5th World Conference on
Teaching and Education

WORLDCTE
World Conference on
TEACHING & EDUCATION

08-10 December 2022 Berlin, Germany

A Model for the Protection of Cybersecurity Threats in Organizations

[*]Olusegun Ademolu Ajigini[1],

[1]*The Independent Institute of Education, South Africa*

Abstract

There is growing focus on the importance of cybersecurity protecting against threats in organizations due to the exponential growth of the Internet in our society due to the tremendous growth of cyber-attacks in organizations. Cyber threats encompass any socially detrimental activity, and include online crimes and terrorism.

In this paper, a model for the protection against cybersecurity threats in organizations was developed. Four factors namely technological, organizational, human and environmental factors were found to have positive influence on cybersecurity threat mitigation in organizations. All the variables in this study were found to be reliable since their Cronbach alpha ranged from 0.778 to 0.832. The sample size was 300 respondents. A random sampling design was used to carry out the research. The statistical tool used was SPSS v25.

The average variance extracted (AVE) were all above 0.5. Also, the composite reliability of the constructs was all over 0.7. Consequently, convergent validity of the constructs was satisfied. Correlation coefficient between two determinants was less than 1. Additionally, the correlation coefficient of the two determinants was less than the individual Cronbach Alpha value (σ) and also the correlation coefficient of the two determinants was less than the average variance (AVE). Consequently, the discriminant validity was said to be satisfied for all the determinants. All the four hypotheses were supported since their *P*-values were less than 0.000 (P-value<0.000).

The study provided the basis for security professionals, security managers and academics to enhance the protection against cybersecurity threats in their organizations. This might ensure the protection of their organizational valuable assets and sensitive information from cyber-attacks.

.

Keywords: Cybersecurity, cyber-attacks, human factor, organizational factor, technological factor, environmental factor.

1. Introduction

Businesses count on data for their survival in the competitive market but data is always in danger of theft or loss (Taherdost, 2022). Thus, companies need to develop models to implement cybersecurity. According to Alawida et al. (2022), there were 1001 data breaches in the United States. In addition, in the year 2020 with the COVID-19 pandemic, the number of breaches increased to 1872 when compared to 1108 in 2019. Thus, COVID-19 resulted in an increased number cyber-attacks.

In recent years, the research community has focused more studies on cybersecurity since it provides the protection of information systems such as software, hardware, data and related infrastructure (Srinivas et al., 2019). Moreover, because of the exponential growth of the Internet; our society, critical infrastructure and the economy are now largely dependent on computer networks and information technology solutions (Jang-Jaccard & Nepal, 2014). This has led to a tremendous growth of cyberattacks in organizations.

Cyber threats encompass any socially detrimental activity and includes online crimes and terrorism (Nam, 2019). Also, the increase in the usage of Internet of Things (IoT) has brought a large scale of distributed denial-of-service (DDoS) attacks and ransomware threats such as cryptolocker (Liao et al., 2016), cryptowall (Cabaj & Mazurcyk, 2016) and wannacry (Mohurle & Patil, 2017). Thus, a new tidal wave of research has been created towards investigating cybersecurity and data privacy (Habibzadeh *et. al.*, 2019).

Cyber attacks affect nations and organizations as well as individuals (Hiller & Russell, 2013). These attacks occur in a networked environment and cause great damage to people, property and systems in far-away places from which the attack originated. The attacks are also influenced by new inventions and technologies thus adding further risks. Growing threats have been encountered in emerging technologies such as cloud computing, social media, critical infrastructure and smartphone technology (Jang-Jaccard & Nepal, 2014). The threats affecting organizations include: rivals stealing company secrets and intellectual property, hackers and criminals stealing credit card data, transferring funds illegally and selling trade secrets (Hiller & Russell, 2013). Additionally, Ghelani (2022) also pointed out that there is vulnerability of corporate information and technology services as well as sensitive data leakage in email and internet access. Consequently, there is a need for organizations to develop security strategy by developing a framework to address these security risks.

Many companies are moving towards the Industry 4.0 paradigm (also referred to as Industrial Internet of Things or Industrial Internet) by making their factories and plants connected to the Internet in order to enhance their productivity (Lezzi et al., 2018). Thus, this makes cybersecurity issues to be one of the most relevant business challenges to be encountered. Berkman *et. al.* (2018) state that cyberattacks and security breaches have side

effects since such attacks not only impinge on the affected organizations but also their rivals/peers (Hinz *et. al.*, 2015; Martin *et. al.*, 2017; Kashmiri *et. al.*, 2017).

Cybersecurity awareness is important in organizations since they are subjected to increasing number of cyberattacks (PwC, 2016; Deloitte, 2017). The attention of US government both at the state and federal levels has been drawn upon due to the increase in cyberattacks on organizations (Berkman *et. al.*, 2018). Due to these issues, organizations are implementing ways to contend with growing cybersecurity threats. Furthermore, organizations have provided initiatives such as hiring directors with IT backgrounds, hiring Chief Information Security Officers, purchasing insurance, obtaining new IT systems with enhanced IT security, constituting IT committees of the Board and developing cybersecurity awareness (Berkman *et. al.*, 2018).

Cybersecurity and cyber threats protection are continual issues that needs persistent attention from the public and private sectors (Hiller & Russell, 2013). Cyber-attacks flourish because they are cheaper, convenient and less risky than physical attacks since it only requires a computer and an Internet connection (Jang-Jaccard & Nepal, 2014). Cyber-attacks are not restrained by distance and geography thus increasing the number and the sophistication of cyberattacks worldwide.

The cyber-attacks have moved away from desktop to other platforms such as tablet PCs, mobile phones and Voiceover IP (VoIP) to avoid detection. There is a notable increase in mobile malware attacks due to the increase in the population of mobile users throughout the World (Jang-Jaccard & Nepal, 2014). There is increase in scams using social engineering and popular social networking sites such as Facebook, Twitter, etc., have been used to deliver and spread malware. Cybercriminals use social engineering to penetrate systems illegally by deceiving people to release their confidential information e.g. passwords or private information (Butler, 2019). A good example is the use of phishing. An alarming number of cyberattacks start with a phishing email (Ashrm, 2018). Also, inside knowledge and personnel have been used to carry out cyberattacks customized to a specific system (Jang-Jaccard & Nepal, 2014). The knowledge of the factors that can determine the protection against cybersecurity threats in organizations can then reduce the threats stemming from cybersecurity risks and regulatory pressures, thus increasing organizational value. In this paper, I empirically developed a model for the protection against cybersecurity threats in organizations. In this paper, a model for the protection against cybersecurity threats in organizations and improvement of their governance is proposed. The paper is structured as follows: Section 1 is the introduction, section 1.1 is about cybersecurity definition, section 1.2 is about protection against cybersecurity threats in organizations. Section 2 is the methodology used, and section 3 focuses on results and discussion. Section 4 is the conclusion.

1.1 What is Cybersecurity?

Table 1 shows the definitions of cybersecurity by various authors.

Table 1. Definitions of Cybersecurity by various Authors

Authors	Definitions of Cybersecurity
Caramancion, K. M., Li, Y., Dubois, E. Jung, E. S. (2022)	"Cybersecurity relates to the protection and defense of personal information, computer systems, and critical infrastructure"
Yusif, S. and Hafeez-Baig, A. (2021)	"Cybersecurity is a growing problem associated with everything an individual or an organization does that is facilitated by Internet. It is high risk problem and must be treated as such, given the highly unpredictability nature of when, how, where and by whom threats may arise from."
O'Connell, M.E. (2012)	"Cybersecurity refers to technologies and techniques that protect programs, networks, computers and data from being damaged, attacked or accessed by unauthorized people"
NIST (2013)	"The ability to protect or defend the use of cyberspace from cyberattacks"
Srinivas *et. al.* (2019)	"Cybersecurity refers to the protection of Internet-connected systems, such as hardware, software as well as data (information) from cyberattacks (adversaries)"
Coventry and Branley (2018)	"Cybersecurity is concerned with safe-guarding computer networks and the information they contain from penetration and accidental or malicious disruption"
Goodman and Lin (2007)	"Cybersecurity concerns with the understanding of surrounding issues of diverse cyberattacks and devising defense strategies (i.e. countermeasures) that preserve confidentiality, integrity and availability of any digital and information technologies"
E.V.A.F.N.a. ENISA (2017)	"All activities necessary to protect cyberspace, its users and impacted persons from cyber threats"
ISACA (2016)	"The protection of information assets by addressing threats to information processed, stored and transported by Internet-worked information systems"

CoNSS CNSS (2015)	"Prevention of damage to, protection of, and restoration of computers electronic systems, electronic communication services, wire communication and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality and nonrepudiation"
Lezzi *et. al.* (2018)	"Cybersecurity aims at protecting the cyberspace (which includes both information and infrastructures) from any cyber threat, or cyberattack"

Figure 1 illustrates the cybersecurity definition.

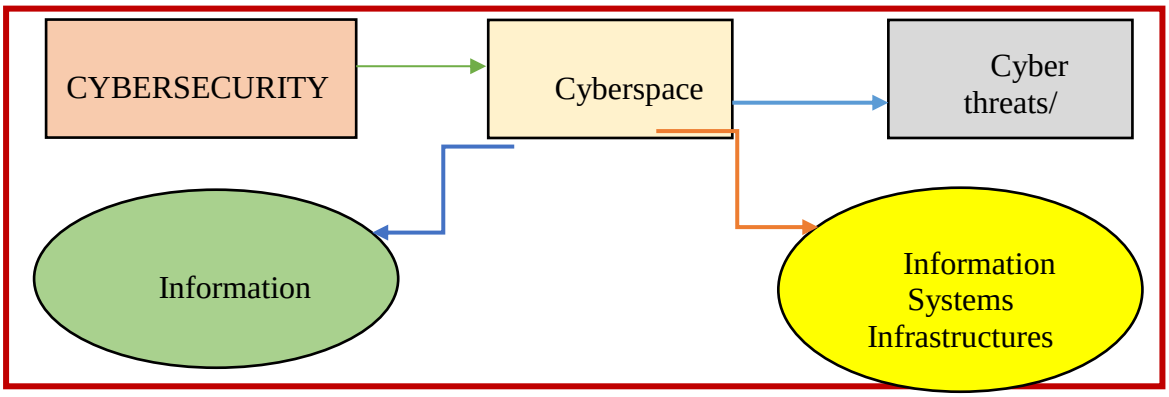

Figure 1. Cybersecurity Definition (Source: Lezzi et al., 2018)

Figure 1 illustrates how cybersecurity aims at protecting cyberspace (which includes both information and infrastructures) from any cyber threat, or cyberattack. This notion of cybersecurity definition was conceptualized by Lezzi *et. al.* (2018).

Cybersecurity is defined as the protection of cyberspace which includes the protection of information and information systems infrastructures and its users from any cyberattacks to ensure its availability, integrity, authentication, confidentiality and nonrepudiation.

1.2 Protection of Cybersecurity Threats in Organizations

Cybercrime and cybersecurity tools and techniques grow concurrently since technology has become pervasive in our daily lives (Choo *et. al.*, 2018). Thus, there is a need to develop innovative managerial, technological and strategic solutions to protect against cybersecurity threats in organizations. The scale of cyber threats to both private and public organizations includes sophisticated malicious software, disruptive activities by online hackers and nationalist criminals and even electronic cyber espionage activities and organized crime (Nam, 2019).

1.2.1 Common Cyberattacks

The cyber risks affecting organizations include: threats, vulnerabilities, the cyber security environment and the company-specific mitigation (Hill & Russell, 2013). Examples of cyberattacks affecting organizations are: Denial-of-Service (DoS) attacks, Trojan horses, worms, viruses, phishing, control system attacks and illegal access (e.g. stealing intellectual property or confidential information) (Srinivas *et. al.*, 2019). Cyberattacks can be initiated by an attacker and they include: phishing, virus, Trojan horse, worm, ransomware, spyware, unauthorized access and control system attacks (Srinivas *et. al.*, 2019). According to Lee (2021), cybersecurity is regarded as a critical component in companies because attacks cause damage such as compliance breaches, reputational harm, penalties, privacy breaches and disruption of operations.

Malware is regarded as the primary choice of weapon to carry out cyberattacks (Jang-Jaccard & Nepal, 2014). Malware are attacks stuffed on a system to compromise the system without the knowledge of the legitimate user. Examples of malware are spyware, Trojan horses, viruses, worms and bot executables. The increase and complexity of fast-growing number of malware has been a major concern on the Internet. The perimeter defense strategy has been used to protect systems against malware by using firewall and anti-virus software installed within intrusion prevention/detection systems. The perimeter systems have been supported by using access control mechanisms in order to give more defined access to certain internal resources (Jang-Jaccard & Nepal, 2014). However, this combination is no longer effective and adequate to protect against malware attacks due to the improvement in malware complexity. Digital forensics can also be used to identify malware presence in systems so as to determine what has occurred or will occur (Choo et al., 2018).

A virus is a contagious program that appends itself to some other programs and replicates itself when the software is executed. A phishing attack is the acquisition of sensitive information such as user banking login details, credit card details, etc. The unsuspecting user will enter private information in the malicious website that contains malware. Then the malware will be used to steal the sensitive information (Jang-Jaccard & Nepal, 2014; Srinivas *et. al.*, 2019). A Trojan horse contains hidden code and implements harmful functions when executed and it is designed to steal the users sensitive information and to seize the systems resources by causing DoS attacks. A worm reproduces itself from one system to another and pursues infecting more systems by using the already infested systems as automated launching pads for attacks on other systems. Worms destroy data and files in the infected systems, and they consume bandwidth and overload web servers of the host networks (Srinivas *et. al.*, 2019). Ransomware is a malware causing legitimate users not to use their systems by performing some unauthorized functions such as locking the screen of the system or locking users files until or unless some specific amount of money (ransom) is paid. Examples of ransomware are crypto-ransomware and WannaCry. Spyware conceals track of sensitive

information from a system, and it monitors the Internet activities (e.g., webpages) that are accessed by a user and transmits the information to attackers (Srinivas *et. al.*, 2019).

1.2.2 Cybersecurity requirements

Cyber risk is increased by threats and vulnerabilities while it is decreased by company's mitigation actions and the cybersecurity environment. Vulnerabilities are caused by employee actions, weak infrastructures, and supply chain (Hill & Russell, 2013). Threats are the external risks caused by hackers and nation states. The vulnerabilities discovered by outsiders will increase threats. Company mitigation includes IT security policies and procedures, technical solutions, contracts with suppliers and service providers. The cybersecurity environment promotes or needs standards for best practice, bylaws, and cybersecurity regulations (Hill & Russell, 2013). The after-effects of a security breach have negative implications such as business intellectual property theft, customer privacy breaches, investors' lost profits, loss of industry competitiveness and loss of jobs in the organizations.

There is evidence of governance mechanism effectiveness as reported by some authors (Higgs *et. al.*, 2016; Steinbart *et. al.*, 2018; Berkman *et. al.*, 2018) that investigated corporate governance and cybersecurity. According to Higgs *et. al.* (2016), organizations that have a more established technology committee are less likely to be affected by security breaches. Moreover, organizations that have a Chief Information Officer in their top management team also perform better by having lesser security issues (Zafar *et. al.*, 2016).

The cybersecurity requirements in general networks are confidentiality (privacy), integrity, authentication, availability, authorization, physical theft of devices, non-repudiation and freshness (Srinivas *et. al.*, 2019). Confidentiality is used to prevent disclosing information to unauthorized users or systems. Integrity is used to protect against any modification or deletion when not authorized. Availability is used to ensure that only authorized users are responsible to deliver, store and process information when necessary (Jang-Jaccard & Nepal, 2014). Authentication is used to identify or verify an authorized user by using smart cards, passwords or biometrics (e.g., fingerprints or iris). Authorization is allowing a user to execute authorized (legal) functions based on the users defined role in the system (Srinivas *et. al.*, 2019). Non-repudiation is the assurance that a user in the system cannot deny the authenticity of his or her signature on a message originated from him or her. Freshness is ensuring that the information or data is recent, and no attacker can replay old messages in the future. This is achieved by using current system timestamps and random access nonce in the transmitted messages among the communication devices (Srinivas *et. al.*, 2019).

1.2.3 Cybersecurity countermeasures

The cybersecurity countermeasures and solutions used for mitigating various attacks are: firewalls, anti-virus software, intrusion detection and prevention systems, encryption, login credentials, awareness programs, operating system updates (Srinivas *et. al.*, 2019).

Cybersecurity presents many challenges to human performance both in the use of IT systems and in interfacing with computer security provisioning (Boyce *et. al*., 2011).

2. Materials and methods

2.1 The conceptual framework

Figure 2 shows the conceptual framework of the study. Four factors namely technological, organizational, human, and environmental may have positive influence on cybersecurity threats in organizations.

2.1.1 Technological factor

The technological factor is considered as a global issue that is affecting the whole world and it refers to the technology that provides protection to the cyber citizen (Muniandy & Muniandy, 2012). This is due to the fact that people are sharing technology, information and the security tools all over the world and there should be a homogeneous solution that addresses security using the technology factor. Technological threats are caused by both chemical and physical processes on information systems (Jouini *et. al.*, 2011). Technology threats can also be in the form of hardware or software or a combination of both (Muniandy & Muniandy, 2012). Technology threats include gaining entry into restricted areas by using physical means and also damage to hardware and software.

Security tools differ in terms of type, costs, effectiveness, number of attacks and complexity (Muniandy & Muniandy, 2012). Cybersecurity tools and activities include cryptography, firewalls, auditing, access control, intrusion detection and prevention systems, strong user authentication, content fillers, end-user and administrator training and insurance (Gallaher *et. al.*, 2008). The attackers and the security community use these technologies since they are freely available. Thus, attackers are able to use these technologies to detect system vulnerabilities before the security community can use them to protect their systems. Werlinger *et. al*. (2008) found the following technological factors in their study: complexity of systems, vulnerabilities in systems and applications, mobile and distributed access and lack of efficient security tools. Thus, technology factor is proposed as:

H_1: Technology factor positively influences the cybersecurity threat in organizations.

2.1.2 Organizational factor

The organizational factor is about the role of organizations in fighting cybercrimes and protecting cyberspace users (Muniandy & Muniandy, 2012). Technological factors are regarded as not the only key to the effectiveness of information security controls; however, the impact of human and organizational factors need to be understood (Botta et al., 2007; Beznosov & Beznosava, 2007).

A model that relates organizational factors such as organizational size, top management support and type of industry with the effectiveness of information security control has been proposed by Kankanhalli *et. al*. (2003). Knapp *et. al.* (2006) conducted a survey of security professionals about the importance of top management support in enforcing IS security within organizations and they found out that it is crucial for top management to implement security controls within organizations.

According to ENISA (2017), organizational factors impacting cybersecurity include organizational culture, the organization-wide cybersecurity strategy, the role of top management and adopted business and employment models. Werlinger *et. al.* (2008) also identified the following organizational factors in their study: risk estimation, open environments, lack of budget, security as a secondary priority, tight schedules, business relationships with other organizations, distribution of IT responsibilities, access control to sensitive data, size of organization and top management support. Thus, organizational factor is proposed as:

H_2: Organizational factor positively influences the cybersecurity threat in organizations.

2.1.3 Human factor

An organization should reflect on the human touch into the IT systems by ensuring that the human point is addressed effectively in any cybersecurity protection plan (Muniandy & Muniandy, 2012). The people or the end users are regarded as the weakest link in IT security chain (Boyce *et. al.*, 2011; Muniandy & Muniandy, 2012). User ignorance is one of the causes of technology failure in most cases (Muniandy & Muniandy, 2012). Human performance research in relation to cybersecurity commences with knowing the tasks that are necessary according to user roles, responsibilities, and requirements by assisting in the assessment of user behavior, performance, and proficiency (Boyce *et. al.*, 2011). The primary actors are computer users, cybersecurity professionals, administrators/supervisors in various roles. Human-made actions are recognized by user objectives during its usage, and it involves malicious and non-malicious threats (Jouini et al., 2014). These threats are classified according to the attacker's intent and can be accidental or intentional threats.

The users' role in the creation and overcoming of vulnerabilities needs to be identified for specific systems and it should be based on the systems' task performance requirements (Boyce *et. al.*, 2011). These include time to complete, the availability of state-of-the-art technology, required information, user knowledge, required accuracy and reliability levels, any human involvement mandated by policy or regulations, user knowledge and skills, and decision requirements.

Users lack the discipline to implement the best practices that they learnt when using information systems (Howard & Prince, 2011). Therefore, users should be educated on the dangers of using the Internet so that they can be more cautious when using the Internet to

perform their tasks (Muniandy & Muniandy, 2012). Social engineering attacks are the exploitation of people by using manipulative methods. Another type of attack involving human interaction is social networking and more attacks are now coming from them (Ciampa, 2010). Password setting is another security attack from human interaction with IT systems. Human factors result from the study of human interaction with information systems, networks as well as practices in an information security environment (Nobles, 2018).

According to Soltanmohammadi *et. al*. (2013), human-enabled errors account for more than 80% of all cyberattacks, data breaches, and ransomware attacks. Security of IT systems fails due to the users' refusal to understand and implement the best practices when surfing the Internet. Consequently, many security problems can be resolved if users understand the security problems and take the necessary protective actions in the cyber space (Muniandy & Muniandy, 2012). Thus, human factor is proposed as:

H_3: Human factor positively influences on the cybersecurity threat in organizations.

2.1.4 Environmental factor

Environmental threats are natural threats that are introduced without malicious intent and committed mistakes are due to unintended actions (Jouini *et. al.*, 2014). They are caused by non-human agents, and they result from natural disasters such as earthquakes, fire, flood, lightning, water, wind, and tidal waves (e.g., tsunami). They also include wars and terrorist attacks (Jouini *et. al.*, 2014).

Thus, environmental factor is proposed as:

H_4: Environmental factor positively influences on the cybersecurity threat in organizations.

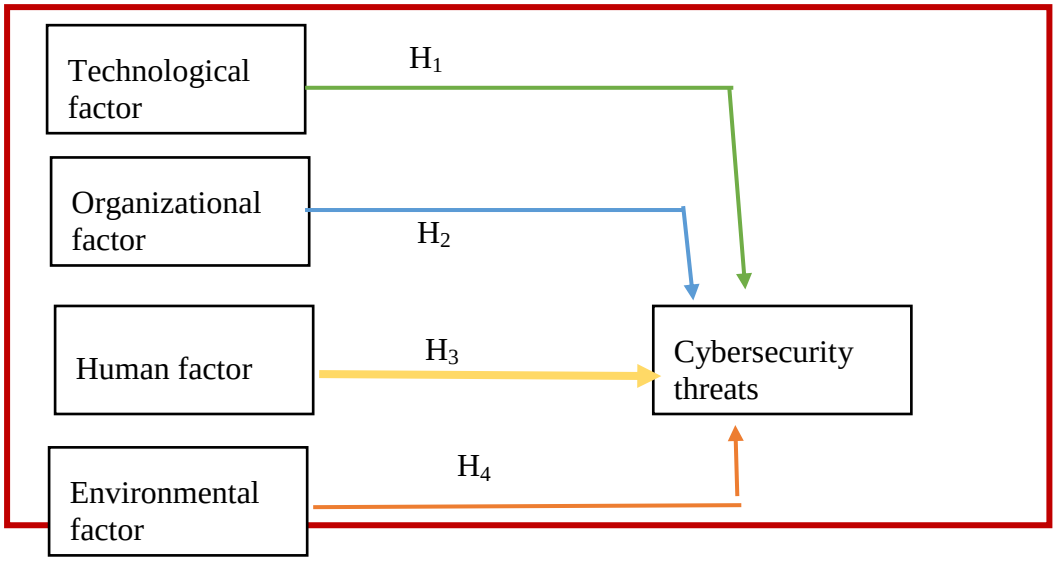

Figure 2. The Conceptual Frame

3. Results and Discussion

3.1 Respondents Demographics

The sample size was 300 respondents, and the random sampling technique was used to carry out the research. The statistical tool used was SPSS v.25. A quantitative study design was used to carry out the research. Table 2 illustrates the survey respondents' descriptive statistics.

Table 2. Descriptive Statistics – Survey Respondents

Type of Organization		
Private	162	54.0%
Public	136	45.3%
Respondent Levels		
Executive Management	22	7.3%
Senior Management	40	13.3%
Middle Management	78	26.0%
IT Specialist	126	42.0%
Developer	34	11.3%
Sex		
Male	128	42.7%
Female	172	57.3%
Race		
Black	128	42.7%
Asian	172	57.3%
Age		
< 25 years	122	40.7%
26 – 35 years	130	43.3%
36 – 45 years	28	9.3%

46 – 55 years	20	6.7%
Employment Basis		
Permanent	32	10.7%
Temporary	146	48.7%
Fixed Term/Contract	102	34%
Other	18	6%
Cybersecurity Knowledge		
Yes	300	100%
No	0	0%
Number of Years in Organization		
2 years or less	146	48.7%
3 – 5 years	28	9.3%
6 – 10 years	104	34.7%
Over 10 years	22	7.3%

From the demographics of the results, more respondents from the private organizations (54%) than public organizations (46%) participated in the study. Most of the respondents were IT specialists (42%) followed by middle managers (26%). More females (57.3%) participated in the study than males (42.7%). Moreover, participants were relatively young with age less than or equal to 35 years (84%) and they were mostly IT specialists. All the respondents who participated in the study had cybersecurity knowledge.

3.2 Data Analysis

A quantitative study design was used, and the data analysis was performed by using the SPSS software. The analysis involved descriptive and inferential statistics by using the SPSS v. 25.

3.2.1 Validity and Reliability Analysis

The consistency of results is assessed by the internal consistency across the factors within a test and the Cronbach alpha is the mostly used internal consistency measure (Taan & Hajjar, 2018). Validity is the most important measure for assessing test quality and it is the amount of which an idea, deduction, or measurement is well-derived and connects precisely to the real world (Brains & Manheim, 2011).

The internal reliability of the scales was investigated, and the validity of the various sub-scales was further explored by examining correlations between the items (Nielsen *et. al.*, 2017).

3.2.2 Reliability Analysis of the Constructs

Cronbach's alpha (Cronbach, 1951) is used to demonstrate that tests and scales that have been constructed or adopted for research projects are fit for the purpose (Taber, 2017). Cronbach's alpha is denoted by (α) and it is also used as an indicator for instrument quality.

Table 3. Data Reliability

Variable	Cronbach Alpha Value (σ)
Technological factor (B)	0.827
Organizational factor (C)	0.804
Human factor (D)	0.800
Environment factor (E)	0.778
Cybersecurity threats (F)	0.827

The Cronbach's alpha for the variables: technological factor, organizational factor, human factor, environmental factor, and cybersecurity threats are 0.827, 0.804, 0.800, 0.778 and 0.827 respectively. The result of the reliability test indicates the range of Cronbach alpha to be between 0.778 to 0.832. Robinson *et. al.* (1991) recommended that the minimum acceptable value for Cronbach alpha is 0.60, hence, the Cronbach alpha of the variables in this study are reliable.

3.2.4 Composite Reliability and Convergent Validity Analysis

Gefen *et. al.* (2000) proposed goodness-of-fit indicators that include assessed standards which are: (a) The composite reliability (CR) of determinants being greater than 0.7; (b) The factor loadings of the variables respective fields are significant; (c) Average variance extracted (AVE) is higher than 0.5. Additionally, Fornell and Larker (1981) state that if AVE is less than 0.5 but composite reliability (CR) is higher than 0.6, then convergent validity of the constructs is satisfied and still adequate.

Table 3.3 illustrates the loading factors (LF), the average variance extracted (AVE), the composite reliability (CR) and the maximum shared variance (MSV). The maximum shared variance (MSV) is the square of the highest correlation coefficient. From this table, the factor loadings of the variables respective fields are significant. The average variance extracted (AVE) are all above 0.5. Also, the composite reliability of the constructs is all over 0.7. Consequently, convergent validity of the constructs is satisfied.

Moreover, the value of each MSV should be less than its corresponding value of AVE and from Table 4, the value of each MSV is less than its corresponding value of AVE. Therefore, this confirms that the items are reliable, and the constructs have convergent validity.

Table 4. Estimation of LF, AE, CR and MSV

Constructs / Items	LF	AVE	CR	MSV
Technological Factor (B)		**0.599**	**0.856**	**0.212**
B1	0.796			
B2	0.799			
B3	0.786			
B4	0.711			
Organizational Factor (C)		**0.584**	**0.848**	**0.243**
C1	0.704			
C2	0.843			
C3	0.770			
C4	0.733			
Human Factor (D)		**0.776**	**0.933**	**0.163**
D1	0.889			
D2	0.878			
D3	0.849			
D4	0.907			
Environmental Factor (E)		**0.655**	**0.883**	**0.216**
E1	0.721			
E2	0.844			
E3	0.795			
E4	0.869			
Cybersecurity Threats (F)		**0.532**	**0.813**	**0.243**
F1	0.817			
F2	0.807			
F3	0.450			
F4	0.778			

3.2.5 Multicollinearity and Discriminant Validity Test

The two important conditions that must be satisfied for discriminant validity to be satisfied are (Gaski & Nevin, 1985): (a) Correlation coefficient between two determinants is less than 1; (b) The correlation coefficient of the two determinants is less than the individual Cronbach Alpha value (σ). Moreover, Fornell and Larker (1981) add another criterion that should be satisfied for discriminant validity: (c) The correlation coefficient of the two determinants is less than the average variance (AVE). The average variance (AV) is the square root of the average variance extracted (AVE).

Table 5 illustrates the estimation of average variance (AV), Cronbach Alpha value (σ) and the variance inflation factor (VIF).

Table 5. Estimation of AV, Cronbach's Alpha, and VIF

(Discriminant Validity Test)

	TransB	TransC	TransD	TransE	AV	σ	VIF
TransB	**0.138**				0.774	0.827	1.196
TransC	0.253	**0.245**			0.764	0.804	1.119
TransD	0.233	0.198	**0.199**		0.881	0.800	1.131
TransE	0.460	0.493	0.404	**0.465**	0.729	0.778	1.177

From the Table 5, (a) Correlation coefficient between two determinants is less than 1; (b) The correlation coefficient of the two determinants is less than the individual Cronbach Alpha value (α); (c) The correlation coefficient of the two determinants is less than the average variance (AVE). Consequently, the discriminant validity is said to be satisfied for all the determinants.

Multicollinearity defects result when the inner meanings of the variables become close to each other. Because of this, the estimation of the variance inflation factor (VIF) must be carried out. According to Ringle *et. al.* (2015), the maximum acceptable value of VIF is 5, although Hair *et. al.* (1995) put the maximum acceptable value of VIF at 10. The values of VIF for all variables lie between 1.119 to 1.196, thus confirming that the data is free from multicollinearity defect.

3.2.6 Inference Statistics – Regression Analysis of the Variables

Table 6 illustrates the summary of the regression model.

Table 6 Summary of the Regression Model

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.783a	,613	,602	,316	,613	57,377	4	145	,000

a. Predictors: (Constant), Environmental factor, Human factor, Organizational factor, Technological factor

The R square value of the regression model in this study is 0.613. The adjusted R square value is 0.602, which implies that the following variables: technological factor, organizational factor, human factor, and environmental factor collectively predict 60.2% for the cybersecurity threats.

The P-value (or the calculated probability) is the probability of the event occurring by chance if the null hypothesis is true (Anaesth, 2016). The P-value is a numerical value between 0 and 1 and is interpreted by researchers in deciding whether to reject or accept the null hypothesis. The P-value is an approach to summarize the incompatibility between a particular set of data and a proposed model for the data (Wasserstein& Lazar, 2016).

In the regression table (Table 3), the P-values of all the variables are as follows: technological factor is 0.000, organizational factor is 0.000, human factor is 0.000 and environmental factor is 0.000. These results indicate that out of the four variables, all of the factors meaningfully contribute to the prediction of cybersecurity threats. All their P-values are 0.00 (i.e., p-values <0.001)- which is less than the maximum threshold of 0.05.

From the unstandardized coefficients of the variable effort expectancy, the beta value of organizational factor is 36.0% which is the variable with the highest contribution towards the prediction of cybersecurity threats. This is followed by technological factor with a beta value of 31.5%. The environmental factor contributes 28.5% towards the prediction of cybersecurity threats while the lowest contribution was from human factor with a beta value of 22.1%.

Table 7 Contribution of Individual Constructs (Regression Table)

Coefficients[a]						
Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	-,343	,329		-1,041	,300
	Technological factor	,251	,046	,315	5,464	,000
	Organizational factor	,358	,054	,360	6,585	,000
	Human factor	,206	,051	,221	4,013	,000
	Environmental factor	,289	,058	,285	5,008	,000
a. Dependent Variable: Cybersecurity threat						

3.2.7 Hypothesis Evaluation

Table 8 illustrates the hypothesis evaluation from the regression model.

Table 8. Hypothesis Evaluation

Hypothesis Codes	Hypothesis	P -Values	Is P < 0.05?	Decision on Hypothesis
H_1	Technology factor positively influences on the cybersecurity threats in organizations	0.000 (P-value<0.001)	Yes	Supported
H_2	Organizational factor positively influences on the cybersecurity threats in organizations	0.000 (P-value<0.001)	Yes	Supported
H_3	Human factor positively influences on the cybersecurity threats in organizations	0.000 (P-value<0.001)	Yes	Supported
H_4	Environmental factor positively influences on the cybersecurity threats in organizations	0.000 (P-value<0.001)	Yes	Supported

According to Anaesth (2016), if P value < 0.01, then the result is highly significant, and the null hypothesis should be rejected. If P value ≥ 0.01 but P value < 0.05, then the result is significant, and the null hypothesis should be rejected. If P value ≥ 0.05, then the result is not significant, and the null hypothesis should not be rejected. In Table 10 based on Anaesth (2016) interpretation of the P value, all the four hypotheses H1, H2, H3 and H4 are supported.

3.2.8 The Resulting Model

The resulting model is shown in figure 3 and it is based on the four hypotheses.

H_1: Technology factor positively influences on the cybersecurity threats in organizations.

The first hypothesis (H_1) of the study predicted a positive relationship between the technological factor and cybersecurity threats. It is significant with a P-value of 0.000 which is below the threshold of 0.05 and is therefore supported. However, the result of the Pearson correlation relationship between cybersecurity threats and technological factor is 0.549 which is moderate according to Dancey and Reddy (2007). The technological factor is considered as a global issue that is affecting the whole world and it refers to the technology that provides protection to the cyber citizen (Muniandy & Muniandy, 2012).

H_2: Organizational factor positively influences on the cybersecurity threats in organizations.

The second hypothesis (H_2) of the study predicted a positive relationship between the organizational factor and cybersecurity threats. It is significant with a P-value of 0.000 which is below the threshold of 0.05 and is therefore supported. However, the result of the Pearson correlation relationship between cybersecurity threats and technological factor is 0.540 which is moderate according to Dancey and Reddy (2007). According to ENISA (2017), organizational factors impacting cybersecurity include organizational culture, the organizational wider cybersecurity strategy, the role of top management, and adopted business and employment models.

H_3: Human factor positively influences on the cybersecurity threats in organizations.

The third hypothesis (H_3) of the study predicted a positive relationship between the human factor and cybersecurity threats. It is significant with a P-value of 0.000 which is below the threshold of 0.05 and is therefore supported. However, the result of the Pearson correlation relationship between cybersecurity threats and technological factor is 0.435 which is moderate according to Dancey and Reddy (2007). This is in consistent with the assertions from Sedgwick (2019) and Herath and Rao (2009) that organizations must also look at the essence of humans not just investing in technological controls and solutions during cybersecurity protection in organizations. Employees should be trained on cybersecurity protection and awareness and employees should be encouraged to report incidents through a reward program (Sedgwick, 2019).

H_4: Environmental factor positively influences on the cybersecurity threats in organizations.

The fourth hypothesis (H_4) of the study predicted a positive relationship between the environmental factor and cybersecurity threats. It is significant with a P-value of 0.000 which is below the threshold of 0.05 and is therefore supported. However, the result of the Pearson

correlation relationship between cybersecurity threats and technological factor is 0.523 which is moderate according to Dancey and Reddy (2007). Environmental threats are natural threats that are introduced without malicious intent and committed mistakes are due to unintended actions (Jouini *et. al.*, 2014).

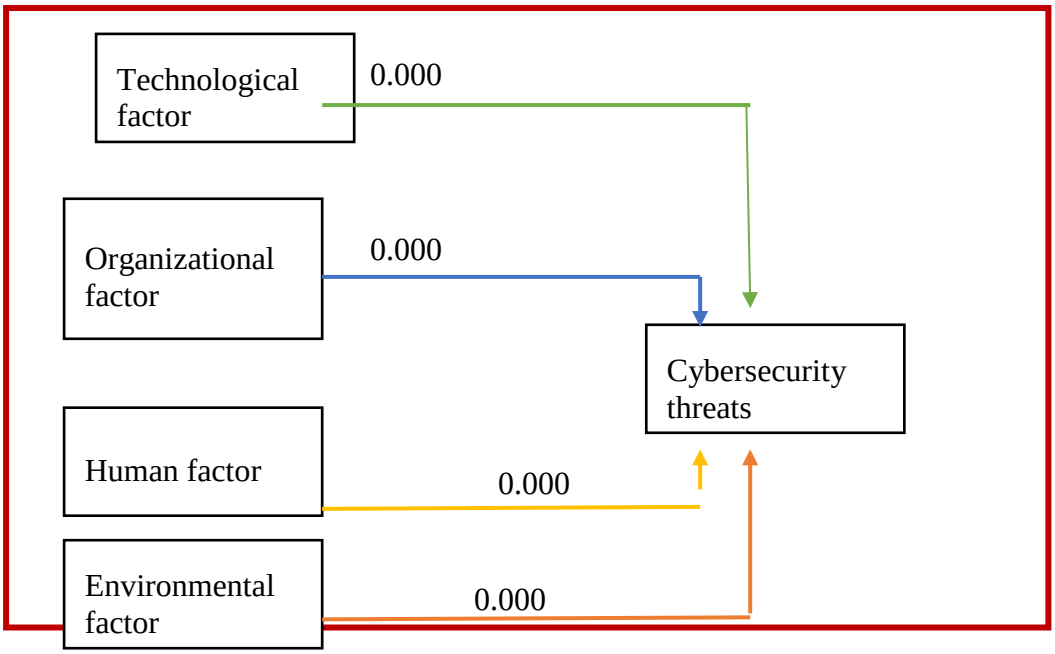

Figure 3. The Model for the Protection against Cybersecurity Threats in Organizations

4. Conclusion

Cyber-attack is a way of exploiting computer systems and networks, and is carried out by using malicious codes to alter algorithms, data or logic. Consequently, it is critical to secure information systems (Jaganathan *et. al*., 2015).

This study investigated the protection against cybersecurity threats in organizations and a model for the protection against cybersecurity threats in organizations was developed. The results showed that all the four constructs namely technological factor, organizational factor, human factor, and environmental factor positively influence cybersecurity threats in organizations.

The technological factor is considered as a global issue that is affecting the whole world and it refers to the technology that provides protection to the cyber citizen (Muniandy & Muniandy, 2012). This is due to the fact that people are sharing the technology, information and the security tools all over the world and there should be a homogeneous solution that addresses security using the technology factor.

The organizational factor is about the role of organizations in fighting cybercrimes and protecting cyber space users (Muniandy & Muniandy, 2012). Technological factors are regarded as one of the keys to the effectiveness of information security controls; however, the impact of human and organizational factors need to be understood as well (Botta *et. al.*, 2007; Beznosov & Beznosava, 2007).

Human factors result from the study of human interaction with information systems, networks as well as practices in an information security environment (Nobles, 2018). An organization should reflect on the human touch into the IT systems by ensuring that the human point is addressed effectively in any cybersecurity protection plan (Muniandy & Muniandy, 2012). The people or the end-users are regarded as the weakest link in IT security chain (Boyce *et. al*., 2011; Muniandy & Muniandy, 2012).

Environmental threats are natural threats that are introduced without malicious intent and committed mistakes and are due to unintended actions (Jouini *et. al.*, 2014). They are caused by non-human agents, and they result from natural disasters such as earthquakes, fire, flood, lightening, water, wind, and tidal waves (e.g. tsunami). They also include wars and terrorist attacks (Jouini *et. al.*, 2014). This research is beneficial to managers of IT security, employees working on IT security and the academia.

References

Akoglu, H. (2018). User's guide to correlation coefficients. Turkish Journal of Emergency Medicine, 91-93.

Alawida, M., Omolara A. E., Abiodun, O. I. & Al-Rajab, M. (2022). *Journal of King Saud University – Computer and Information Services*, vol. 34, 8176 – 8206.

Ali, Z., & Bhaskar, S. B. (2016). Basic statistical tools in research & data analysis. *Indian Journal of Anaesthesia*, vol 60 No.9,pp. 662-669.Available: https://doi:10.4103/0019-5049.190623.

American Society of Healthcare Risk Management [ASHRM], (Producer), (2018) Cybersecurity: Protecting your organization from the dreaded breach [video webinar]. Available: http://learning.ashrm.org/.

Anaesth, I. J. (2016). Basic statistical tools in research and data analysis. Indian Journal of Anaesthesia, vol. 60 No. 9, pp. 662-669. Available: https://doi:10.4103/0019-5049.190623.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting & Public Policy*, vol. 37, pp. 508-526. Available: https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Beznosov, K., & Beznosova, O. (2007). On the imbalance of the security problem space and its expected consequences. *Information Management & Computer Security*, vol. 15, No 5, pp. 420-431.

Botta, D., Werlinger, R., Gagne, A., Beznosov, K., Iverson, L., Fels, S., & Fisher, B. (2007). Towards understanding IT security professionals and their tools. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, ACM, Pittsburgh, PA, pp. 100-111.

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011). Human performance in cybersecurity: A research agenda. *Proceedings of the Human Factors and Ergonomics Society*, 55th Annual Meeting, pp. 1115-1119.

Brains, W., & Manheim, R. (2011). *Empirical Political Analysis* 8th edition. Boston, MA: Longman, pp. 105.

Butler, S. M. (2019). Cybersecurity: Why should we be concerned*? Journal of Radiology Nursing*, vol. 38, pp, 13-14.

Cabaj, K., & Mazurczyk, W. (2016). Using software-defined networking for ransomware mitigation: The case of cryptowall. *IEEE Network*, vol 30, No. 6, pp. 14–20.Available: https://doi.org/10.1109/MNET.2016.1600110NM.

Caramancion, K. M., Li, Y., Dubois, E, & Jung, E. S. (2022). The missing case of disinformation from the cybersecurity risk continuum: A comparative assessment disinformation with other cyber threats. data, vol 7, pp. 49. Available: https://doi.org/10.3390/data7040049

Choo, K. R., Bishop, M., Glisson, W., & Nance, K. (2018). Internet- and cloud of-things cybersecurity research challenges and advances. *Computers & Security*, vol. 74, pp. 275-276. Available: http://dx.doi.org/10.1016/j.cose.2018.02.008

CoNSS CNSS (2015). *Committee on national security systems (CNSS) glossary*.

Coventry, L., & Branley, D. (2018). *Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas,* vol. 113, pp. 48-52. Available: https://doi.org/10.1016/j.maturitas.2018.04.008

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, vol. 16, No.3, pp. 297–334. Available: https://doi:10.1007/bf02310555.

Dancey, C. P., & Reidy, J. (2007). *Statistics without mathematics for psychology*. Pearson Education.

Deloitte (2017). *Cybersecurity reporting survey*. Available:

https://www.Deloitteacademy.Co.Uk/media/823595/deloitte-uk-governance-in-focus-cyber-risk- reporting.Pdf

European Union *Agency for Network and Information Security (ENISA), (2017).* Cyber security culture in organisations. Available: www. enisa.europa.eu.

E.V.A.F.N.a ENISA (2017). *Overview of cybersecurity and related terminology*.

Fisher, W.P. Jr. (2007). Rasch Measurement Transaction. Transaction of the Rasch Measurement, *SIG American Educational Research Association*,vol, 21, No. 1, pp.1095.

Fornell, C., Larcker, D.F. (1985). Evaluating structureal equation models with unobservable variables and measurement error. Journal of Marketing Research, Vol. 18, No 1, pp. 39-50. https://doi.org/10.2307/3151312.

Gallaher, M. P., Link, A. N., & Rowe, B. R. (2008). *Cyber Security. Cheltenham*: Edward Elgar Publishing Limited.

Gaski, J. F., & Nevin, J. R. (1985). The differential effects of exercised and unexercised power sources in a marketing channel. Journal of Marketing Research, pp. 130-142.

Gefen, D., Straub, D. W., Boudreau, M. C. (2000). Structural equation modelling and regression: Guidelines for research practice.

Ghelani, D. (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: *A Review. American Journal of Science, Engineering and Technology*. Vol. 3, No. 6, pp. 12-19

Goodman, S. E., & Lin, H. S. (2007). *Toward a safer and more secure cyberspace*. The Nat'l Academics Press.

Guetterman, T. C. (2019). Basics of statistics for primary care research, *Fam Med Community Health*, vol. 7, No 2, pp.1-13. Available: https://doi:10.1136/fmch-2018-000067.

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities & Society*, vol. 50, pp. 101660. Available: https://doi.org/10.1016/j.scs.2019.101660

Hain, C. A., & Francis, L. (2004). Development and validation of a co-worker relationship scale. *65th Annual Convention of the Canadian Psychological Association*, Newfoundland, Canada.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1995). *Multivariate data analysis*. 4th edition. New Jersey: Prentice Hall Inc.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, vol. 18, pp. 106-125.

Higgs, J.L., Pinsker, R.E., Smith, T.J., & Young, G.R. (2016). The relationship between board-level technology committees and reported security breaches. *J. Inform. Syst*., vol 30, No 3, pp. 79–98.

Hiller, J. S., & Russell, R.S. (2013). The challenge and imperative of private sector cybersecurity: An

international comparison. *Computer Law & Security Review*, vol. 29, pp. 236-245.

Avaiable: http://dx.doi.org/10.1016/j.clsr.2013.03.003

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Inform. Manage*., vcol. 52, No3, pp. 337–347.

Howard, D., & Prince, K. (2011). *Security 2020- Reduce Security Risks This Decade*. Indianapolis: Wiley Publishing, Inc.

ISACA (2016). *Cybersecurity fundamentals glossary*.

Jaganathan, V., Cherurveettil, P. & Sivashanmugam, P. M. (2015). Using a prediction model to manage cybersecurity threats. *The Scientific Journal*. pp 1-5. Available: http://dx.doi.org/10.1155/2015/7033713.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer & System Sciences, vol. 80,pp. 973-993. Available: http://dx.doi.org/10.1016/j.jcss.2014.02.005

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, vol. 32, pp. 489-496.

Kankanhalli, A., Teo, H. H., Tan, B.C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, pp. 23.

Kashmiri, S., Nicol, C.D., & Hsu, L. (2017). Birds of a feather: Intra-industry spillover of the target customer data breach and the shielding role of it, marketing, and CSR. *J. Acad. Market. Sci*., vol. 45.No2, pp. 208–228.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F.N. (2006). Information security: management's effect on culture and policy. *Information Management & Computer security*, vol. 14, No 1, pp. 24-36.

Kutner, M. H., Nachtsheim, C. J., Neter, J., & Li, W. (2005). *Inferences in regression and correlation analysis. In: Applied Linear Statistical Models* (International Edition), (5th ed.), Singapore: McGraw-Hill/Irvin, pp. 40-99.

Lee, I., (2021). Cybersecurity: Risk management framework and investment cost analysis, *Business Horizons*, Avaiable: https://doi.org/10.1016/j.bushor.2021.02.022.

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework, *Computers in Industry*, vol. 103, pp. 97-110. Available https://doi.org/10.1016/j.compind.2018.09.004

Liao, K., Zhao, Z., Doupe, A., & Ahn, G. J. (2016). Behind closed doors: Measurement and analysis of cryptolocker ransoms in bitcoin. 2016 *APWG symposium on electronic crime research (eCrime)*, pp. 1–13. Available: https://doi.org/10.1109/ECRIME.2016.7487938.

Manikandam, S. (2011). Measures of central tendency: Median and mode. Journal Pharmacol Pharmacolther, vol. 2, pp. 214-215.

Martin, K.D., Borah, A., & Palmatier, R.W. (2017). Data privacy: effects on customer and firm performance. *J. Market*., vol 81, No 1, pp.36–58.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack. *International Journal*, vol, 8, No. 5.

Muniandy, L., & Muniandy, B. (2012). State of cybersecurity and the factors governing its protection in Malaysia. *International Journal of Applied Science and Technology*, Vol 2, No 4, pp. 106-112.

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, vol. 58, pp. 101122. Available: https://doi.org/10.1016/j.techsoc.2019.03.005

Nielsen, K., Antino, M., Sanz-Vergel, A., & Rodrigueze-Munoz, A. (2017). Validating the job crafting questionnaire (JCRQ): A multi-method and multi-sample study: Journal of Work, Health & Organisations, Vol 31, No 1, pp. 82-99. https://doi.org/10.1080/02678373.2017.1293752

NikMuhammed, N. M., Jantan, M., & Md'Taib, F. (2010). Moderating effect of information processing capacity to investment decision making and environmental scanning. *Business Management Quarterly Review*, vol 1 pp., 9-22.

NIST (2013). *Glossary of key information security terms, NISTIR 7298r*, (2nd ed.), Richard Kissel, Gaithersburg

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *Holistica*, Vol. 9, No 3, pp. 71-88. Available: DOI:10.2478/hjbpa-2018-0024.

O'Connell, M. E. (2012). Cyber security without cyber war. *J. Confl. Secur. Law*, vol 17, pp. 187–209.

Pallant, J. (2010). *SPSS Survival Manual* (5th ed.). Backshire, England: McGraw Hill.

PwC (2016). *The global state of information security*. Available:

http://www.Pwc.Com/sg/en/publications/assets/pwc-global-state-of-informationsecurity-survey-2016.Pdf

Ringle, C. M., Wende, S., & Becker, J. M. (2015). SmartPLS3 bonningstedt: SmartPLS. Available: http://www.smartpls.com

Schober, P., Boer, C., & Schwarte, L. A. (2018). Correlation coefficients: Appropriate use and interpretation. *Journal of Anesthesia & Analgesia*, vol. 126, pp. 1763-1768.

Sedgwick, S. (2019). *The human factor of cybersecurity*, IDG Communications. ABN 14.001 592 650.

Soltanmohammadi, S., Asadi, S., & Ithnin, N. (2013). Main human factors affecting information system security. *Interdisciplinary Journal of Contemporary Research in Business*, vol 5, No7, pp. 329-354.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cybersecurity: Framework, standards and recommendations. *Future Generation Computer Systems*, vol. 92, pp. 178-188. https://doi.org/10.1016/j.future.2018.09.063

Steinbart, P.J., Raschke, R.L., Gal, G., & Dilla, W.N. (2018). *The influence of a good relationship between the internal audit and information security functions on information security outcomes*. Account., Org. Soc.

Taan, S., & Hajjar, E. L. (2018). Statistical analysis: Internal consistency reliability and construct validity. *International Journal of Quantitative and Qualitative Research Methods*, vol 6, No 9, pp. 27-38.

Taber, K. S. (2017). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Res Sci Educ*, vol. 48, pp. 1273-1296.

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronic*s, vol.11, pp. 181. https://doi.org/10.3390/electronics11142181

Wasserstein, R. L., & Lazar, N. A. (2016). The ASA's statement on P-values: Context, process and purpose. *The American Statistician*, vol 70, No 2, pp. 129-133. Available: http://dx.doi.org/10.1080/00031305.2016.1154108.

Werlinger, R., Hawkey, K., & Beznosov, K. (2008). An integrated view of human, organizational and technological challenges of IT security management. *Information*

Management & Computer Security, vol 17, No1 pp. 4-19. DOI 10.1108/09685220910944722.

Yusif, S. & Hafeez-Baig, A (2021): A conceptual model for cybersecurity governance, *Journal of Applied Security Research*, DOI:10.1080/19361610.2021.1918995

Zafar, H., Ko, M.S., & Osei-Bryson, K.M. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Inform.Syst. Front*., vol 1.No 6, pp. 1205–1215.