ISSN 2519-9781

A framework for Information Security Management Adoption in Higher Education Institutions in Somalia: Perspectives PMT and TOE

Dr. Abdulkadir Jeilani Mohamud

Lecturer, Faculty of Computer Science & IT, Mogadishu University

Email: eilani216@gmail.com

Abstract

This research paper examines the level of information security in higher education institutions in Somalia by identifying the factors influencing information security management. This research was applied by using protection motivation theory and technology organization environment framework, so the paper examines the interrelationship of perceived severity threat, perceived response efficacy, response cost, relative advantage, top management support and size of the organization and information security management. Using explanatory (causal) research design and cluster sampling technique, four – hundred forty-five questionnaires were disseminated to information security managers, ICT managers, IT expertise and IT lecturing at private and public universities in Mogadishu – Somalia; three hundred and eight two involved in the study. The data gathered was analyzed using structural equation model, the results propose that of perceived severity threat and size of the organization were significant to the information security management;

relative advantage, response cost, response efficacy, top management support were not significant to the information security. Suggestions for the results and research limitations identified.

Keywords: Information security management, Protection Motivation Theory, Technology Organization Environment, Higher Education Institutions,

1 Introduction

According to the widely use of technology, this brings individuals, organizations, and nations highly vulnerable to attack information systems, such as cybercrime, information theft, hacking, and others. It's important to ensure information security by expanding the information – communication infrastructure and establish a system to safeguard against information security threats. Information security starts with computer security or system privacy. The need for information security is the need to secure physical locations, hardware, and software from threats(Tietoturvallisuuden, 2010).

In addition, security refers to as the quality or state being secure to be free from threats, also the word security can describe the prevention against enemies from those who would do harm intentionally or accidentally. Reaching the suitable level of information security for an institution also requires having multiple various parts (multifaceted) system(Tietoturvallisuuden, 2010). Security can be classified as follows: physical security to prevent physical items, objects or areas from unauthorized access. Personnel security to protect the individual or group of individuals who are authorized to access the organization and its operations. Operation security to prevent the details of a particular operation or series of activities. Communication security to protect communication media, technology and content. Network security to protect networking components, connections and contents. Information

security to protect the confidentiality, integrity, and availability of information assets, whether the location to store, processing or transmission. It's achieved via the application of policy, education, training, awareness, and technology. There are four types of information security such as hacking, denial of service, malicious code and social engineering.

Information is the result of processing, manipulating and organizing data, which is simply a collection of facts. Regarding ISO/IEC 27001 defined Information as an 'asset', it is something that has value and should, therefore, be protected. Protecting information – related crimes or to minimize the damage such crimes can cause this is called information security. According to the Committee on National Security refers to information security as the protection of information and its critical elements, including the systems and hardware that use, store and transmit that information. Information security includes broad areas of information security management, computer, and data security and network security. The primary threats to information security are data interception, interruption, modification and fabrication and physical theft of equipment. To identify the three levels (low, moderate or high) depends upon the impact an organization or individuals to information security breach such as loss of confidentiality, integrity or availability.

In addition there are prior studies the investigated incremental adoption of information security in health-care organizations: implications for document management (Lorence & Churchill, 2005), understanding information security stress: focusing on the type of information security compliance activity (C. Lee, Lee, & Kim, 2016), introduction to information security broadcast encryption (Tietoturvallisuuden, 2010), information security evaluation: a holistic approach (Aghroum, 2017), persona – centred information security awareness (Ki-Aries & Faily, 2017),exploring the effects of information

security management awareness and perceived service quality (Kuo, 2018), the impact of information security threat awareness on privacy-protective behaviors (Mamonov & Benbunan-fich, 2018), the influence of good relationship between the internal audit and information security functions on information security outcomes (Steinbart, Raschke, Gal, & Dilla, 2018), understanding key skills for information security managers (Haqaf & Koyuncu, 2018). This research struggled to identify the research gap which is the degree of information security management in higher education institution in Somalia.

2 Theoretical Framework and Hypotheses

2.1 Protection Motivation Theory

PMT can be used to understand the protection themselves after receiving fear such as perceived threat severity, response efficacy, response cost (cost-effectiveness), relative advantage. PMT in the context of information security, if the institution is affected by a threat, all employees and students within the higher education institution are likely to feel some effects(Herath & Rao, 2009). PMT is used to persuade people to follow the communicator's recommendations and predict users' intention to protect themselves after receiving fear-arousing recommendations. Protection motivation theory describes any danger for which there is an active recommended response that can be accepted by the individual(Floyd, Prentice-Dunn, & Rogers, 2000).

2.1.1 Perceived Threat Severity

According to (Chen et al., 2015) the perceived severity attack is defined as to an individuals' understood the awareness of the potential and practical harm of the behavior to themselves or others. Other research proposes that perceived threat severity as the decisions of home wireless network users to implement security policy and mechanism(Crossler, 2010).

2.1.2 Response Efficacy

Response efficacy refers to a person's perception to take and recommended action step will actually protect the threat(Herath & Rao, 2009). The backing up data on personal computer system is another key prevention of data(Crossler, 2010). Response efficacy concerns perceptions that adopting a particular behavioral response will be effective in reducing the threat of information privacy(Teitel et al., 1991)

2.1.3 Response Cost

Response cost is the term used for removing reinforcement for undesirable or disruptive behavior.

2.1.4 Relative Advantage

According to (Rogers, 1995) describes the relative advantage as the degree to which an invention is perceived as being better than the idea it overtakes. Relative advantage refers the degree to which an innovation is seen as better than the idea, program or product it replaces(Kim & Ammeter, 2014).

2.2 Technology – Organization – Environment

TOE is used as the process by which a firm adopts and implements technological innovations influenced by the technological context, the organizational context and the environmental context(DePietro, Wiarda, & Fleischer, 1990). The technological context includes internal and external technologies that are related to the organization technologies may contain both types of equipment as well as processes(DePietro et al., 1990). Prior technological innovation researchers have identified different groups of variables that are possible determinants or organizational adoption of innovation particularly for information system (IS). They identified that these contexts have positive influences directly on the adoption of IS. In the organizational factors include top management support and size of the higher education institution.

2.2.1 Top Management Support

Top management support has been mentioned as a key predictor in the adoption and implementation of information security management. The senior technology officer is normally the chief information officer (CIO) also titles as vice president of information, VP of information technology and VP of systems may be used. The primary task or responsibility of CIO is advising the owner of the company or chief executive officer, president on the strategic planning that affects the management of information in the organization. The CIO work with subordinate managers to develop tactical and operational plans for the division and to enable planning and management of the systems that support the organization. The chief information security officer (CISO) may also be referred to as the manager for IT security, the security administrator subordinate to the chief information officer (CIO) has primary responsibility for evaluating, managing and implementation of information security(Tietoturvallisuuden, 2010). Top management support for information security and its significance as a primary organizational objective is likely to increase the insights of the internal audit and information security functions that they share a common goal, which, in turn, should improve relationships between these organizational units (Kane, 2010). The information security manager (ISM) is an administrative title or role related to information security and is unlike from the information security expert with regard to function. "The ISM is mainly responsible for: Ensuring that security processes, systems, policies, standards, and guidelines are established, communicated and improved across the entire organization to protect information assets; Making security-related decisions; Collaborating with internal and external stakeholders for all operations; and Supervising the security experts' teams"(Haqaf & Koyuncu, 2018).

2.2.2 Size of the Higher Education Institution

According to (The Complete University Guide, 2016) the type of the university we will look at the following various areas such as the age, size, and reputation amongst other things.

The from 2004 to 2012 most of the higher education sector are established around 34 universities(Studies, 2013). There are other universities that are established before that period such as Indian Ocean University (1993), Mogadishu University (1997), Hamar University (1999) and SIMAD University (1999).According the size of the university it's considered the number of students are in the university, over 50,000 students are currently enrolled at the higher education institution across Somalia country as the study drawn by Heritage (2013).

Based on the above discussion, the researcher proposes the following hypotheses:

H1. There is a negative relationship between severity attack and low Information security management in HEI.

H2. Response efficacy is positively and significantly related to need information security management in HEI

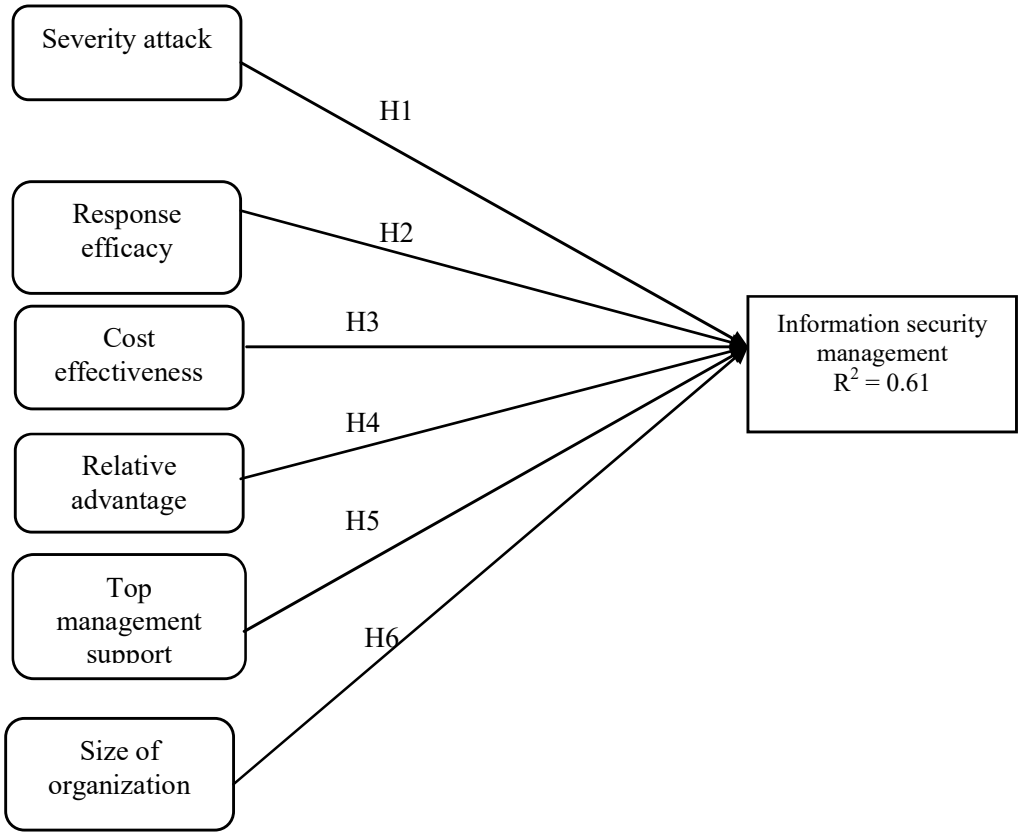
H3. Cost-effectiveness is positively and significantly related to the need information security management in HEI.

H4. Relative advantage is negatively and significantly related to the need for information security management in HEI.

H5. Top management support is negatively and significantly related to the need for information security management in HEI.

H6. There is a significant relationship between the Size of organization and the need information security management in HEI.

Fg1. The framework of the study



3 Research Method

3.1 Sample and Procedure

A large number of public or private universities in Somalia special Mogadishu city was used as the framework for the study. In this study, the population refers to the ICT managers, IT lecturers, IT expertise and knowledge were select for filling up the questionnaire. This study was adopted by the clustering technique in which a group refers by area of work, residence, organizational and other members with the same characteristics(Omair, 2014).

An online survey using *kobocollect* was used to collect the data in this study around 445. Before that data analysis, the data were screened and removed the outliers. Final 382 data were usable for the goal of this study.

3.2 Instrument

Using questionnaire is one of the simplest methods for data collection (Eccles et al., 2011), in this study a questionnaire was used and Likert five-point scale operated such as 1 represented strongly disagree and 5 represented strongly agree. The following factors were studied such as perceived severity threat, response efficacy, response cost, perceived of benefits, top management support, size of the higher education institution and information security management. Reliability and validity were employed in order to ensure the data.

4 Results and Discussions

4.1 Profile of Respondents

The below table1 indicates the respondents' profile. Male respondents made up 90.1% of the sample while few of females made up 9.9%. The majority of respondents hold master degrees (70.2%), 28.8% hold bachelor degree while 1.8% hold doctorate (Ph.D.) degree. The majority of respondents have experienced between 2 – 4 years (67.8%), 16.0% have experienced between 5 – 7 years, 13.9% have experienced less than 2 years, 2.1% between 8 – 9 years while 0.6% have experienced more than 10 years. More than half percentage (50.5%) were member of ICT department, 33.2% of respondents were member of faculty administration staff 10.2% were member of the institution administration final 6.0% of the respondent were IT lecturing staff. The majority of higher education institution indicated their students between 10001 – 3000 (45.5%), 41.1% in between 1 – 1000 students, 11.8% in between 4001 – 7000 while 0.3% above 10001.

Table1: Respondents' profile (n= 382)

Characteristics	Frequency(n)	Percentage (%)
Gender		
Male	344	90.1
Female	38	9.9
Academic qualification		
Bachelor degree	110	28.0
Master degree	268	70.2
Ph.D. degree	7	1.8
Years of experience		
Less than 2 years	53	13.9
Between 2- 4 years	256	67.8
Between 5 – 7 years	61	16.0
Between 8 – 9 years	8	2.1
More than 10 years	1	0.6
Current position		
Head/Member of the institution administration	39	10.2
Dean/ Member of faculty of administration staff	127	33.2
Head/Member of ICT department	193	50.5
IT lecturing staff	23	6.0
Number of students		
1 – 1000	157	41.1
1001 – 3000	174	45.5
٤٠٠١– 7000	45	11.8
7001 - 10000	5	1.3
Above 10001	1	0.3

4.2 Level of Information Security Management

The above table 2 shows the majority of the higher education institution 91.4% that they haven't chief information security officer, 2.1% in – placed and while 6.5% planned to have CISO. Regarding (Tietoturvallisuuden, 2010) chief information security officer play an important role for assessment, management, and implementation of information security in the organization. The majority of the respondent identify that they haven't any team-based security (76.4%), 9.9% have a team and while 13.6% planned to have. Internal audit plays an important role in controlling and balancing the information security and access 88.7% identified they haven't any internal audit, 1.8% in – placed and 9.4% planned. The majority of the respondents didn't encrypt their data (91.9%), 5.5 in –placed while 2.6% planned. Authentication and authorization are two main ways to ensure the authorized user and unauthorized according the above study indicate 99.2% in – placed authentication and 99.7% in – placed authorization which is the user should ask username and password when entering the system. Audit data use to trace which clients accessed what and which way it does not really offer any protection against security threats, so the study indicates 89.8% have no any audit, 7.6% have and while 2.6% planned to have an audit to their data. One – time password another way to ensure the data safety 81.2% identified none the main reason the respondent identified difficult to memorize the password, 9.7% in – placed and final 9.2% planned. The above discussion identifies that there is low of information security.

Table2: level of information security management to the higher education institutions ($n = 382$)

Items	Frequency(n)	Percentage (%)
Chief information security officer(CISO)		
None	349	91.4
In – placed	8	2.1
Planned	25	6.5
Team-based security		
None	292	76.4
In – placed	38	9.9
Planned	52	13.6
Internal audit		
None	339	88.7
In – placed	7	1.8
Planned	36	9.4
Encryption data		
None	351	91.9
In – placed	21	5.5
Planned	10	2.6
Authentication data		
None	3	0.8
In – placed	379	99.2
Planned		
Authorization data		
None		
In – placed	381	99.7

Items	Frequency(n)	Percentage (%)
Planned	1	0.3
Auditing data		
None	343	89.8
In – placed	29	7.6
Planned	10	2.6
One- time password		
None	310	81.2
In – placed	37	9.7
Planned	35	9.2

4.3 Reliability and Validity

The below table 3 Structural equation modeling was applied to identify the correlation between construct variables. In the convergent validity must to be tested factor loading and average variance extracted in the above table all factor loadings between $0.662\ and\ 0.928$ and loadings should be greater or equal 0.5(B. M. Byrne & van de Vijver, 2010) and all AVE must be greater than 0.5 (Fornell and David F. Larcker, 1981). Further construct reliability (CR) is comparable to Cronbach alpha and should be greater than 0.70 and consider as reliable(Joe F. Hair, Sarstedt, Ringle, & Mena, 2012). All squared multiple correlations (R – square) must be at least 0.40 (Bollen, 1989). Above table 3 all SMC between $0.438\ and\ 0.870$.

Table 3: Reliability and validity

Construct	Item	Factor loading	SMC	CR	AVE	Alpha
Information security management(ISM)	ISM1	0.662	0.438	0.858	0.604	0.856
	ISM2	0.871	0.758			
	ISM3	0.789	0.622			
	ISM4	0.772	0.599			
Severity attack (SA)	SA1	0.887	0.786	0.901	0.698	0.760
	SA2	0.919	0.844			
	SA3	0.698	0.487			
	SA4	0.823	0.677			
Response efficacy (RE)	RE1	0.809	0.654	0.841	0.639	0.774
	RE2	0.828	0.685			
	RE3	0.761	0.579			
Cost effectiveness(CE)	CE1	0.810	0.656	0.905	0.761	0.885
	CE2	0.870	0.756			
	CE3	0.933	0.870			
Relative Advantage(RA)	RA2	0.896	0.802	0.915	0.587	0.718
	RA3	0.899	0.808			
	RA4	0.859	0.738			
Top management support(TMS)	TM1	0.904	0.817	0.941	0.799	0.928
	TM2	0.921	0.848			
	TM3	0.901	0.811			
	TM4	0.850	0.722			
	TM5	0.758	0.574			
Size of Higher Education Institution(SHEI)	SHEI1	0.786	0.618	0.861	0.581	0.913
	SHEI2	0.928	0.861			
	SHEI3	0.921	0.848			
	SHEI4	0.884	0.781			

The below table shows the relationship between variables in the lower diagonal and the bold numbers are square-root average variance extracted. According to (Campbell & Fiske, 1959) discriminant validity should also be higher than the correlations among different traits measured by the same method.

Table 4 discriminant validity

	MaxR (H)	ISM	SHEI	TMS	RA	CE	RE	SA
Information security management(ISM)	0.876	**0.777**						
Size of higher education institution(SHEI)	0.921	0.552	**0.766**					
Top management support(TMS)	0.951	0.385	0.529	**0.893**				
Relative advantage(RA)	0.909	0.411	0.532	0.137	**0.766**			
Cost effectiveness(CE)	0.894	0.172	0.170	0.246	0.243	**0.849**		
Response efficacy(RE)	0.767	0.406	0.278	0.276	0.290	0.116	**0.799**	
Severity Attack(SA)	0.908	0.881	0.496	0.353	0.357	0.134	0.393	**0.835**

4.4 Hypotheses Testing Results

Hypothesis 1: suggests there is positive relationship between severity attack and low information security management in higher education institutions ($\beta = 0.668, t = 15.734$) are significant ($p < 0.001$) this proposes that higher education institutions who are low protecting of

their system will increase their prevention for information theft this supports with previous studies(Mohamed & Ahmad, 2012a) and (Son & Kim, 2015).

Hypothesis 2: proposes response efficacy and the need information security are negatively not support was found $(\beta = -0.043, t = -1.107)$ and significant$(p > 0.05)$.

Hypothesis 3: suggests a positive relationship between cost-effectiveness and the need for information security $(\beta = 0.054, t = 1.032)$ and significant$(p > 0.05)$, so the hypothesis not supported.

Hypothesis 4: proposes relative advantage and the need information security management are positively related$(\beta = 0.012, t = 0.188)$, the hypothesis was not supported at significant level$(p > 0.05)$.

Hypothesis 5: suggests there is positive relationship between top management support and the need for information security management$(\beta = 0.005, t = 0.099)$ and the hypothesis not supported where p-value$(p > 0.05)$.

Hypothesis 6: there is a significant relationship between the size of organization and the need for information security management$(\beta = 0.181, t = 4.498)$, the hypothesis supported since$(p < 0.001)$.

Table 4 summary of hypotheses test

Hypothesis	Findings
H1: There is a significant relationship between severity attack and low Information security management in HEI	Supported
H2: Response efficacy is negatively and significantly related to need information security management in HEI	Not supported
H3: Cost-effectiveness is positively and significantly related to the need information security management in HEI	Not supported
H4: Relative advantage is positively and significantly related to the need for information security management in HEI	Not supported
H5: Top management support is positively and significantly related to the need for information security management in HEI	Not supported
H6: There is a significant relationship between the Size of organization and the need information security management	Supported

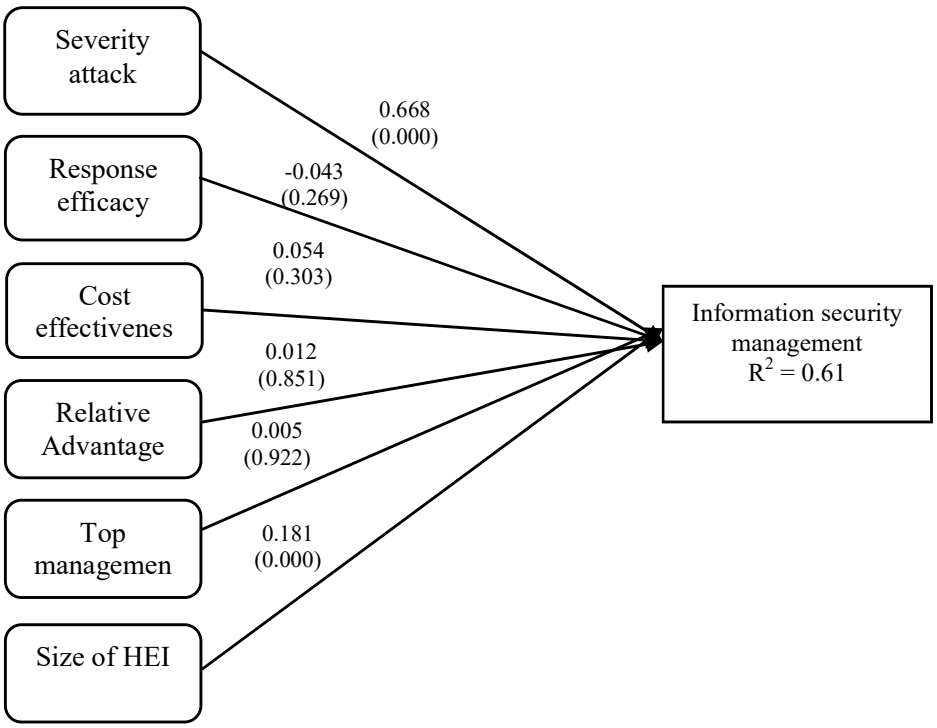


Fig2. Research Model

4.5 Model Fit

To evaluate the measurement of the model, this study used the absolute values of skewness and kurtosis to ensure the normal distribution where skewness 0.1770 to -1.054 and kurtosis -0.545 to1.350, this shows that there was no indication none – normality. According to (In'nami & Koizumi, 2011) identified the skewness should be less than 3 and kurtosis should be less than 8.

Assessing confirmatory factor analysis is the measurement of the model fit with maximum likelihood. In the confirmatory factors analysis suggested to remove one item from a relative advantage (RA1), it was 27 items and 26 items were validated and fit the data sufficiently. All standardized factor loadings must be more than 0.5(Joseph F; Hair, Black, Babin, & Anderson, 2010). The following was the model fit statistics: the chi-square $= 531.08$ and degree of freedom$= 297$; CMIN/DF (the Relative χ^2) $= 1.788$ this should be less 5 (Bentler, 1990; Marsh, Barnes, & Hocevar, 1985) Goodness of fit index (GFI)$= 0.907$ (Cheung & Liu, 1997) comparative fit index (CFI) $= 0.969$ (Bentler, 1990; Faulon & Hatcher, 1994) (IFI) $= 0.970$; Tucker-Lewis index (TLI) $= 0964$; Normed fit index (NFI) $= 0.934$; Relative fit index(RFI) $= 0.923$; Root mean square Residual (RMR) $= 0.072$ and Root mean square error adjusted (RMSEA) $= 0.045$ (M. M. Byrne & Thompson, 2001)as show in the above table, all loadings were significant.

Table 6: Summary of model fit

Model	Required	Calculated
Chi-Square		531.086
DF		297
Relative Chi-Square		1.788
P	P<0.001	0.000
GFI	>=0.9	0.907
AGFI	>=0.9	0.882
CFI	>=0.9	0.969
IFI	>=0.9	0.970
NFI	>=0.9	0.934
TLI	>=0.9	0.964
RFI	>=0.9	0.923
RMR	<=0.08	0.072
RMSEA	<=0.08	0.045

5 Conclusion and Suggestions

5.1 Information Security Management

The main goal of this study was too drawn the level of information security management in the higher education institution in Mogadishu – Somalia. The researcher was tested the hypotheses of the following factors which are a part of protection motivation theory and technological organizational environmental models.

In the Protection Motivation Theory (perceived severity threat, response efficacy, cost-effectiveness, relative advantage). In the

Technological organizational environmental (top management support and size of the organization)

5.1.1 Perceived Severity Threat

Higher education institution those are perceived the severity attack of losing students' information and academic staff such student's results, identities to theft have apprehensions with information security management(Mohamed & Ahmad, 2012b). The study proposes that severity attack has significance to the information security management. The previous study emphasizes to adopt anti-virus program (Y. Lee & Kozar, 2008). Another study using ant-virus program anti-spyware software(Chenoweth, Minch, & Gattiker, 2009).

5.1.2 Response Efficacy

Perceived response efficacy refers to the perception that a suggested duplicating response is an effective way for the organization or individuals to protect from any other threats(Woon & Tan, 2005). According to this study there is no significant relationship between response efficacy and information security which indicates that most of higher education institution has low awareness or protection for information privacy.

5.1.3 Cost Effectiveness

Information security is continuously altering that needs continuous adaption to new changing of information security threats, the decision-makers require to implement information security strategy with cost-effectiveness (Wang, 2011). In the study there is no relationship between cost-effectiveness and information security, the reason is that most of the higher education institution in Somalia not met any loss of financial and information there is no budget for information security.

5.1.4 Relative Advantage

Hundreds of thousands of organizations are applied the standards of information security management by BS77779 and ISO/IEC these standards are n't only focusing IT security but also people, process, information and IT security, most of organizations require to deal with how these international standards are suitable in solving the insider threat(Humphreys, 2008). In this study the researcher identified that there is no relationship between relative advantage and information security.

5.1.5 Top Management Support

Regarding the study top management support has no significance to the information security management, the reason is that most of the higher education institution has no chief information security officer (CISO). According to (Reddick, 2009) management support on information security depends upon five of six factors.

5.1.6 Size of the Higher Education Institution

Overall, The large organization has a tendency to adopt technology innovation more than small and medium-sized institution(Gutierrez, Boukrami, & Lumsden, 2015). In this study the researcher identifies that size of higher education institutions in Somalia has positive related to information security management adoption, the universities those are large in size, early opening and reputation more than small size, or late open universities.

5.2 Contributions to the Theory

Nations, Organizations, and individuals are more dependent on the information communication technology these widely use brings highly vulnerable to attack information systems, such as stealing data, hacking, cyber terrorism, cybercrime, and others. Since information is something has a value and should be protected, so information security management

refers controls that organization needs to ensure their sensitive data is protected from attackers.

Based on the two theories Protection Motivation Theory and Technology Organization Environment, the research extends and confirms a research model in acquisition into information security management adaption in higher education institutions. The results propose a level of information security management.

Understanding the importance of information security in higher education institution this brings to minimize the risks and pro-actively limiting the impact of security breach.

5.3 Limitations and Direction for Future Research

This research study has some limitations, first, the sample size was 382 only higher education institutions thus the findings could not be generalized to the entire institution as too broad. The future research may consider by including longitudinal approach using various samples. Second, the content of the study limited the level of information security management in HEI, it also needs to identify the degree of information security in financial institutions.

References

Aghroum, C. (2017). Information security evaluation: a holistic approach. *Sécurité et Stratégie*, *7*(3), 83. https://doi.org/10.3917/sestr.007.0083

Bentler, P. M. (1990). Fit Indexes, Lagrange Multipliers, Constraint Changes and Incomplete Data in Structural Models. *Multivariate Behavioral Research*. https://doi.org/10.1207/s15327906mbr2502_3

Bollen, K. A. (1989). A New Incremental Fit Index for General Structural Equation Models. *Sociological Methods & Research*.

https://doi.org/10.1177/0049124189017003004

Byrne, B. M., & van de Vijver, F. J. R. (2010). Testing for measurement and structural equivalence in large-scale cross-cultural studies: Addressing the issue of nonequivalence. *International Journal of Testing*, *10*(2), 107–132. https://doi.org/10.1080/15305051003637306

Byrne, M. M., & Thompson, P. (2001). A positive analysis of financial incentives for cadaveric organ donation. *Journal of Health Economics*. https://doi.org/10.1016/S0167-6296(00)00065-5

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*.

https://doi.org/10.1037/h0046016

Chen, F., Deng, P., Wan, J., Zhang, D., Vasilakos, A. V., & Rong, X. (2015). Data mining for the internet of things: Literature review and challenges. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1155/2015/431047

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to the adoption of protective technologies. In *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*.

https://doi.org/10.1109/HICSS.2009.74

Cheung, C. K., & Liu, E. S. C. (1997). Parental distress and children's problems among single-parent families in China. *Journal of Genetic Psychology*. https://doi.org/10.1080/00221329709596665

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2010.311

DePietro, R., Wiarda, E., & Fleischer, M. (1990). The context for change: Organization, Technology, and Environment. *The process of technology innovation*.

Eccles, M. P., Hristos, S., Francis, J. J., Stamp, E., Johnston, M., Hawthorne, G., … Hunter, M. (2011). Instrument development, data collection, and characteristics of practices, staff, and measures in the Improving Quality of Care in Diabetes (iQuaD) Study. *Implementation Science*. https://doi.org/10.1186/1748-5908-6-61

Faulon, J. L., & Hatcher, P. G. (1994). Is There Any Order in the Structure of Lignin? *Energy and Fuels*. https://doi.org/10.1021/ef00044a018

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Fornell and David F. Larcker. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research, 18*(1), 39–50. Retrieved from http://www.jstor.org/stable/3151312 .

Gutierrez, A., Boukrami, E., & Lumsden, R. (2015). Technological, organizational and environmental factors influencing managers' decision to adopt cloud computing in the UK. *Journal of Enterprise Information Management*. https://doi.org/10.1108/JEIM-01-2015-0001

Hair, Joe F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*. https://doi.org/10.1007/s11747-011-0261-6

Hair, Joseph F; Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate Data Analysis. *Vectors*.

https://doi.org/10.1016/j.ijpharm.2011.02.019

Haaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management*, *43*(July), 165–172. https://doi.org/10.1016/j.ijinfomgt.2018.07.013

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*. https://doi.org/10.1057/ejis.2009.6

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*. https://doi.org/10.1016/j.istr.2008.10.010

In'nami, Y., & Koizumi, R. (2011). Structural equation modeling in language testing and learning research: A review. *Language Assessment Quarterly*. https://doi.org/10.1080/15434303.2011.582203

Ki-Aries, D., & Faily, S. (2017). Persona-centered information security awareness. *Computers and Security*, *70*, 663–674. https://doi.org/10.1016/j.cose.2017.08.001

Kim, D., & Ammeter, T. (2014). Predicting personal information system adoption using an integrated diffusion model. *Information and Management*. https://doi.org/10.1016/j.im.2014.02.011

Kuo, R. Z. (2018). EMRS Adoption: Exploring the effects of information security management awareness and perceived service quality. *Health Policy and Technology*, *7*(4), 365–373. https://doi.org/10.1016/j.hlpt.2018.10.012

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers and Security*, *59*, 60–70. https://doi.org/10.1016/j.cose.2016.02.004

Lee, Y., & Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multi-theoretical perspective. *Information and Management*. https://doi.org/10.1016/j.im.2008.01.002

Lorence, D. P., & Churchill, R. (2005). Incremental adoption of information security in health-care organizations: Implications for document management. *IEEE Transactions on Information Technology in Biomedicine*, *9*(2), 169–173.

https://doi.org/10.1109/TITB.2005.847137

Mamonov, S., & Benbunan-fich, R. (2018). Computers in Human Behavior The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32–44. https://doi.org/10.1016/j.chb.2018.01.028

Marsh, H. W., Barnes, J., & Hocevar, D. (1985). Self-Other Agreement on Multidimensional Self-Concept Ratings. Factor Analysis and Multitrait-Multimethod Analysis. *Journal of Personality and Social Psychology*. https://doi.org/10.1037/0022-3514.49.5.1360

Mohamed, N., & Ahmad, I. H. (2012a). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008

Mohamed, N., & Ahmad, I. H. (2012b). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008

Omar, A. (2014). Sample size estimation and sampling techniques for selecting a representative sample. *Journal of Health Specialties*. https://doi.org/10.4103/1658-600x.142783

Reddick, C. G. (2009). Management support and information security: an empirical study of Texas state agencies in the USA. *Electronic Government, an International Journal*. https://doi.org/10.1504/eg.2009.027783

Rogers, E. M. (1995). Diffusion of Innovations. *Elements of Diffusion* (pp. 1–20). https://doi.org/citeulike-article-id:126680

Son, J. W., & Kim, S. (2015). Dipeptidyl peptidase 4 inhibitors and the risk of cardiovascular disease in patients with type 2 diabetes: A tale of three studies. *Diabetes and Metabolism Journal*. https://doi.org/10.4093/dmj.2015.39.5.373

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. *Accounting, Organizations and Society*, *71*, 15–29. https://doi.org/10.1016/j.aos.2018.04.005

Studies, H. I. for P. (2013). The State of Higher Education in Somalia : Privatization, rapid growth, and the need for regulation. *Heritage Institute for Policy Studies*, (August), 1–26.

Teitel, D. F., Klutz, R., Steendijk, P., van der Velde, E. T., van Bel, F., & Baan, J. (1991). The end-systolic pressure-volume relationship in the newborn lamb: Effects of loading and inotropic interventions. *Pediatric Research*.

https://doi.org/10.1203/00006450-199105010-00012

The Complete University Guide. (2016). Top UK University League Tables and Rankings 2016.

Tietoturvallisuuden, T. (2010). Introduction to Information Security Broadcast encryption. *Network*, 1–26.

Wang, H. (2011). The Economics of Information Security Investment. *Advanced Materials Research*. https://doi.org/10.4028/www.scientific.net/amr.219-220.1550

Woon, I., & Tan, G. (2005). A protection motivation theory approach to home wireless security. In *International Conference on Information Systems (ICIS)*.