Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning

Research · October 2021

DOI: 10.13140/RG.2.2.10562.71365

CITATIONS
0

READS
27

3 authors:

Jared Ngare
Moi University
3 PUBLICATIONS **0** CITATIONS
SEE PROFILE

James Ochieng Ogalo
Kisii University
14 PUBLICATIONS **6** CITATIONS
SEE PROFILE

Esau Mneria Mengich
Maseno University
3 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Journal of African Interdisciplinary Studies (JAIS): **ISSN 2523-6725** (online)
October 2021 Vol. 5, No. 10

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya

By

Ngare Jared Nyamiaka
Department of Computing Sciences, School of Information Sciences and Technology
Kisii University, Corresponding mail: jngare.orient@gmail.com, jngare@mu.ac.ke
P. O Box 3900 – 30100 Eldoret – Kenya, Tel: +254 722334639

Co Authors
James Ochieng Ogalo
Senior Lecturer - School of Information Sciences and Technology,
Department of Computing Sciences,
Kisii University, P.O. Box 408-40200. Kisii.
E- mail: ogalojames@kisiiuniversity.ac.ke, Tel: +254 0721622234

&

Esau Mneria Mengich
Lecturer - School of Business and Economics,
Department of Management Sciences,
Maseno University
P.O. Box 3275-40100, Kisumu. – Kenya
E-mail: esaumengich@gmail.com, Tel: +254 0792458671

Abstract
Information security policies are essential for the safety of Information Systems because they serve as a blueprint for the success of all information systems. The weakest link in information security is human activity, often known as human culture. Despite organizations' focusing on technology in information security, there are still concerns of poor information security management in higher learning institutions. The objective of this paper is to propose a framework to support organization culture incorporation into information security management. Research findings suggest that organizations majorly depend on technology and ignore the human component in formulating policies. With organizations depending majorly on technology in securing information systems, it is my recommendation that attention should now be focused on incorporating the human dimension with social cultural human centric approach in the overall framework for information security and start viewing the user as an asset instead of perceiving the user as a security threat.

Keywords: Information Security, Organization culture, Framework

Journal of African Interdisciplinary Studies (JAIS): **ISSN 2523-6725** (online)
October 2021 Vol. 5, No. 10
Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya

By

Ngare Jared Nyamiaka, James Ochieng Ogalo & Esau Mneria Mengich

1. Introduction

Public entities and private organizations have both been facing threats to information security. Securing this information has been a challenge to most of this organizations, institutions of higher learning included. Because enterprises have become increasingly reliant on Information Systems (IS) for competitive advantages and activities, information protection concerns are becoming extremely relevant, in particular for businesses in the online commerce world (Barton, Tejay, Lane, & Terrell 2016). Furthermore, information security management has become a popular topic among practitioners and academics alike (Soomro, Shah, & Ahmed, 2016).

As vast volumes of data are collected and analyzed in electronic media, information systems management issues have often risen because of the intrinsic weakness of information technology (Chang & Ho, 2006). According to the 2005 CSI/FBI computer crime and security study Gordon, Loeb, Lucyshyn, and Richardson, (2005), attacks on computer networks or misuse of such networks have gradually decreased over time, despite a minor decrease in both the overall annual loss per business and the average reported loss per accident. The analysis also suggested a decline in the amount of organizations documenting intrusions into the law enforcement agencies. The main factor given for not disclosing to law enforcement agencies is the fear of adverse attention and negative publicity. This phenomenon may be attributed to the fact that in recent years, organizations have based their information protection strategies primarily on technological concerns such as encryption / decryption, access management, and intrusion detection technology. While organizations are continually planning, building and integrating information technology programs, the topic of maintaining employees' engagement and awareness of information technology goals has become an extremely relevant aspect to consider; (Susanto, Almunawar, Saad, Saeed, Alghathbar, Khan & Pitman 2018).

According to a study carried out by Koskosas, Kakoulidis, and Siomos, (2011), security breaches might be internal or external, 66 percent of computer attacks in Greece were carried out by employees which implies that information security effectiveness is influenced in part by the positive behavior and understanding of those who utilize it. Human existence is complicated and multifaceted, and it gets even more complicated in organizations where the culture resists the criteria of control and predictability that developers typically anticipate from technologies. Employees behaviour has a major influence on an organization's information security, according to Lim, Chang, Ahmad, and Maynard (2012) in their book "Towards an organization culture framework for information security practices," published in Melbourne, Australia. As a result, the corporate culture that influences acceptable employee conduct is considered. Information security should complement an organization's objective, be cost-effective, and seamlessly incorporate technology, procedures, and people into the organization's culture.

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

2. Statement of the Problem

Information loss arising from security lapses is rapidly affecting organizations and individuals. Most empirical studies on Information systems management work have studied the technological aspect of this crucial problem, although human involvement is largely rooted in safeguarding and protecting Information systems.

Information management policies failure can be ascribed to a variety of causes, including difficulties in implementation, which are heavily influenced by employee views and behavior (Siponen, Mahmood, & Pahnila, 2014). Rather than weak protection strategies, a larger percentage of major security breaches may arise from bad security conduct on the part of staff.

Researchers say that significant risks to Information protection are created by incompetent workers who don't obey the rules and procedures of the organization. Cases of security violations for information systems recorded in universities are quite unusual in Kenya. This does not indicate, however, that there are no such instances, nor does it suggest that the universities' information systems are stable. No matter how sophisticated or comprehensive a security technology solution is, it can be rendered ineffective due to a failure to identify between sensitive information assets, poorly organized operational procedures, or weak attitudes toward security inside the business, according to Schinagl, S., & Shahim, A. (2020).

The motivation and push for this research stems from persistent concerns about poor information security management in institutions of higher learning, which can result in significant monetary losses that are typically kept hidden from the public eye for fear of unwanted publicity.

2. Methodology

This study employed a descriptive research approach with primarily questionnaires to collect sample data which was analysed quantitatively.

3. Empirical Review

This section delves further into the literature of prior similar investigations on the subject. Non-technical issues are at least as essential as technological ones in preserving the organization's classified information, according to (Sindhuja & Kunnathur, 2015). Nevertheless, the relevance of non-technical information security management problems has been underscored in most of the prior research on information security management, which appears to be quantitative in nature. Studies have concluded that organizations require a philosophy of information protection with human centric approaches well as technical frameworks to maintain a safe atmosphere for digital assets (Kayworth & Whitten, 2012), (Zakaria, Jarupunphol, & Gani, 2003). There is a significant lack of focus in the existing information security policy literature on developing countries.

4.1 Information Security Management Systems

Data is an essential commodity for businesses and government departments and must therefore be carefully secured. Much of the information is currently produced, collected, transported or analyzed at least in part, using information technology (IT) both in business and government functions. In addition, however, knowledge from all other stages of business processes must be properly covered. IT protection events such as leakage or misuse of

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

information can have wide-ranging, negative business impacts or can prohibit an entity from conducting its activities resulting in high costs (Stouffer, Falco, & Scarfone, 2011).

Information Technology security issues may have far-reaching effects that damage an organization or interfere with the success of its activities and thus result in high costs. Practical evidence has demonstrated that improving information protection strategy also enhances information security more efficiently and sustainably than investing in computer technologies. Nonetheless, initiatives initially introduced to enhance information security can still have a beneficial impact in the security framework and could turn out to be cost-effective. Investments in information security will, in certain situations, also lead to medium-term cost savings. The beneficial side effects that can be derived from this include improved standard of service, enhanced consumer trust, enhancement of the IT environment and operational procedures as well as the application of convergence benefits by greater incorporation of information technology systems into current frameworks, (Stouffer et al., 2011).

The management level is responsible for ensuring the regulatory legislation and arrangements where third parties are dealt with so that essential business procedures are not disrupted; information security has interfaces with other parts of the organization so involves some sensitive business processes and activities. Consequently, only the level of administration or management will insure that information security policy is implemented seamlessly into current corporate systems and processes; the level of policy administration is accountable for the effective delivery of resources.

Consequently, the category of administration or management has a strong degree of accountability for information security. Lack of oversight, insufficient information management policy or incorrect choices can have far-reaching negative effects as a result of security events as well as lost resources and low expenditure. Stouffer et al., (2011) claims that the public concept of information security confirms that senior management appears to ignore information security and wants to delegate security to the IT team.

The goal of an organization's information system is to allow connectivity to its resources from anywhere, at any time, via closed and accessible networks. It has to do with issues of confidentiality and privacy in the administration of information systems. Individuals, methods, and technology are all included in the socio-technical approach to the knowledge structure (Garba, Armarego, Murray, & Kenworthy, 2015).

Mistrust is at the heart of today's information security management, which is getting increasingly complex. Security steps are set in motion to detect intruders at the entrance, to shield the customer from mistakes and to avoid abuse. Security experts have concluded over the last two years that compliance monitoring will only function if it is integrated within the organization's operational and administrative framework, (Albuquerque Junior & Santos, 2015).

4.2 Information Security Evolvement and Technological Advancements

Much has been written about how information security has evolved through time, from a solely technological understanding in the 1970s to its modern mainstream position within businesses (Van Niekerk & Von Solms, 2006). From a historical standpoint, Von Solms (2006) claims that the evolution of methods to Information Security Management Systems (ISMS) over the last forty to fifty years may be divided into four waves (Technological, management, institutional and governance waves) as depicted in the figure 4.2 below.

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

This evolutionary concept is a highly effective timeline technique for discussing ICTs in currently developing countries because it was designed from the perspective of technologically developed countries. Over the defined time periods, each wave symbolizes the overall approach and management of information technology. The formulation of an ICT evolution route will be crucial to our understanding of ICT technology differentiators and the sophistication of information security system settings in countries that are still in the early stages of this journey. Some countries may not have achieved development rates of the third or fourth wave yet.

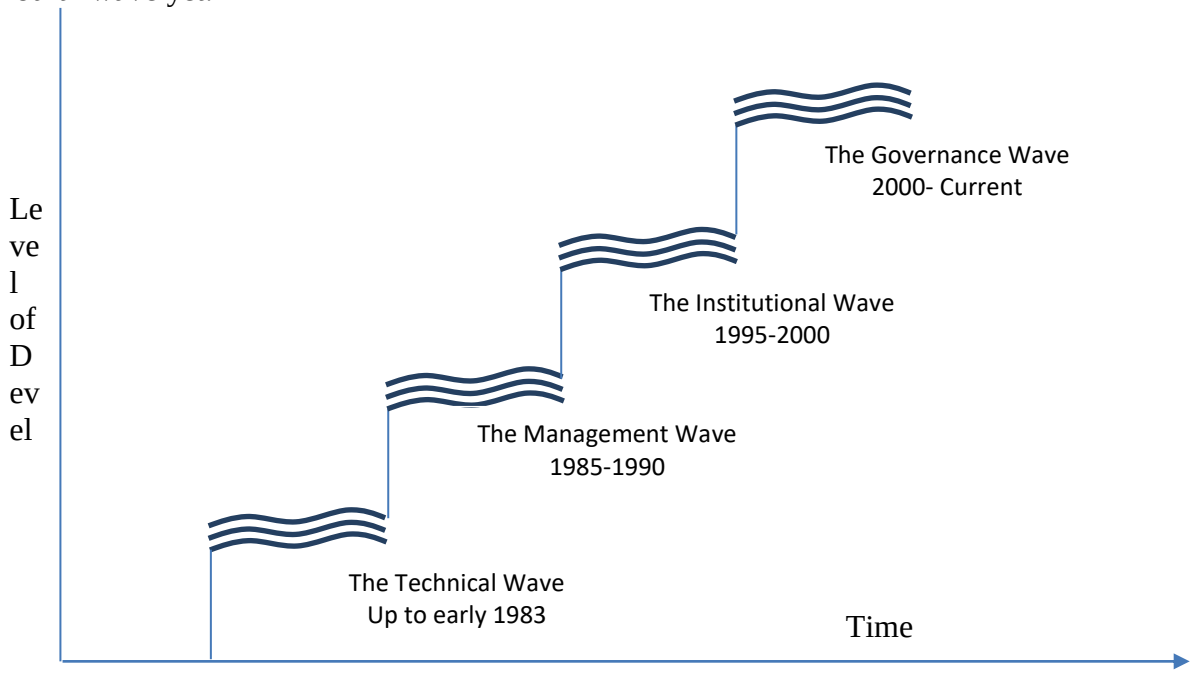

Figure 4.2 ISMS development waves

In a broader sense, information security in modern environments refers to both people and procedures, as well as technologies. The societal adoption of security technology, often known as organizational security culture, is discussed in a small number of literature publications (Alfawaz, 2011).

According to Stewart and Jürjens, (2017), open networks are not necessarily secure within the infrastructure itself, priority must be given to information protection aspects. Studies that assess the elements that contribute to successful information security management at both the macro and micro levels, as well as a personal understanding of their relationship, are essential.

4.3 Information Security Policy Implementation – Organizational Perspective and Culture Traits

Organizations have unwritten set of rules and principles that its members follow. This set of norms and values, according to Dutta and McCrohan (2002), is part of the organization's culture The culture of a business can influence employee attitudes toward an information security strategy, which can create the difference between successful and unsuccessful policy implementations. Management's grasp of how an organization's norms, values, and value systems effect employee attitudes toward security is crucial when establishing and

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

implementing new information security policies or procedures (Bang, Y., Lee, D. J., Bae, Y. S., & Ahn, J. H. 2012).

According to the 2007 CSI Computer Crime and Security Survey, eliminating information security threats exclusively through technology solutions is not achievable (Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. 2010). The analysis proved the need for employee training due to a history of data breaches caused by "basic human error and negligence" Human error such as injuries or employees who refuse to follow information security regulations, continues to be a significant danger to data security. The organizations cultural atmosphere is most likely to blame for some employees' problems.

Over the last 40 years, several studies have centered on information technology and organizational culture. Researchers including Alesina, A., Giuliano, P. (2015), Chang S. E., & Ho, C, B. (2006), and Kunnathur, A. S. & Li, L. (2020) agree that information security and organizational culture have an unspoken relationship.

According to Chang & Lin, (2007) model of organization culture traits, ~~C~~consistency is concerned with order, rules & regulations, uniformity & efficiency. Organizations should not put more efforts to technical aspects of security because they will usually change with time. Given that technology systems must be managed and used by humans, it's plausible to conclude that data security is a social and organizational issue. A robust security product would not be able to secure an organization without a strong management strategy and execution. Information security is widely acknowledged to be more of an organizational or managerial issue than a technological one.

4.4 Information Security Culture versus Organization Culture

Every business relies on computer assets such as digital records, hardware, software, and networks to function in today's digital environment. In order to safeguard digital assets, information systems practitioners must work even quicker and stay ahead of the curve due to the rapid developments and advancements in the information technology industry. However, using technologically based measures for information protection is insufficient. The honesty and efficiency of those who adopt and implement information protection tests are critical to their performance (Dhillon, 2001).

Although there may be adequate protection mechanisms in place, such as firewalls, the human factor will ultimately triumph over technology if management does not properly manage them or if users do not understand how to properly operate a firewall. Users engage with device objects in some fashion at every stage and for every reason. This indicates that, as experts have previously argued, the human element is the weakest link in information security. Interaction is the weakest link in terms of information security (Schneier, 2015; Martins et al., 2015). Over time, the way individuals interact with data assets and behave in the workplace may become the way things are done in an organization. Organizational culture is formed when the way things are handled becomes part of the organization's tradition.

It is necessary for the appropriate behavior towards information security to become part of an organizational culture. The actions of workers against information must be appropriate and must be part of the organization's daily existence. Client information must be handled confidentially, or only approved maintenance workers should perform repairs and maintain computer equipment, to name a few examples. To accomplish this, the organization must cultivate an information security culture, but this is rarely done owing to a culture that encourages employees to behave in ways that could lead to information security breaches.

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

4.5 Organizational Culture Behavior and Information Security Management's Effectiveness

Organizational culture refers to a system of common values, ideas, and convictions that influence how people act in the workplace (Alvesson & Sveningsson, 2015). These shared beliefs have a significant impact on people within the firm, influencing how they act, speak, and operate. According to Alvesson and Sveningsson, (2015), an organization establishes and maintains a distinct culture that provides direction and guidelines for its members' actions. Each business, like individuals, has its own distinct identity.

An organization's culture is its own identity. Chatman and O'Reilly (2016) both mentioned this Organizational culture is a hidden but powerful effect in communities of people who work together, influencing the actions of the community's leaders. In corporate management study the idea of organizational culture has been translated from anthropology. Almost every scholar has a unique perspective on culture, yet different scholars have different interpretations of organizational culture (Chatman & O'Reilly, 2016). According to Alesina and Giuliano (2015), corporate culture evolves as a result of ongoing dialogues among the institution's executives over views, concepts, and resources.

Internal / external orientation and flexibility / control orientation are the two basic classifying criteria. According to Pakdil and Leonard (2015), Collaborative culture, growth culture, hierarchical culture, and logical culture are the four types of organizational culture. They also stressed the importance of all four forms of corporate culture being reflected in an organization's traits and ideals as depicted in the figure below.

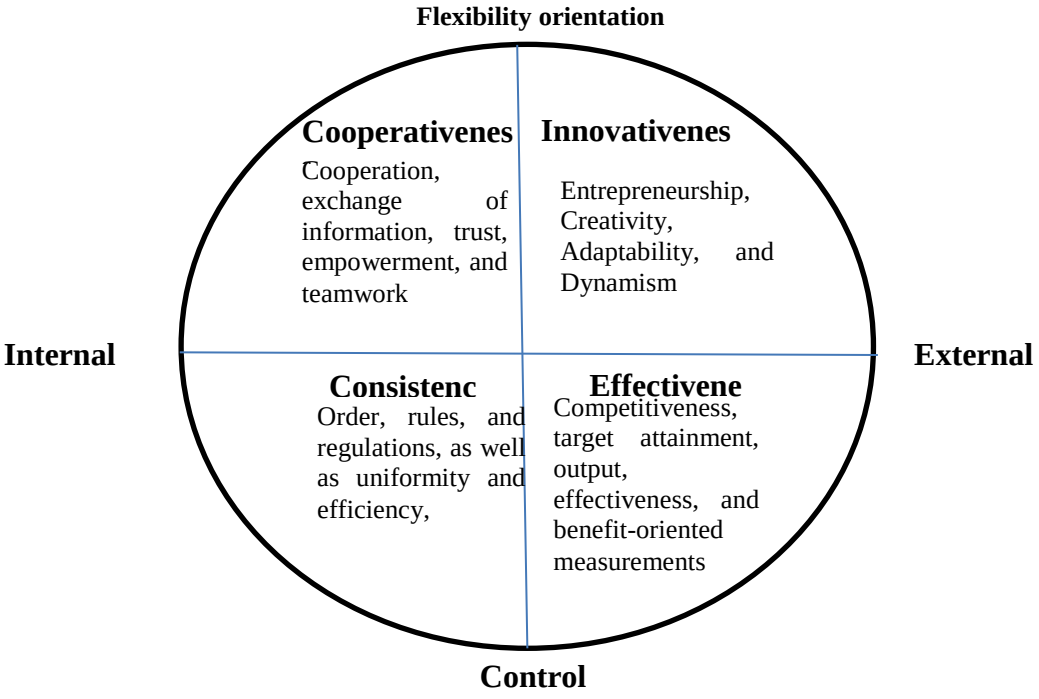

Figure 4.5 Model of organizational culture traits - Chang & Lin, (2007)

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

6. Cultures that support the deployment of information security management

Since many of staff's core beliefs and conduct habits have been deemed corporate culture, and the organization's information protection would be influenced by these behavior patterns. According to Zheng, Yang, and McLean (2010), the most essential component in describing an organization's success or failure is culture. Organizational culture has a direct impact on the organization's productivity and the efficiency of information management activities, administrators will pay close attention to corporate culture as a key component in achieving security goals.

Unfortunately, many businesses are searching for quick and simple technological answers to their security issues. The organization's information security is not required if the latest hardware or software technologies are used but consumers or human factors involved in an information network do not obey or are unaware of protection requirements, or if the enterprise's technology strategies do not suit its culture in general. In other words, purchasing and using security items and equipment would be meaningless without a fundamental adjustment in the organization's security culture that directly influences security policy. Human components will always play a part in information security. As previously indicated, 80 percent of security concerns were ascribed to poor staff protection, indicating that worker ineptitude is considerably more important than technological flaws in the occurrence of such issues. As a result, it's critical to train and manage problem-prone individuals (Zheng et al., 2010).

5. Discussions

The study sought to propose a framework to support organization culture incorporation into information security management.

The fundamental aims of this study were to determine the most appropriate framework that can be adopted when discussing issues of information security and organization culture, and to conduct a systematic review to determine the essence of its impact on information security management. The amount of agreement in terms of the means and standard deviations is provided in table 5.1 below, based on the descriptive statistics for the relevant survey findings from the study data.

5. 1 Regressions model summary

Regression analysis is a predictive modeling technique that examines the relationship between a dependent (target) and an independent (s) variable (predictor). This method is used to forecast, model time-series data, and discover the causal relationship between variables.

Model Summary

Model Summary

					Change Statistics				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change
1	.745[a]	.556	.532	.205	.556	23.746	4	76	.000

a. Predictors: (Constant), EF_3, CP_6, CY_1, IN_5

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

The strength of the relationship (Correlation coefficient) was (R=0.745), (r<0.8) thus the researcher's analysis was reliable since the relationship was not too strong where the researcher could have experienced multicollinearity.

In this case (R = 0.745), which was a strong positive relationship. This suggested that the model was a relatively good predictor of the outcome.

R Squared value of my model was (R^2 = 0.556) meaning that the proportion of variation in the outcome variable was 55.6%, i.e. 55.6% of Predictor variables may clarify the variation in the results.

5.4 ANOVA

Table 6 ANOVA

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.005	4	1.001	23.746	.000[b]
	Residual	3.205	76	.042		
	Total	7.210	80			

a. Dependent Variable: INT_1

b. Predictors: (Constant), EF_3, CP_6, CY_1, IN_5

To test whether or not the model which included Effectiveness, Innovativeness, Cooperativeness and Consistency was a major indicator of the variable outcome, a test using ANOVA indicated that the regression model considerably predicted the outcome since (r=0.000) since (p<0.05). With (r=0.000), the null hypothesis was rejected as alternative hypothesis accepted. The value F=23.746 is the extent of how my variables were varying.

The findings thus revealed that the model was a strong indicator of the effectiveness of management of information security, F (4, 76) = 23.746, p = .000.

5.5 Coefficients

Table 7 Coefficients

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound
1	(Constant)	2.152	.118		18.221	.000	1.917	2.387
	CP_6	-.047	.024	-.172	-1.977	.052	-.094	.000
	IN_5	-.090	.032	-.327	-2.792	.007	-.155	-.026
	CY_1	-.074	.031	-.265	-2.376	.020	-.137	-.012
	EF_3	-.061	.025	-.206	-2.447	.017	-.111	-.011

a. Dependent Variable: INT_1

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

For a model to have been perceived to significantly contribute positively, its p value must be less than 0.05. By reading over the rows for each of the predictor variables in the above table and with 95% confidence interval, it came out clearly that:

Since (p>0.05), cooperativeness did not have a significant impact on the model (p=0.052).

Innovativeness significantly contributed to the model (p=0.007), since (p<.05).

Consistency significantly contributed to the model (p=0.020) since (p<0.05).

Effectiveness significantly contributed to the model (p=0.017) since (p<0.05).

5. 6 Predictive model

A multiple regression was used to see if organizational culture qualities including cooperativeness, innovation, consistency, and effectiveness might predict the efficacy of information security management at Moi University's information systems. The model explained 55.6 percent of the variance and was a significant predictor of the effectiveness of Information Security Management for Information Systems, F(4,76) = 23.746, p =.000, while Innovativeness contributed significantly to the model (B =-0.090, p=0.07), according to the results of the regression. Cooperativeness did not contribute substantially to the model (B = -.047, p=0.052), but Consistency did (B = -0.074, p=0.020) and Effectiveness did (B = -.061, p=0.17).

The association between multiple independent or predictor variables and one dependent or criterion variable is usually described by multiple regressions.

Equation for multiple regressions

$Y=B_0+B_1X_1+B_2X_2+B_3X_3+B_4X_4$ + error

By using the multiple regression formulae above,

Y= Information Security Management

B_0= Constant

X_1= Cooperativeness

X_2= Innovativeness

X_3= Consistency

X_4= Effectiveness

i) $Y=B_0+B_1X_1+B_2X_2+B_3X_3+B_4X_4$

ii) $Y=2.152 + (-0.047)X_1 + (-0.090)X_2 + (-0.074)X_3 +(-0.061)X_4$

Therefore the proposed model was:

$Y=2.152 + (-0.047) X_1 + (-0.090)X_2 + (-0.074)X_3 +(-0.061)X_4$ + Error

6. Research gaps in information security management

According to previous studies on information security and information protection management in Kenyan universities, there is a dearth of scholarly and technical literature on ISM, and specifically ISC. According to Alnatheer and Nelson (2009), when describing and implementing information security management, it is critical to see the user as an asset. ISM largely ignores the human dimension, focusing instead on technical and procedural measures, and perceiving the user as a security threat rather than a security asset, according to (Schlienger & Teufel, 2002). According to Alnatheer & Nelson, (2009), Alvesson & Sveningsson, (2015) and Alshaikh et al., (2016), when describing and performing information security monitoring, the value of considering the user as an asset has been suggested. It was also earlier suggested by Schlienger & Teufel, (2002) who also stresses

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

that ISM largely disregards the human aspect, with the primary emphasis being on technological and operational interventions with users viewed as security enemy not security assets. The researcher then explores the issues that arise from this understanding, and suggests a conceptual change to a centric social cultural orientation.
The researcher is not offering answers, guidance on this methodology but is exploring certain elements that may help create a framework for Information security management.

7. Conclusion

Information security systems ought to be run and maintained by individuals, however, without a clear security management strategy in procedure, a technical protection solution alone cannot secure organizations security systems. Organizations will follow a holistic approach that integrates all facets of information management and corporate culture, concentrating not just on the obvious and identifiable "outside" artifacts and behavioral patterns, but rather on the unseen and often unnoticed "within" human existence, operation, and connections.

8. Recommendations

To organizations, a culture favorable to information management activity is incredibly necessary because knowledge must be a critical asset in modern businesses. Therefore, organizations should delve at corporate culture to analyze how it impacts the success of applying ISM in order to appreciate and enhance the internal conduct with regard to information protection.
The responsibility for information security personnel must be clearly defined and communicated to all employees. Without an information security governance system, organizations would find it difficult to further move towards successful application of the principles of information security management.

Information security should be described as a corporate priority at the corporate level. This indicates that senior management is responsible for defining security strategies. As a result, they will need enough help to carry out this initiative. This job may be given to a Chief Information Security Officer (CISO), although the responsibility rests with upper management as a whole.

The various branch heads are then in charge of dealing with the information management strategy and enforcing it within their respective departments. They ought to be empowered sufficiently to follow the security strategy; because it is not easy to enforce such a program without their help. For this protection strategy to be enforced, management must identify and monitor the numerous security steps. Their workers must also be eligible and educated. Security obedience actions must be rewarded, intentional violations and infringement of protection policies punished. The Safety Plan will therefore be routinely audited and benchmarked.

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

9. Proposed Framework for Information Security Management

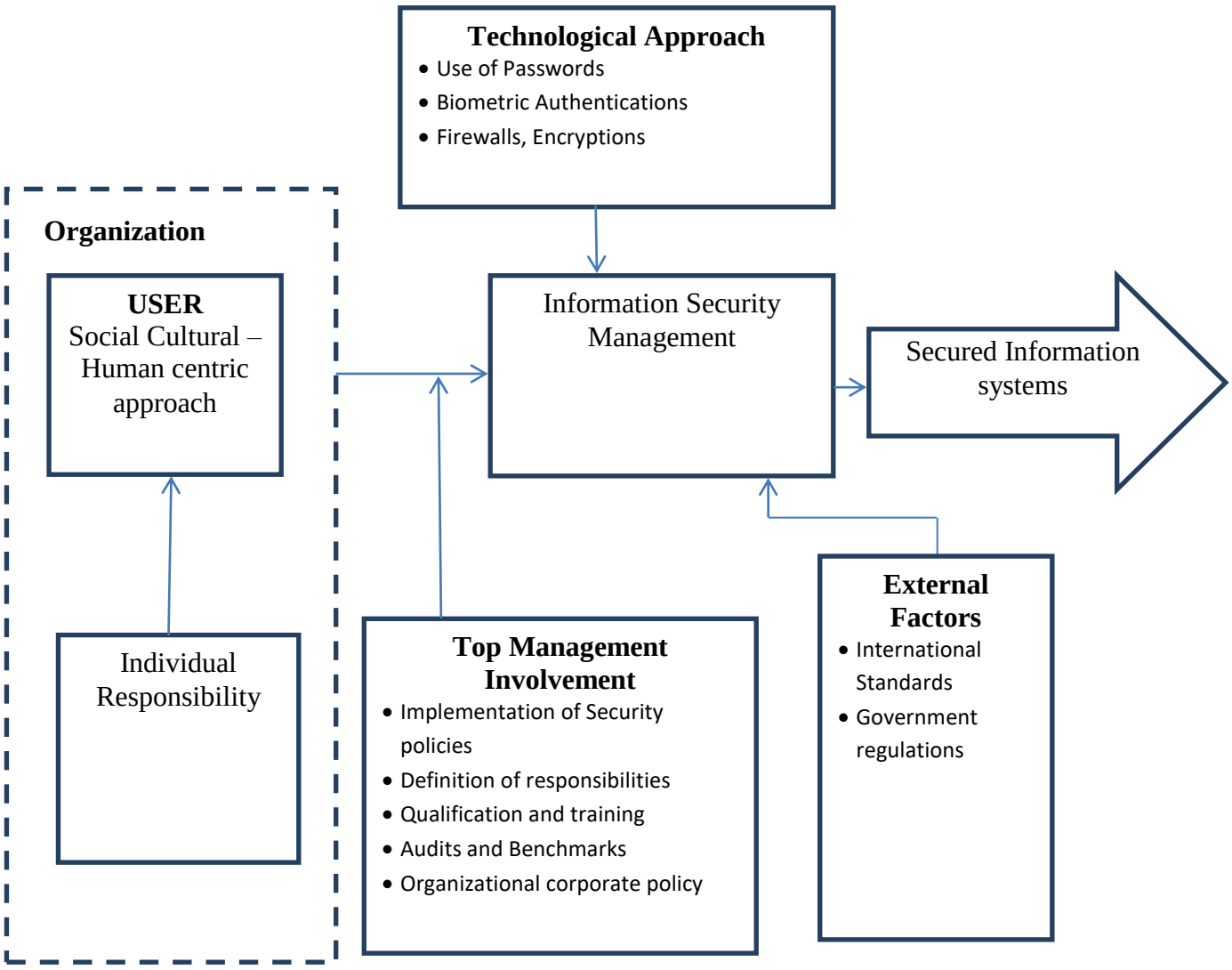

Figure 1 Proposed framework for Information Security Management

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

References

Alesina, A., & Giuliano, P. (2015). Culture and institutions. *Journal of Economic Literature, 53*(4), 898-944.

Alkahtani, A. H. (2015). The influence of leadership styles on organizational commitment: The moderating effect of emotional intelligence. *Business and Management Studies, 2*(1), 23-34.

Alnatheer, M., & Nelson, K. (2009). Proposed framework for understanding information security culture and practices in the Saudi context.

Alvesson, M., & Sveningsson, S. (2015). *Changing organizational culture: Cultural change work in progress*: Routledge.

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68*, 145-159.

Bang, Y., Lee, D. J., Bae, Y. S., & Ahn, J. H. (2012). Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. international journal of information management, 32(5), 409-418.

Carr, J. Z., Schmidt, A. M., Ford, J. K., & DeShon, R. P. (2003). Climate perceptions matter: A meta-analytic path analysis relating molar climate, cognitive and affective states, and individual level work outcomes. *Journal of applied psychology, 88*(4), 605.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*.

Chang, S. E., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*.

Chatman, J. A., & O'Reilly, C. A. (2016). Paradigm lost: Reinvigorating the study of organizational culture. *Research in Organizational Behavior, 36*, 199-224.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & security, 20*(2), 165-172.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. *Journal of Information privacy and security, 11*(1), 38-54.

Jo, S. J., & Joo, B.-K. (2011). Knowledge sharing: The influences of learning organization culture, organizational commitment, and organizational citizenship behaviors. *Journal of Leadership & Organizational Studies, 18*(3), 353-364.

Koskosas, I., Kakoulidis, K., & Siomos, C. (2011). Information security: Corporate culture and organizational commitment. *International Journal of Humanities and Social Science, 1*(3), 192-195.

Lim, J. S., Chang, S., Ahmad, A., & Maynard, S. (2012). Towards an organizational culture framework for information security practices. In *Strategic and practical approaches for information security governance: Technologies and applied solutions* (pp. 296-315): IGI Global.

Lin, C., Kunnathur, A. S., & Li, L. (2020). The Cultural Foundation of Information Security Behavior: Developing a Cultural Fit Framework for Information Security Behavior Control. *Journal of Database Management (JDM), 31*(2), 21-41.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human factors and information security: individual, culture and security environment. Defence science and technology organisation edinburgh (australia) command control communications and intelligence div.

Pakdil, F., & Leonard, K. M. (2015). The effect of organizational culture on implementing and sustaining lean processes. *Journal of Manufacturing Technology Management*.

Citation: Ngare, J. N; Ogalo, J. O & Mengich, E. M. (2021). Proposed Information Security Framework for Organizational Culture in Institutions of Higher Learning, Kenya. *Journal of African Interdisciplinary Studies.* 5(10), 137 – 150.

Shahab, A., Sobari, A., & Udin, U. (2018). Empowering leadership and organizational citizenship behavior: the mediating roles of psychological empowerment and emotional intelligence in medical service industry.

Schwepker, C. H., & Schultz, R. J. (2015). Influence of the ethical servant leader and ethical climate on customer value enhancng sales performance. Journal of Personal Selling & Sales Management, 35(2), 93-107.

Sindhuja, P., & Kunnathur, A. S. (2015). Information security in supply chains: a management control perspective. *Information & Computer Security*.

Stair, R., & Reynolds, G. (2015). *Principles of information systems*: Cengage Learning.Steinmetz, H., Knappstein, M., Ajzen, I., Schmidt, P., & Kabst, R. (2016). How effective are behavior change interventions based on the theory of planned behavior? *Zeitschrift für Psychologie*.

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security*.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication, 800*(82), 16-16.

Susanto, H., Nabil Almunawar, M., Abu Saad, B., Saeed, F., Alghathbar, K., Khan, B., . . . Pitman, G. (2018). Computer forensics education. In *Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standards* (Vol. 18, pp. 1-18): Addison-Wesley Computer Sciences.

Van Niekerk, J., & Von Solms, R. (2006). *Understanding Information Security Culture: A Conceptual Framework.* Paper presented at the ISSA.

Zakaria, O., Jarupunphol, P., & Gani, A. (2003). *Paradigm mapping for information security culture approach.* Paper presented at the Proc. of the 4th Australian Conference on Information Warfare and IT Security.

Zohar, D. M., & Hofmann, D. A. (2012). Organizational culture and climate.