Routledge
Taylor & Francis Group

JOURNAL OF HIGHER EDUCATION POLICY AND MANAGEMENT

Journal of Higher Education Policy and Management

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cjhe20

Organisational characteristics as antecedents of enterprise security risk management adoption in Kenya's accredited universities

Levis Omusugu Amuya & Peterson Mwai Kariuki

To cite this article: Levis Omusugu Amuya & Peterson Mwai Kariuki (2023): Organisational characteristics as antecedents of enterprise security risk management adoption in Kenya's accredited universities, Journal of Higher Education Policy and Management, DOI: 10.1080/1360080X.2023.2235772

To link to this article: https://doi.org/10.1080/1360080X.2023.2235772

JOURNAL OF HIGHER EDUCATION POLICY AND MANAGEMENT
https://doi.org/10.1080/1360080X.2023.2235772

Organisational characteristics as antecedents of enterprise security risk management adoption in Kenya's accredited universities

Levis Omusugu Amuya and Peterson Mwai Kariuki

Institute of Criminology, Forensics, and Security Studies, Dedan Kimathi University of Technology, Nairobi, Kenya

ABSTRACT

Academic institutions today are experiencing a legion of security risks that are increasingly impeding their mission of producing high-quality graduates, guarding reason and educational integrity, and ultimately advancing human civilisation. The Enterprise Security Risk Management (ESRM) model represents a potential solution to the dynamic threats that accredited universities face today. However, ESRM adoption is largely absent, slow, and inconsistent in Kenya's accredited universities. Only a few attempts have been made to understand what drives security risk management adoption in these universities. Based on seven in-depth interviews with Chief Security Officers across larger accredited universities in Kenya and utilising an overarching innovation adoption model, we examine the organisational predictors of ESRM adoption in these universities. Within the limitations of this study, the data collected highlight the fundamental role of university executive commitment, security governance, and security risk management training in enhancing the diffusion of ESRM systems in universities. We have discussed managerial implications and suggested future research directions.

KEYWORDS

Enterprise security risk management (ESRM); ESRM adoption; university security risk management; security governance; university executive commitment

Introduction

For universities, security risks are internal or external events and practices that compromise assets, processes, and educational mission and objectives, including academic integrity (Birks et al., 2020; Lundquist, 2015; Maranga & Nelson, 2019). Some of the documented internal security risks in universities include academic misconduct and staff failure to report student malpractices (Birks et al., 2020, Bermingham et al., 2010; De Maio et al., 2020), fraud, student unrest, theft, sex scandals, personnel and student data breaches, and drug abuse (Downes, 2017; Lundquist, 2015; Maranga & Nelson, 2019). The security risks at the external level include cybercrime activities, such as hacking and modification of data, adverse media coverage, contract cheating, terrorist attacks, mass shootings, and other marauding information security risks (Davies & Al Sharefeen, 2022; Downes, 2017; Lundquist, 2015; Maranga & Nelson, 2019). Given their diverse goals of

CONTACT Levis Omusugu Amuya lokamuya@gmail.com Institute of Criminology, Forensics, and Security Studies, Dedan Kimathi University of Technology, Nairobi, Kenya

service to communities, teaching, and research (Lundquist, 2015), universities are expected to operate in well-organised internal environments that can promote and encourage integrity, ethical conduct, and other intellectual activities. However, this is repeatedly not possible with the persistence of the aforementioned security risks that have threatened higher education goals and objectives (Birks et al., 2020; Oduor, 2020; Omanga, 2017). Consequently, more stakeholders, including the public, regulatory and accreditation agencies, and members of the campus community, have become involved and continue to scrutinise universities to check their responses to new risks (Lundquist, 2015; Malki & Aldwais, 2019; Perera et al., 2020). In such an environment, the adoption of Enterprise Security Risk Management (ESRM) is increasingly being considered as a viable solution to the many security risks that universities face as they strive achieve their educational objectives.

Initially, most universities globally attempted to address their security risks by adopting Enterprise Risk Management (ERM) to some extent (Kageyama, 2014; Lundquist, 2015; Malki & Aldwais, 2019; Perera et al., 2020). As one of the radical concepts borrowed from the corporate world, ERM is founded on a defined scope, a formal risk management process, and is run by a dedicated department, unlike the budding ESRM, which has no specific departmental structure (B. Allen & Loyear, 2017; Fraser et al., 2021). Also, unlike ESRM, whose focus is only on the management of security risks to institutional assets, ERM deals with all aspects of organisational risk, including operational, environmental, and especially financial (Fraser et al., 2021). The ERM framework also does not sufficiently consider the risks conventionally associated with security (American Society of Industrial Security [ASIS International], 2010). Thus, universities continued to experience plundering security risks despite their attempts to adopt the ERM framework, pointing to the potential unsuitability of this framework in the academic milieu (Malki & Aldwais, 2019; Perera et al., 2020). The ERM model was conceived and nurtured in the corporate world, and questions on whether or not it is suitable within the higher education context have emerged more recently (Malki & Aldwais, 2019; Perera et al., 2020). Professional security organisations, such as ASIS International and the Alliance for Enterprise Security Risk Management (AESRM), have since made a compelling case for adopting ESRM due to the perceived flaws of ERM (American Society of Industrial Security [ASIS International], 2017). ASIS International that developed ESRM is not principally for the corporate sector alone, but its membership is drawn from all sectors, including security practitioners from the higher education sector worldwide. ASIS International made ESRM its strategic priority in 2016 (ASIS International, 2017) and to date, ESRM evaluation empirical studies are largely missing, especially in the higher education sector (Amuya et al., 2023). Even so, the previous literature confirms that risk management practices and models arrived fairly late into universities (Amuya et al., 2023; Ramirez & Christensen, 2013).

ESRM is a practical management process and philosophy that applies fundamental risk principles to manage all security risks that organisations face in a comprehensive and all-encompassing approach (M. Allen, 2019; American Society of Industrial Security [ASIS International], 2019). It redefines the thinking and perspectives on the role that security plays in organisations, refocusing an institution's efforts to work in partnership with all primary stakeholders to identify and mitigate security risks (B. Allen & Loyear, 2017; Petruzzi & Loyear, 2016). Unlike ERM, ESRM uses risk

management principles to manage all security-specific risks, especially in organisations like universities, which are characterised by complex management structures, shared governance practices, and multiple stakeholders (B. Allen & Loyear, 2017; Lundquist, 2015). The role of university security professionals in assisting faculty and departments to address dynamic risks such as academic misconduct and contract cheating in the digital age (Davies & Al Sharefeen, 2022) is becoming a necessity. However, there is often some tension between professional and academic staff that threatens collaboration in academic institutions (C. Graham & Regan, 2016). In this context, ESRM adoption provides opportunities for more collaboration between academics and security practitioners in designing and implementing comprehensive security risk management approaches that promote the realisation of desired student outcomes (C. M. Graham, 2013).

However, the uptake of general risk management practices in universities has been rather slow and inconsistent, as shown in previous studies (Kageyama, 2014; Lundquist, 2015; Malki & Aldwais, 2019; Perera et al., 2020). The rarity of risk management applications in universities can be explained by the fact that these institutions have over and over again considered themselves a class of knowledge organisations with predominantly intangible asset bases that are not prone to security risks common to other businesses (Lundquist, 2015; Perera et al., 2020). This can help explain why university staff, in some cases, exhibit complacency and ambivalence in their responses to threats like student plagiarism as most have attitudes, perceptions, and beliefs that trivialise these risks (De Maio et al., 2020; Lynch et al., 2021), making them less of security issues for their institution. In other contexts, threats like plagiarism are taken seriously (Bermingham et al., 2010; Birks et al., 2020), although they continue to persist due to advancements in technologies, weak controls, and disconnect between academic staff and policy (De Maio et al., 2020). At the same time, risk management literature suggests that there are limited studies that examine the role of organisational factors in influencing universities to adopt risk management models (Edwards, 2012; Tamrat & Teferra, 2020). Since the higher education sector has become a hotbed of security risks (Lundquist, 2015; Tamrat & Teferra, 2020) and confronts the same risks as those in the corporate world, it would be useful to determine the factors that help them adopt innovative risk management models.

The current study is based on seven focused interviews with Chief Security Officers (CSOs) from larger public and private accredited universities (referred to hereafter as accredited universities) in Kenya, using Braun and Clarke's (2006) thematic analysis approach for data analysis. Accredited universities are an essential segment of Kenya's higher education sector, and according to the country's Commission for University Education [CUE] (2021), Kenya had 39 accredited public universities and 36 accredited private universities, as of December 2022. Like in most countries, accredited universities in Kenya are experiencing multiple security risks and ongoing reform (Maranga & Nelson, 2019; Njoroge et al., 2019). However, these universities are, to a great degree, latecomers in terms of adopting risk management models like ESRM (Amuya et al., 2023; Kiura & Mango, 2017). The mixture of risk pervasiveness, reform, and being late in implementing business-like risk management models makes accredited universities in Kenya a promising case for research on the antecedents of ESRM adoption. The focused interviews formed part of an extensive mixed-methods study of predictors of ESRM

adoption in Kenya's accredited universities, where we found that organisational characteristics are important catalysts of ESRM adoption (Amuya, 2023).

The study fills various gaps in the ESRM adoption literature. Firstly, based on perceptions of university security practitioners in Kenya, we will provide new evidence on the internal drivers of ESRM adoption in accredited universities. Previous contributions in this area have demonstrated that internal values, norms, and cultures, leadership, risk management committees, regulatory pressures, and calls for effective corporate governance are among the key drivers of risk management practice (e.g., De Maio et al., 2020; Dooley et al., 2013; Hommel et al., 2013; Lundquist, 2015; Lynch et al., 2021; Towers et al., 2010). However, in addition to their overreliance on data from developed countries and use of potentially insufficient measures, these previous studies did not examine the broader spectrum of what drives risk management adoption and institutionalisation in the context of ESRM (e.g., Christopher & Sarens, 2015; Edwards, 2012; Figueroa, 2016; Hommel et al., 2013; Lundquist, 2015). Secondly, it is an important addition to the few existing qualitative studies on security risk management in higher education, which are demanded by both practitioners and researchers to better understand the predictors of the ESRM adoption in accredited universities (Figueroa, 2016; Lundquist, 2015). Finally, our findings would enable university security professionals and decision-makers to develop more effective policies for ESRM adoption as they focus explicitly on organisational characteristics that ensure acceptance and consequent adoption of the framework.

Literature review

ESRM has been described as an innovation or a new philosophy in the academic risk management literature (Adekanye & Rahman, 2018; Pulido, 2021). According to Damanpour and Schneider (2006), an innovation refers to any new product, program, service, or process that an organisation adopts to improve its performance. Although there is substantive industry support for the ESRM innovation (ASIS International, 2019), there is only anecdotal evidence on the drivers of its adoption (Gill, 2021). There are only limited studies on ESRM adoption in reputable academic databases because the topic is fresh and empirical outcomes are still in the infantile phase (Kwateng et al., 2022). Nevertheless, there have been significant scholarly efforts to examine the drivers of general risk management adoption across universities globally. In Australia, for instance, studies have shown that organisational values, norms, and cultures, leadership, and the socio-political or external environments are critical to risk management adoption (De Maio et al., 2020; Dooley et al., 2013; Lynch et al., 2021; Towers et al., 2010). Another strand of research has examined the influence of the external environment, finding that Australian universities are adopting risk management and quality assurance policies and practices in response to periodic government reviews and regulatory requirements stipulated by the Australian Universities Quality Agency (Christopher & Sarens, 2015; Davies & Al Sharefeen, 2022; Edwards, 2012; Towers et al., 2010).

Similarly, in other countries like the US, England, South Africa, Malaysia, and Indonesia, researchers have also shown that universities are adopting varied risk management models due to the influence of the top management, the establishment of risk

management committees, human resource development practices, regulatory pressures, and calls for effective corporate governance (Huber, 2011; Lundquist, 2015, Sityata et al., 2021; Priyarsono et al., 2019; Malki & Aldwais, 2019; Figueroa, 2016; Hommel et al., 2013). In Kenya, the University Act No. 42 of 2012 mandated all universities to institute accountable stewardship of their resources and guarantee competent service provision to their stakeholders. As a result, some researchers have shown that, like elsewhere, most universities in Kenya have adopted some form of risk management models in response to regulatory pressure (Kiura & Mango, 2017; Njoroge et al., 2019). It has also been shown that at the organisational level, the presence of highly qualified and competent personnel, training sessions on risk management, and the advancement of management systems contribute to increased diffusion of risk management and performance among academic institutions in Kenya (Thuku, 2011).

Adoption is time and again complex on an organisational level, and it is challenging to advocate for change in routine practice when decision-makers within institutions do not see the need for changes (Damanpour & Schneider, 2006; Wisdom et al., 2014). According to Aarons et al. (2011), individuals in organisations may have difficulty knowing, weighing, or selecting appropriate innovations to solve particular problems, or their decision to adopt is often complicated by organisational factors such as leadership, culture, and values. Given the significance of the organisational environment in innovation adoption and the dearth of literature related to ESRM adoption in higher education, we explore the enablers of adoption of this strategy. In other words, what predicts ESRM adoption in Kenya's accredited universities? To answer this question, our study is based on overarching constructs of adoption of innovations developed by Wisdom et al. (2014) following their synthesis of 20 innovation adoption frameworks and theories. Wisdom et al. (2014) identified key characteristics likely to accelerate adoption of innovations in all organisational contexts, such as socio-political influence, organisational characteristics, innovation characteristics, staff/individual characteristics, and client characteristics. However, our focus in the present study is only on organisational characteristics as they exemplify the intersection of the environment and employees (Wisdom et al., 2014).

Organisational adoption of innovations

Innovation adoption frameworks have identified key organisational characteristics that influence adoption. One of the factors is an organisation's absorptive capacity, or an organisation's existing skills and knowledge that enable it to identify and implement new initiatives (Aarons et al., 2011; Greenhalgh et al., 2004). Another factor is organisational leadership and includes the CEO's influence, top management support, and leadership promotion of innovations (Aarons et al., 2011; Wisdom et al., 2014). Indirect and direct networking with innovation developers, professional associations, and consultants is another important organisational factor influencing adoption (Greenhalgh et al., 2004). Also, innovation adoption is driven by training readiness and efforts, and it includes organisational support for training, built-in methods for maintaining staff competence and performance, continuation of training, and communication about innovations (Aarons et al., 2011; Greenhalgh et al., 2004). Other factors include readiness for change or an organisation's self-perceived ability to undertake change; norms, values, and

cultures; operational size and structure; and social climate that includes social pressure to adopt (Aarons et al., 2011). Given the paucity of academic research explaining the factors affecting organisational adoption of ESRM adoption in universities, the present study adopts a contextual approach to highlight the organisational factors which might influence the diffusion of ESRM.

Methods

Recruitment and data collection

Our population of interest were the Chief Security Officers (CSOs) from the main campuses of larger public and private accredited universities in Kenya. Seeking subjective views from senior-level executives is a commonly embraced practice in top-notch higher education studies (e.g., De Maio et al., 2020; Lynch et al., 2021). Out of a total of 60 accredited universities in Kenya, a sample of 27 public and the 25 private were first selected using proportionate sampling (Out of 75 accredited public and private universities, 15 were excluded because they lacked defined security departments, and had relatively unsophisticated structures, fewer programs, and smaller student populations). Sampled accredited universities were then ranked according to the highest number of approved academic programs as reported by CUE (2018, 2020). The ranking of these accredited universities was also based on the highest budgetary allocation during the 2021–2022 financial year and the highest number of accredited university campuses. In risk management adoption literature, evidence shows that larger organisations have a high likelihood of engaging in risk management programs (e.g., See Anton & Nucu, 2020 for a full review). Based on this finding, the first five accredited universities in each category were selected purposively for the study, totalling to 10 public and private accredited universities. These universities were also selected on the basis that they had extensive risk management policies, and were implementing elements of ESRM, although they call it different things. Qualitative studies entail in-depth interviews or observations in social contexts, and as a result, qualitative researchers often sacrifice scope for detail. As Ochieng' and Jwan (2014) argue, these researchers do not focus on whether or not the sample size is large enough to be statistically representative of the whole population but on whether the selected sample provides access to sufficient data to enable them to address the research questions. This argument further justified our choice of a smaller sample size in the current study.

Data for the study was gathered based on focused interviews with the participants as part of the larger study on the predictors of ESRM adoption in Kenya's universities (Amuya, 2023). Research approval was obtained from Dedan Kimathi University of Technology's school of postgraduate studies and the National Commission for Science, Technology, and Innovation (NACOSTI) before conducting the interviews. Permission to collect data from security departments was also obtained from the research directorates in the sampled universities. All the 10 CSOs were visited and a total of seven, three from private and four from public accredited universities, were available to be interviewed. The interviews were conducted face to face with each interview lasting approximately 30 minutes. The interviews were recorded through note-taking and the questions

were based on a semi-structured guide. The current paper is based on two primary questions; (1) How would you describe the management of risks in your university? (2) What were the enabling organisational factors behind your university's adoption of ESRM or any of its elements?

Analysis

Braun and Clarke's (2006) thematic analysis approach was used for the analysis of data. The process involved transcribing the data, familiarising with it, coding it, and paraphrasing the participants' statements. After transcribing the data, we familiarised with it to make sense of it and made notes on initial thoughts while searching for patterns and meanings (Braun & Clarke, 2006). We then deleted unnecessary words and repetitions from the focused interview transcripts after developing a general idea of the themes that emerged from the data. The next step involved open coding, which entailed conceptualising and highlighting data deemed relevant to the study to generate codes. This was then followed by arranging data into broader categories, including "Organisational Leadership, 'Training Readiness and Efforts', and 'Security Governance' as they emerged. By the end of this process, we had developed satisfactory evidence of each theme using vivid examples from the data by way of narratives and verbatim. The outcome of the initial coding was later verified against the codes developed by an independent researcher before we reached a consensus regarding the final codes, thereby ensuring inter-rater reliability as recommended by Braun and Clarke (2006).

Results

The participants unanimously described ESRM adoption processes in their universities as largely documented and undergoing continuous improvement. They explained that given the nature of what accredited universities do, security policies are introduced slowly to ensure that they do not fall out of business due to budgetary implications. This is to mean that these universities, amid funding limitations, have other priorities that supersede those of security risk management. Also, a majority ($n = 5$) of the CSOs explained that their universities were just beginning to review their security risk management processes and design the correct terminology that will reflect all areas of risk that they face. The organisational factors described under Wisdom et al. (2014) overarching innovation adoption theory are partially represented by the current results as the participants only focused on three main predictors of adoption, including leadership, training and security governance. The responses from participants highlight the significance of these enabling factors and demonstrate the degree of importance these factors are given by CSOs. The results of the study are presented in the following section.

Organisational leadership

Five participants ($n = 5$) believed that the goodwill from the top management drove the decision to adopt ESRM in their universities. While projecting this point, a CSO in a private accredited university explained that 'the security department can only implement that which has been permitted by the top executives who approve budgets,

formulate some of the risk management policies, appoint members of the Security Council, supervise, monitor, and sometimes evaluate security programs' (Participant #04, personal interview, 12 April 2022). Other interviewees agreed that top executives in the university set the tone for ESRM adoption. Commenting on this, a CSO from a public university reflected:

> In my eight years of practice as a security professional in university settings, I have noticed that one goes nowhere in implementing any security project without the 'blessings' of those at the top. It is the top executives that can help my teams to deal with hurdles, encourage us to improve our practices, and demonstrate commitment to the work that the security department does. If I have to say objectively, commitment from my bosses is all that I need to deal with any kind of risk because this commitment gives me everything that I need to run this (security) department. (Participant #07, personal interview, May 11, 2022)

Participants unanimously associated commitment from the top with the development of a security risk management framework for ESRM implementation, involvement of university executives in ongoing security reviews, and leadership promotion of ESRM. In the words of a CSO from a public accredited university, 'we cannot fully embed risk management practices into the university's strategic activities, functions, and decision making without a detailed framework that we can work with to meet different expectations' (Participant #07, personal interview, 11 May 2022). A CSO from a private accredited university also acknowledged that the security department would be more comfortable that it is addressing the right risks if the top leaders were involved in initial and subsequent security reviews. He commented that 'I am more relieved when the management invites me to attend a meeting where the security needs of the university are being reviewed' (Participant #03, personal interview, 24 March 2022).

However, some CSOs, especially in private accredited universities, also expressed concerns that top executives can be a major barrier to the adoption of ESRM in their institutions. One of the CSOs recalled how the management deals with security officers in the university:

> My friend, it can be hard to deal with professors and doctors in academia because I think they always see security officers as messengers or mere watchmen. We are here just to receive directions without much questions. In fact, sometimes, they can ask me to recommend something, but it takes years to implement it. I have a phone in this office, and the only time it rings is when there is a problem or when they need security services. So, how do you serve as an equal partner in security risk management in such an environment? I think leadership commitment should begin by executives acknowledging the role of security in the university. (Participant #06, personal interview, April 06, 2022)

The consensus was that although top university executives may take security issues seriously, it is common for them to take long before implementing the recommendations made by security professionals in universities. One of the participants from a public university cited that in many instances, he had recommend to the university management that some students should be suspended for gross misconduct, such as academic dishonesty as captured by CCTV cameras, but these recommendations have repeatedly been ignored. Some participants ($n = 4$) implied that although risk management practices are at their universities' core, they have no say when it comes to implementation, especially when dealing with academic malpractice. Others ($n = 3$) suggested that while

top-level commitment to ESRM adoption is acknowledged in their universities, it is not included in mission statements. This can jeopardise ESRM adoption because the top management chooses what to commit to and what to ignore during strategic planning.

Training efforts

Participants ($n = 7$) unanimously agreed that the diffusion of ESRM processes in their institutions is driven by periodic and rigorous training. They admitted that universities cannot fully adopt ESRM and make it part of their culture without training. In the words of a CSO from a public accredited university, 'to introduce a security program is easy, but to make it the way of life in the university requires that people are trained on a continual basis' (Participant #02, personal interview, 20 April 2022). The same CSO explained the importance of training as follows:

> Once the university establishes a policy environment and defines key objectives in the area of security, there is little success that can be realised without training employees in the process aspects of the relevant risk management systems. We use training as a way of communication because we expect that our security and other employees understand what is exactly required of them. (Participant #02, personal interview, April 20, 2022)

Participants also specifically associated the existence of updated security risk management training programs and hiring and retraining of staff with ESRM adoption in their institutions. A CSO from a private accredited university viewed an up-to-date security risk management training program as a 'necessity that will enable the university to respond to changing needs, especially as student populations in the institution keep presenting unique challenges' (Participant #04, personal interview, 12 April 2022). Another CSO from a public university stressed the need to hire and retrain staff to improve their skills. While explaining this point, the same officer intimated:

> Implementing security risk management programs requires that we have competent employees who can lead the process. I believe that when we retrain security staff, we are just acknowledging the need for flexibility and adaptability as we strive to address insecurity issues in the university. For us, we have induction training for our staff whenever new policies are introduced, and we ensure that everyone knows what they are supposed to do. (Participant #07, personal interview, May 11, 2022)

Although CSOs unanimously stated that training plays a major role in driving ESRM adoption, they also pointed out that there are cases when university executives are reluctant to fund recommended training programs. Most participants ($n = 5$) indicated that not all employees could attend security awareness training, the management takes longer periods before approving training program, and that training programs are only explained on paper but rarely actualised in practise due to budgetary constraints. At the same time, six participants ($n = 6$) contended that most universities do not develop their training programs based on training needs assessment. While these institutions may provide training opportunities in the area of security, it remains questionable whether these programs are based on explicit training needs assessment. As a CSO from a private accredited university stated:

> I am hardly involved in designing these training programs, and I think it is a culture that dictates how things are done in this university. For example, I am not even involved in the hiring of employees. All I always see is a new employee working around the administration block. Now, how do I recommend security-related training for employees I did not even know how they were hired? My role here is sometimes similar to that of a mere messenger. (Participant #06, personal interview, April 06, 2022)

Security governance

Another factor that emerged from the analysis is associated with organisation's self-perceived ability to direct and steer innovation adoption initiatives. Some of the CSOs ($n = 4$) explained that there was an attempt among their universities to consider security during strategic and operational planning cycles and establish a Security Council that elevates security as one of the pertinent considerations during reviews and evaluations. While explaining the role of the Security Council, one of the CSOs in a public university explained that:

> The university has an active Security Council, which comprises stakeholders drawn from different departments and faculties. This Council partners with executive officials in the university to articulate goals, strategies, priorities and solutions that support the university's mission of teaching, research, and public service. (Participant #01, personal interview, March 10, 2022)

During stakeholder sessions, universities explicitly develop attainable, realistic, and measurable objectives aligned with their mission and objectives. Another CSO from a public accredited university shared this by explaining that:

> This university has a culture of reviewing its existing programs and data during Council meetings to identify the components of its risk management framework, collect information, and engage with key stakeholders on areas such as employment practices, academic misconduct, student life, strategic sourcing, and so on. As part of our governance at the department (security), we always work with all our risk managers from different campuses to solidify our efforts to engage in security governance effectively. (Participant #05, personal interview, April 18, 2022)

It also emerged that despite the existence of consultations among universities leaders and stakeholders in the Security Council to foster governance, the outcomes or recommendations made during such meetings are not always implemented, especially in private accredited universities, where CSOs were sceptical. A CSO from a private university explained that:

> Sometimes, our executive officials strive to create the impression that they fully understand their responsibility and accountability when it comes to security. But this effort is usually not genuine in my view. As a CSO, I can be fully engaged in decision making about security, but I mostly turn out to be a passive participant during board meetings. I always wonder if my views are considered because Board members seem to speak the same language and I have to implement what they recommend or meet their interests in some ways. (Participant #03, personal interview, March 24, 2022)

Such sentiments underscore that university leaders do not necessarily consider security as an important part of their governance responsibility and they believe that when it comes to governing security, CSOs are not persuasive enough. In the words of a CSO from a private accredited university, 'it is very difficult [for me as a CSO] to convince the

university management how security contributes to profits in the university. Quantifying the Return on Investment for security is always difficult' (Participant #06, personal interview, 6 April 2022).

Discussion

The role of university security professionals in assisting faculty and departments to address dynamic security risks has become a necessity. ESRM adoption provides opportunities for more collaboration between university leaders and security in designing and implementing comprehensive approaches to deal with changing security risks. In view of this significance, the present study attempted to identify organisational predictors of ESRM adoption in Kenya's accredited universities. Based on focused interviews with security executives in large accredited universities across Kenya, the results partially support the constructs advanced in the middle-range theory of innovation adoption developed by Wisdom et al. (2014).

The influence of the internal organisational context was supported by three major themes. The first one related to the leadership commitment and support for ESRM adoption in universities. Participants highlighted that the development of a security risk management framework for ESRM implementation, involvement of university executives in ongoing security reviews, leadership promotion of ESRM, and goodwill from the top management accelerated ESRM adoption in their universities. This finding is in line with previous literature which suggests that risk management programs in academic institutions can only be implemented subject to the presence of commitment from the management team (Lynch et al., 2021; Malki & Aldwais, 2019; Priyarsono et al., 2019).

However, while top-level commitment, participation, and support for ESRM adoption are acknowledged, they are not included in universities' mission statements, according to participants. This makes university executive commitment to ESRM adoption in Kenya's universities seem like a discretionary condition rather than a policy requirement. This is a challenge to ESRM adoption, considering that other department leaders, including CSOs, constantly look at the behaviours and actions of top leaders to determine whether they are compliant with the actions that support what may have been documented about the organisation's commitment to ESRM (Kageyama, 2014). Security professionals in the current study expressed concerns that senior universities leaders frequently treat them as 'messengers', a role that make them feel inferior. This finding is not surprising considering that C. Graham and Regan (2016) found evidence indicating that there are regularly some strained relations between professional and academic staff in universities. De Maio et al. (2020) also found that although there are procedures and policies in place to address academic misconduct, academic leaders often respond to this misconduct in ways that are inconsistent with the responses expected of them, painting a picture of lack of commitment to risk management practices among academic staff. Organisational commitment can only be meaningful if it is integrated into university, so that there is no room for staff discretion when it comes to risk management.

The second theme involved training initiatives and efforts in the area of security risk management. Participants underscored that the existence of a comprehensive security risk management training program and the hiring and retraining of staff are non-negotiable drivers of ESRM adoption. In their view, academic institutions cannot fully

adopt ESRM without the training of employees on its essential elements. This finding aligns with previous research on implementation of risk management which magnifies the significance of training and staff competency (Priyarsono et al., 2019; Thuku, 2011). Birks et al. (2020) found that greater consistency in policies and procedures, especially a focus on training for both students and staff, is key to addressing academic misconduct mutations that continue plaguing academic institutions globally. Staff and students training on security issues improves their understanding of their responsibilities, increases their awareness, and consequently fast-tracks the diffusion of risk management practices (Nnorom et al., 2020). Also, Dawson et al. (2019) found that training of markers, for instance, can improve their ability to identify contract cheating. On the other hand, it also emerged that university executives are often reluctant to fund recommended training programs, do not support the development of training programs based on training needs assessments, and do not commit enough resources for training. According to Schneller et al. (2022), the broader implementation of converged security management in organisations is often slow due to the lack of specific training available to practitioners.

Security governance emerged as the third key factor that is believed to be pivotal to promoting ESRM adoption in universities. In most universities, especially publicly accredited ones, the Security Council drives security governance by partnering with the strategic and operational planning committees and integrating security into internal processes and functions. This finding is consistent with those of Kageyama (2014) and Amuya et al. (2023), who underscored the need for establishing a cross-functional risk council or committee that discusses and addresses risk in universities. Along the similar lines, C. M. Graham (2013) found that pedagogical partnerships between professional staff and other stakeholders in the university are important for the implementation of programs and ultimate realisation of positive student outcomes. Priyarsono et al. (2019) also found that risk management adoption in IPB University increased significantly following the establishment of a risk management team consisting of lecturers from different faculties and departments.

However, CSOs also highlighted that the mere existence of consultations among university leaders and stakeholders through the Security Council does not necessarily mean that recommendations made during such meetings are consistently implemented. Even where university executives are fully engaged in decision-making about security, groupthink may impede the free flow of ideas. Given that CSOs indicated how they are often considered 'passive participants' in board meetings, we can project a situation where these professionals agree with whatever the highest-ranking individuals in the room say during these meetings. C. Graham and Regan (2016) found that professional workers in universities tend to feel undervalued by 'senior managers' as most university leaders often value university staff in academic roles when making strategic decisions.

Limitations

The present study was an attempt to gain insight into organisational features that drive ESRM adoption in accredited universities. Due to the exploratory nature of the study, the potential limitations warrant a discussion as they significantly affect the generalisability of results. Firstly, the sample was too small since the data was only collected from seven

larger public and public accredited universities. We addressed this limitation by purposely selecting public and private universities to reduce the noise associated with industry disparities. In another effort to avoid interference associated with fluctuating professional backgrounds, we chose respondents who had similar ranks in accredited universities. Secondly, the study gathered data from each university from a single respondent, the CSO from the main campus, whose views may not perfectly reflect what drives ESRM adoption in universities. While CSOs are key to strategic ERSM management, the rest of the stakeholders were not interviewed to triangulate the arguments given by these professionals. We minimised the effect of this limitation by targeting only senior-level officers with intimate knowledge of risk management adoption in their institutions. Finally, the sample consisted mainly of accredited universities located in Kenya's urban areas. Nevertheless, the study was qualitative and exploratory, and we believe that the findings will be useful in the design of future quantitative or mixed-methodology studies to target universities across geographical settings and test hypotheses.

Conclusion

Since ASIS International elevated ESRM into its strategic priority in 2016, professional security organisations and pundits are continually calling for the adoption of this management philosophy to help complex organisations like universities to deal with different security risks (M. Allen, 2019). However, drivers of ESRM adoption in accredited universities, especially at the organisational level, have not received scholarly attention. In the present study, we used the constructs within the middle-range theory of innovation adoption developed by Wisdom et al. (2014) to identify the organisational-level predictors of universities' adoption of ESRM.

Within the limitations of this study, we found that for universities, ESRM adoption effort is not won or lost at the tactical levels but at the strategic levels, where adoption decisions are often made. Without the unwavering support from the higher echelons of university management, CSOs lose the temerity to discuss ESRM adoption efforts with certainty. What is still needed is for top executives to 'walk the talk' by giving ESRM adoption the attention it deserves during the broader strategic planning process. But still, this cannot be possible if CSOs are still incapable of demonstrating the Return on Investment for ESRM to the executives. Furthermore, intensifying security risk management training efforts is a prerequisite for ESRM adoption in universities. In addition, exercising effective security governance can be effective in driving ESRM adoption. With active security councils, universities can craft effective security objectives, discuss security during planning cycles, and clarify the security-related responsibilities of all employees. Although our findings are based on a small sample, the three themes of organisational leadership, training, and security governance may be applicable outside Kenya's accredited universities that formed part of this study.

Further studies could improve upon the research design and elaborate the findings more. It would be beneficial to include more universities across Kenya to develop a more representative sample and gather varied perspectives across top management circles in different departments and faculties to gain a better understanding of the predictors of ESRM adoption. Including a sample of university officials at various organisational levels would help capture a more inclusive range of opinions regarding

ESRM adoption. Also, there is a potential that universities are confronted with the challenge of introducing the ESRM philosophy that is undeveloped for complex sectors into an institutional culture that is already sceptical of new management models and practices. In such a scenario, the rationale for examining ESRM adoption enablers is that the framework would potentially be a viable solution to the security risks that universities face today. To support this rationale and eventually convince higher education researchers and security professionals on the effectiveness of ESRM further, future studies need to evaluate the whole intervention, adoption process, properties, maturity level, and factors facilitated and/or hindered its implementation, and present, analyse, and discuss the findings. Finally, future studies could also consider other drivers of adoption according to innovation adoption framework, including socio-political influence, innovation characteristics, staff/individual characteristics, and client characteristics for a more panoramic understanding of the predictors of ESRM adoption in academia.

Acknowledgements

This article is part of the Master of Forensics and Security Management thesis at the Institute of Criminology, Forensics, and Security Management, Dedan Kimathi University, Kenya. Special thanks to all the thesis advisors from the university, including Dr. Consolata Ndung'u –Thuranira, for helpful feedback and guidance. Thanks also to the security executives that agreed to participate in this study.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Levis Omusugu Amuya http://orcid.org/0000-0002-0203-631X
Peterson Mwai Kariuki http://orcid.org/0000-0001-9282-6667

Declaration of conflicting interests

The authors declare no conflicts of interest in regard to research, authorship, and/or publication of this article.

References

Aarons, G.A., Hurlburt, M., & Horwitz, S. M. (2011). Advancing a conceptual model of evidence-based practice implementation in public service sectors. *Administration and Policy in Mental Health and Mental Health Services Research*, *38*(1), 4–23. doi:10.1007/s10488-010-0327-7

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. doi:10.5121/ijnsa.2018.10502

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

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. doi: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*. ASIS Online. https://www.asisonline.org/publications–resources/news/blog/esrm-an-enduring-security-risk-model/

American Society of Industrial Security [ASIS International]. (2010). *Enterprise security risk management: How great risks lead to great deeds (a benchmarking survey and white paper)*. The CSO Roundtable of ASIS International.

American Society of Industrial Security [ASIS International]. (2019). *Enterprise Security Risk Management Guideline*. American Society of Industrial Security. https://www.asisonline.org/publications–resources/standards–guidelines/esrm-guideline .

Amuya, L.O. (2023). *Predictors of Enterprise Security Risk Management adoption in accredited universities in Kenya* (Unpublished master's thesis). Dedan Kimathi University of Technology.

Amuya, L.O., Kariuki, P. M., & Thuranira, C. N. (2023). Influence of security governance on enterprise security risk management adoption in chartered universities in Kenya. *Kabarak Journal of Research & Innovation*, *13*(2), 15–27. https://ojs.kabarak.ac.ke/index.php/kjri/article/download/633/229

Anton, S.G., & Nucu, A. E. A. (2020). Enterprise risk management: A literature review and agenda for future research. *Journal of Risk and Financial Management*, *13*(11), 281. doi:10.3390/jrfm13110281

Bermingham, V., Watson, S., & Jones, M. (2010). Plagiarism in UK law schools: Is there a postcode lottery? *Assessment & Evaluation in Higher Education*, *35*(1), 1–14. doi:10.1080/02602930802471801

Birks, M., Mills, J., Allen, S., & Tee, S. (2020). Managing the mutations: Academic misconduct in Australia, New Zealand and the UK. *International Journal for Educational Integrity*, *16*(1), 1–15. doi:10.1007/s40979-020-00055-5

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

Christopher, J., & Sarens, G. (2015). Risk management: Its adoption in Australian public universities within an environment of change management–A management perspective. *Australian Accounting Review*, *25*(1), 2–12. doi:10.1111/auar.12057

Commission for University Education [CUE]. (2018). *Approved Academic Programs Offered in Chartered Universities in Kenya in Accordance with the Universities Act*. https://www.cue.or.ke/index.php?option=com_phocadownload&view=category&download=11:approved-academic-programmes-offered-universities-in-kenya-november-2018&id=12:general&Itemid=192

Commission for University Education [CUE]. (2021). *Universities Authorised to Operate in Kenya*. https://www.cue.or.ke/images/phocadownload/Accredited_Universities_Kenya_June2021.pdf

Damanpour, F., & Schneider, M. (2006). Phases of the adoption of innovation in organisations: Effects of environment, organisation and top managers 1. *British Journal of Management*, *17*(3), 215–236. doi:10.1111/j.1467-8551.2006.00498.x

Davies, A., & Al Sharefeen, R. (2022). Enhancing academic integrity in a UAE safety, security defence emergency management academy–the Covid-19 response and beyond. *International Journal for Educational Integrity*, *18*(1), 1–18. doi:10.1007/s40979-022-00110-3

Dawson, P., Sutherland-Smith, W., & Ricksen, M. (2019). Can software improve marker accuracy at detecting contract cheating? A pilot study of the Turnitin authorship investigate alpha. *Assessment & Evaluation in Higher Education*, *45*(4), 473–482. doi:10.1080/02602938.2019.1662884

De Maio, C., Dixon, K., & Yeo, S. (2020). Responding to student plagiarism in Western Australian universities: The disconnect between policy and academic staff. *Journal of Higher Education Policy & Management*, *42*(1), 102–116. doi:10.1080/1360080X.2019.1662927

Dooley, A., Wormell, P., & McCallum, P. (2013). The purpose and function of academic boards and senates in Australian universities. In *National Conference of Chairs of Academic Boards/*

Senates. Retrieved September 5, 2017. http://www.uws.edu.au/__data/assets/pdf_file/0006/710475/Purpose_and_Function_of_Academic_Boards_-_Final_-_March_2014.pdf

Downes, M. (2017). University scandal, reputation and governance. *International Journal for Educational Integrity*, *13*(1), 1–20. doi:10.1007/s40979-017-0019-0

Edwards, F. (2012). The evidence for a risk-based approach to Australian higher education regulation and quality assurance. *Journal of Higher Education Policy & Management*, *34*(3), 295–307. doi:10.1080/1360080X.2012.678725

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

Fraser, J.R., Quail, R., & Simkins, B. (Eds.). (2021). *Enterprise risk management: Today's leading research and best practices for tomorrow's executives*. John Wiley & Sons.

Gill, M. (2021, January 19). *Enterprise Security Risk Management (ESRM); the Holy Grail or a Concept Found Wanting?* Outstanding Security Performance Awards. https://theospas.com/enterprise-security-risk-management-esrm-the-holy-grail-or-a-concept-found-wanting/

Graham, C., & Regan, J. A. (2016). Exploring the contribution of professional staff to student outcomes: A comparative study of Australian and UK case studies. *Journal of Higher Education Policy & Management*, *38*(6), 595–609. doi:10.1080/1360080X.2016.1211935

Graham, C.M. (2013). *Pedagogical partnerships and professionalisation: Changing work and identities of professional staff at one Australian university* (Doctoral dissertation). University of Technology Sydney

Greenhalgh, T., Robert, G., Macfarlane, F., Bate, P., & Kyriakidou, O. (2004). Diffusion of innovations in service organisations: Systematic review and recommendations. *The Milbank Quarterly*, *82*(4), 581–629. doi:10.1111/j.0887-378X.2004.00325.x

Hommel, U., King, R., & Thomas, H. (2013). The emergence of risk-based regulation in higher education: Relevance for entrepreneurial risk taking by business schools. *Journal of Management Development*, *32*(5), 537–547. doi:10.1108/02621711311328309

Huber, M. (2011). The Risk University: Risk identification at higher education institutions in England. In *Centre for analysis of risk and regulation*. London School of Economics and Political Science. http://eprints.lse.ac.uk/38891/1/The_risk_university_Risk_identification_at_higher_education_institutions_in_England.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

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 and Computer Security*, *30*(3), 422–451. doi: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

Lynch, J., Salamonson, Y., Glew, P., & Ramjan, L. M. (2021). "I'm not an investigator and I'm not a police officer"-a faculty's view on academic integrity in an undergraduate nursing degree. *International Journal for Educational Integrity*, *17*(1), 1–14. doi:10.1007/s40979-021-00086-6

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. doi:10.33423/jabe.v21i9.2684

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. https://ijcsn.

org/IJCSN-2019/8-4/Emerging-Issues-in-Cyber-Security-for-Institutions-of-Higher-Education.pdf

Njoroge, P., Ogalo, J., & Ratemo, C. M. (2019). A framework for effective information security risk management in Kenyan public universities. *International Journal of Social Sciences and Information Technology*, *4*(10), 1–19. https://www.ijssit.com/main/wp-content/uploads/2019/10/Framework-For-Effective-Information-Security-Risk-Management-In-Kenyan-Public-Universities.pdf

Nnorom, S.U., Ezenwagu, S., & Nwankwo, B. C. (2020). Security management practices in the 21st century for improved university administration. *IEEESEM Publications*, *8*(7), 1–14. https://www.ieeesem.com/researchpaper/SECURITY_MANAGEMENT_PRACTICES_IN_THE_21ST_CENTURY_FOR_IMPROVED_UNIVERSITY_ADMINISTRATION.pdf

Ochieng', O.C., & Jwan, J. O. (2014). The qualitative approach as a viable option in social science research in Kenya. *IOSR Journal of Humanities & Social Science (IOSR-JHSS)*, *19*(12), 64–74. doi:10.9790/0837-191246474

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

Omanga, D. (2017). *Shocking reality of Kenyan universities on the brink of collapse*. The Standard. https://www.standardmedia.co.ke/article/2001280952/shocking-reality-of-kenyan-universities-on-the-brink-of-collapse

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 & Research*, *8*(10), 155–172. https://www.ijern.com/journal/2020/October-2020/14.pdf

Petruzzi, J., & Loyear, R. (2016). Improving organisational resilience through enterprise security risk management. *Journal of Business Continuity & Emergency Planning*, *10*(1), 44–56.

Priyarsono, D.S., Widhiani, A. P., & Sari, D. L. (2019, August). Starting the implementation of risk management in a higher education institution: The case of IPB University. *IOP Conference Series: Materials Science & Engineering*, *598*(1), 012107. IOP Publishing. doi:10.1088/1757-899X/598/1/012107

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

Ramirez, F.O., & Christensen, T. (2013). The formalisation of the university: Rules, roots, and routes. *Higher Education*, *65*(6), 695–708. doi:10.1007/s10734-012-9571-y

Schneller, L., Porter, C. N., & Wakefield, A. (2022). Implementing converged security risk management: Drivers, barriers, and facilitators. *Security Journal*, *36*(2), 1–17. doi:10.1057/s41284-022-00341-6

Tamrat, W., & Teferra, D. (2020). Private higher education in Ethiopia: Risks, stakes and stocks. *Studies in Higher Education*, *45*(3), 677–691. doi:10.1080/03075079.2019.1582010

Thuku, M.K. (2011). *Relationship between risk management practices and organisational performance of universities in Kenya*. (Unpublished master's thesis). University of Nairobi.

Towers, S., Alderman, S. N., & McLean, S. V. (2010). A risk based approach to course quality assurance. In *Proceedings of AuQF 2010 Quality in Uncertain Times*. AUQA Occasional Publication Series. https://eprints.usq.edu.au/43358/8/risk%20based%20approach.pdf.

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. doi:10.1007/s10488-013-0486-4