Hadlington, 2017). Impulsivity and internet abuse has been mentioned to impact the employees' intentions to use cybersecurity protocols practices. Employees who have exposure to cybersecurity attacks and know the loss of meaningful content have shown prominent support for the cybersecurity policies (Snider et al., 2021), and their attitude toward cybersecurity practices increases that activating the rise in digital workplace performance. A systematic review (Triplett, 2022) has highlighted that humans were the weakest link between the transmission of cybersecurity data and information and version. They have highlighted the role of leadership in the development of skills in the employees through education, training, and communication that pile up the digital workplace performance. Human factors like attitudes, behaviors, and intentions of the employees for cybersecurity have been narrated to be influenced by perception about the cybersecurity practices, external factors like age and gender, and the working environment provided by the organization (Maalem Lahcen et al., 2020).

A study has investigated the cybersecurity challenges faced by the employees (Muthuswamy & Nithya, 2023), and they have discussed lack of training, inside risks, insufficient authentication, and social engineering attacks as crucial factors that influence the behaviors for using the cybersecurity practices and their digital workplace performance vary. The concept of the employees' intentions has been provided insight by Saeed (2023), and they have enlightened the employees' perception of cybersecurity and the need for more security measures at individual and organizational levels to enhance employee attitudes toward cybersecurity and digital workplace performance. The significance raised by the literature about the attitudes and behavior toward cybersecurity has provided enough insight to the researcher for the following hypothesis development to evaluate in Iraq:

H2: *The attitudes towards cybersecurity mediate the association between organizational cybersecurity and digital workplace performance.*

2.4 Mediation of policy and compliance in the digital workplace

The impact of organization compliance policy on security approaches and organizational performance has been in the limelight of different researchers' discussions for a long time. The components of the compliance theory, coercive control, remunerative control, and certainty of control have been investigated (Chen, Ramamurthy, & Wen, 2012), and the study results narrated that remuneration control is a suitable alternative policy to prevent the violation of security concerns. The policy compliance for the information security system is shortly named as cybersecurity policies and compliances; in this context, a case study has highlighted that lack of justice, privacy, and weak organizational culture provides ways for employees to breach security standards (Alshare, Lane, & Lane, 2018) and it has suggested the managers of the companies reshape their security policies and compliances to ensure the fruitful practices of cybersecurity and improvement in the workplace performance. Another cross-culture study has evaluated smartphone usage for work purposes in increasing rates of cybersecurity breaches and illustrated that those companies who understand the importance of smartphone cybersecurity behavior should focus on the National policies about cybersecurity and must maintain the trust of their customers b as a priority by the regulation of cybersecurity behavior in their employees and keeping their data secure (Ameen et al., 2021).

Employees' perception of the organizational security policy and compliances has been noticed to be influenced by organizational support, the status of employment, and organizational commitment (Sharma & Warkentin, 2019); permanent employees have shown more honesty and determination in working under the security policies and compliances of organization than seasonal employees. The effectiveness of the privacy policies and compliances on the trust and behavioral intentions of the employees to participate in digital workplaces have been empirically highlighted by Peltoniemi (2020), and it has suggested the focus on the efforts of policies to impact the participation of digital workplaces, that extend the performance. Studies in the literature have enlightened the vitality of the national and company policies for the improvement of the employees' policy compliance and ways to enhance their digital workplace performance.

A literature review has condensed the term for security policy and compliance as ISPC [information security policy compliance], and they have elaborated the past studies' discussions by highlighting the gap in the literature about the ISPC and the security behavior of the employees for the organizations (Ali et al., 2021). This study has picked the mentioned gap and has developed the following hypothesis for empirical testing:

H3: *Company policy compliance mediates the association between organizational cybersecurity and the digital workplace performance of employees.*

3. Methodology

3.1 Research Design

Mc Combes (2021) states that a research design is the strategy of a researcher to answer research questions in his study. A well-planned research design is necessary for a study as it assists the researcher in ensuring that the method employed matches the research objectives of the study. In this study, a quantitative method-based survey design is utilized to analyze the role of organizational cybersecurity in digital workplaces in Iraq. The survey tool is appropriate for this study as it provides the benefit of collecting first-hand primary data from respondents. Basis on the survey instrument, more reliable and valid data can be collected efficiently. Moreover, surveys are cost-efficient, versatile, and generalizable (Nigel, 2009). The design for the research method adopted in this study is illustrated in Figure 1.

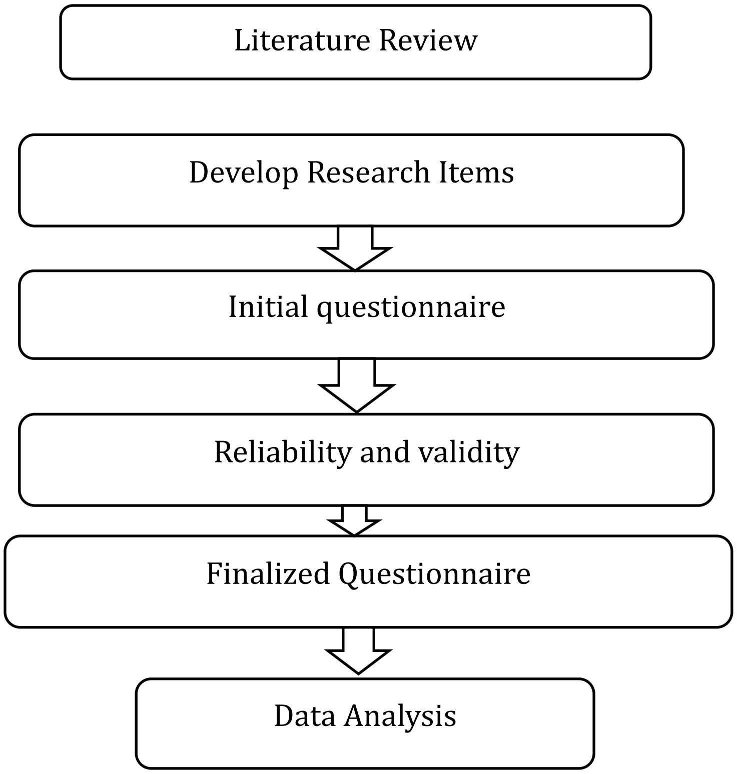

Figure 1. Research Design

3.2 Data collection process

After the development of the questionnaire reliability test was conducted to ensure the reliability and validity of the questionnaire; after the reliability test and assuring the validity of the questionnaire, the final version of the questionnaire was distributed among the respondents via email. The sample of this study comprises the digital workplaces in Iraq that are engaged in several security practices. The data was collected from employees working the digital workplaces in Iraq. The sample was selected using the probability sampling technique to distribute the questionnaire to the sample on a random basis (Glen, n.d.). Initially, 500 questionnaires were distributed to employees working in digital workplaces. On the basis of collected responses, 430 efficient responses were finalized.

3.3 Response rate

The questionnaire was distributed to 500 randomly selected employees in the digital workspace in Iraq. In the initial response, 450 responses were gathered, out of which 20 were not valid due to numerous reasons like incomplete responses. As a result, only 430 responses were finalized, and the overall response rate was 86% which is considered a good response for the present study. Moreover, the response rate is proper for this study as it fulfills the criteria of Robinson (2018), comprising a minimum of 10 responses per variable. In the present study, four variables were selected, and the number of 430 valid responses is considered adequate and reliable for this study.

3.4 Reliability analysis

In this study, the survey questionnaire is developed by adopting the measurement scales from previous studies. In order To analyze the internal consistency of selected variables, the reliability of the scale is measured using Cronbach's Alpha. The coefficients of Cronbach's Alpha assess the internal reliability of variables by utilizing the statistics to determine that collected items consistently matched with similar characteristics. Cronbach's Alpha calculates the level of agreement on a standardized scale ranging from 0 to 1. Higher values are considered an indicator of the higher reliability of items (Frost, 2016). In this study, Cronbach's Alpha is used to evaluate the reliability of the proposed contents. Since the acceptable values in this study range from 0 to 1, it is considered that all the items used in this study are reliable.

3.5 Measurement Items

The measurement items for this study have been adopted from past empirical studies. In order to determine the answers, a five-point Likert scale is utilized. The levels of the Likert scale consist of; Level 1- Strongly Disagree, Level 2- Disagree, Level-3 Neutral, Level-4 Agree, and Level-5 strongly agree. The details of the measurement scale, along with items and citation sources, are highlighted in the following tables.

3.5.1 Independent variables

- *Organizational Cybersecurity*

8 items were used to measure this variable. All the items have been adopted from studies of Hasan et al. (2021), from which the items of 'organizational culture' has been utilized. The detail of the items is presented in Table 1.

Table 1. Measurement items with sources

SR.	Determinant	Statement	Source
1.	Organizational Cybersecurity	"Our organization emphasizes security knowledge sharing across different organizational units."	Hasan et al. (2021)
2.		"Our organization emphasizes sharing cyber security incidents."	
3.		"Our organization emphasizes sharing cyber security failures."	
4.		"Our organization encourages contributions from team members to improve the cyber security of the organization."	
5.		"Our organization endorses coordination of activities across different units to improve cyber security."	
6.		"Our organization emphasizes collaboration across different groups to solve cyber security issues."	
7.		"In our organization, following rules and maintaining a secure running institution are important."	
8.		"In our organization, there is a commitment to security development."	

- *Attitude towards cybersecurity*

Attitude toward cybersecurity was measured through a 4-item scale adapted from the study of Ifinedo (2012).

Table 2. Measurement items for attitude toward cybersecurity

SR.	Determinant	Statement of items	Source
1		Following the organization's information/cyber system security policy is a good idea.	Adapted from Ifinedo (2012)
2		Following the organization's information/cyber system security policy is a necessity.	
3		Following the organization's information/cyber system security policy is beneficial.	
4		Following the organization's information/cyber system security policy is pleasant.	

- *Policy and Compliance*

The scale of intention to policy compliance with security is developed by Bulgurcu, Cavusoglu, and Benbasat (2010), which consists of 3 items. The items of the scale are presented in Table 3.

Table 3. Measurement items with sources

SR.	Determinant	Statement of items	Source
1.	Policy Compliance	"I intend to comply with the requirements of the information security policy (ISP) of my organization in the future."	Bulgurcu et al. (2010)
2.		"I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future."	
3.		"I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future."	

3.5.2 Dependent Variable

- *Digital Workplace*

The scale of the digital workplace was developed by Meske and Junglas (2021), which is modified and used by Muthuswamy (2023). The scale consists of 5 items. The measurement items and source are presented in Table 4.

Table 4. Measurement items with sources

SR.	Determinant	Statement of items	Source
1.	Digital Workplace	"I intend to actively support the change process towards a digitally transformed workplace."	Developed by Meske and Junglas (2021), used and modified by Muthuswamy (2023)
2.		"I plan to accompany the change process towards a digitally transformed workplace."	
3.		"I intend to actively participate in the change process towards a digitally transformed workplace."	
4.		"I plan to constructively participate in the change process towards a digitally transformed workplace."	
5.		"I intend to provide proactive feedback regarding the change process towards a digitally transformed workplace."	

3.6 Data analysis

The analysis in this study to evaluate the collected data and to answer research questions efficiently is done by employing advanced analysis using SEM. Statistical analysis was conducted to screen the data, and initial statistical analysis was done to analyze the validity and reliability of measurement scales. Following it, SEM, by using AMOS 18th version, is utilized by the researcher to evaluate the formulated hypothesis in the section of literature review. AMOS, in this regard, is an efficient tool as it helps to formulate additional models to highlight complicated associations more accurately. This software is also useful as it assists in the formulation of multiple databases for analysis and enhances the parameters of analysis. AMOS brings forth the outcomes in tabular forms to present the standardized regression coefficients (Tang & Jia, 2011). Moreover, as this study tends to analyze the direct association among independent variables (organizational cyber security, attitude towards cyber security, and policy compliance on the dependent variable digital workplace, thus, AMOS is appropriate for this study.

4. Results

4.1. Outliers and normality

In order to check any form of high and low outliers in the collected data, a frequent test has been run. The analysis result has highlighted no outliers of low and high values in the data. The data were screened to find the missing values, and then a few missing values were adjusted according to the trend of other responses. To calculate the normality of the data, skewness, and kurtosis analysis were applied. The value of skewness has been analyzed on the basis of a standard range of -1 to +1. The following has represented the values of skewness, and all their values have fallen under the prescribed range of limit. The mean values of the variables were also lying above 3, which indicated the respondents had mostly checked the option towards agreement of the ideologies of the items about the variables.

Table 5. Descriptive statistics:

Descriptive Statistics							
	N	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**	**Skewness**	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
DIGWORK	280	1.00	5.00	3.3514	1.24431	-.298	.146
OC	280	1.00	5.00	3.3683	.97649	-.541	.146
ATT	280	1.00	5.00	3.4937	1.03877	-.404	.146
PC	280	1.00	5.00	3.3714	1.22991	-.338	.146
Valid N (listwise)	280						

4.2. KMO and Bartlett's Test

The KMO test has been conducted to investigate the suitability of the data according to the targeted sample population. This test has been used to evaluate the appropriates of the sample for the model, and if the value of KMO is above 0.8 or close to 1, the sample size shows the significance for the model, and in the following table, the value of KMO is .901, and has supported the effectiveness of the sample size for the model. The Bartlet test has been conducted and the significance value of the sphericity has portrayed there was no redundancy of the data.

Table 6. KMO and Bartlett's Test:

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.901
Bartlett's Test of Sphericity	Approx. Chi-Square	6499.600
	df	190
	Sig.	.000

4.3. *Factor analysis*

The rotated component analysis has been performed and the following table presenting the factor loading of the items of every variable, and the threshold range of the factor score above from 0.6 and near to 1 has been assumed for the significance and authenticity of the items factor loading, and the table values have their significance as all of values are within the prescribed range.

Table 7. Factor loading of the questionnaire items:

Rotated Component Matrix				
	Component			
	1	2	3	4
OC1	.857			
OC2	.822			
OC3	.756			
OC4	.724			
OC5	.739			
OC6	.860			
OC7	.854			
OC8	.560			
PC1				.831
PC2				.845
PC3				.839
ATT1			.842	
ATT2			.859	
ATT3			.833	
ATT4			.805	
DW1		.948		
DW2		.942		
DW3		.951		
DW4		.939		
DW5		.963		

4.4. *Convergent and discriminant validity*

The convergent validity and the discriminant validity has been collectively called as construct validity. The convergent validity explained the similarity between the selected constructs, means that the selected constructs are related to the variable or not. It has three indicators i.e., AVE [Average Variance Extracted] has a threshold range of value to be above 0.5, CR [critical ratio] should be above 0.6, and the MSV (Cheung & Wang, 2017; Ginty, 2013). The discriminant validity highlights the concept of the relationship or correlation of the items and the construct should by more significant with each ither than with any external construct, and the prescribed range for the value of correlation is above 0.8 (Cheung & Wang, 2017). The discriminant validity has been comprised of self-correlation and the cross-variable correlation. The following table has presented the values of AVE, CR, and the self and cross variable correlation, and all the narrated values are within the pre-defined range.

Table 8: Convergent and discriminant validity.

	CR	AVE	MSV	MaxR(H)	ORGCYBER	DIGITWORK	ATTIT	POLICCOM
ORGCYBER	0.938	0.657	0.522	0.970	0.811			
DIGITWORK	0.980	0.907	0.093	0.985	0.304***	0.952		
ATTIT	0.891	0.672	0.216	0.893	0.465***	0.230***	0.820	
POLICCOM	0.946	0.854	0.522	0.947	0.723***	0.188**	0.426***	0.924

4.5. Model fitness

The confirmatory factor analysis CFA has been used to evaluate the model fitness. The values of IFI, GFI, CMIN, and RMSEA have been analyzed with the comparison to the prelude standards and the table has presented the appropriateness of these values and has reflected the validity and significance of the variables and their constructs for the fitness of the designed model.

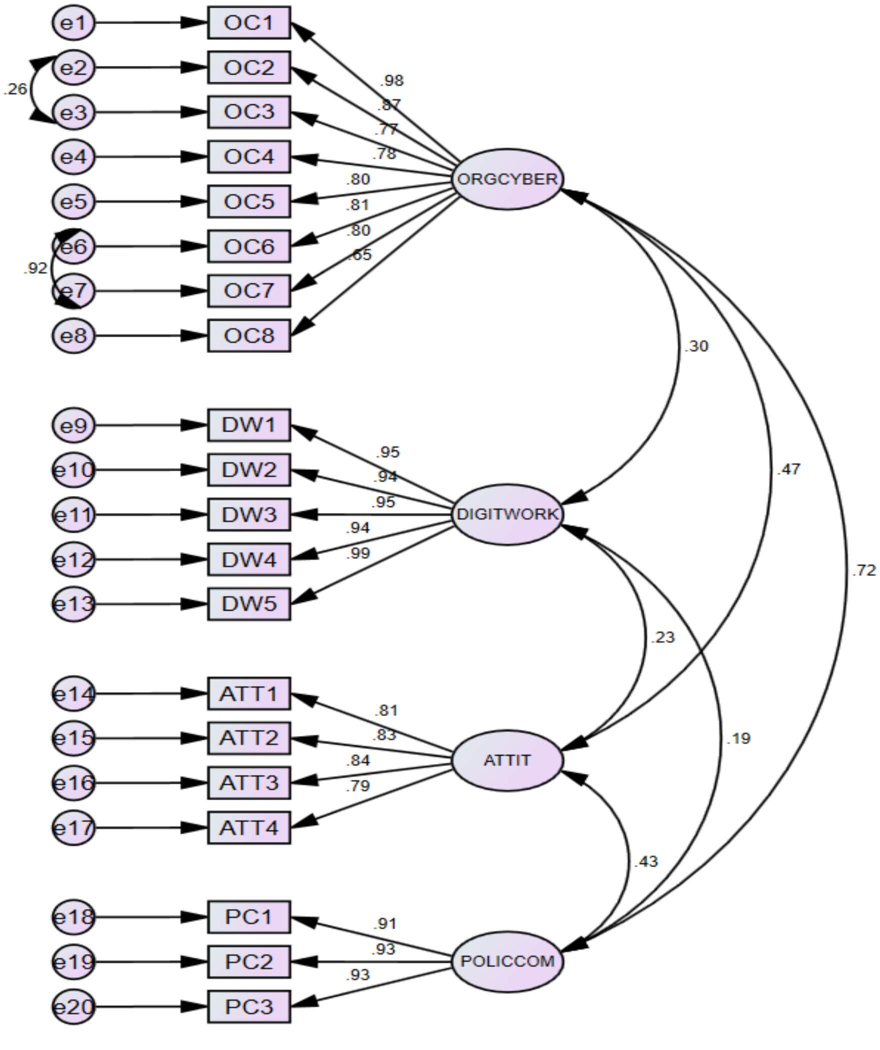

Figure 2. The CFA analysis for the model fitness.

Table 9. Model fitness

	Acceptable range	Value
CMIN	≤3	2.135
GFI	≥0.8	0.85
IFI	≥0.9	.972
CFI	≥0.9	.972
RMSEA	≤0.08	.064

4.6. Hypothesis testing (direct effects)

The researcher has used the structural equational modeling SEM to calculate the regression value to accept or reject the developed hypotheses. The first hypothesis has stated the direct association of independent variable organizational cybersecurity on the dependent variable digital workplace, and the results of the analysis SEM has calculated .305 as the standardized estimated regression value of this relationship with the significance of .01, and the significance value was less than .05 and it has supported the synthesized hypothesis in positive aspect.

Table 10. Direct effects

Parameter			Estimate	Lower	Upper	P
DIGWORK	<---	OC	.305	.161	.461	.011

Hypothesis testing (indirect effects)

This study has investigated two indirect effects on the digital workplace. The calculated regression value for the mediation of PC was -0.020, with the significance of .117, as the significant value was above than .01 or .05 so the H3 was rejected. For the confirmation of H2, the table has provided the regression value of 0.018 and p-value of 0.100, this value was also above than the standard p-value for the acceptance, causing the third hypothesis to be rejected.

Table 12. Indirect effects

Indirect Path	Standardized Estimate	Lower	Upper	P-Value
OC --> PC --> DIGWORK	-0.020	-0.070	0.002	0.117
OC --> ATT --> DIGWORK	0.018†	-0.006	0.063	0.100

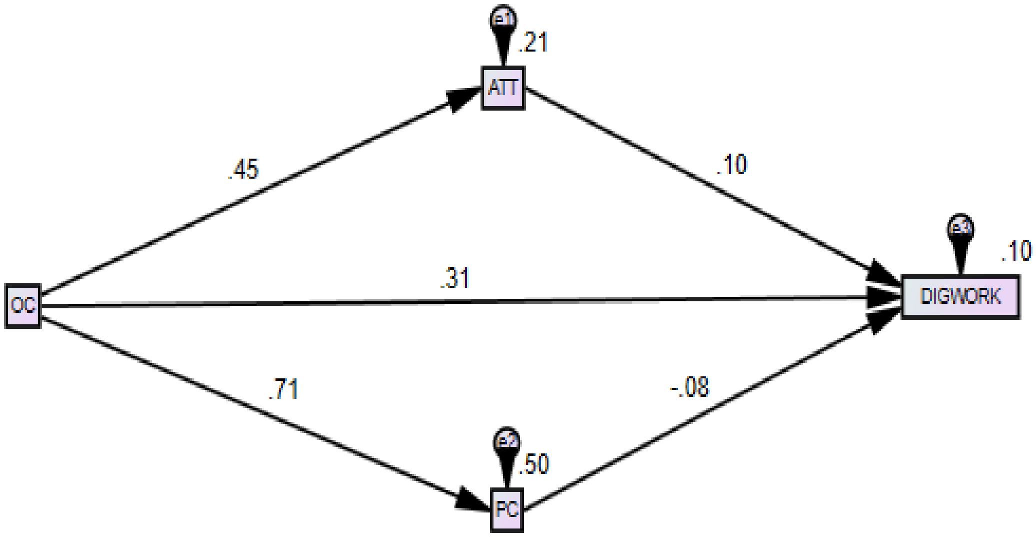

Figure 3. SEM diagram

5. Discussion

The present study was aimed at analysing the impact of cybersecurity determinants on the digital workplace in the context of Iraqi organizations. Moreover, the study also examined the managerial and employee perspective on cybersecurity in Iraq's organizations. The study also evaluated the impact of policy and compliance measures on the general cybersecurity anticipation within Iraq's digital workplace. Based on the objectives of the present study, the hypothesis was formulated that organizational cybersecurity determinants significantly and positively impact digital workplace performance. The findings of the survey have approved this hypothesis. Thus, H1 is supported. Various previous studies have also reported a positive relationship between organizational determinants of cybersecurity and digital workplace performance (Hasan et al., 2021; Rahiman et al., 2021). Based on the research objectives, the second hypothesis was that the employee attitude towards cybersecurity has a significant impact on digital workplace performance. However, the findings of the research indicate that employee attitudes towards cybersecurity have no significant effect on digital workplace performance. Thus, H2 is rejected. Furthermore, the research objectives led to the formulation of a third hypothesis that company policy compliance has a significant impact on the digital workplace performance of employees. The findings indicate that H3 is approved. Previous studies have also reported a significant effect of company policy compliance on digital workplace performance (Ameen et al., 2021; Chen et al., 2012; Peltoniemi, 2020).

5.1. Conclusion

In conclusion, the present research investigated the role of organizational cybersecurity determinants on digital workplace performance in Iraq's organizations. The study presented valuable insights into the attitude and perspective of employees at a digital workplace regarding cybersecurity policies and their compliance measures. The study also explored the impact of cybersecurity policies on the overall environment of a digital workplace in the context of Iraq's organization. The findings of this research highlighted the importance of organizational determinants of cybersecurity in designing and ensuring a secure and productive digital workplace. The data analysis reported a significant positive association between organizational cybersecurity determinants and digital workplace performance. The present study offered valuable insights into the impact of these cybersecurity determinants within an organization. The insights related to these determinants can help organizations shape different strategies to avoid cyberattacks on their digital assets. This indicates the significance of an organization's investment in efficient and effective cybersecurity measures to protect digital assets and provide a cyber-secure digital workplace to its employees. Furthermore, the study examined the impact of employee attitudes towards cybersecurity on digital workplace performance. Employee attitude has no significant influence on digital workplace performance. However, the organization can still raise employee awareness about cybersecurity policies and compliance measures because policy compliance measures play an essential role in fostering a cyber-secure digital workplace with excellent performance. Thus, cybersecurity policy and compliance measures are primary factors encouraging employees to adhere to the cybersecurity system. The establishment of effective cybersecurity policies can help the organization in cyber risk management and establish a healthy digital workplace.

5.2. Implications

The present research has both theoretical and practical implications. From a theoretical perspective, this research contributes to the existing literature on the study of organizational cybersecurity and the digital workplace within the framework of Dynamic System Theory. By analysing the cybersecurity determinants within an organization and developing a digital workplace, this study expands the theoretical research of organizational cybersecurity. Moreover, this study can help in the identification of various mediating and moderating factors which affect the development of a digital workplace and its cybersecurity. From a practical perspective, the present research can offer insights into operative determinants of cybersecurity within an organization. The findings of this research can help an organization adopt best practices to enhance the cybersecurity system. This can ensure security in a digital workplace. These findings can help various Iraqi organizations design excellent cybersecurity strategies. Thus, leaders and policymakers can update their existing cybersecurity policies and compliance measures in light of the results of this research. Moreover, an understanding of employee perspectives on cybersecurity policies and compliance can help policymakers design training programs for employees to raise awareness of cybersecurity. The study also suggests ways to optimise the cybersecurity system in a digital workplace. This can lead to enhanced efficiency and a safe environment in an organization. The findings of this research can also help an organization in developing effective risk management strategies. Thus, organizations can plan to avoid any potential threat to their cybersecurity. The present study also offers insights into decision-making processes concerning resource allocations to the cybersecurity system in an organization. The study implies that organizations should prioritise funding their cybersecurity system by allocating necessary resources. Organizations can invest in cybersecurity training and install cybersecurity technology. These training programs can raise awareness against cyber threats and make employees more vigilant in dealing with cyber threats. As a result, the cybersecurity system ensures the competitive survival of an organization. Thus, the present study highlights the significance of organizational determinants of cybersecurity on digital workplace performance in Iraq. Thus, the study paves the way for future studies on cybersecurity systems to meet the challenges of cyberattacks in the digital era. With the digital revolution, digital asset protection has become every organization's primary objective. Thus, the insights of the present study can be used to accelerate the efforts of establishing an efficient and effective cybersecurity system.

5.3. Limitations and Recommendations

The present study offers insights into the organizational cybersecurity determinants and their impact on the digital workplace in Iraq. It also explores the managerial and employee perspective on cybersecurity in Iraqi organizations. However, this study has its limitations. First, as a primary study, the primary research has a limited sample size. This small sample size reduces the generalisability of the findings of this study. Thus, these findings do not apply to a broader Iraqi organization population. Moreover, the present research focuses on Iraq, and its results are associated with various cultural, socio-economic, and political aspects specific to Iraq. Therefore, its findings cannot be applied to other geographical regions without considering their cultural, socio-economic and political factors. The application of Dynamic System Theory introduces its limitations in this study. Dynamic System Theory is based on the association of various variables. However, organizational determinants of cybersecurity and its employee perspectives involve multiple factors, making it daunting to analyse all the relevant variables. Moreover, the digital workplace is a multifaceted phenomenon, and it is dynamic in nature. The pertinent other variables can be explored in future research. Furthermore, respondents may not provide honest responses in self-administered survey questionnaires. Therefore, future studies could explore the role of employee training and awareness of cybersecurity in developing a digital workplace. Moreover, the impact of organizational structure and leadership practices on the development of digital workplaces could also be explored in future research.

References

Al Duhaidahawi, H. M. K., Zhang, J., Abdulreda, M. S., Sebai, M., & Harjan, S. (2020). The Financial Technology (Fintech) and Cybersecurity: Evidence From Iraqi Banks. *International Journal of Research in Business and Social Science, 9*(6), 123-133. https://doi.org/10.20525/ijrbs.v9i6.914

Ali, R. F., Dominic, P., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: a Systematic Literature Review for Identifying the Transformation Process From Noncompliance to Compliance. *Applied Sciences, 11*(8), 3383. https://doi.org/10.3390/app11083383

Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information Security Policy Compliance: a Higher Education Case Study. *Information & Computer Security, 26*(1), 91-108. https://doi.org/10.1108/ICS-09-2016-0073

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping Customers' Data Secure: a Cross-cultural Study of Cybersecurity Compliance Among the Gen-mobile Workforce. *Computers in Human Behavior, 114*, 106531. https://doi.org/10.1016/j.chb.2020.106531

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A Dynamic Simulation Approach to Support the Evaluation of Cyber Risks and Security Investments in Smes. *Decision Support Systems, 147*, 113580. https://doi.org/10.1016/j.dss.2021.113580

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: an Empirical Study of Rationality-based Beliefs and Information Security Awareness. *MIS quarterly, 34*(3), 523-548. https://doi.org/10.2307/25750690

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems, 29*(3), 157-188. https://doi.org/10.2753/MIS0742-1222290305

Cheung, G. W., & Wang, C. (2017). Current Approaches for Assessing Convergent and Discriminant Validity With Sem: Issues and Solutions. In *Academy of Management Proceedings* (pp. 12706). Academy of Management Briarcliff Manor, NY 10510. https://doi.org/10.5465/AMBPP.2017.12706abstract

Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology, 9*, 744. https://doi.org/10.3389/fpsyg.2018.00744

Frost, J. (2016). *Cronbach's Alpha: Definition, Calculations & Example*. Statistics. https://statisticsbyjim.com/basics/cronbachs-alpha/

Ginty, A. T. (2013). Construct Validity. In *Encyclopedia of behavioral medicine* (pp. 487-487). Springer. http://dx.doi.org/10.1007/978-1-4419-1005-9_861

Glen, S. (n.d.). *What is Probability Sampling?* Scribbr.
https://www.scribbr.com/methodology/probability-sampling/

Golenia, L., Schoemaker, M. M., Otten, E., Mouton, L. J., & Bongers, R. M. (2017). What the Dynamic Systems Approach Can Offer for Understanding Development: an Example of Mid-childhood Reaching. *Frontiers in Psychology, 8*, 1774. https://doi.org/10.3389/fpsyg.2017.01774

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438-457. https://doi.org/10.1145/581271.581274

Gordon, L. A., & Loeb, M. P. (2006). Economic Aspects of Information Security: an Emerging Field of Research. *Information Systems Frontiers, 8*(5), 335-337. https://doi.org/10.1007/s10796-006-9010-7

Gull, H., Alabbad, D. A., Saqib, M., Iqbal, S. Z., Nasir, T., Saeed, S., & Almuhaideb, A. M. (2023). E-commerce and Cybersecurity Challenges: Recent Advances and Future Trends. In *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications* (pp. 91-111). IGI Global. https://doi.org/10.4018/978-1-6684-5284-4.ch005

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. http://dx.doi.org/10.1016/j.heliyon.2017.e00346

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the Cyber Security Readiness of Organizations and Its Influence on Performance. *Journal of Information Security and Applications, 58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Jarjees Al-Tae, A. K., Al-Dhalimi, H. A.-H., & Jabbar Al-Shaibani, A. K. (2020). Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study. *Systematic Reviews in Pharmacy, 11*(12), 469-476. https://www.sysrevpharm.org/abstract/relationship-of-cybersecurity-and-the-national-security-of-the-country-iraq-case-study-67372.html

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior. *International Journal of Information Management, 45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and Insight on the Behavioral Aspects of Cybersecurity. *Cybersecurity, 3*(1), 1-18. https://doi.org/10.1186/s42400-020-00050-w

Mc Combes, S. (2021). *What Is a Research Design | Types, Guide & Examples*. Scribbr. https://www.scribbr.com/methodology/research-design/

Meske, C., & Junglas, I. (2021). Investigating the Elicitation of Employees' Support Towards Digital Workplace Transformation. *Behaviour & Information Technology, 40*(11), 1120-1136. https://doi.org/10.1080/0144929X.2020.1742382

Muthuswamy, V. V. (2023). Cyber Security Challenges Faced by Employees in the Digital Workplace of Saudi Arabia's Digital Nature Organization. *International Journal of Cyber Criminology, 17*(1), 40–53. https://doi.org/10.5281/zenodo.4766603

Muthuswamy, V. V., & Nithya, N. (2023). Role of Cyber Security on Employees' Digital Workplace Performance: Exploring the Effects of Employees' Digital Awareness and Organizational Support. *International Journal of Cyber Criminology, 17*(1), 54–71. https://doi.org/10.5281/zenodo.4766604

Nigel. (2009). *Surveys and Questionnaires*. National Institute for Health Research. https://www.rds-yh.nihr.ac.uk/wp-content/uploads/2013/05/12_Surveys_and_Questionnaires_Revision_2009.pdf

Peltoniemi, A. (2020). *Perceived Effectiveness of Privacy Policy and Its Association With Trust and Behavioral Intention to Participate in a Digital Workplace Wellness Program* (Master's thesis, University of Jyväskylä). http://urn.fi/URN:NBN:fi:jyu-202012167177

Poehlmann, N., Caramancion, K. M., Tatar, I., Li, Y., Barati, M., & Merz, T. (2021). The Organizational Cybersecurity Success Factors: an Exhaustive Literature Review. In *Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20* (pp. 377-395). Springer. https://doi.org/10.1007/978-3-030-71017-

Rahiman, H. U., Nawaz, N., Kodikal, R., & Hariharasudan, A. (2021). Effective Information System and Organisational Efficiency. *Polish Journal of Management Studies, 24*(2), 398-413. https://doi.org/10.17512/pjms.2021.24.2.25

Remac, M. (2017). *The European Union Agency for Network and Information Security (ENISA)-Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA)*. Policy Commons. https://policycommons.net/artifacts/2060012/the-european-union-agency-for-network-and-information-security-enisa/2813103/

Robinson, M. A. (2018). Using Multi-item Psychometric Scales for Research and Practice in Human Resource Management. *Human resource management, 57*(3), 739-750. https://doi.org/10.1002/hrm.21852

Saeed, S. (2023). Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. *Sustainability, 15*(7), 6019. https://doi.org/10.3390/su15076019

Sharma, S., & Warkentin, M. (2019). Do I really belong?: Impact of employment status on information security policy compliance. *Computers & Security, 87*, 101397. https://doi.org/10.1016/j.cose.2018.09.005

Snider, K. L., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, Cyber Threats, and Attitudes Toward Cybersecurity Policies. *Journal of Cybersecurity, 7*(1), tyab019. https://doi.org/10.1093/cybsec/tyab019

Tang, S., & Jia, L. (2011). AMOS: A New Tool for Management Innovation in It Industry. In *Electrical Engineering and Control: Selected Papers from the 2011 International Conference on Electric and Electronics (EEIC 2011) in Nanchang, China on June 20-22, 2011, Volume 2* (pp. 793-800). Springer. https://doi.org/10.1007/978-3-642-21765-4_99

Thelen, E., Ulrich, B. D., & Wolff, P. H. (1991). Hidden Skills: a Dynamic Systems Analysis of Treadmill Stepping During the First Year. *Monographs of the society for research in child development, 56*(1), 1-103. https://doi.org/10.2307/1166099

Tisdale, S. M. (2015). Cybersecurity: Challenges From a Systems, Complexity, Knowledge Management and Business Intelligence Perspective. *Issues in Information Systems, 16*(3), 191-198. https://pdfs.semanticscholar.org/5e0b/b009f7b87d3fff87b20e156a56a726f891fb.pdf

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy, 2*(3), 573-586. https://doi.org/10.3390/jcp2030029

Wiens, C. (2022, October 25). *5 Critical Factors That Impact an Organization's Cybersecurity Efficacy*. Cybersecurity. https://securityboulevard.com/2022/01/5-critical-factors-that-impact-an-organizations-cybersecurity-efficacy/