

# Socio-Technical Perspective in Determining the Factors and Components for Minimizing Cybersecurity Threat

Eko Haryadi <sup>1</sup>, Abdul Karim <sup>1</sup>, Lizawati Salahuddin <sup>1</sup>

<sup>1</sup> Centre for Advanced Computing Technology, Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Malaysia

**Abstract** – Smart city development necessitates careful planning and control. Many factors contribute to failures in smart cities, such as the lack of attention in dealing with cyber security threats, misappropriation of internet facilities, and limitedness of awareness and knowledge of basic-level cybersecurity to safely perform daily activities. Numerous studies have discovered that procrastinating, impulsive, forward-thinking, and risk-taking behaviours vary across organizations, which may help to explain why different organizations adhere to security policies. This research aims to analyse the socio-technical structural relationship of socio-technical perspective in determining the factors and components for minimizing security threat. The research uses a mixed-methods study while the results regarding the contribution of socio-technical components to the improvement of work behaviour in minimizing cybersecurity threats and proposes new analysis result of the contribution work behaviours as contribution and a positive influence for minimizing cybersecurity threat toward successful smart city.

**Keywords** – Socio technical, cybersecurity, threat, behaviour, smart city implementation.

---

DOI: 10.18421/TEM123-66

<https://doi.org/10.18421/TEM123-66>


**Corresponding author:** Eko Haryadi,  
Fakulti Teknologi Maklumat dan Komunikasi,  
Universiti Teknikal Malaysia Melaka, Malaysia  
**Email:** [eko.ehy@bsi.ac.id](mailto:eko.ehy@bsi.ac.id)

Received: 16 April 2023.

Revised: 14 July 2023.

Accepted: 24 July 2023.

Published: 28 August 2023.

 © 2023 Eko Haryadi, Abdul Karim & Lizawati Salahuddin; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

The article is published with Open Access at <https://www.temjournal.com/>

## 1. Introduction

Basic knowledge of cyber security awareness and knowledge is necessary for all employees to support their daily work safely [1]. Data security depends on access control, which can be accomplished through physical control, authorization, and authentication [2]. Approximately 80% of firms report employee misuse of the access to commercial software, according to a survey from study [3].

Misappropriating computer use for hacking or breaking into someone else's territory is violating network security. Employees perpetrate a mistake by denial of service (DoS) attacks against other institutions. Employees utilized existing internet access and applications to perform DoS attacks. An outsider will investigate when this attack coming and obtain the internet protocol address of the attacker's gateway.

The consequences of infringement will have a major impact on the trust of citizens and investors (business actors) in the assurance of legal protection and data protection. The biggest impact that emerged is a lawsuit against the government.

There is an increasing lack of enterprises with adequate levels of cybersecurity personnel, knowledge, and competence. Many businesses are unaware of how to recognize and respond to digital hazards because cyber risk management has not kept pace with digital transformation and analytics [4]. The mere implementation of ICT is not sufficient to ensure high standards [5].

The fact that their workers represent potential security vulnerability in the event of a cyberattack. The staff is their largest information technology (IT) security risk. They are endangering the company's IT security strategy with their carelessness. Businesses understandably worry about being harmed from the inside, as seen by this reality. Human factors and the actions of employees account for 100% of cybersecurity concerns [6].

Adhering to security policies is one of the main behaviours to protect computers and network systems. Method for bolstering cybersecurity and mitigating the effects of social engineering as well as hacking cognition based on user behaviour may be gleaned from a study of these phenomena [7]

Some smart city technologies, according to [8], are more vulnerable to a cyberattack than others. The most susceptible targets for attacks include traffic signal types, emergency warning systems, and street video surveillance. Malicious actors could have a significant negative impact by hacking these systems. Cyberattacks can cause a great deal of harm, including the disruption or compromise of essential services like the electricity or water system. Ransomware attacks frequently even prevent city employees from accessing city computers and networks, putting an end to operations until sizable payments are made [9]. Companies are now required to use cloud-based platforms and remote workforces because of COVID-19.

According to IBM (2020), the typical annual loss from a data breach was almost four million dollars. Also, 130 Twitter accounts were the target of a breach, which led to hackers defrauding \$121,000 in Bitcoin through almost 300 transactions [10]. In contrast, Cisco predicts that by 2023, there will be 15.4 million DDoS attacks globally [11]. What's interesting is that manufacturing companies account for almost a quarter of all ransomware attacks, followed by professional services at seventeen percent of attacks and then government organizations at thirteen percent of attacks [12]. Considering this, internal organizational errors account for more than 90 percent of cybersecurity issues [13].

The consequences of inappropriate behaviour and work habits trigger cybersecurity threats so that smart city implementation will be hampered. Hence, it is crucial to scrutinize the socio-technical aspects that can provide contribution to improve work behaviour as trigger to ICT usage optimization. The socio-technical dimensions include technology, task, organizational structure, actor, and environment. Each of these dimensions will involve many attributes that are used as research indicators so that able to contribute to behaviour improvement.

## 2. Literature Review and Methodology

Using ICT to foster urban innovation, sustainability, and "smartness" has become a new paradigm for public-private partnerships in city planning [14]. The problems with ICT stem from the technical aspects of ensuring the safety of the network.

Data protection (encryption, authentication, and authorization), device connectivity, and interchange, an intuitive user experience, and the ability to locate new services are all essential components of a smart city. Some general challenges before smart city implementation include economic, technological, and infrastructural challenges, while some of the challenges after implementation include cultural and people challenges [15].

Privacy and security issues become important aspects that can have a major and detrimental impact on Indian citizens when the proposed smart city is concerning the use of information technology service-based [16]. The recent rise of the notion of "smart cities" reflects a mix of technology, human resources, and governance, and it provides difficulties to city regulators in design, administering, and regulating contemporary town in the digital age [17]. Smart cities involve remote interaction and automation which will have an impact on increasing security and privacy issues [18]. Lack of high-level planning to successfully sustain smart city development, which in turn leads to loss of resources, poor construction efficiency, and hidden dangers of information system security and all that disrupts China's smart city development process [19]. In Indonesia, the performance of smart city has not been fully accompanied by a design to involve the quality of human resources [20].

The public's lack of awareness of current online platforms is a barrier to smart city implementation, and the government's failure to guarantee that the best possible use is made of existing apps and platforms is another [21]. When it comes to maintaining public confidence in smart city infrastructure and ensuring its continued viability, sound governance of the technological and security measures in place is crucial. The confidence that citizens have in smart city systems and services is essential to their use, and anything that breaches that privacy is likely to have a significant effect on both [22]. Cybersecurity threats (such as information leakage and malicious cyberattacks) in this field impact smart city behavior because of the reliance on different smart city components on ICT. Therefore, because of the widespread use of smart city technologies throughout the world, cybersecurity must progress in the same way [23].

Research defined as the logical and rigorous search for new and pertinent information on a certain topic. Research techniques consist of the many processes, strategies, and algorithms used in research [24]. The research conducted by the researcher is a mixed-methods study.

Qualitative data collection by utilizing semi-structured interviews was conducted to analyze the structural relationship of socio-technical perspective in determining the factors and components for minimizing security threats. The semi-structured discussion direction is developed to handle discussions with officials of the ministry of communication and information at Karawang City, West Java, Indonesia, including the head of E-government implementation, the head of infrastructure and technology, and the head of encryption and information security, the criteria for selecting interviewers are based on their professional competence, trained, experienced in the field of ICT and work positions under the theme of ICT and security as well as the application of smart cities [25].

The next step is to do quantitative data collection. Quantitative data collection was continued as a second stage to evaluate the research model. Due to the limited population size, only 110 employees participated in the questionnaire survey.

The questionnaire has been created in Bahasa in addition to the English version. The questionnaire is broken down into ten primary parts, and there are a total of fifty-one questions to be answered implementing a Likert scale that ranges from 1 to 7 that represent of as extremely contradict to forcefully compromise. One illustration of a questionnaire that can be found in the point of training is the statement "Regularly participating in ICT training may both expand knowledge and decrease vulnerabilities in the ICT area." [26].

The following are the ten points that are used as measurements: competence, which is to assess member of staff performance, is one of the primary variables that may disturb an organization's or company's progression [27], work organization is to measure knowing and understanding work culture is a priority which is greatly influences employee behavior [28], training is to measure the ability of employee in ICT skill to improve company performance [29], IT awareness is important factor for improving cyber security behavior in organizations [30].

Quality of technology is a factor to achieve goal and objectives [31], infrastructure as main factors to increase competency [32], work organization is a factor to increase competency [33], company procedure is factor to improve work behaviors [34], work group is to understand how important a team work to increase work performance [35] and successful implementation of cybersecurity is defined the aspect of donating to the success of smart city implementation [36].

In terms of data analysis, for the qualitative method develop themes using NVivo while for the quantitative method during data investigation utilizes explanatory study, structural equation modeling, and exploratory factor analysis.

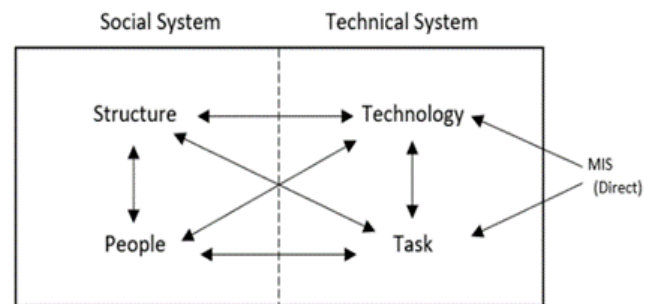


Figure 1. Socio-technical perspective [37]

Figure 1, which depicts the organization of the socio-technical system drawn from [37], has been adopted in this study in proposing a new framework for minimizing cybersecurity threats in smart city.

### 3. Results and Discussion

This section discusses the results of the research accompanied by some evidence of research results.

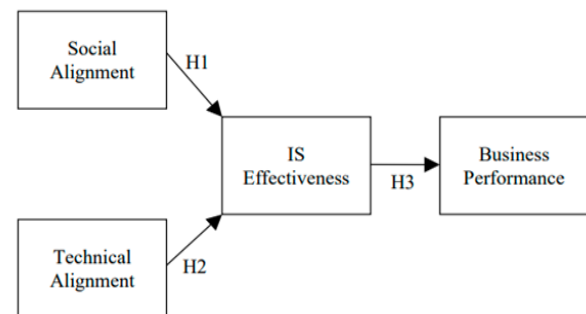


Figure 2. Reference research model [38]

The initial research model (Fig. 2) refers to researchers that used nine independent variables, with one intervening variable, and one dependent variable [38].

#### 3.1. Analysis Model

The analysis model was constructed based on the components described in Figure 1 which took the socio-technical component which was combined with the research model developed by [38].

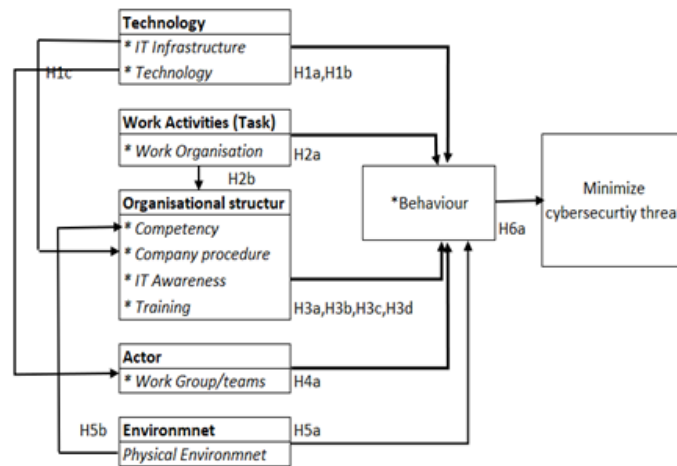


Figure 3. Initial research model

In Figure 3, it is explained in the initial model using four main factors namely, technology, task, organizational structure, actor, and environment. For each factor, the sub-factors are mentioned which are used as research variables, namely IT infrastructure, technology, work organization, competence, procedures, IT awareness, training, work groups, and physical environment. The study hypothesis can be examined in Table 1.

Table 1. List of study hypothesis.

No	Code	Hypothesis	Variable
1	H1a	IT Infrastructure makes a positive contribution to Behavior	X1
2	H1b	Technology makes a positive contribution to Behavior	X2
3	H1c	IT Infrastructure makes a positive contribution to Competency	X1
4	H1d	Technology makes a positive contribution to Workgroup	X2
5	H2a	Work organization makes a positive contribution to Behavior	X3
6	H2b	Work organization makes a positive contribution to Competency	X3
7	H3a	Competency makes a positive contribution to behaviors	X4
8	H3b	The company makes a positive contribution to behaviors	X5

Independent

9	H3c	IT Awareness makes a positive contribution to behaviors	X6	
10	H3d	Training makes a positive contribution to behaviors	X7	
11	H4a	Workgroup makes a positive contribution to Behavior	X8	
12	H5a	The environment makes a positive contribution to behavior	X9	
13	H5b	The environment makes a positive contribution to competencies	X9	
14	H6	Behaviors will give a contribution and a positive influence on minimizing cyber security threats.	X10	Intervening
15		Minimize cybersecurity threat	Y	Dependent

### 3.2. Qualitative Study Analysis

Seven officials from the Ministry of Communication and Informatics were interviewed, and each question posed was tailored to align with the factors or research variables employed. Furthermore, researchers personally approached officers of people interviewed. After they agreed to participate in the interview, an interview appointment is listed. The date, time, and place of the session appropriate for the respondent are determined. The day before the session, a follow-up phone reminder was made to both remind the participants about the session and confirm their attendance. The results of the interviews generally show their agreement on the role of each factor contributing to the behavior.

However, there are several important things to note as follows: IT infrastructure does not have a positive effect on behavior, the physical environment does not have a positive effect on both behavior and competence, and company procedure does not have a positive effect on behaviors. Thus, with the statement above, it changes the hypothesis by eliminating the following hypotheses:

- H1a → IT Infrastructure makes a positive contribution to Behavior
- H3b → The company makes a positive contribution to behaviors
- H5a → The environment makes a positive contribution to behavior
- H5b → The environment makes a positive contribution to competencies.

The results of the hypothesis can be seen in Figure 4.

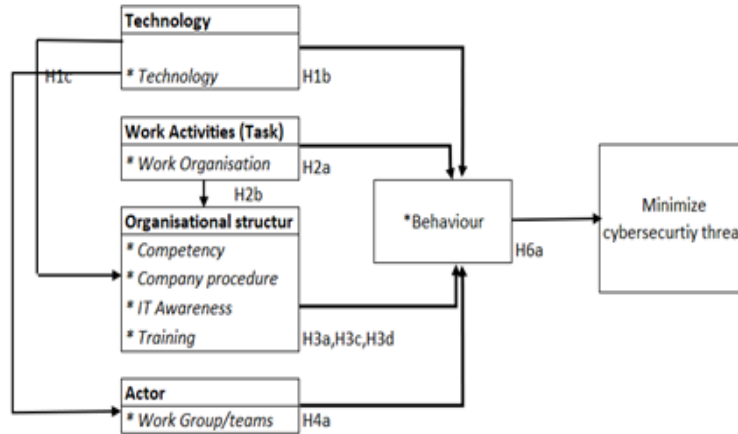


Figure 4. Revised research model based on interview finding

### 3.3. Quantitative Study Analysis

The respondents of the research are divided into several profiles that comprise categories such as age, skills in using a computer, and year of service. The outcomes of calculating the frequency allocation of the characteristics of respondents based on period can be noticed in the subsequent Table 2.

Table 2. Attributes of respondents by age

		Count	Table N %
Age	<30 Years	62	63.90%
	31-40 Years	17	17.50%
	41-50 Years	13	13.40%
	<51 Years	5	5.20%
	Subtotal	97	100.00%

Table 2 delivers the features of respondents based on years, the conclusions are drawn as follows, respondents aged <30 years were 62 respondents or 63.9% of all respondents, while respondents aged 31-40 years were 17 respondents or 17.5% of overall respondents, while respondents aged 41-50 years were 13 respondents or 13.4% of all respondents, while respondents aged ≥ 51 years were 5 respondents or 5.2% of overall respondents.

Thus, the highest frequency of respondent characteristics based on age is in respondents aged <30 years, while the lowest frequency of respondent characteristics based on age is in respondents aged <51 years.

Table 3. Attributes of respondents based on years of join.

		Count	Table N %
Years Of Service	<10 years	76	78.40%
	11-20 years	14	14.40%
	>21 years	7	7.20%
	Subtotal	97	100.00%

According to Table 3, the respondent's attributes based on the tenure of service, respondents with <10 years of service were 70 respondents or 78.4% of the total respondents, respondents with 11-20 years of service as many as 14 respondents or 14.4% of the total respondents, respondents who had a working period of ≥ 21 years were 7 respondents or 7.2% of all respondents. Thus, the highest commonness of respondents' attributes based on the tenure of service is on respondents who have worked for <10 years, while the lowest frequency of respondents' characteristics based on tenure is on respondents who have worked for ≥ 21 years.

Table 4. Characteristics of respondents based on skill level

		Count	Table N %
Level Of Skills	Somewhat unskilled	2	2.10%
	Moderate skillful	31	32.00%
	Skillful	42	43.30%
	Very Skillful	19	19.60%
	Extremely skillful	3	3.10%
	Subtotal	97	100.00%

As can be seen in Table 4 the skill level of the first rank is occupied by employees with skillful abilities of 43.3%, then moderate skilled at 32% and very skilled at 19.6%.

Inferential analysis using the SEM analysis technique was analyzed using smart partial least squares (PLS) software. The in question structural analysis is based on variance, which is the basis of analytical research. The test is run in two phases. A measurement model (outer model), including outer loading testing, average variance extracted (AVE), and composite reliability (CR) using Cronbach's alpha (CA), is implemented in the first phase to calculate the validity and construct reliability of each indicator.

The final phase involves running an inner model structural test to see if there is any interrelationship between the variables. Examining the R-square (R<sup>2</sup>, the goodness fit model), path coefficient, and two-tail t significance test values is how inner model testing is done. Please refer to Figure 5 path coefficient and t-value to determine whether the path coefficient is significant for the research hypothesis. Following two model evaluation phases, the outcomes of the SEM model investigation can address research hypotheses.

In the measurement model test, multiple criteria need to be met. The first criterion is the test of construct validity, which involves assessing the value of the outer loading. The second criterion is the test of construct reliability, which includes examining the (AVE), (CR), and (CA). The discussion of these tests focuses on construct validity (specifically convergent validity) to determine if a variable effectively measures its intended concept. Additionally, the study tested the validity of the dimension prototype presented in the paper [39]. The use of the outer loading values allows for the test of convergent validity. If the indicator of outer loading is more elevated than 0.7, it is said to encounter convergent validity in a respectable category [40].

The second one is construct reliability test to ascertain the consistency of a measurement, the study's testing of the measurement model's reliability was conducted [41]. High consistency in measuring the indicator's latent construct is a sign of high reliability. The values of CA, CR, and AVE were used in tests to gauge the construct reliability's value.

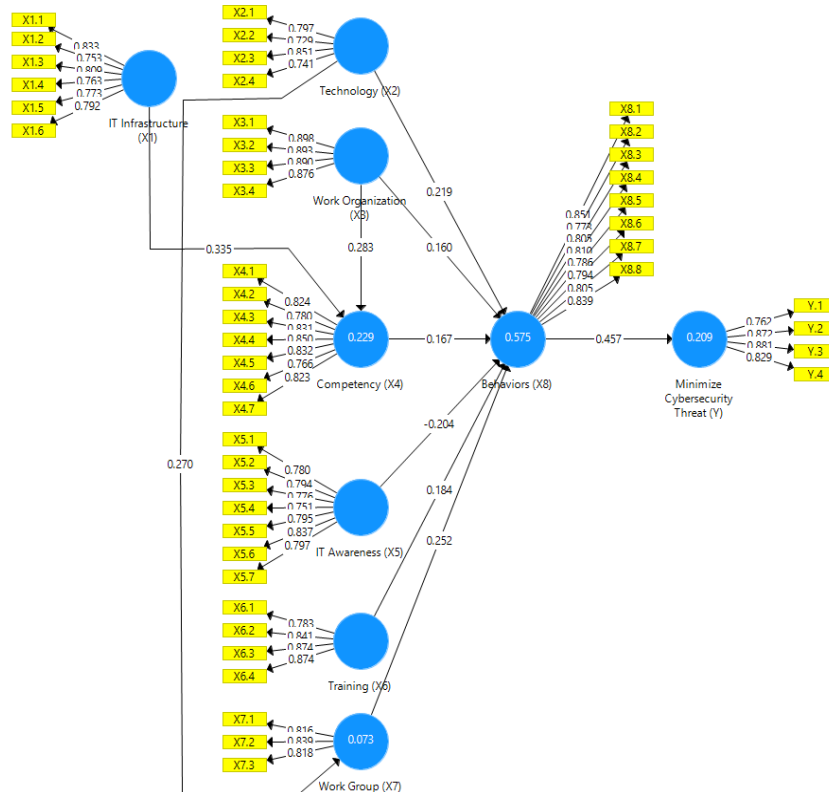


Figure 5. Path coefficient and outer loading.

**3.4. Normality Test**

The variables in the submitted model of this study were verified to ensure that the data met the normality presumption. It measures the influences that can occur due to the model size. As the model scope of this study is 97 (number of respondents who return the form), it appropriate with the requisite sample was stipulated by study [42], hence strengthening the normality distribution of constructs. Hereinafter, the skewness, and kurtosis of each variable have been used to evaluate normality. Further, [43] define that data is regular if its skewness is between -2 to +2 and kurtosis is between -7 to +7. Table 5 indicates that the skewness and kurtosis grade of the current data are below the respective cut-off points; hence there is no extreme departure from the normality assumption. Thus, the outcome in Table 5 proves that the normalcy assumptions of the data are met, and the collected data does not infringe on the normality contention.

*Table 5. Result of Normality Test*

Constructs	Skewness	Kurtosis Statistic
IT Infrastructure	-0.486	-0.111
Technology	-0.799	-0.156
Work Organization	-0.855	-0.377
IT Awareness	-0.642	-0.424
Training	-0.211	-0.432
Competency	-0.720	-0.295
Work Group	-0.133	-0.466
Behavior	-0.760	-0.233
Minimize cybersecurity	-0.099	-0.658

**3.5. Convergent Validity**

Each indicator of the observed latent variable provides a value of outer loading greater than 0.7 [43], as shown in Table 6, and that value suffices to meet the convergent validity requirements.

*Table 6. Outer loading to test convergent validity*

Variable	SLF							
	1	2	3	4	5	6	7	8
IT Infrastructure – X1	0,833	0,753	0,809	0,763	0,773	0,792		
Technology - X2	0,797	0,729	0,851	0,741				
Work Organization – X3	0,898	0,893	0,890	0,876				
Competency – X4	0,824	0,780	0,831	0,850	0,832	0,766	0,823	
IT Awareness – X5	0,780	0,794	0,776	0,751	0,795	0,837	0,797	
Training – X6	0,783	0,841	0,874	0,874				
Work Group - X7	0,816	0,839	0,818					
Behaviors – X8	0,851	0,773	0,805	0,810	0,786	0,794	0,805	0,839
Minimize Cybersecurity - Y	0,762	0,872	0,881	0,829				

*Table 7. The CA, CR and AVE*

	CA	CR	AVE
IT Infrastructure (X1)	0,879	0,900	0,907
Technology (X2)	0,785	0,793	0,862
Work Organization (X3)	0,912	0,915	0,938
Competency (X4)	0,916	0,918	0,933
IT Awareness (X5)	0,900	0,908	0,921
Training (X6)	0,865	0,881	0,908
Work Group (X7)	0,767	0,777	0,864
Behaviors (X8)	0,924	0,928	0,938
Minimize Cybersecurity Threat (Y)	0,859	0,894	0,903

A variable is considered reliable if it has CR>0.70, AVE>0.50, and a CA>0.7. According to test results of Table 7, all indicators that measure or shape latent variables are said to have high reliability. As an outcome, the indicators of the measurement benchmark (outer model) for each latent variable consistently measure the latent variables. As a result, the measurement model can be utilized to try the analysis of the hypothesis.

**3.6. Discriminant Validity**

Fornell-Larcker criterion and cross-loadings were applied to check for discriminant validity. Table 8 shows the effects of the Fornell-Larcker measure.

Table 8. Correlation between latent variables and square root

	IT Infrastructure	Technology	Work Organization	Competency	IT Awareness	Training	Work Group	Behaviors	Minimize Cybersecurity
IT Infrastructure	0,788								
Technology	0,154	0,781							
Work Organization	0,194	0,316	0,889						
Competency	0,390	0,310	0,348	0,816					
IT Awareness	0,249	0,343	0,249	0,359	0,790				
Training	0,274	0,276	0,334	0,156	0,337	0,844			
Work Group	0,140	0,270	0,176	0,285	0,368	0,183	0,824		
Behaviors	0,221	0,510	0,444	0,465	0,534	0,439	0,495	0,808	
Minimize Cybersecurity Threat	0,200	0,291	0,162	0,302	0,232	0,228	0,235	0,457	0,837

3.7. Evaluation of the Structural Model

Evaluation of the structural model allows the researcher to establish how well empirical data support the research model. The main point for evaluating the structural sample in PLS-SEM include collinearity assessment, the importance of the path coefficients, the level of the R2 values, the f2 effect size, the predictive relevance (Q2), and the q2 effect size [43]. The following sections explain each of the analyses.

3.8. Collinearity Assessments

Collinearity assessment was conducted to show some construct: IT Infrastructure, technology, work organization, IT awareness, training, competency, work group, behavior, minimize cybersecurity. Table 9 presents the results of collinearity assessment. All VIF results are clearly below than threshold of 5.00. Thus, collinearity among the predictor constructs is not a matter in the structural sampling.

Table 9. Collinearity assessment

Constructs	VIF
IT Infrastructure	1.973
Technology	1.625
Work Organization	2.871
IT Awareness	2.538
Training	2.204
Competency	2.108
Work Group	1.578
Behavior	2.511
Minimize cybersecurity	2.057

3.9. Structural Model Path Coefficients

Appropriate with study [43], bootstrapping process was applied to deliver standard errors and t-statistics. Table 10 reveals the path coefficient, the t-values, and their importance levels (p-values) obtained from the bootstrapping. Data in bold indicates the most important exogenous construct on the respective endogenous construct.

Table 10. Direct influence path coefficient and tcount

	Original Sample (O)	Sample Mean (M)	(STDEV)	T Statistics $(\frac{O}{\sqrt{STDEV}})$	P Values
X1 → X4	0.335	0.358	0.097	3.462	0.001
X2 → X7	0.270	0.285	0.092	2.918	0.004
X3 → X4	0.283	0.287	0.086	3.274	0.001
X2 → X8	0.219	0.221	0.076	2.860	0.004
X3 → X8	0.160	0.148	0.080	1.992	0.047
X4 → X8	0.167	0.173	0.078	2.135	0.033
X5 → X8	-0.204	-0.206	0.082	2.502	0.013
X6 → X8	0.184	0.192	0.073	2.514	0.012
X7 → X8	0.252	0.246	0.070	3.607	0.000
X8 → Y	0.457	0.469	0.082	5.594	0.000

The t value > 1.96 indicates a positive and significant direct effect [43]. Based on the direct influence path coefficient in Table 10, all the direct influence path coefficients are positive.

3.10. Coefficient of Determination

There are myriad ways to examine the SEM structural model, including testing the coefficient of determination or R<sup>2</sup> value, both path coefficients of direct and indirect effects, then testing the significance of direct and indirect effects. The R<sup>2</sup> value ranges from 0 to 1. The higher the R<sup>2</sup> value indicates the higher the prediction accuracy [43]. The test is further elucidated as follows. The R<sup>2</sup>, which shows how much exogenous and endogenous variables influence each other, is displayed in Table 11



Table 11. R<sup>2</sup> Value

Endogenous construct	R <sup>2</sup>
Behaviors	0,575
Minimized Cybersecurity Threat	0,209

Table 11 clearly shows that the R<sup>2</sup> value of the minimized cybersecurity threat variable is 0.209 (20.9%) which can be interpreted as the influence of behaviors on minimized cybersecurity threat is 20.9%, while the remaining is 79.1% influenced by other factors not observed. The R<sup>2</sup> value of the behavior variable is 0.575 (57.5%) which can be interpreted as the influence of technology, work organization, competency, IT awareness, training, and work group to behavior of 57.5%, while the residual 42.5% is influenced by other factors not examined

**3.11. Predictive Relevance**

The predictive relevance (Q<sup>2</sup>) test is to assess whether the model makes meaningful predictions is the goal of the Q-square (Q<sup>2</sup>) test evaluation. If the Q<sup>2</sup> value is greater than zero and was obtained using the blindfolding procedure, that is the criterion used to determine whether the model has a relevant prediction [29].

Table 12. Q<sup>2</sup> value

Endogenous construct	Q <sup>2</sup>
Behaviors	0,357
Minimize Cybersecurity Threat	0,131

All latent variables' Q<sup>2</sup> results are greater than zero (Table 12). This indicates that the model is relevant for prediction or that it can be modified and developed in future research models.

**3.12. The Effect Size F2 and Q2**

The analysis f-square effect size (F2) is to test the f-square value which aims to verify the category of influence of exogenous variables on endogenous variables, which are diverged into three classifications, namely low, medium, and large. The criteria for testing the value of F are 1) 0.02≤F<0.15 is low; 2) 0.15≤F<0.35 is medium; and 3) greater than or equal to 0.35 is high [30]. The output of data analysis results for the F-square value is shown below in Table 13:

Table 13. F-square effect size (f<sup>2</sup>)

Exogenous	Endogenous	
	Work Behaviors	Minimize Cybersecurity Threat
Competency	0,050	
IT Awareness	0,070	
Technology	0,088	
Training	0,064	
Work Group	0,122	
Work Organization	0,047	
Work Behaviors		0,265

Based on the f square value above, the results show that the influence of technology, work organization, competency, IT awareness, training, and work group on work behaviors is in a low category because it has f square value is 0.02≤F<0.15. The effect of work behaviors on minimize cybersecurity threat is in the medium category because it has an f square value of 0.15≤F<0.35

Additional testing is the immediate effect in the research; the model is done by examining at the path coefficient value on each path of the research hypothesis and observed by a t-test to discover the path coefficient value or the consequence value in the influential classification.

**3.13. Hypothesis Testing**

The results of two types of hypotheses testing with positive and negative results, the components involved are technical components consisting of technical and work activities, as well as social components consisting of organizational structures and actors. The two types of hypothesis testing are as follows

- A. The first hypothesis has a positive direct effect of x1 on x4, the statistical hypothesis experimented is the positive immediate impact of x1 on x4. Statistical hypothesis: H0: β41 ≥ 0, H1: β41 > 0, H0 is rejected, if Tcount ≥ 1.96 given that the direct effect of x1 on x4 was calculated using structural equation modeling, the value of the path coefficient for p41 was found to be 0.335, and Tcount of 3.462 was found to be greater than 1.96; hence, the null hypothesis H0 was confirmed to be true. The conclusions of the investigation of the hypotheses indicated that X1 has a direct and positive encouragement on X4.

B. The seventh hypothesis has a negative direct effect of X5 on X8, the statistical hypothesis tested is the negative direct effect of X5 on X8. Statistical hypothesis: H0:  $\beta_{85} \geq 0$ , H1:  $\beta_{85} < 0$ , H0 is rejected, if Tcount 1.96. Based on the conclusions reached via the application of the structural equation when modeling the direct impact of X5 on X8, the route coefficient value

of p85 is -0.204, and Tcount is (2.502) to be greater than 1.96; thus, H0 is accepted. This indicates that X5 does have a direct influence on X8. The outcomes of the examination of the hypotheses indicate that X5 has a direct and negative influence on X8. A complete report of the outcomes of the hypothesis tests is shown in table 14.

Table 14. Resume of hypothesis examination outcomes

Immediate Influence	Path Coefficient	T count	T table	Test conclusion
IT Infrastructure (X1) -> Competency (X4)	0.335	3.462	1.96	H0 declined, H1 received. There is a positive immediate impact of X1 on X4
Technology (X2) -> Work Group (X7)	0.270	2.918	1.96	H0 declined, H1 received. There is a positive immediate impact of X2 on X7
Work Organization (X3) -> Competency (X4)	0.283	3.274	1,96	H0 declined, H1 received. There is a positive immediate impact of X3 on X4
Technology (X2) -> Behaviors (X8)	0.219	2.860	1.96	H0 declined, H1 received. There is a positive immediate impact of X2 on X8
Work Organization (X3) -> Behaviors (X8)	0.160	1.992	1.96	H0 declined, H1 received. There is an immediate positive impact of X3 on X8
Competency (X4) -> Behaviors (X8)	0.167	2.135	1.96	H0 declined, H1 received. There is a positive immediate impact of X4 on X8
IT Awareness (X5) -> Behaviors (X8)	-0.204	2.502	1.96	H0 declined, H1 received. There is an immediate negative impact of X5 on X8
Training (X6) -> Behaviors (X8)	0.184	2.514	1.96	H0 declined, H1 received. There is a positive immediate impact of X6 on X8
Work Group (X7) -> Behaviors (X8)	0.252	3.607	1.96	H0 declined, H1 received. There is a immediate positive impact of X7 on X8
Behaviors (X8) -> Minimize Cybersecurity Threat (Y)	0.457	5.594	1.96	H0 declined, H1 received. There is a positive immediate impact of X9 on Y

3.14. Result Model

Figure 6 illustrates the final model for minimizing security threats in Karawang city. It shows that all socio-technical components including technology, work organization, competency, training, and the team can be fulfilled and contribute to improving work behavior, and subsequently, work behaviors

can be used as a reference and efforts to minimize security threats in Karawang city. The determining factor for each technology component is the use of the latest information technology and the use of artificial intelligence which is supported by data management and network security through strong controls through standards and procedures.

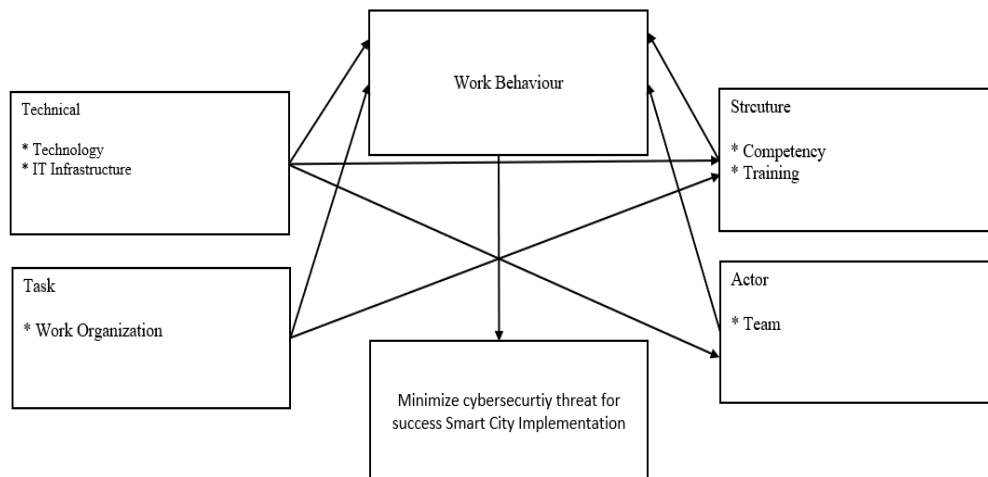


Figure 6. Final model for minimizing security threat

#### 4. Conclusion

Implementation of a smart city that is exempted from cyber security threats is a challenge for organizations. The research implemented two technical dimensions (technical and task), two social dimensions (organization structure and actor), and some attributes (technology, IT infrastructure, work organization, competency, training, and team) to support work behaviors. The research based on construct validity testing, meets convergent validity in a good category, whereas, for the reliability test it can be concluded that all signs that measure form latent variables take good reliability. In terms of f-square effect size analysis, work behavior provides a relatively good contribution effect towards minimizing cybersecurity threat, even though the results of the analysis have a low effect. In future research, it is expected that the model generated from this research can be composed with a control and risk framework to get more accurate results. Hence, various kinds of disturbances or threats during smart city implementation can be resolved earlier.

#### References:

- [1]. Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference, August 2015*.
- [2]. Esiefarienrhe, B. M., & Ekka, A. H. (2018). Modified role-based access control model for data security. *International Journal of Scientific and Technology Research*, 7(11), 182–186.
- [3]. BNP. (2021). *80 % of organizations report employee abuse of access to business applications*. Retrieved from: <https://www.securitymagazine.com/articles/96439-80-of-organizations-report-employee-abuse-of-access-to-business-applications> [accessed: 04 February 2023].
- [4]. Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2015). Strategy, not technology, drives digital transformation. *MIT Sloan Management Review*.
- [5]. Zadoo, S., Handoo, V., Kotru, A., & Gupta, S. (2022). Optimizing the Usage of ICT for Enhancing Quality in Teaching-Learning Assessment Processes: Case Study. *International Journal of Combined Research & Development (IJCRD)*, 5(11).
- [6]. Kaspersky Lab. (2018). *The Human Factor in IT Security - How employees are making businesses vulnerable from within*. Kaspersky. Retrieved from: <https://www.kaspersky.com/blog/the-human-factor-in-it-security/> [accessed: 25 February 2023].
- [7]. Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, 12, 561011.
- [8]. Teale, C. (2021). *The smart city tech most at risk for cyberattacks report*. Smartcities Dive. Retrieved from: <https://www.smartcitiesdive.com/news/the-smart-city-tech-most-at-risk-for-cyberattacks-report/597365/> [accessed: 12 March 2023].
- [9]. Trapenberg Frick, K., Mendonça Abreu, G., Malkin, N., Pan, A., & Post, A. E. (2021). *The cybersecurity risks of smart city technologies: What do the experts think?* 1–18. CLTC. Retrieved from: <https://cltc.berkeley.edu/wp-content/uploads/2021/03/Smart-City-Cybersecurity.pdf> [accessed: 14 March 2023].
- [10]. Leswing, K. (2020). *Twitter hackers who targeted Elon Musk and others received \$121,000 in bitcoin, analysis shows*. Cnbc Llc. <https://www.cnbc.com/2020/07/16/twitter-hackers-made-121000-in-bitcoin-analysis-shows.html> [accessed: 27 March 2023].
- [11]. Cisco, T., & Internet, A. (2020). Cisco: 2020 CISO Benchmark Report. *Computer Fraud & Security*, 2020(3). [https://doi.org/10.1016/s1361-3723\(20\)30026-9](https://doi.org/10.1016/s1361-3723(20)30026-9)
- [12]. Camille Singleton. (2020). *Ransomware 2020: Attack Trends Affecting Organizations Worldwide*. Securityintelligence. Retrieved from: <https://securityintelligence.com/posts/ransomw-are-2020-attack-trends-new-techniques-affecting-organizations-worldwide/> [accessed: 27 March 2023].

- [13]. Aronovich, A. (2018). Why Educating *Your Employees on Cyber Intelligence and Security Will Reduce Risk*. Cybint.
- [14]. Yeh, H. (2017). The effects of successful ICT-based smart city services: From citizens' perspectives. *Government Information Quarterly*, 34(3), 556–565. Doi: 10.1016/j.giq.2017.05.001
- [15]. Behzadfar, M., Ghalehnoee, M., Dadkhah, M., & Highlight, N. M. (2017). International Challenges of Smart Cities. *Armanshahr Architecture & Urban Development*, 10(20), 79–90.
- [16]. Chatterjee, S., & Kar, A. K. (2018). Effects of successful adoption of information technology enabled services in proposed smart cities of India: From user experience perspective. *Journal of Science and Technology Policy Management*, 9(2), 189–209. Doi: 10.1108/JSTPM-03-2017-0008
- [17]. Allahar, H. (2020). What are the challenges of building a smart city? *Technology Innovation Management Review*, 10(9), 38–48. Doi: 10.22215/TIMREVIEW/1388
- [18]. Rahman, W. F. W. A., Abdalla, A. H., & Islam, M. R. (2021). The proposed framework and challenges towards smart city implementation. *Journal of Physics: Conference Series*, 2084(1).
- [19]. Huang, K., Luo, W., Zhang, W., & Li, J. (2021). Characteristics and problems of smart city development in China. *Smart Cities*, 4(4), 1403–1419. Doi: 10.3390/smartcities4040074
- [20]. Handayani, D. W., Syafarudin, S., & Mufliah, L. (2021). Problem Realisasi Kebijakan Smart City di Indonesia: Kasus Kota Bandar Lampung. *JISPO Jurnal Ilmu Sosial dan Ilmu Politik*, 11(1), 35–62.
- [21]. Syalianda, S. I., & Kusumastuti, R. D. (2021). Implementation of smart city concept: A case of Jakarta Smart City, Indonesia. *IOP Conference Series: Earth and Environmental Science*, 716(1), 1–10. Doi: 10.1088/1755-1315/716/1/012128
- [22]. Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Information Systems Frontiers*. Doi:10.1007/s10796-020-10044-1
- [23]. Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports*, 7, 7999–8012. Doi: 10.1016/j.egy.2021.08.124
- [24]. Almalki, S. (2016). Integrating Quantitative and Qualitative Data in Mixed Methods Research—Challenges and Benefits. *Journal of Education and Learning*, 5(3), 288. Doi: 10.5539/jel.v5n3p288
- [25]. Davis, M. C., Challenger, R., Jayewardene, D. N. W., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics*, 45(2), 171–180. Doi: 10.1016/j.apergo.2013.02.009
- [26]. Marouf, L., & ur Rehman, S. (2004). Human resource development policies and practices for the IT and information workforce in Kuwaiti companies. *Library Review*, 53(7), 351–355. Doi: 10.1108/00242530410552287
- [27]. Sudaryana, Y. (2021). Effect of Competence, Organizational Culture, and Motivation towards Employee Performance at PT Kukuh Tangguh Sandang Mills. *Jurnal Ekonomi & Bisnis JAGADITHA*, 8(1), 23–29. Doi: 10.22225/jj.8.1.2687.23-29
- [28]. Tianya, L. (2015). Organizational Culture & Employee Behavior: Case study. *Lahden Ammattikorkeakoulu Lahti University of Applied Science*, 1–53.
- [29]. Barba Aragón, M. I., Jiménez Jiménez, D., & Sanz Valle, R. (2014). Training and performance: The mediating role of organizational learning. *BRQ Business Research Quarterly*, 17(3), 161–173. Doi: 10.1016/j.cede.2013.05.003
- [30]. Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016). Cyber security awareness and its impact on employee's behavior. In *Research and Practical Issues of Enterprise Information Systems: 10th IFIP WG 8.9 Working Conference, CONFENIS 2016, Vienna, Austria, December 13–14, 2016, Proceedings 10*, 103–111. Springer International Publishing.
- [31]. Asli, S. M. G., Gilaninia, S., & Homayounfar, M. (2016). Information Technology and Its Impact on Job Behavior. *Oman Chapter of Arabian Journal of Business and Management Review*, 5(11), 1–6. Doi: 10.12816/0031493
- [32]. Jabbouri, N. I., & Zahar, I. (2015). The effect of IT infrastructure on organizational performance via the role of core competences: empirical study in Iraqi banks. *Journal of Islamic and Human Advanced Research*, 5(1), 1–11.
- [33]. Yusmariono. (2017). Hubungan Antara Budaya Organisasi Dengan kompetensi Sosial Guru. *Jurnal Benchmarking*, 1(1), 42–46.
- [34]. Gunningham, N., & Kagan, R. A. (2005). Regulation and business behavior. *Law and Policy*, 27(2), 213–218. Doi: 10.1111/j.1467-9930.2005.00197.x
- [35]. Sanyal, S., & Hisam, M. W. (2018). The Impact of Teamwork on Work Performance of Employees: A Study of Faculty Members in Dhofar University. *IOSR Journal of Business and Management*, 20(3), 15–22.
- [36]. Alam, R. G., & Ibrahim, H. (2021). Cybersecurity implementation success factors in smart city. *Journal of Theoretical and Applied Information Technology*, 99(13), 3353–3364.
- [37]. Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective. *MIS Quarterly*, 1(3), 17–32.
- [38]. Lee, S. M., Kim, K., Paulson, P., & Park, H. (2008). Developing a socio-technical framework for business-IT alignment. *Industrial Management and Data Systems*, 108(9), 1167–1181. Doi: 10.1108/02635570810914874
- [39]. Strauss, M. E., & Smith, G. T. (2009). Construct validity: Advances in theory and methodology. *Annual Review of Clinical Psychology*, 5, 1–25. Doi: 10.1146/annurev.clinpsy.032408.153639

- [40]. Astuti, C. C. (2021). PLS-SEM Analysis to Know Factors Affecting the Interest of Buying Halal Food in Muslim Students. *Jurnal Varian*, 4(2), 141–152. Doi: 10.30812/varian.v4i2.1141
- [41]. Sun, L., Ji, S., & Ye, J. (2018). Partial Least Squares. In *Multi-Label Dimensionality Reduction*. Chapman and Hall/CRC. Doi: 10.1201/b16017-6
- [42]. Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and psychological measurement*, 30(3), 607-610.
- [43]. Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Sage publications.