Socio Technical Framework to Improve Work Behavior During Smart City Implementation

Eko Haryadi[1], Abdul Karim[2], Lizawati Salahuddin[3]
Centre for Advanced Computing Technology, Fakulti Teknologi Maklumat dan Komunikasi[1, 2, 3]
Universiti Teknikal Malaysia Melaka, Malaysia[1]

***Abstract*—Every organization uniquely adheres to security culture. Numerous studies have discovered that procrastinating, impulsive, forward-thinking, and risk-taking behaviors vary across organizations, which may help to explain why different organizations' adherence to security policies. This study describes the human aspect of a government organization in contributing to the successful implementation of a smart city by minimizing cybersecurity threats. Improper employee behavior and lack of understanding of cybersecurity will negatively contribute to the successful development of smart cities. The purpose of this research is to develop a framework to determine the factors to improve work behavior in terms of the contribution of social and technical factors. The use of a socio-technical approach to explain how socio-technical integration can contribute to improving work behavior by using mixed methods. The results indicated that several socio-technical factors which include technology, IT infrastructure, work organization, competency, training, and teamwork contribute to improving work behaviors which can be used as a basis for minimizing cybersecurity threats in smart city implementation.**

***Keywords*—Framework; socio technical; cybersecurity; behavior; threat; smart city**

I. Introduction

Information and communication technology (ICT) has had an impact that can be felt in all sectors of human development. ICTs provide recent potential for the restoration soundness systems, new methods of citizens' authority, and active inclusion in their community at both charitable and political tiers. The elaboration of ICT has made a huge difference in the world. ICT affects many fields where it becomes a tool that enables the exchange of enormous information. ICTs deliver immensity and profound information to those who did not beforehand have this science and thus the chance for social and economic mobility.

Access to ICTs can have a profound influence on people's sense of empowerment and aptitude to be active participants in their society at both the political and social levels. ICT can intensify the empowerment of civil society by enhancing their proficiency to work as an organized network both within and beyond the frontier [1]. An ICT has altered the lives of society at the operative level. Technology gives people the operative power to commit, notify, create, study, perform, and demolish.

Technology also has its enchantment and attraction. Technology is not only an important means of human headway but also the most glorious human invention. Technological developments are difficult to stem because social entities show a tendency to dominate and exploit operatively weaker entities [2]. The ICT has succeeded in improving the lives and broadening the horizons of society, but also facilitates the manipulation of society. Stunning sounds emanate from billions of screens and speakers around the world, and they shape people's thoughts and behavior.

Increasingly the means possessed by humans will be able to facilitate progress and human life but do not always lead to this goal. The effects of tool advancements depend to a large extent on the social and political environment that decides how these tools are used, and their operational strength. Society is getting stronger, but this does not mean that people's life has become preferable, wiser, and more beautiful. To make the world and life better, means must be used in a way that decrease misery, nescience, and devastation, for these are the basic dimensions by which human progress must be measured [2].

System improvement in urban areas based on the active use of information technology requires specialists with adequate qualifications, therefore, the methodological development of human resources needs to be considered from a bilateral approach position both in terms of executor and users [3]. Human resource development which is reviewed from two perspectives (executor and user) is necessary for the realization of smart city implementation.

The role of ICT is very substantial hence humans are very dependent on technology and humans cannot live without technology and it is very difficult and almost impossible to work without ICT. In everyday life, there are many cases where most people consciously or unconsciously use ICT purely [4].

Human teamwork in distributed knowledge-sharing groups relies on information and communication technology (ICT) functionality to support achievement. By adapting the level of detail of the information to the situation knowledge must be shared efficiently. In certain situations, information can be exchanged by involving people who work in collaboration [5].

Human development is one of the main factors that capture the core of livelihood in a community. In the current information age, the reach and diffusion of information and communication technology (ICT) that can reach remote countries in the world make it a stimulus to attain the preference for human development targets. The high population growth in urban areas will cause a lot of population problems as well as economic activity. [6].

Human factors contribute significantly to computer security, the human weaknesses that may cause unintentional jeopardize to the company or organization [7]. Cybersecurity is expanding to resolve the range of attack types while the attackers counter with their innovative hacking systems. Cybersecurity uses different approaches to upgrade detection of the threats [8].

Two things are the core elements of organizational culture, namely in the form of basic assumptions and beliefs. Collective norms and values will influence employee behavior. Organizational culture is consequently expressed in the collective values, norms, and knowledge of the organization. Several things are expressions of norms and values, namely artifacts and handbooks, rituals, and anecdotes [9]

Organizational culture can have dissimilar subcultures based on sub-organizations or purposes. Information Security Culture is a subculture concerning common company functions. It should support all activities so that information security becomes a natural aspect of the daily activities of every employee. Information security must become a natural aspect of employees' daily activities so that it can support all activities [9]

Another problem is cyberattacking have succeeded in defeating technical security solutions by utilizing human factor vulnerabilities related to security awareness, and skills and manipulating the human element to inadvertently grant access to important industrial assets. Knowledge and skills capability level contribute to human analytical proficiency to heighten cyber security readiness [10]

Human involvement is necessary to complement a technically based security approach to ensure overall cybersecurity. Human factors and organizational factors contribute to affecting the security of computing systems. The factors that appear on the user side are risk behavior, trust, lack of motivation, and inadequate use of technology while on the management side are inadequate workload and staff knowledge.

Information security violations can be classified in several different ways. The study [11] mentioned that based on several studies performed by other researchers provided thirteen attacks that cover all the computer security risk factors, and eventually defined “nine factors (that) can cover all risks as main factors”. These factors are an excess privilege, error, and omission, denial of service, social engineering, unauthorized access, identity thief, phishing, malware, and unauthorized copy.

Information security practice accommodate all sociocultural quantify that support technical security methods, employee recognize that information security is a natural aspect to support daily activities. To utilize this socio-cultural behavior effectively and efficiently, management models and socio technical framework are required. The company must determine that the information security culture must be part of the organizational culture.[12] The contribution of the human factor in the failure to secure and protect systems, services, organizations, and information is tremendous [8]. The interrelationship of human and organizational factors and computer and information security vulnerabilities is very significant. The factors that contribute to improving work behaviors to reduce cybersecurity threats and how the socio-technical factors contribute to improving work behavior is a discussion that will be explained in the results of study because human factors significantly influence people’s interaction with information security hence generating many risks [13].

II. Literature Review

A. Smart City

The smart city concept continues to experience rapid development from year to year by following the flow of technological developments and innovations. The latest smart city concept, smart city 4.0, was just launched in 2017 by the innovation acceleration group from the University of Berkeley, California, United States. The Smart City 4.0 concept emerged as an action from the industrial revolution 4.0 by bringing initiatives to develop the skills of young innovators and entrepreneurs in the technology industry. Smart City 4.0 aims to develop skills for the industrial revolution 4.0 and accelerate technology development for young innovators, start-ups, and technology companies to create the best solutions to make cities smarter, safer, and more sustainable. [14].

Further, [15] identified two types of Japanese smart city initiatives: business-led initiatives conducted in conjunction with large-scale urban developments and government-led initiatives that are anchored within the vision statements of municipalities. Several experts have defined smart cities, [16] defined the smart city as a city that should integrate IT infrastructures, and social and economic issues to, more useful, and more flexible responses. Further, [17] mentioned that a smart city should be a city well performing in a forward-looking way with six smart characteristics (also called soft factors: smart economy, smart mobility, smart environment, smart people, smart living, smart governance), built on the smart combination of endowments and activities of self-decisive, independent, and aware citizens.

B. Cybersecurity

Cyber security is an important issue in the infrastructure of every company and organization. A company or organization based on cybersecurity can achieve high status and countless successes because this success is the result of the company's ability to protect personal and customer data from competitors. Organizations and competitors’ customers and individuals are rude. The company or organization must first and foremost provide this security in the best way to build and develop itself [18].

Cybersecurity includes practical steps to protect information, networks, and data from internal or external threats. Cybersecurity professionals protect networks, servers, intranets, and computer systems. Cybersecurity ensures that only authorized individuals have access to that information[19]. According to [19] Information Security is an effort to protect physical and digital data from unauthorized access, disclosure, misuse, unauthorized alteration, and deletion. Operational Security includes the processes and decisions made to control and protect data.

C. Behaviour

Behavior is the way a person or thing acts or reacts. The definition of behavior is based on the opinion of clinical psychologists and psychotherapists [20]. Behavior is an essential means for individuals to externalize information from their (entirely internal) psychical systems to their external surroundings. [21]

D. Socio Technical Concept

A socio-technical system (STS) consists of humans using technology to perform assignment through an operation within a social system (association) toward reaching a specified purpose. Numerous of the issues and losses of management information systems and administration science or operations research projects have been attributed to corporate behavioral concerns [29]. A socio-technical system (STS) consists of the complicated relations between sociable humans and technological systems. [22]

Socio-technical systems are distinguished by a high capacity of social complexity as well as technical intricacy to perform the essential positions of community [23] There was a synergistic combination of people, technology, organizational structures, and processes, including the operating environment in which all of this occurs [15]. The prefix socio is always associated with individuals and community in general, while 'technical' denotes something related to machines or technology. [22] The general structure of the STS and the elements that make up its complex social and technical dimensions are described differently by various researchers.

E. Related Works

Sociotechnical systems include physical and technical artifacts, organizations, scientific components, and legal [24]. Technical subsystems in an organization to solve complex issues [29]. The social subsystem consists of the organizational structure, which encompasses authority structures, reward systems, knowledge, skills, attitudes, values, needs and within the organization, employees can work by utilizing technological artifacts (tools, devices, and techniques) to achieve job satisfaction and economic performance [17]. As shown in Fig. 1, the socio-technical system, describes the interrelated nature of the organizational system, embedded in the external environment consisting of goals, people, buildings, technology, culture, and process [25].

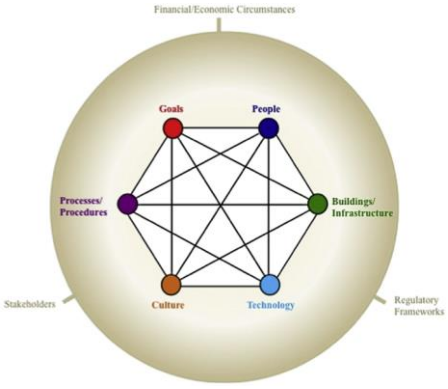


Fig. 1. Socio-technical system, illustrating the interrelated nature of an organizational system, embedded within an external environment from [25].

Refer to Fig. 2. The information technology or information systems when developed require several social sub-system factors (user roles, social interaction) and technical sub-system factors (technical infrastructure, system access) [26].

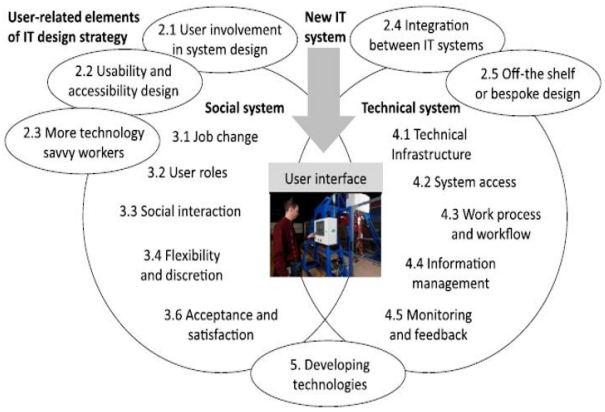


Fig. 2. Elements of the IT introduction and socio-technical system that may affect or be affected by the user-interface from [26].

The supporting elements in establishing a security system that is linked to Socio-technical will depend on the security requirements for the organization to determine the nature of ICT a culture of security to be cultivated. Apart from that, there are other defining requirements policies, and types of countermeasures (security systems) to be implemented. Next comes the security section requirements impose demands on the people who will interact with the system. Other activities such as motivation, training, and education need to be done thoroughly. In security culture issues, culture has effects on attitudes and beliefs, which in turn play a part in individual behaviors actions, and or reactions [30]

Based on Fig. 2, Fig. 3, a generic motif that can be accepted is the necessity and importance of work behavior to minimize cyber security threats. The questions here can rather be:

1) What are the factors that contribute to improving work behaviors to reduce cybersecurity threats?

2) How can socio-technical factors contribute to improving work behavior

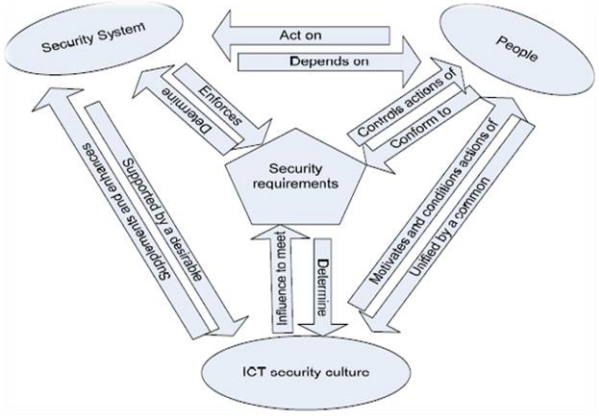


Fig. 3. An organizational framework showing ICT security culture in relation to other ICT security controls from [30].

III. Research Methodology

The research methodology is described in Fig. 4.

1) Literature review: Literature reviews are more concentrated on the main studies according to the title of the research and those related to data collection both for interviews and research surveys. The literature review that emerged includes the concept and definition of smart city, definition of cybersecurity, concept of behavior, and socio-technical concept. The components and elements in the socio-technical will be used as a reference for building questions for qualitative studies and become question points in quantitative studies using the Likert scale model.

2) Initial model: This stage is the initial model used in this study. Referring to Fig. 1, the initial model adopts all socio-technical components, which consist of structure, technical, people, tasks, and environment. This initial model will then be used as a reference for processing questions for qualitative and point surveys for quantitative studies.

3) Qualitative model: The interview process is part of a qualitative study, namely by gathering as much information as possible from appointed and agreed sources. the results of this interview change the initial model by eliminating some of the components, namely by removing the environment hence that there will be four main components, namely structure, technical, people, and tasks.

4) Quantitative model: An interview to collect qualitative data will be carried out which is then followed by quantitative data collection by employing a survey questionnaire in the second phase [27]. Numerical data for quantitative research were collected and analyzed using statistical methods [28]. The model from the results of a qualitative study becomes a reference in a quantitative study the survey questionnaire will exclude an environmental component.

5) Final model: The final model is based on the quantitative finding. Data collection and data examination are essential when applying structural equation modeling (SEM). Several issues need to be addressed when utilizing a questionnaire survey. These issues include response rates, non-response bias, common method bias, missing data, and data distribution.

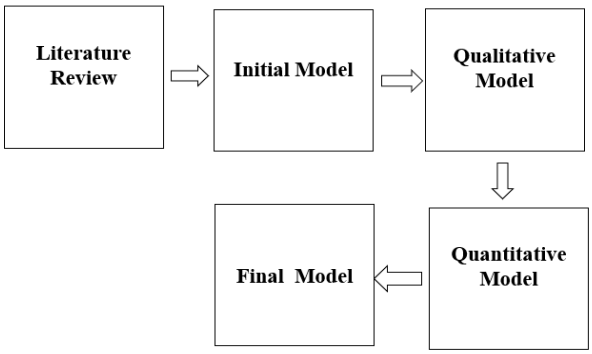


Fig. 4. Research methodology.

IV. Result and Discussion

Being a part of continual research, this investigation is based on primary data origins gathered in West Java – Indonesia. Using mix-method research, is specifically primary analysis that contains the collection of data (interview and survey data), organizing it in some fashion (a social-technical framework) based on some factors of technological environment, personnel development, and organizational support. Fig. 5 shows the interaction between a social and technical system and the point interviews and questionnaires were made based on socio-technical components [29],[31] to obtain in-depth information about what factors influence improving work behavior. Each question and point questionnaire has been validated by several experts who are competent in their fields. Interviews were conducted thoroughly with several employees in the communication and information department which were conducted randomly and were conducted before the questionnaire process began.

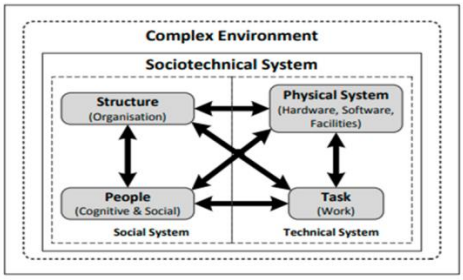


Fig. 5. Socio-technical perspective [29].

The initial model as shown in Fig. 6, propose includes technical, social, and environmental dimensions. Hypotheses that can emerge from the initial model which are displayed sequentially, are IT infrastructure has a positive influence on behavior, technology have a positive influence on behavior, IT infrastructure has a positive influence on competency, technology has a positive influence on work group, work organization has a positive influence on behavior, work organization has a positive influence on competency, competency has a positive influence on behaviors, company procedure have a positive influence on behaviors, IT awareness have a positive influence on behaviors, training have a positive influence on behavior, work group have a positive influence on behavior, environment have a positive influence on behavior, environment have a positive influence on competencies, and behaviors will give contribution and a positive influence for minimizing cyber security threat toward successful smart city implementation.

The interview process involved limited Ministry of Communication and Informatics (Kominfo) staff and employees; the number of interviewees was seven people. The interview process is carried out in stages and at different times according to the agreement. Some of the questions posed to them included:

- What is the impact of the external environment on competence?
- How does the organization provide direction regarding work behavior and culture?

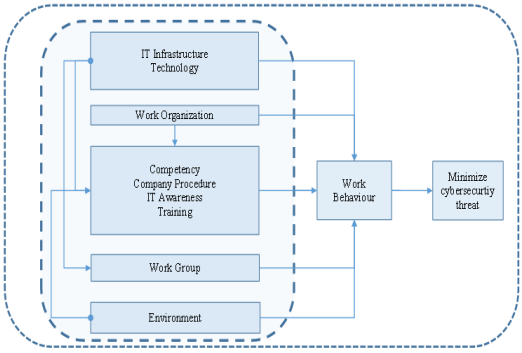


Fig. 6. Initial model.

The answer to the questions above is:

I believe the influence of the external environment on competency is not so significant that I can even say that there is no influence. (Respondent 1)

External factors do have the opportunity to contribute to employee competency but are very small and not significant (Respondent 3)

The qualitative method by using the interview process finally abolishes several hypotheses, as shown in Fig. 7 namely environment has a positive influence on behavior, environment has a positive influence on competencies, IT infrastructure has a positive influence on behaviors, and company procedure has a positive influence on behaviors.

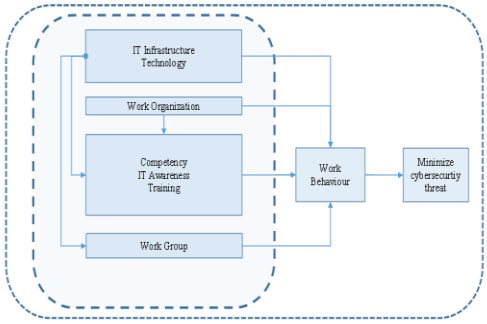


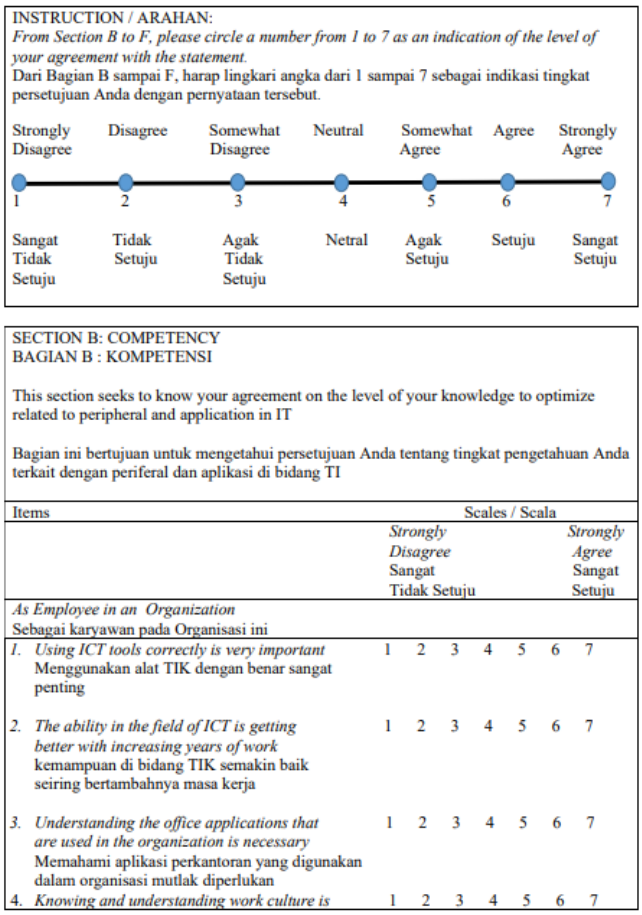
Fig. 7. New model based on qualitative result.

The questionnaires were delivered to employees who work at Kominfo. A total of 110 questionnaires were distributed to the Kominfo office in three districts, and 97 people filled out and returned the questionnaire form within two months. Table I shows the total questionnaire distributed which shows the data collected and which can be used.

TABLE I. DISTRIBUTION OF QUESTIONNAIRE

Office (District)	Distributed	Collected	Unusable	Usable
Karawang	55	43	0	43
Bandung	66	50	0	50
Purwakarta	10	4	0	4
Total	130	97	0	97

An example of a question sheet for a survey questionnaire is listed in Fig. 8.



INSTRUCTION / ARAHAN:
From Section B to F, please circle a number from 1 to 7 as an indication of the level of your agreement with the statement.
Dari Bagian B sampai F, harap lingkari angka dari 1 sampai 7 sebagai indikasi tingkat persetujuan Anda dengan pernyataan tersebut.

Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
1	2	3	4	5	6	7
Sangat Tidak Setuju	Tidak Setuju	Agak Tidak Setuju	Netral	Agak Setuju	Setuju	Sangat Setuju

SECTION B: COMPETENCY
BAGIAN B : KOMPETENSI

This section seeks to know your agreement on the level of your knowledge to optimize related to peripheral and application in IT

Bagian ini bertujuan untuk mengetahui persetujuan Anda tentang tingkat pengetahuan Anda terkait dengan periferal dan aplikasi di bidang TI

Items	Scales / Scala						
	Strongly Disagree Sangat Tidak Setuju						*Strongly Agree* Sangat Setuju
As Employee in an Organization Sebagai karyawan pada Organisasi ini							
1. *Using ICT tools correctly is very important* Menggunakan alat TIK dengan benar sangat penting	1	2	3	4	5	6	7
2. *The ability in the field of ICT is getting better with increasing years of work* kemampuan di bidang TIK semakin baik seiring bertambahnya masa kerja	1	2	3	4	5	6	7
3. *Understanding the office applications that are used in the organization is necessary* Memahami aplikasi perkantoran yang digunakan dalam organisasi mutlak diperlukan	1	2	3	4	5	6	7
4. *Knowing and understanding work culture is*	1	2	3	4	5	6	7

Fig. 8. Form questionnaire.

The data represented in this area defines analysis data such as mean, minimum, maximum, standard deviation, median, and mode. Presentation of data descriptions starts from exogenous variables, namely IT infrastructure (X1), technology (X2), work organization (X3), IT awareness (X5), and training (X6) followed by endogenous variable competency (X4), workgroup (X7), behaviors (X8) and minimize cybersecurity threat (Y), descriptions of each variable are presented successively starting from variables X1, X2, X3, X4, X5, X6 X7, X8 and Y. As shown in Table II to Table X.

TABLE II. LATENT VARIABLE FOR IT INFRASTRUCTURE

	No.	Mean	Median	Min	Max	Standard Deviation	Excess Kurtosis	Skewness
X1.1	1.000	5.680	6.000	4.000	7.000	0.844	-0.540	-0.167
X1.2	2.000	5.763	6.000	4.000	7.000	0.822	-0.628	-0.096
X1.3	3.000	5.794	6.000	4.000	7.000	0.811	-0.678	-0.071
X1.4	4.000	5.680	6.000	4.000	7.000	0.781	-0.328	-0.158
X1.5	5.000	5.691	6.000	3.000	7.000	0.854	-0.004	-0.261
X1.6	6.000	5.691	6.000	4.000	7.000	0.829	-0.738	0.088

TABLE III. LATENT VARIABLE FOR QUALITY OF TECHNOLOGY (X2)

	No.	Mean	Median	Min	Max	Standard Deviation	Excess Kurtosis	Skewness
X2.1	7.000	5.845	6.000	4.000	7.000	0.889	-0.970	-0.135
X2.2	8.000	5.804	6.000	4.000	7.000	0.893	-0.779	-0.219
X2.3	9.000	5.701	6.000	4.000	7.000	0.875	-0.708	-0.121
X2.4	10.000	5.577	6.000	4.000	7.000	0.906	-0.738	-0.150

TABLE IV. LATENT VARIABLE FOR WORK ORGANIZATION (X3)

	No.	Mean	Median	Min	Max	Standard Deviation	Excess Kurtosis	Skewness
X3.1	11.000	6.072	6.000	4.000	7.000	0.900	-0.867	-0.490
X3.2	12.000	5.897	6.000	4.000	7.000	0.902	-0.833	-0.306
X3.3	13.000	6.010	6.000	4.000	7.000	0.891	-0.924	-0.376
X3.4	14.000	5.938	6.000	4.000	7.000	0.883	-0.794	-0.334

TABLE V. LATENT VARIABLE FOR COMPETENCY (X4)

	No.	Mean	Median	Min	Max	Standard Deviation	Excess Kurtosis	Skewness
X4.1	15.000	5.753	6.000	4.000	7.000	0.920	-0.727	-0.291
X4.2	16.000	5.763	6.000	4.000	7.000	0.906	-0.812	-0.185
X4.3	17.000	5.784	6.000	4.000	7.000	0.933	-0.855	-0.247
X4.4	18.000	5.742	6.000	4.000	7.000	0.888	-0.631	-0.271
X4.5	19.000	5.804	6.000	4.000	7.000	0.959	-0.796	-0.377
X4.6	20.000	5.784	6.000	4.000	7.000	0.864	-0.482	-0.340
X4.7	21.000	5.742	6.000	4.000	7.000	0.945	-0.739	-0.353

TABLE VI. LATENT VARIABLE FOR IT AWARENES (X5)

	No.	Mean	Median	Min	Max	Standard Deviation	Excess Kurtosis	Skewness
X5.1	22.000	5.897	6.000	4.000	7.000	0.879	-0.662	-0.350
X5.2	23.000	5.938	6.000	4.000	7.000	0.859	-0.612	-0.374
X5.3	24.000	6.072	6.000	4.000	7.000	0.911	-0.511	-0.644
X5.4	25.000	5.845	6.000	4.000	7.000	0.889	-0.826	-0.224
X5.5	26.000	5.794	6.000	3.000	7.000	0.952	-0.169	-0.593
X5.6	27.000	5.804	6.000	4.000	7.000	1.012	-0.806	-0.505
X5.7	28.000	5.866	6.000	4.000	7.000	0.926	-0.906	-0.280

TABLE VII. LATENT VARIABLE FOR TRAINING (X6)

	No.	Mean	Median	Min	Max	Standard Deviation	Excess Kurtosis	Skewness
X6.1	29.000	5.979	6.000	4.000	7.000	0.773	-0.282	-0.372
X6.2	30.000	5.897	6.000	4.000	7.000	0.831	-0.674	-0.241
X6.3	31.000	5.897	6.000	4.000	7.000	0.793	0.174	-0.568
X6.4	32.000	5.979	6.000	4.000	7.000	0.812	-0.060	-0.548

TABLE VIII. LATENT VARIABLE FOR WORKGROUP (X7)

	No.	Mean	Median	Min	Max	Standard Deviation	Excess Kurtosis	Skewness
X7.1	33.000	5.887	6.000	4.000	7.000	0.785	-0.297	-0.315
X7.2	34.000	5.814	6.000	3.000	7.000	0.877	0.340	-0.648
X7.3	35.000	5.845	6.000	4.000	7.000	0.877	-0.441	-0.434

TABLE IX. LATENT VARIABLE FOR BEHAVIOUR (X8)

	No.	Mean	Median	Min	Max	Standard Deviation	Excess Kurtosis	Skewness
X8.1	36.000	5.763	6.000	4.000	7.000	0.950	-0.731	-0.384
X8.2	37.000	5.856	6.000	4.000	7.000	0.908	-0.799	-0.295
X8.3	38.000	5.784	6.000	4.000	7.000	0.888	-0.897	-0.095
X8.4	39.000	5.825	6.000	4.000	7.000	0.812	-0.839	-0.016
X8.5	40.000	5.784	6.000	4.000	7.000	0.840	-0.725	-0.098
X8.6	41.000	5.969	6.000	4.000	7.000	0.902	-0.874	-0.366
X8.7	42.000	5.845	6.000	4.000	7.000	0.854	-0.564	-0.301
X8.8	43.000	5.804	6.000	4.000	7.000	0.893	-0.654	-0.307

TABLE X. LATENT VARIABLE FOR MINIMIZE CYBERSECURITY THREAT (Y)

	No.	Mean	Median	Min	Max	Standard Deviation	Excess Kurtosis	Skewness
Y.1	44.000	5.856	6.000	3.000	7.000	0.984	-0.281	-0.626
Y.2	45.000	6.021	6.000	3.000	7.000	0.963	0.080	-0.816
Y.3	46.000	5.969	6.000	4.000	7.000	0.879	-0.704	-0.402
Y.4	47.000	5.979	6.000	3.000	7.000	0.941	0.508	-0.787

The quantitative process provides changes to the qualitative model by removing some of the attributes of the social dimension. The elimination of some attributes on the social dimension was due to the results of the questionnaire which was processed using structural equation modeling. Table XI shows the processing results of the quantitative method using SEM modeling. This hypothesis shows a negative result of IT awareness of work behavior, so the last model shown in Fig. 9 does not include the relationship between IT awareness and work behavior. The descriptive Analysis of Research Variables is shown in the table.

The framework created in this study is a communion of the framework composed by [30] and the research results resulting from the processing of structural equation models (SEM). The quantitative results show that the social dimension presents a great contribution than the technical dimension, this does not mean that social factors are more prominent, the contribution of both dimensions must still be required because both dimensions must continue to exist to be able to contribute to the development of the formation the work behavior. The factors that play a role in improving work behavior according to the research questions are as follows as shown in Fig. 5. The researcher divides the main factors contributing to increased work behavior into three parts, namely, personal development which consists of training and competency, organizational support which consist of teamwork and work organization, and

technological environment which consists of technology and IT infrastructure.

TABLE XI. HYPOTHESIS TESTING

Immediate impact	Path Coefficient	T count	Examination Conclusion
IT Infrastructure to competency (X1→X4)	0.335	3.462	H0 is refused, H1 is accepted. There is a positive direct effect of X1 → X4
Technology to work group (X2→X7)	0.270	2.918	H0 is refused, H1 is accepted. There is a positive direct effect of X2 → X7
Work Organization to competency (X4→X4)	0.283	3.274	H0 is refused, H1 is accepted. There is a positive direct effect of X3 → X4
Technology to behaviors (X2→X8)	0.219	2.860	H0 is refused, H1 is accepted. There is a positive direct effect of X2 → X8
Work Organization to behaviors (X3→X8)	0.160	1.992	H0 is refused, H1 is accepted. There is a direct positive effect of X3 → X8
Competency to behaviors (X4→X8)	0.167	2.135	H0 is refused, H1 is accepted. There is a positive direct effect of X4 → X8
IT Awareness to behaviors (X5→X8)	-0.204	2.502	H0 is refused, H1 is accepted. There is a direct negative effect of X5 → X8
Training to behaviors (X6→X8)	0.184	2.514	H0 is refused, H1 is accepted. There is a positive direct effect of X6 → X8
Work group to behaviors (X7→X8)	0.252	3.607	H0 is refused, H1 is accepted. There is a direct positive effect of X7 → X8
Behaviors to Minimize Cybersecurity Threat (X9→Y)	0.457	5.594	H0 is refused, H1 is accepted. There is a positive direct effect of X9 → Y

T Table = 1.96

Based on Fig. 9, the researcher makes a detailed elucidation by placing personal development as a fundamental basis then followed by organizational support and technological assistance. In most cases, personal development is a process of self-development owned by someone to achieve success in the world of work. In consort with personal development, employees can manage themselves well when working enterprise. The principal objective of this personal development is to dig up the potency that exists within oneself so that it can withstand to encounter all the alteration times that encircle it. Two factors need to be done for the self-development process, which can be through training and competency improvement.

According to [32] competence is the ability to act and think consistently that is owned by someone equipped with skills, basic attitudes, knowledge, and values. Competence is a person's skills and direct and indirect conduct that enable the person to effectively undertake a given assignment or assigned character. Hence, competence is not only about the capability or awareness that an employee has but the compliance to do what is known and can yield advantages.

According to [32] competence is the ability to act and think consistently that is owned by someone equipped with skills, basic attitudes, knowledge, and values. Competence is a person's skills and direct and indirect conduct that enable the person to effectively undertake a given assignment or assigned character. Hence, competence is not only about the capability or awareness that an employee has but the compliance to do what is known and can yield advantages.

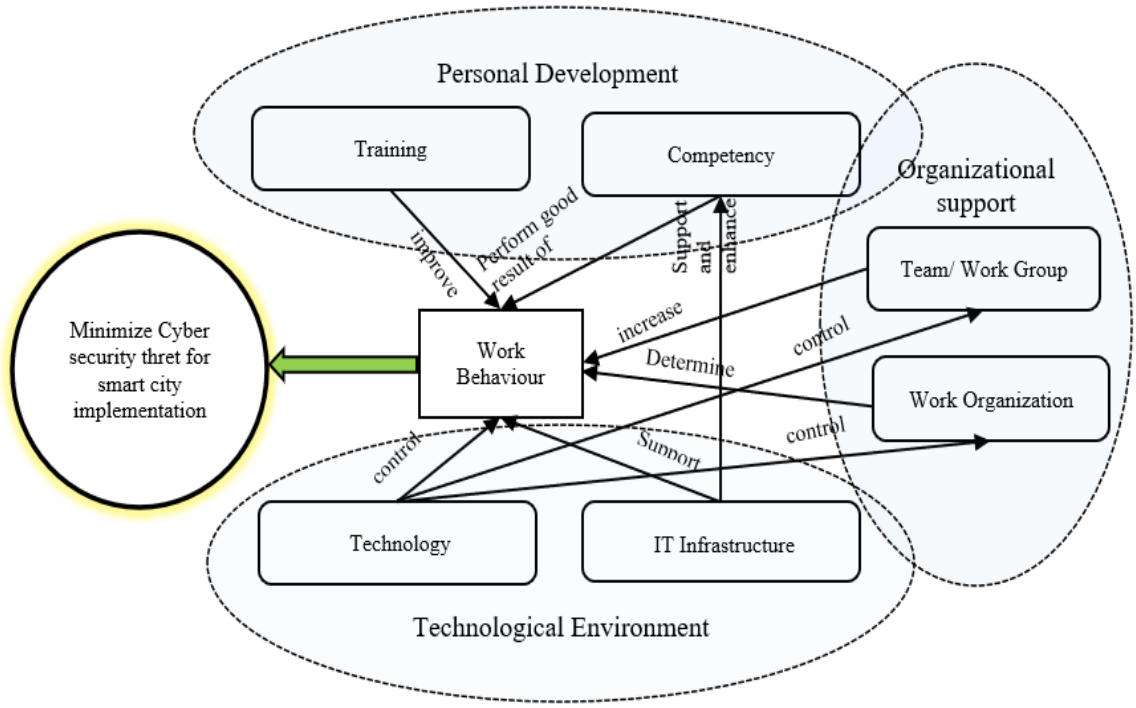


Fig. 9. Final model.

Training is one way to intensify competence [33]. Therefore, competence and training are two interconnected things. To rectify competency through training related to improving work behavior, there are several types of training that employees must obtain. Training is a key tool to increase the firm's organizational learning capability at individual, group, and organizational levels and, through this effect, training may affect performance. Some of the important training for employees, number one is the understanding importance of cybersecurity; cybersecurity is critical because it helps to protect organizations and individuals from cyber-attacks. Cybersecurity awareness is contributed to avert data breaches, identity stealing, and other types of cybercrime. Organizations are compulsory to apply strong cybersecurity measures to protect their data and customers. Behavior in the case of cybersecurity incidents, insider threats occur when an employee's careless behavior or lack of security awareness leads to a security breach.

For example, an employee might use an insecure password or fall for a phishing scam [34]. Malicious insider threats happen in case an employee intentionally causes a security breach.

Another compulsory training is how to defend against cyber-attack; this training will educate the employee to do some action against cybersecurity threats for example Turning on Multifactor Authentication. Implement multifactor authentication on your accounts and make it significantly less likely you'll get hacked [35].

Managing password security and a secure password is further important training for the user [36]. Robust passwords can assist defend against cyberattacks and reduce the hazard of a safety violation. The password generally is long—at least twelve symbols—and include uppercase letters, lowercase notes, digits, and certain symbols [37].

Robust passwords should not have any private data. Workplace protection directs to the measures put in place to save individuals, investments, and data from physical and digital threats. These hazards can reach in different shapes, running from robbery, roughness, and destruction to digital safety risks such as cyberattacks, data violations, and hacking.

Comprehending and protecting sensitive information is the other important training, the information needs to be protected to prevent that data from being misused by third parties for fraud, such as phishing scams and identity theft [38]. Data protection is also essential to help control cybercrimes by ensuring details (specifically banking) and reference report are covered to prevent deception.

The employee should know cyber-attack tactics [39], during a cyber-attack, the attacker gains unauthorized ace ss to a computer system, network, or device for stealing, modifying, or destroying data. The attacker may use a variety of tactics, including malware, social engineering, or exploiting vulnerabilities in software or systems. Further incident response is an organized, strategic approach to detecting and managing cyber-attacks in ways that minimize damage, recovery time, and total costs. Detecting phishing emails, emails with bad grammar, and spelling mistakes, emails with an unfamiliar greeting or salutation, inconsistencies in email addresses, links and domain names, and suspicious attachments, emails requesting login credentials, payment information, or sensitive data. [40].

Teamwork is part of the actor which is a social dimension. The objective of the entertainers in the organization is to emphasize the position recreated by human beings toward gaining protection. The actors include management and employees, and other stakeholders who execute or influence the way work organizational tasks are carried out and work organization is part of work activities. The purpose of work activities in the organization is to emphasize the purpose and implementation of suitable duties by individuals in extra operation and competency areas, using tools and resources, towards security. The work activities refer to the actual tasks and the way they should be carried out.

Technology and IT infrastructure are part of the technology from the technical dimension. The purpose of technology in the organization is to emphasize the tools and resources used by people in carrying out work activities towards achieving security. The technology includes any useful technical resources that can aid humans in performing their security duties, for example, information, equipment, frameworks, and computers.

In this research, the researcher uses two dimensions on the technical side, namely technology in general refers to Technology as the application of scientific knowledge to the practical aims of human life or, as it is sometimes phrased, to the change and manipulation of the human environment.

While IT infrastructure is part of the technology, more specifically the combined components needed for the operation and management of enterprise IT services and IT environments. The components of IT infrastructure are made up of interdependent elements, and the two core groups of components are hardware and software. The hardware uses software like an operating system to work, and likewise, an operating system manages system resources and hardware. operating systems also make connections between software applications and physical resources using networking components to produce a new framework, as shown in Fig.10., researchers adopted an ICT security framework from [30] as support and contribute to minimize cyber security threat for smart city implementation

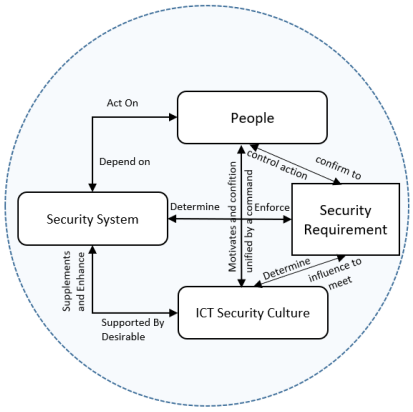


Fig. 10. ICT Security framework [30].

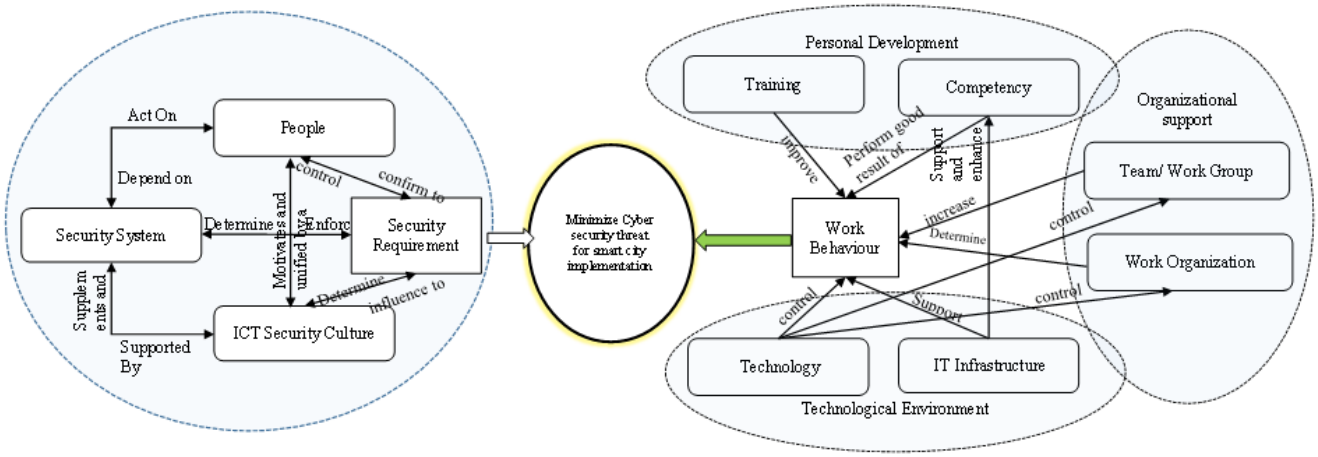


Fig. 11. Socio technical framework to improve work behavior.

Fig. 11 shows the relationship between the socio-technical components and their role in improving work behavior to minimize cyber security threats during smart city implementation. Planned training well and followed by all employees will improve work behavior. Training will contribute to employee competence and perform a good result to the work behavior. In addition, to be able to improve competency, good IT infrastructure support is needed. Organizational contributions make a dominant contribution, consisting of teams and organizational work that improve and determine work behavior. The level of success of the organization is determined by the support provided by the technology environment. The last component that contributes to improving work behavior is support from technology and IT infrastructure, implementation of backup systems, use of operating systems (OS), data communication devices, network security systems, anti-virus, and monitoring systems will have a major impact on work behaviors so that it is expected to be able to contribute to minimizing cyber security attacks in the framework of the successful implementation of smart cities.

V. Conclusion and Future Work

The results of the study show that social and technical factors contribute to increased work behavior; this is shown from the results of the quantitative method which produces a summary of hypotheses where there is only one hypothesis that shows negative results so that it cannot be used in the formulation of the framework proposed by the researcher. In this study, three main factors contribute to improving work behavior, namely personal development which consists of training and competency, organizational support which consists of teamwork and work organization, and technological environment which consists of technology and IT infrastructure to be able to contribute to minimizing threats cybersecurity.

In the future, organizations will experience many challenges, so to keep all problems better in the field of cybersecurity, a social-technical framework that is developed which aims to improve work behavior in a positive direction will be stronger when combined with a control framework by adopting a control objective for Information and related technology (COBIT) and using the program and risk framework by implementing the NIST Cybersecurity Framework.

References

[1] K. Shade, O. Awodele, and S. Okolie, “ICT: An Effective Tool in Human Development,” Int. J. Humanity. Soc. Sci., vol. 2, no. 7, pp. 157–159, 2012.

[2] M. Radovan, “ICT and Human Progress,” Inf. Soc., vol. 29, no. 5, pp. 297–306, 2013, doi: 10.1080/01972243.2013.825686.

[3] E. Avdeeva, T. Davydova, N. Skripnikova, and L. Kochetova, “Human resource development in the implementation of the concept of ‘smart cities,’” E3S Web Conf., vol. 110, no. April 2019, doi: 10.1051/e3sconf/201911002139.

[4] M. Sharma, “Influence of ICT and Its Dynamic Change in Daily Life of Human Being,” J. Contemp. Issues Bus. Gov., vol. 27, no. 3, pp. 1–5, 2021, doi: 10.47750/cibg.2021.27.03.085.

[5] S. Garrett and B. Caldwell, “Describing functional requirements for knowledge sharing communities,” Behavior. Inf. Technol., vol. 21, no. 5, pp. 359–364, 2002, doi: 10.1080/0144929021000050265.

[6] P. Jayaprakash and R. R. Pillai, “The Role of ICT and Effect of National Culture on Human Development,” J. Glob. Inf. Technol. Manag., vol. 24, no. 3, pp. 183–207, 2021, doi: 10.1080/1097198X.2021.1953319

[7] E. Metalidou, C. Marinagi, P. Trivellas, and N. Eberhagen, “The Human Factor of Information Security: Unintentional Damage Perspective,” Procedia - Soc. Behav. Sci., vol. 147, pp. 424–428, 2014, doi: 10.1016/j.sbspro.2014.07.133.

[8] E. Kadena, “Human Factors in Cybersecurity: Risks and Impacts,” vol. 2015, pp. 51–64, 2021, doi: 10.37458/ssj.2.2.3.

[9] H. Green, “Cognitive Behavioral Therapy Explained GRAEME WHITFIELD & ALAN DAVIDSON Abingdon,” Drug Alcohol Rev., vol. 27, no. 4, pp. 459–460, 2008, doi: 10.1080/09595230802089917.

[10] U. D. Ani, “Human factor security: evaluating the cybersecurity capacity of the industrial workforce,” J. Syst. Inf. Technol., vol. 21, no. 1, pp. 2–35, 2019, doi: 10.1108/JSIT-02-2018-0028.

[11] N. Badie and A. H. Lashkari, “A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP,” vol. 2, no. 9, pp. 9331–9347, 2012.

[12] T. Schlienger and S. Teufel, “Information security culture – from analysis to change,” no. July 2003, pp. 183–195.

[13] K. Parsons, A. Mccormac, M. Butavicius, and L. Ferguson, “Human Factors and Information Security: Individual, Culture and Security Environment”.

[14] Y. Yun and M. Lee, "Smart City 4.0 from the perspective of open innovation," J. Open Innov. Technol. Mark. Complex., vol. 5, no. 4, 2019, doi: 10.3390/joitmc5040092.

[15] A. Deguchi, "Society 5.0: A people-centric super-smart society," Soc. 5.0 A People-centric Super-smart Soc., pp. 1–177, 2020, doi: 10.1007/978-981-15-2989-4.

[16] H. Yeh, "The effects of successful ICT-based smart city services: From citizens' perspectives," Gov. Inf. Q., vol. 34, no. 3, pp. 556–565, 2017, doi: 10.1016/j.giq.2017.05.001.

[17] M. Behzadfar, M. Ghalehnoee, M. Dadkhah, and N. M. Highlight, "International Challenges of Smart Cities *," Arman. Archit. Urban Dev., vol. 10, no. 20, pp. 79–90, 2017.

[18] N. Danilina and A. Majorzadehzahiri, "Social factors of sustainability for a smart city development," IOP Conf. Ser. Mater. Sci. Eng., vol. 869, no. 2, 2020, doi: 10.1088/1757-899X/869/2/022027.

[19] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, 2021, doi: 10.1016/j.egyr.2021.08.126.

[20] R. M. Bergner, "What is behavior? And so what?" New Ideas Psychol., vol. 29, no. 2, pp. 147–155, 2011, doi: 10.1016/j.newideapsych.2010.08.001.

[21] J. Uher, "What is Behavior? And (when) is Language Behavior? A Metatheoretical Definition," J. Theory Soc. Behav., vol. 46, no. 4, pp. 475–501, 2016, doi: 10.1111/jtsb.12104.

[22] G. H. Walker, N. A. Stanton, P. M. Salmon, and D. P. Jenkins, "A review of sociotechnical systems theory: A classic concept for new command and control paradigms," Theory. Issues Ergon. Sci., vol. 9, no. 6, pp. 479–499, 2008, doi: 10.1080/14639220701635470.

[23] P. P. Y. Wu, C. Fookes, J. Pitchforth, and K. Mengersen, "A framework for model integration and holistic modelling of socio-technical systems," Deci's. Support Syst., vol. 71, pp. 14–27, 2015, doi: 10.1016/j.dss.2015.01.006.

[24] H. Rohracher, "A sociotechnical mapping of domestic biomass heating systems in Austria," Bull. Sci. Technol. Soc., vol. 22, no. 6, pp. 474–483, 2002, doi: 10.1177/0270467602238890.

[25] M. C. Davis, R. Challenger, D. N. W. Jayewardene, and C. W. Clegg, "Advancing socio-technical systems thinking: A call for bravery," Appl. Ergon., vol. 45, no. 2 Part A, pp. 171–180, 2014, doi: 10.1016/j.apergo.2013.02.009.

[26] M. Maguire, "Socio-technical systems and interaction design - 21st century relevance," Appl. Ergon., vol. 45, no. 2 Part A, pp. 162–170, 2014, doi: 10.1016/j.apergo.2013.05.011.

[27] J. W. Creswell and J. D. Creswell, Mixed Methods Procedures. 2018.

[28] O. D. Apuke, "Quantitative Research Methods: A Synopsis Approach," Kuwait Chapter Arab. J. Bus. Manag. Rev., vol. 6, no. 11, pp. 40–47, 2017, doi: 10.12816/0040336.

[29] R. P. Bostrom and J. S. Heinen, "MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes," MIS Q., vol. 1, no. 3, pp. 17–32, 1977.

[30] C. N. Tarimo, J. K. Bakari, L. Yngström, and S. Kowalski, "A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards a Culture of ICT Security-The Case of Tanzania.," Inf. Syst. Secur. Assoc., no. January, pp. 1–12, 2006.

[31] M. Malatji, "Socio-technical systems cybersecurity framework," Inf. Comput. Secur., vol. 27, no. 2, pp. 233–272, 2019, doi: 10.1108/ICS-03-2018-0031.

[32] F. Draganidis and G. Mentzas, "Competency based management: A review of systems and approaches," Inf. Manag. Comput. Secur., vol. 14, no. 1, pp. 51–64, 2006, doi: 10.1108/09685220610648373.

[33] S.-C. Wong, "Competency Definitions, Development and Assessment: A Brief Review," Int. J. Acad. Res. Progress. Educ. Dev., vol. 9, no. 3, 2020, doi: 10.6007/ijarped/v9-i3/8223.

[34] H. Z. Zeydan, A. Selamat, M. Salleh, and F. Computing, "Study on Protection Against Password Phishing," vol. 32, no. 5, pp. 797–801, 2014, doi: 10.5829/idosi.wasj.2014.32.05.14536.

[35] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," Cryptography, vol. 2, no. 1, pp. 1–31, 2018, doi: 10.3390/cryptography2010001.

[36] M. Yıldırım and I. Mackie, "Encouraging users to improve password security and memorability," Int. J. Inf. Secur., vol. 18, no. 6, pp. 741–759, 2019, doi: 10.1007/s10207-019-00429-y.

[37] H. Orman, "Twelve random characters," IEEE Internet Comput., vol. 17, no. 5, pp. 91–94, 2013.

[38] M. Templ and M. Sariyar, "A systematic overview on methods to protect sensitive data provided for various analyses," Int. J. Inf. Secur., vol. 21, no. 6, pp. 1233–1246, 2022, doi: 10.1007/s10207-022-00607-5.

[39] C. Nobles, "Botching Human Factors in Cybersecurity in Business Organizations," HOLISTICA – J. Bus. Public Adm., vol. 9, no. 3, pp. 71–88, 2018, doi: 10.2478/hjbpa-2018-0024.

[40] F. Carroll, J. A. Adejobi, and R. Montasari, "How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society," SN Comput. Sci., vol. 3, no. 2, pp. 1–10, 2022, doi: 10.1007/s42979-022-01069-1.