Influence of Security Governance on Enterprise Security Risk Management Adoption in Chartered Universities in Kenya

Levis Omusugu Amuya[1], Peterson Mwai Kariuki[1], and Consolata Ndung'u Thuranira[2].

[1]*Institute of Criminology, Forensics, and Security Studies, Dedan Kimathi University of Technology, Nairobi, Kenya.*

lokamuya@gmail.com

[2]*Department of Business Administration, Dedan Kimathi University Technology, Kenya.*

Submitted 31st October 2022, Accepted 10th January 2023 and Published 07th March 2023

ABSTRACT

The purpose of this study was to investigate the influence of security governance on Enterprise Security Risk Management (ESRM) adoption in Kenya's chartered universities. We utilized the diffusion of innovation theory to explain security governance as an organizational characteristic that steers and guides ESRM adoption in universities. From a target of 60 chartered universities, we randomly selected a sample of 22 public and 20 private chartered universities. We collected data from a security executive from the main campus of each of the sampled universities using a self-administered questionnaire. Spearman's correlation results revealed that security governance had a strong, positive, and statistically significant influence on ESRM adoption; r_s (33) =.524; p =.002. Ordinal logistic regression analysis indicated a good model, which explained 53.4% of the variance in ESRM adoption. Therefore, security governance has a significant influence on ESRM adoption. We have discussed managerial implications and suggested future research directions.

Key Words: University security risk management, Enterprise security risk management, ESRM adoption, ESRM maturity model, security governance

I. INTRODUCTION

As a practical management approach to security risks, Enterprise Security Risk Management (ESRM) promotes the continuous evaluation of the full range of security risks to organizations within their broad portfolio of critical assets (American Society of Industrial Security [ASIS International], 2019; Allen, 2019). Its main objective is to tie an enterprise's security practices to its overall strategy and objectives using globally recognized risk management principles. In the context of ESRM, an 'enterprise' can be an organization, learning institution, or other business entity that engages in security risk management (Allen & Loyear, 2017). When complex organizations like universities adopt ESRM, they gain the ability to enumerate security threats, launch and actualize mitigation plans, and manage all security incidents that may threaten their ability to meet their foundational objectives (Marquez-Tejon et al., 2022; Allen & Loyear, 2017). Also, adopting ESRM redefines the thinking and perspectives on the role that security plays in organizations, refocusing the efforts of security professionals to work collaboratively with institutional leaders and other primary stakeholders to detect and alleviate security risks of concern (Petruzzi & Loyear, 2016; Marquez-Tejon et al., 2022). The full adoption of ESRM and its projected benefits to an institution can only be realized in the presence of its building blocks, key among them the establishment of security governance mechanisms (ASIS International, 2017; Schneller et al., 2022).

Security governance is considered a guiding and steering force that assists institutions to provide direction and allows them to apply Security Risk Management (SRM) activities and practices in ways that befit the relevant threat environment in which they operate (Talbot & Jakeman, 2009). Governance of security encompasses a wide range of activities such as fine-tuning organizational structures; designing roles and responsibilities; overseeing security-related tasks; allocating needed resources for the security function; measuring outcomes; and assessing the adequacy of security reviews and audits (Allen et al., 2018; Tan et al., 2017). Fay and Patterson (2018) define security governance as a set of practices and responsibilities exercised by an institution to strategically direct its operations while facilitating the achievement of objectives and appropriately managing its security risks. Therefore, an organization practices security governance by managing security-related responsibilities, involving all stakeholders, and treating security as a non-negotiable business requirement. For universities, effective security governance in which professional and academic personnel understand their security responsibilities offers a realistic, straightforward, and actionable model for dealing with all the security risks that modern security practitioners and the organizations that employ them face (Fay & Patterson, 2018).

In Kenya, universities face a universe of security risks, among them information security breaches, thefts, sexual assaults, adverse media coverage, burglaries, student unrest, and terror threats (Odhiambo et al., 2015; Maranga & Nelson, 2019; Ndiege, 2020). As a result of these risks, most higher learning institutions have scaled down their operations, while others have laid off sections of their workers due to the associated financial impediments (Mutegi, 2017; Oduor, 2020). Because of the risks that universities face and the attendant consequences, there has been heightened scrutiny by education stakeholders and watchdogs in Kenya to pressure universities to report their Security Risk Management (SRM) strategies, institute accountable stewardship of resources, and guarantee competent service provision (Kiura & Mango, 2017; Mange et al., 2019). It is in this context that ESRM has gained considerable momentum in the industry as a necessity in universities' twenty-first-century SRM practice (Allen & Loyear, 2016; Allen, 2019).

Even though ESRM has been suggested as a potential solution to security risks, higher education risk management literature shows that there are limited studies that examine the role of security governance in influencing its adoption, especially in complex organizational settings (Calderon and Pero, 2013; Toma et al., 2014). Most existing risk management studies are more bent toward examining Information Security Governance (ISG) in organizations as a driver of security strategy adoption, a focus that does not address the wider scope of security governance (e.g., Tan et al., 2017; Ribbers et al., 2002; Posthumus & Von Solms, 2004). While a few authors have researched different risk management models, especially Enterprise Risk Management (ERM), in the higher education sector (Lundquist, 2015; Setapa et al., 2015; Malki & Aldwais, 2019; Perera et al., 2020), no recent research focuses on the nexus between ESRM adoption and security governance structures at the internal level. Therefore, based on the perceptions of university security executives in Kenya, the study will provide new evidence on the relationship between ESRM adoption and security governance in the higher education sector. The findings will enable university security practitioners and decision-makers to develop more effective security governance policies as they focus explicitly on institutionalizing ESRM practices to help them address the emerging security risks within their operational environments

II. LITERATURE REVIEW

A. Security Governance and ESRM Adoption

There are only limited studies on security governance and ESRM adoption in reputable academic databases because the topic is fresh and empirical outcomes are still at the infantile phase (Kwateng et al., 2022). However, a great deal of security governance studies have found that security decision-making depends on existing governance processes and structures (Peterson et al., 2000; Ribbers et al., 2002; Posthumus & Von Solms, 2004; Tan et al., 2017). These studies underscore that the level of security strategy adoption would be higher when institutions use an ISG framework (Posthumus & Von Solms, 2004), empower lower and middle-management-level decision-makers (Tan et al., 2017), and promote governance by building a common consensus among all stakeholders (Peterson et al., 2000; Ribbers et al., 2002). Researchers have also found that corporate governance is a fundamental business concept that provides the base for managing security risks in a more business-oriented fashion (Allen et al., 2018; Ogeng'O & Omar, 2015). Although ISG is a substantial part of enterprise governance, recent developments in SRM have heightened the need to expand security governance in all areas, including people, operations, and business continuity, to deal with the dynamic and complex settings in which organizations like universities operate today (Soomro et al., 2016; Allen et al., 2018).

Allen (2005) identified six fundamental beliefs, behaviors, capabilities, and actions facilitating holistic security governance in organizations. First, security is endorsed at the institutional level. Second, security occupies the same position as other business requirements. Third, security is considered during regular operational and strategic planning processes. Fourth, all departmental and function leaders have a holistic understanding of how security enables running of business. Fifth, security is wholly integrated into enterprise processes and functions, such as risk management and audit or compliance. Finally, all employees with access to enterprise systems comprehend their distinct responsibilities in preserving and protecting the firm's security condition (Allen, 2005; Kiura & Mango, 2017). For universities, these employees include both academic and professional or non-academic staff that often have access to university systems and processes (Lundquist, 2015). These elements are expected to affect risk management models like ESRM positively, although previous studies have not examined this influence. The expectation is that the manifestation of the above elements in an organization would positively affect ESRM adoption.

B. Theoretical Framework

The study was anchored on the Diffusion of Innovation (DOI) theory developed by Everett M. Rogers in 1962 (Rogers, 2003). ESRM has largely been described as an innovation in the academic risk management literature (Adekanye & Rahman, 2018; Pulido, 2021). According to the DOI theory, adoption of innovation is the implementation of internally developed or borrowed ideas, including products, policies, systems, processes, services, or programs, that were new to the institution at the time of their adoption (Pateli et al., 2020). Adoption of innovations like ESRM is addressed at different levels of the institution, such as business units or functional teams (Pateli et al., 2020). Although organizational adoption of innovation is driven by different classes of factors, such as innovation and environmental characteristics, organizational features play a substantial role in this process. In DOI research, organizational characteristics are often conceptualized in terms of management support, structure, internal influence, training readiness and efforts, and size of the organization (Wisdom et al., 2014; Pateli et al., 2020).

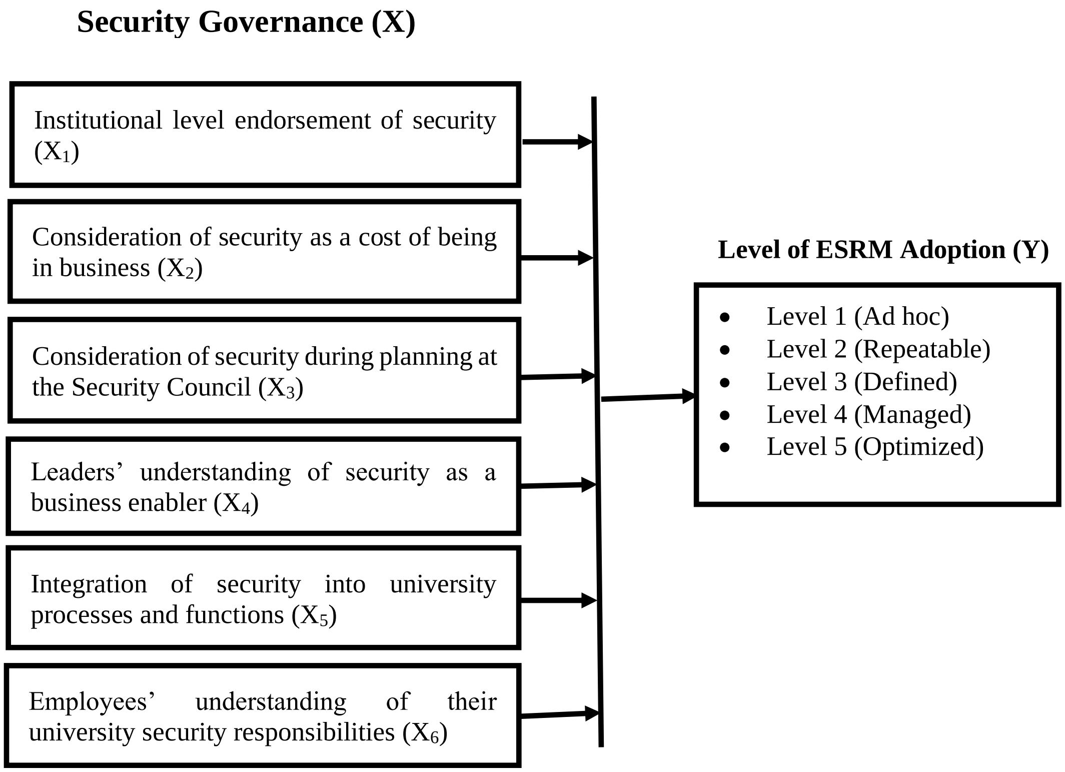
The major dimension of concern for the current study is that of internal influence, which includes cultures, norms, and values, and absorptive capacity (Wisdom et al., 2014; Pateli et al., 2020). Internal governance mechanisms, such as security governance processes, help organizations to identify, interpret, disseminate, and use innovations like ESRM (Rogers, 2003; Wisdom et al., 2014). In other words, internal influence in the form of security governance steers and directs innovation adoption efforts. However, the role of internal influences, especially governance processes, in influencing risk management adoption in the higher education sector has not been adequately examined in the existing literature. Therefore, it would be instructive to expand the application of DOI theory in understanding how security governance drives universities to adopt ESRM, considering their unique organizational dimensions, such as shared governance (Lundquist, 2015).

C. Conceptual Framework

Security governance was the independent variable for the study and we operationalized it in terms of the security governance metrics developed by Allen (2005), as shown in Figure 1. These metrics were measured in terms of five Likert-type items that ranged from 5 (strongly agree) to 1 (strongly disagree). ESRM adoption was the dependent variable for the study, and it was measured using a five-level ESRM Maturity Assessment Model developed by ASIS in 2019 (Harisaiprasad, 2020). In Level 1 (Ad hoc) of this model, ESRM processes do not exist or are performed in an ad hoc, uncontrolled, or reactive manner. In Level 2 (Repeatable), ESRM processes exist and are repeatable, although they are unlikely to be rigorous. In Level 3 (Defined), processes are defined and documented and are utilized to create consistency at all levels of the organization. In Level 4 (Managed), ESRM processes are measured against established metrics, and the management can fine-tune and adapt the processes to specific initiatives. In Level 5 (Optimized), processes are reviewed and proactively improved based on measurable results (Harisaiprasad, 2020).

Figure 1:

Conceptual Framework for Security Governance and ESRM Adoption


Security Governance (X)
Institutional level endorsement of security (X_1)
Consideration of security as a cost of being in business (X_2)
Consideration of security during planning at the Security Council (X_3)
Leaders' understanding of security as a business enabler (X_4)
Integration of security into university processes and functions (X_5)
Employees' understanding of their university security responsibilities (X_6)
Level of ESRM Adoption (Y)
Level 1 (Ad hoc)
Level 2 (Repeatable)
Level 3 (Defined)
Level 4 (Managed)
Level 5 (Optimized)

III. METHODOLOGY

The aim of the study was to examine the influence of security governance on ESRM adoption as perceived by university security executives. Consequently, we adopted a quantitative research design to test the relationship between security governance, the independent variable, and ESRM adoption, the dependent variable. The relationship between the two variables was also examined using a descriptive correlation design. Our population of interest was security executives, including Chief Security Officers (CSOs) and Senior Security Officers (SSOs) from 31 public and 29 private chartered universities in Kenya as of December 2021 (Commission for University Education [CUE], 2021). We used a proportionate random sampling strategy to select 22 public and 20 private chartered universities. A total of 33 respondents completed self-administered questionnaires, among them 17 security executives from public and another 16 from private chartered universities.

To ensure validity and reliability, we subjected the draft questionnaire to a pilot test involving seven universities within Nairobi and Kiambu Counties. Based on the pilot results, we performed standardization and addressed potential ambiguities in the data collection tools. The piloting results also informed the exclusion of all constituent university colleges. We conducted an exploratory factor analysis to verify the construct validity of security governance metrics. The findings indicated that all the constructs had factor loadings of greater than .505 or good, as Tabachnick and Fidell (2007) recommended. The security governance metrics also had an overall

Cronbach's Alpha score of .768, indicating a very strong degree of internal consistency (Tavakol & Dennick, 2011; Bonett & Wright, 2015). We analyzed quantitative data using Spearman's correlation analysis in SPSS to test the influence of security governance on ESRM adoption. Because an ordinal scale was used to measure ESRM adoption, we adopted ordinal logistic regression analysis to determine whether security governance explained changes in the level of ESRM adoption in universities.

IV. RESULT

A. Correlation between Security Governance and ESRM Adoption

We performed Spearman's rank correlation to determine the influence of security governance on respondents' rating of the level of ESRM adoption in their universities. The results in Table 1 show a strong positive and statistically significant relationship, r_s (33) = .524; p =.002. The results suggest that the level of ESRM adoption in universities increases with an increase in security governance.

Table 1:

Correlation between Security Governance and the Level of ESRM Adoption

Latent Variables		Level of ESRM Adoption	Security Governance
Level of ESRM Adoption	Spearman's Correlation Coefficient	1.000	.524**
	Sig. (2-tailed)	.	.002
	N	33	33
Security Governance	Spearman's Correlation Coefficient	.524**	1.000
	Sig. (2-tailed)	.002	.
	N	33	33

**. Correlation is significant at the 0.01 level (2-tailed).

We further conducted Spearman's correlation analysis test between security governance constructs as perceived by university security executives and the level of ESRM adoption. According to Table 2, security executives' evaluation of employees' understanding of their university security responsibilities had the strongest influence on the level of ESRM adoption, r_s (33) = .545; p = .001, followed by consideration of security during planning at the Security Council, r_s (33) = .508; p =.003.

Table 2:

Correlation between Security Governance Constructs and ESRM Adoption

Constructs		Level of ESRM Adoption
Level of ESRM Adoption	Spearman's Correlation Coefficient	1.000
	Sig. (2-tailed)	.
	N	33
Enactment of SRM at the institutional level	Spearman's Correlation Coefficient	.237
	Sig. (2-tailed)	.184
	N	33
Treatment of SRM like all other business requirements	Spearman's Correlation Coefficient	.199
	Sig. (2-tailed)	.267

	N	33
Consideration of security during planning at the Security Council	Spearman's Correlation Coefficient	.508**
	Sig. (2-tailed)	.003
	N	33
University leaders' understanding of SRM as a business enabler	Spearman's Correlation Coefficient	.179
	Sig. (2-tailed)	.320
	N	33
Integration of security into university processes and functions	Spearman's Correlation Coefficient	.455**
	Sig. (2-tailed)	.008
	N	33
University employees' understanding of their university security responsibilities	Spearman's Correlation Coefficient	.545**
	Sig. (2-tailed)	.001
	N	33

B. *Ordinal Logistic Regression Analysis and Hypothesis Testing*

We formulated and tested a hypothesis using collected data to determine whether security governance attributes influence ESRM adoption among Kenya's chartered universities. Our hypothesis stated as follows:

$H_0$1: Security governance has no significant influence on ESRM adoption in public and private chartered universities in Kenya.

We tested the hypothesis using model fitting information test, Goodness-of-fit, Pseudo R-Square, and the parameter estimates test. The ordinal logistic regression tests are given below:

Test: Logit $[P(Y \leq j)] = \alpha j - \Sigma\{\beta 1X1\}$ + €

Goodness-of-Fit test conditions: Reject if $p \geq .05$, Accept if $p \leq .05$

The model fitting information test results in Table 3 show that the log-likelihood that there was a significant improvement in the final model relative to the base model [χ^2 (6) = 21.830, p =.001]. Therefore, the regression model for this study gave better predictions and consequently indicated that the model fitted the data well. Also, the results of goodness-of-fit in Table 3 indicate that Pearson Chi-square statistic [χ^2 (102) = 110.755, p = 0.260] provided non-significant test results, suggesting a good model fit. Hence, we rejected the null hypothesis and concluded that security governance has a significant influence on ESRM adoption. Further, as shown in Table 3, the Nagelkerke R-Square value (R^2 = .532) indicates that 53.2 per cent of the variance in the level of ESRM adoption was explained by security governance.

Table 3:

Ordinal Logistic Regression Results

Model Fitting Information				
Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	73.801			
Final	51.971	21.830	6	.001
Link function: Logit.				
Goodness-of-Fit				
	Chi-Square	df	Sig.	
Pearson	110.755	102	.260	
Deviance	47.341	102	1.000	
Link function: Logit.				
Pseudo R-Square				

Cox and Snell	.484
Nagelkerke	.532
McFadden	.274
Link function: Logit.	

In addition, Table 4 shows the parameter estimates for security governance (X) constructs. According to the results, security executives' evaluation of university employees' understanding of their security responsibilities (X_6) had a positively and statistically significant influence on the level of ESRM adoption. These employees include both full-time and part-time professional and academic staff in the university (Lundquist, 2015). For every one-unit increase in security executives' evaluation of university employees' understanding of their university security responsibilities (X_6), the log-likelihood of the level of ESRM adoption being at or into the optimized level (Y =5) increased by a factor of 1.517 within the log-odds scale (β3 = 1.517; p =.010). This means that universities scoring higher on security executives' evaluation of employees' understanding of their SRM responsibilities were more likely to have optimized levels (Y=5) of ESRM adoption.

Table 4:

Parameter Estimates for Security Governance (X_1……X_6)

		Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
							Lower Bound	Upper Bound
Threshold	[Y = 1.00]	-6.662	2.014	10.944	1	.001	-10.609	-2.715
	[Y = 2.00]	-3.892	1.131	11.840	1	.001	-6.109	-1.675
	[Y = 3.00]	1.151	.494	5.425	1	.020	.182	2.119
	[Y = 4.00]	1.978	.560	12.476	1	.000	.881	3.076
Location	X_1	.138	.429	.104	1	.748	-.703	.979
	X_2	-.515	.481	1.148	1	.284	-1.457	.427
	X_3	.497	.633	.617	1	.432	-.744	1.739
	X_4	-.500	.454	1.216	1	.270	-1.390	.389
	X_5	1.109	.680	2.659	1	.103	-.224	2.441
	X_6	1.517	.593	6.554	1	.010	.356	2.679
Link function: Logit.								

V. DISCUSSION

We sought to examine the influence of security governance on ESRM adoption in Kenya's public and private chartered universities based on the evaluations of security professionals. In the context of ESRM, security governance involves various activities, including adjustment of organizational structures; management of security-related tasks; design of explicit roles and responsibilities; measurement of outcomes; and evaluation of security reviews to determine their sufficiency (Allen, 2005; Tan et al., 2017; Kiura & Mango, 2017). According to the DOI theory, the decision to adopt or use and the actual adoption and utilization of programs are largely influenced by organizational features, such as absorptive and internal influence from governance processes and structures. Effective security governance has become a necessity in universities as part of their security risk management effort in the face of marauding external and internal risks.

Correlation results revealed that security governance had a strong, positive, and statistically significant relationship with the level of ESRM adoption, r_s (33) = .524; p =.002. The specific security governance metrics that had a positive and statistically significant influence on ESRM adoption included university employees' understanding of their university security responsibilities, r_s (33) = .545; p = .001, consideration of security during planning at the Security Council, r_s (33) = .508; p =.003, and integration of security into university functions and processes, r_s (33) = .455; p =.008. These results concur with the previous studies that find the adoption of security strategies to be higher when institutions use an ISG framework to assign responsibilities with respect to security (Posthumus & Von Solms, 2004). In particular, the finding that consideration of security during planning at the Security Council is consistent with those of Kageyama (2014), who underscores the need for establishing a cross-functional risk council or committee that discusses and addresses risk in universities. The strong correlation between security governance and ESRM adoption accentuates how this committee serves as a reminder of the university's commitment to the ESRM process (Kageyama, 2014).

Ordinal logistic regression analysis revealed that security governance positively and significantly predicted the level of ESRM adoption. Specifically, the Nagelkerke R-Square value (R^2) was .532, implying that 53.2% of the variance in the level of ESRM adoption was explained by security governance. Parameter estimates for ordinal logistic regression analysis determined that the log-likelihood of the level of ESRM adoption being at or into the optimized level (Y =5) increased with an increase in university employees' understanding of their university security responsibilities ($X3_6$) within the log-odds scale (β3 = 1.517; p =.010). According to Allen (2005), security governance is often demonstrated when employees with access to systems within an organization comprehend their distinct security-related responsibilities Universities have complex organizational structures with a vast number of both academic and professional staff that have an impact on how security practices are performed due to their access to different systems (Lundquist, 2015). Kiura and Mango (2017) underscore the pressing need for the top executives in universities to assume direct responsibility for security management, which, as noted in their survey, would improve the entire practice of university security and risk management. The results can also be explained by the DOI theory that associates the increase in the level of program or innovation adoption with organizational governance structures favoring transformation (Wisdom et al., 2014).

VI. CONCLUSION

Based on our results, we conclude that one of the cardinal components of ESRM adoption in universities is the establishment of a security council that oversees security governance issues. Security governance is a guiding and steering force that assists universities to provide direction and permits them to apply ESRM activities and practices in ways that befit the relevant threat environment in which universities often find themselves. Based on the DOI theory, security governance is a prerequisite for the adoption of innovations like ESRM. University Security Councils are better positioned to continually seek opportunities to deal with shared SRM challenges, advance collective SRM priorities, empower lower and middle management level decision-makers, and promote synergy among stakeholders, resulting in increased ESRM adoption.

We recommend that universities need to consistently apply and reinforce recognition, rewards, and consequences associated with security policy compliance as part of their security governance. This will ensure that all employees with access to university systems understand their distinct responsibilities in preserving and protecting the security condition. Also, university security departments need to establish ESRM or Security Councils that actively engage in regular operational and strategic planning cycles and develop attainable, realistic, and measurable objectives for security. By establishing regular schedules for discussing security risks, university executives will conduct and revisit ESRM processes, provide regular updates about critical security risks, and share needed information with all stakeholders to meet obligations with respect to ESRM.

Our study is also not without limitations. We used cross-sectional data and subjective measures from university security executives to determine the influence of security governance on ESRM adoption. We did not determine the years that universities in the sample started adopting their ESRM strategies. Therefore, we suggest that a study that takes into consideration the number of years that universities have adopted ESRM would further enhance our understanding of how security governance influences how ESRM ascends through the different levels over time. Furthermore, we gathered data from each university from a single respondent, the CSO or SSO. Although most informants held positions of responsibility in university security departments, they were not all chief risk officers, faculty, or departmental leaders. As a result, their individual perceptions of their universities' ESRM adoption might not accurately represent the divergent opinions of other players in top management teams. Therefore, we suggest that further studies should develop ways to gather varied perspectives across top management circles.

VII. REFERENCES

Adekanye, M. O., & Rahman, S. S. (2018). The effect of information technology using Enterprise Security Risk Management. *International Journal of Network Security & its Applications (IJNSA, 10*(5), 13-23. https://doi.10.5121/ijnsa.2018.105

Allen, B. J., & Loyear, R. (2016). *The manager's guide to enterprise security risk management: Essentials of risk-based security*. Rothstein Publishing.

Allen, B., & Loyear, R. (2017). *Enterprise security risk management: concepts and applications*. Rothstein Publishing.

Allen, B., Kelly, T., Loyear, R., Poole, A., Awojulu, A., Kmetetz, A. & Yuan, H. (2018). Security Risk Governance: A Critical Component to Managing Security Risk. *Journal of Applied Business & Economics, 20*(1), 132-146. https://doi.org/10.33423/jabe.v20i1.322

Allen, J. (2005). *Governing for enterprise security*. Carnegie Mellon University/Software Engineering Institute.

Allen, M. (2019). Enterprise security risk management. In *The chief security officer's handbook*: *Leading your team into the future* (pp. 19-33). Elsevier Science. https://doi.org/10.1016/B978-0-12-818384-7.00002-1

American Society of Industrial Security [ASIS International]. (2017, November 29). *ESRM: An enduring security risk model.* https://www.asisonline.org/publications--resources/news/blog/esrm-an-enduring-security-risk-model/

American Society of Industrial Security [ASIS International]. (2019, September 06). *Enterprise security risk management guideline.* https://www.asisonline.org/publications--resources/standards--guidelines/esrm-guideline

Bonett, D. G., & Wright, T. A. (2015). Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning. *Journal of Organisational Behaviour*, *36*(1), 3-15. https://doi.org/10.1002/job.1960.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Calderon, T. G., & Pero, K. (2013). Examining the maturity of enterprise risk management initiatives in colleges and universities. *Internal Auditing*, *28*(4), 19-28. http://search.proquest.com/docview/1431991658?accountid=7098

Commission for University Education [CUE]. (2021, June 01). *Universities authorized to operate in Kenya*. https://www.cue.or.ke/images/phocadownload/Accredited_Universities_Kenya_June2021.pdf

Deck, S. C. (2015). *Enterprise risk management at higher education institutions: How management concepts support its implementation* [Doctoral dissertation]. University of Maryland University College.

DiMaggio, P.J. & Powell, W.W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organisational fields, *American Sociological Review*, *48*(2), 147-160. https://doi.org/10.2307/2095101

Fay, J. J. & Patterson, D. (2018). *Contemporary security management*, (4th edn.). Elsevier Inc.

Figueroa, F. A. (2016). *Improved institutional risk reduction at universities through better states of preparation* [Doctoral dissertation]. Texas Tech University.

Harisaiprasad, K. (2020, September 16). *Addressing risk using the new enterprise security risk management cycle*. Information Systems Audit and Control Association (ISACA). https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2020/volume-5/addressing-risk-using-the-new-enterprise-security-risk-management-cycle_joa_eng_0920.pdf

Kageyama, A. (2014). The implementation process of enterprise risk management in higher education institutions. *International Review of Business*, (14), 61-80. https://core.ac.uk/download/pdf/143635076.pdf

Kakabadse, A., Morais, F., Myers, A., & Brown, G. (2020). *University governance: A risk of imminent collapse*. Henley Business School. https://www.kakabadse.com/uploads/universities-governance_final_13-10-2020.pdf

Kiura, S. M., & Mango, D. M. (2017). Information Systems Security Risk Management (ISSRM) model in Kenyan private chartered universities. *European Journal of Computer Science and Information Technology*, *5*(2), 1-15. https://www.eajournals.org/wp-content/uploads/Information-Systems-Security-Risk-Management-ISSRM-Model-in-Kenyan-Private-Chartered-Universities.pdf

Kwateng, K. O., Amanor, C., & Tetteh, F. K. (2022). Enterprise risk management and information technology security in the financial sector. *Information & Computer Security*, 30(3), 422-451. https://doi.org/10.1108/ICS-11-2020-0185

Lundquist, A. E. (2015). *Enterprise Risk Management (ERM) at US colleges and universities: Administration processes regarding the adoption, implementation, and integration of ERM*. Western Michigan University. https://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=2183&context=dissertations

Malki, S., & Aldwais, N. K. (2019). Enterprise risk management at the State University of New York: A benchmark for Saudi universities. *The Journal of Applied Business and Economics*, *21*(9), 54-74. https://doi.org/10.33423/jabe.v21i9.2684

Mange, D. M, Onyango, G. A & Waweru, S. N. (2019). Management challenges facing Kenya's public universities and implications for the quality of higher education. *Journal of African Interdisciplinary Studies*. 3(7), 77 – 93. http://cedred.org/jais/index.php/issues

Maranga, M. J., & Nelson, M. (2019). Emerging issues in cyber security for institutions of higher education. *International Journal of Computer Science and Network*, *8*(4), 371-379. http://ijcsn.org/IJCSN-2019/8-4/Emerging-Issues-in-Cyber-Security-for-Institutions-of-Higher-Education.pdf.

Marquez-Tejon, J., Jimenez-Partearroyo, M., & Benito-Osorio, D. (2022). Security as a key contributor to organisational resilience: A bibliometric analysis of enterprise security risk management. *Security Journal*, *35*(2), 600-627. https://doi.org/10.1057/s41284-021-00292-4

Mutegi, P. (2017, February 02). *Higher education crisis looms as 11 public universities face cash crunch.* Nation Media Group. https://www.businessdailyafrica.com/bd/economy/higher-education-crisis-looms-as-11-public-universities-face-cash-crunch-2138328

Ndiege J., O. (2020). *Enhanced security equipment and its effects on crime in selected higher learning institutions in Kenya.* [Unpublished master's thesis]. Kenyatta University

Odhiambo, E. O. S., Wasike, S., &Kimokoti, S. N. (2015). Learning institutions' vulnerability to terrorism. An overview of issue coverage in nowadays' media and specialized literature & a case study of Garissa university college, Kenya. *Journal of Defense Resources Management*, *6*(2), 21-31. http://www.jodrm.eu/issues/volume6_issue2/03_odhiambo_wasike_kimokoti.pdf.

Oduor, A. (2020). *Vice-Chancellors set to lay off workers in a bid to stay afloat.* The Standard. https://www.standardmedia.co.ke/education/article/2001396298/mass-layoffs-in-varsities-loom

Ogeng'O, P. M., & Omar, N. (2015). Factors affecting successful implementation of enterprise risk management in Kenyan parastatals. A case study of Kenya Revenue Authority. *The International Journal of Business & Management*, *3*(12), 143-166. http://www.internationaljournalcorner.com/index.php/theijbm/article/viewFile/128393/89042.

Pateli, A., Mylonas, N., & Spyrou, A. (2020). Organizational adoption of social media in the hospitality industry: An integrated approach based on DIT and TOE frameworks. *Sustainability*, *12*(17), 7132.

Perera, A. A. S., Rahmat, A. K., Khatibi, A., & Azam, S. (2020). Review of literature: implementation of enterprise risk management into higher education. *International Journal of Education and Research*, *8*(10), 155-172. https://www.ijern.com/journal/2020/October-2020/14.pdf.

Peterson, R., Ribbers, P., & O'Callaghan, R. (2000). Information technology governance by design: Investigating hybrid configurations and integration mechanisms. In *Proceedings of the 20th International Conference on Information Systems*, Australia, 435-452. https://core.ac.uk/download/pdf/6714902.pdf.

Petruzzi, J., & Loyear, R. (2016). Improving organisational resilience through enterprise security risk management. *Journal of business continuity & emergency planning*, *10*(1), 44-56.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638-646. https://doi.org/10.1016/j.cose.2004.10.006

Pulido, J. O. (2021). How innovative leadership will move ESRM implementation forward. *Journal of Global Leadership.* http://www.icglconferences.com/articles/innovative-leadership-will-move-esrm-implementation-forward/

Ribbers, P. M., Peterson, R. R., & Parker, M. M. (2002, January). Designing information technology governance processes: Diagnosing contemporary practices and competing theories. In *Proceedings of the 35th annual Hawaii international conference on system sciences* (pp. 3143-3154). IEEE Computer Society.

Rogers, E. M. (2003). *Diffusion of innovations*, 5th edn. Free Press.

Schneller, L., Porter, C. N., & Wakefield, A. (2022). Implementing converged security risk management: drivers, barriers, and facilitators. *Security Journal*, 1-17. https://doi.org/10.1057/s41284-022-00341-6.

Setapa, M., Zakuan, N., Saman, M. Z. M., Ariff, M. S. M., Zaidin, N., & Sulaiman, Z. (2015, March). The impact of enterprise risk management practices on Malaysian public higher educational institution performance: A literature review. In *2015 International Conference on Industrial Engineering and Operations Management (IEOM)* (pp. 1-7). IEEE, https://doi.org/10.1109/IEOM.2015.7093782

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Speck, B. W. (2011). The myth of shared governance in higher education. *International Journal of Organisation Theory and Behaviour*. *14*(2), 200-235. https://doi.org/10.1108/IJOTB-14-02-2011-B004.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics*, (5th edn.). Pearson Education.

Talbot, J. &Jakeman, M. (2009). *Security risk management body of knowledge*. John Wiley & Sons, Inc

Tan, T., Maynard, S., Ahmad, A., & Ruighaver, T. (2017). Information security governance: a case study of the strategic context of information security. *Pacific Asia Conference on Information System (PACIS) 2017 Proceedings*. *43*. http://aisel.aisnet.org/pacis2017/43

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53-55. https://doi.org/10.5116/ijme.4dfb.8dfd

Toma, S. V., Alexa, I. V., & Şarpe, D. A. (2014). Identifying the risk in higher education institutions. *Procedia Economics and Finance*, *15*, 342-349. https://doi.org/10.1016/S2212-5671(14)00520-6.

Wisdom, J. P., Chor, K. H. B., Hoagwood, K. E., & Horwitz, S. M. (2014). Innovation adoption: A review of theories and constructs. *Administration and Policy in Mental Health and Mental Health Services Research*, *41*(4), 480-502. https://doi.org/10.1007/s10488-013-0486-4.

Zikmund, W.G., Babin, B.J., Carr, J.C., & Griffin, M. (2013). *Business research methods*, (9th Edn.). Cengage Learning.