WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Metric Scale-Based Assessment Framework for Risks Categorization and Associated Harm for LMS in Public Universities of Kenya.

Kiplimo Jacob,*Mburu Samuel, *Muriuki Janerose

School of Health Sciences, Kirinyaga University

1.1 ABSTRACT

The development and rapid adoption of e-learning by public universities in Kenyan has been one of the information and communication technology's (ICT) applications success stories. The COVID-19 pandemic crisis with its associated disruptions highlighted the significance and necessity of embracing technology in education such as the e-learning. As a result, the higher education especially the public universities in Kenya has undergone significant changes in terms of the learning approaches and management in recent years. However, the rapid growth in e-learning approaches in the public universities, has not come without risks. Like any other internet-based systems anywhere in the world, the learning management systems (LMS) used in the Kenyan public universities are prone to cybercrimes such as hackers' attack. Hence, given the inherently insecure internet, which is the backbone for the LMS, there is an urgent need for effective risk intervention, mitigation measures as well as fool-proof tools for not only their assessment and management, but also ensure secure and safe to use systems. The main goal of this study was to develop a metric scale-based assessment framework for the risks, related harms associated with the LMS of the public universities in Kenya. This framework was based on the identified most common risks and harms to the LMS. Using a cross-sectional survey, the researcher collected both quantitative and qualitative data, for the purpose. Consequently, appropriate quantitative and qualitative methods as well as tools were used to collect the required data. The obtained data was analyzed using quantitative methods such as descriptive and inferential statistics, as well as qualitative interpretive analysis e.g. thematic analysis. Importantly, this study identified the skills gap, human error, poor infrastructure, technology challenges and lack of safeguards as the most common risks to the LMS of the studied public universities in Kenya. Of essence, among the most common risks identified by this study, poor infrastructure and technology challenges had the most influence on the harm caused by the risks to the LMS. The ultimate results of this study was a comprehensive framework for risk assessment and management, which may be used for not only LMS, but also as an important forensic investigation tool, by other stakeholders. More importantly, the findings from this study and framework tool might have a direct impact on the current practice of forensic investigations and LMS risks management by not only changing our current knowledge of cybercrimes, but also how it has evolved.

Keywords*: *Learning Management System (LMS), E-Learning, Risks and Harms to LMS, Risk Assessment Framework.

1.2 Background to the Study.

The popularity and use of the computer networks and internet have increased over the years hence giving stakeholders more possibilities to get access to information, education, and other digital resources in order to improve our professional and personal lives at any convenient time in place. The biggest beneficiary of this technology has been the education system. It has become very important in classroom teaching, the concept of anywhere, anytime, encourages life-long learning and limits the challenge of distance [1].

However, digital resources have come with not only a lot of advantages but also their own challenges, such as the security of personal. According to a report by the Communication Authority of Kenya (CAK) [2], there has been a sharp rise in cybercrimes due to the crucial role played by ICT in the mitigation of COVID-19 pandemic crisis and associated disruptions. Hence, it is important to protect the integrity of the system, availability and confidentiality of personal data, against this threat [3].

The security of the LMS is important because a risk can dramatically lead to loss of crucial data. Additionally, the hacking of an LMS may totally prevent any learning taking place [4]. Although, various research and studies have been done previously to identify the risks and threats associated with LMS by researchers and scholars, the most common risks have not been clearly delineated or fully identified. Likewise, the few studies that have identified the risks associated with LMS have not been able to categorize them based on the extent of harm they can cause to the systems.

For that reason, the identification, categorization of the risks associated with the LMS and a metric score based assessment framework is an essential tool for interested stakeholders such as forensic investigators of systems such as the LMS. It is an essential tool for identifying risks and threats of their LMS, for the management and system administrators of the institutions of higher learning using LMS for teaching purposes in their systems. This way, they can take appropriate action depending on the level of risk and extent of harm they have encountered. Therefore, with corrective measures taken after the level of risk has been identified, the data of participants using the LMS is secured.

The LMS is a software which has brought a revolution on e-learning in the modern world with the advancement of technology [5]. The Kenyan institutions of learning have made tremendous steps in achieving the use of LMS for academic purpose. But new reports and evidence from researchers and academic institution using the LMS suggests that they are prone to various threats and risks associated with their use [6].

This study aimed to investigate the risks facing the LMS of public universities in Kenya, the associated factors and develop a metric-scale based assessment framework as a forensic tool for risk categorization, based on the extent of harm they are capable of. This tool will enable forensic investigators and the other interested stakeholders using LMS such as institutions of higher learning, system administrators, lecturers and students to easily identify this risks and the category they belong to.

1.3 The Scope of the Study.

This study is a mixed method type of research that used interviews, extensive literature review and questionnaires to collect the required primary and secondary data. Due to the number and wide geographical distribution of the universities in Kenya, this study was carried out only in randomly selected public universities. The respondents of the research were limited to the system administrators managing the LMS in the selected universities. Since, the aim was to identify risks facing the LMS, develop a metric scale-based assessment framework for easy identification and categorization of risks, the study identified six key specific variables on which to obtain information.

1.4 The General Objective of the Study.

The main objective of this study was to investigate the most common risks and extent of their harm to LMS of public universities in Kenya for developing a metric scale-based assessment framework as a forensic tool for their categorization.

1.4.1 The Specific Aims.

1. To identify the most common risks facing LMS of public universities in Kenya and the extent of harm they cause.
2. To examine the determinants or associated factors for the identified risks facing the LMS of public universities in Kenya.
3. To develop a metric scale-based assessment framework for categorization of the identified risks to the LMS, that can also be used a forensic investigation tool.

1.5 The Research Questions of the Study.

1. What are the major risks facing LMS of public universities in Kenya and the extent of harm they cause?
2. What are the determinants or associated factors for the risks to LMS of public universities in Kenya and the extent of harm?
3. What are the current assessment frameworks being used for risk and extent of harm categorization for LMS of public universities in Kenya, if at all, and how do they work?

According to the published literature, ICT was acknowledged as the primary delivery system for e-learning in the Government of Kenya Sessional Paper on Policy Framework for Education and Training from June, 2012, Kibuku et al [7]). Furthermore, the implementation of e-learning requires a thriving ICT infrastructure, which Kenya's lacks terribly. However, when it comes to essential ICT infrastructure and internet connectivity, which averages 69% between urban and rural areas, the country is characterized by a significant digital divide [8]. Hence infrastructure as a risk has not been categorized by the paper.

Online learning relies on the internet to be carried out because it is an Internet-based learning approach [9]. On the other hand, there are a lot of criminal activities and security risks occurring online. As a result, the environment for online learning is invariably subject to ongoing security issues, attacks, and threats. Unfortunately, without careful preparation and without a complete grasp of the security issues of online learning such as identifying the risks and categorizing them, institutions may not achieve their goal of using the internet to improve and make learning easy. Therefore, identifying risks such as skills gap and categorizing them will enable the institutions to carry out secure online learning. Likewise, cybercrime investigators will also easily identify this risk when reported to them.

From the empirical review and critiquing of the published literature, a number of key gaps in current knowledge and research have been identified. These include;

- Inadequate or total lack of local studies of the most common risks, associated harms to LMS as majority of studies were done in Europe, Asia, or America.
- Inadequate or total lack of studies focusing on the evolution of cybercrimes especially post COVID-19 pandemic.
- Lack of enough studies focusing on the increased adoption of technology such as online learning on LMS and the impact on cybercrime.

- Lack of comprehensive assessment frameworks specifically designed for risks and associated harms to LMS for public universities in Kenya.

It is against the background of the aforementioned gas that motivated the researcher to develop and conduct this study, to delineate clearly this issues.

2.1 Materials and Method

This study applied a hybrid research design of cross-sectional survey, that combined cross-sectional and survey designs. A hybrid research is a design that combines very specific elements and procedures of two or more different designs to harness the strength of both. Thus, the design may use both quantitative and qualitative types of research to enrich, the overall study. In particular, the cross-sectional survey design was chosen for this study since it enabled the researcher to measure multiple explanatory factors and outcome variables, such as the frequencies of various observations comprising risks, and harm to the LMS, simultaneously at that particular single point in time, using just a cross-section of the target population. This information was the building blocks required for development of the risk assessment framework. Though primarily qualitative, the strengths of surveys including ability to study the participants in their natural environment such as work places and to work with both quantitative as well as qualitative data was what this study required. Subsequently, a semi-quantitative survey integrated with the cross sectional study and used to collect both numerical, categorical and qualitative data.

2.2 The Target Population.

The target populations of this study was public universities' staff, working in the ICT departments such as the system administrators and analysts. This population was chosen because they were the ones dealing with day to day running and management of the LMS. Hence, they were the most informative when it came to matters of the LMS, such as handling all online learning activities in a university including; coordinating and overseeing the installation, administration, upkeep, and support of new and existing servers, networks, and systems. They were also involved in the setting up, installation, management of the institution's network, systems and software, e.g. LMS analysis as well as administration. They are also tasked with setting up and keeping up a system for data and program file backups. In addition, they maintain network integrity by regularly updating network system security to offer the most up-to-date defense against viruses and other kinds of network vulnerabilities. The target population of this study also included the system administrators and IT managers. This is because they were the ones tasked with running day-to-day system administration and management. Hence, they had a bigger role in managing the LMS. Finally, a few key informants' interviewees from the directorate of criminal investigation (DCI), working in cybercrime investigation were also included.

Given that there were only 26 fully fledged public universities, in Kenya according to the Kenya Universities and Colleges Central Placement Service (KUCCPS) website, these were the only ones included in this study. The universities are widely distributed across all the regions in Kenya. The study used the list of all the public universities as the sampling frame to select a sample for the research among the 26 fully fledged public universities. The lists of the staff working in the selected public university's ICT departments were used as the sample units. Apart from the public universities ICT staff, the researcher also interviewed a few selected forensic investigation experts from the police service as key informants.

2.3 The Sampling Technique.

A simple random sampling technique was used to select participants of the cross-sectional study. This was to allow generalization to the wider population. However, given that only a small sample was required for qualitative study due to the detailed and intensive interpretative analysis involved, purposeful sampling was used to select the key informants. Subsequently, 15 key informants with characteristics relevant to the study and to the wider population, were selected for interviewing. The study's selected sample was intended to be a fair reflection of the wider population. Apparently, sampling mistake is reported to occur when, for any reason, the selected study's sample does not accurately reflect the population [10].

2.4 Eligibility Criteria.

Only public universities and staff working in ICT departments of the selected universities were recruited to participate in this study. All other learning institutions including private universities and staff working in other departments apart from ICT will be excluded from participating in the study.

2.5 Ethical Consideration.

For both the quantitative and qualitative phases of data collection, the researcher obtained an informed consent form from each participant before being allowed to participate in the study. This was after explaining to them how their rights to anonymity, confidentiality of the information they would give would be guaranteed, any potential or fore seen risk (if at all) and any benefits of participating in the study. The informed consent form also contained full information about the research, contact addresses, the objective of the study, the role they were going to play throughout the research, their right to withdraw at any time, not to answer any question they did not want to, and that they were not going to be coerced or forced to participate.

2.6 Collection of Evidence on Common Risks.

To begin with, a very extensive preliminary research involving the search and review of relevant documents as well as published literature was done using "academic research databases". This was to establish the theoretical framework for the study by identifying key study variables, concepts and relationships, important in explaining the problem being addressed. Consequently, the academic research databases searched for relevant articles included; open access journals, sage journals, Google Scholar, University of Chicago Press, etc. The preliminary literature review was with reference to the study objectives and asked research questions about risks as well as harms associated with LMS. In addition, a review of relevant documents such as the ISO 9001: 2015 standards, quality management systems (QMS) manuals was conducted to summarize and synthesis information on risk-based thinking, risk assessment and management.

Thereafter, survey method using a structured closed-ended questionnaire was used to collect quantitative data on the most common risks and associated harms to LMS. Hence, to obtain required information on these variables the questionnaires were self-administered to LMS system administrators and ICT managers from the selected public universities in Kenya learning. These were required to fill the questionnaires to provide the required information on the most common risks they have come across related to the LMS in their institutions. Thereafter, structured interview schedule was used to collect qualitative data by interviewing a few key informants who were thought to be the most accessible and willing to participate. A total of 15 key informants were selected from the directorate of criminal investigation (DCI), headquarters, in Nairobi, Kenya. The key informants were deemed to be experts in the subject area (forensic investigation) and the most informative. As such, triangulation of the data by collecting information on same issues using different methods was used to not only improve the validity of the findings, but also to enrich the study.

2.7 Development of Risk Profile.

The data about the most common risks to LMS and their consequences were collected using questionnaires, extracted, analyzed using descriptive statistics and summarized using frequency tables. The identified risks to LMS were ranked according to the likelihood of their occurrence, the results of which are summarized in Tables 4.2. and 4.3. To enrich the study, qualitative data on the same was collected though interviewing of the selected key informants. Likewise, this was organized and summarized using summary table of themes as well as sub-themes, as shown in Table 4.4. The qualitative data was analyzed using thematic analysis and presented according to the consolidated criteria for reporting qualitative research (COREQ) checklist [11]. The final results were used to develop risk profile indicating the most common risks and the severity of their consequences on the LMS.

2.8 Development of a Metric Scale-based Assessment Framework.

This research used structured semi closed-ended questionnaires and interviews of key informants using open-ended interview schedule to collect both quantitative and qualitative data that was used in the development of the assessment framework. Using a 5–point Likert scale, a list of the identified risks ranked from the highest to lowest based on their frequencies (percentages). The levels of this scale were denoted by degree adjectives like "highly likely", "very highly likely", etc. The Likert scale was selected for use in this study because it is frequently used in research to express participants' thoughts and attitudes toward a topic or subject matter. Although there are different kinds of rating scales to assess opinions, it uses questionnaires, which are frequently used interchangeably with a rating scale. Hence, to rank people's opinions of things, events, or other people from low to high or from bad to good, Likert Scales are utilized. A scale is a continuum with extremes at the highest and lowest points and middle points in between [12].

2.9 Sampling Methods and Procedure.

Given that all full-fledged public universities in Kenya were only 32 in number, the "Census Approach" was used to determine the sample size. Therefore, all the 32 universities were included in the study. However, due to the wide geographical distribution of the 32 fully fledged universities only 12 could be accessed for studying. The sampling approach is the one in which only a small number of the population's representative objects are chosen, and data are gathered from them. You choose a sample rather than gathering data for and from all the population units. Assuming each of the 12 universities had 10 ICT staff, a total study population of 120 was assumed. And since the researcher wanted to achieve a response rate of at least 60%, a sample size of at least 72 was required. In total 91 questionnaires were available for analysis which translated into a response rate of 75.5%, good enough to avoid the issues of low response or non- response bias.

2.10 Study Tools and Instruments.

This study therefore used structured closed-ended questionnaires, open-ended interview schedules and the researcher's field notebook to collect both quantitative and qualitative data. The questionnaires were carefully designed, structured into different sections with a mixture of questions and statements using a yes/no answer questions and questions or statements with a 4-point Likert and rating scales for measuring the opinions of the respondents such as "strongly disagree", "disagree", "agree", and "strongly agree", "adequate", "very adequate", "inadequate", "very inadequate", "likely", "highly likely", "unlikely", "highly unlikely", "low", "moderate", "high rates", etc.

This study required information from participants such as demographic data e.g. age, name, education level, sex and employment status. The level of rank in their occupation was also be sought since senior system administrators have more access to university systems compared to junior system administrators. To design the study tools, operational definitions of the new variables was done. Consequently, risk was defined as uncertainty about how

an action will affect or implicate something that people value, frequently focused on unfavorable, unpleasant outcomes while harm is the unfavorable outcome of a threat being realized [13]. The likelihood of the risks and harms occurring was assessed using 3 point Likert scale such as "very rare", "rare" and "common". Likewise, a 5-point scale was used to assess the impact of identified risks on the LMS such as "Insignificant", "low", "moderate", high, "disastrous". Hence, the operationalizing of the variables enabled the designing of study tools to collect adequate and exhaustive information and had more insight on the various risks as well as technology. Similarly, specific information related to the study variables was obtained from the study participants.

2.11 Study Validity

The reliability of a research study's findings in predicting actual outcomes among people who behave similarly outside of the actual study is referred to as validity [14]. In a nutshell, quantitative study validity is about the accuracy/truthfulness and generalizability of the results. In contrast, qualitative study validity relates to honesty and genuineness of the data as accurate as well as true representative of the problem. The level of assurance that the causal relationship under test is reliable and unaffected by other variables or factors is known as internal validity. On the other hand, the degree to which research findings can be extrapolated (generalized) to different contexts, settings, populations, or events is referred to as external validity [15]. This study validated the results by discussing the findings in the context of other previous similar studies, respondents' validation by revisiting some selected key informants after data analysis, for their feedback.

2.12 Validity and Reliability Testing of the Study Tools.

The designed study tools were pretested to a few participants and the feedback used to update them. The Cronbach's alpha coefficient was used to test the internal consistency of the study items/elements and a value of at least 0.7 used as the ideal. Other methods of ensuring validity and reliability for qualitative data included the use of theoretical sampling, respondent validation, triangulation, constant comparison of codes and themes. The inclusion of a contradicting evidence/deviant case evidence or an extreme response was also done. The qualitative data was collected until saturation point and exhaustion of the interview schedule were reached.

2.13 The Extraction of Data.

The required information from the reviewed research articles, documents and questionnaires were extracted and recorded manually in the notebook or in an excel spreadsheet.

3.0 Data Collection Organization, Processing and Analysis.

The study obtained data collection authorization from the school of health science of Kirinyaga university, license from national commission for science, technology and innovations (NACOSTI, Kenya) and ethical approval from the ethics and research committee (ERC) of Kabianga University. Thereafter, the selected participants were called by the researcher to request for an interview, upon which they were granted, a date was scheduled. At the beginning of every interview, the purpose and the terms of the interview were explained and the letter of informed consent presented to the participants. The responses were organized into a table format, and coded manually (sorting, categorization and theme identification). The quantitative data was cleaned and the categorical data coded by assigning it numerical values, for the subsequent statistical analysis. In contrast, the qualitative data was coded using qualitative coding methods for the interpretive qualitative analysis. To code the qualitative data, after data familiarization through multiple reading and review of the textual extracts, based on the study objectives the relevant section of the text was identified, highlighted and labeled. A posterior, deductive hybrid coding methods combining both descriptive and process coding techniques were used to assign the codes. The initial codes were then sorted and categorized to reduce them into a number of emerging themes. A third coding stage or theming was used to develop sub-themes and to link them to the posterior codes.

This study used both descriptive statistics to describe the data and inferential statistics to determine any significant associations between the explanatory variables and the outcome. The IBM SPSS statistical software version 26.0 was used for the statistical analysis. Specifically, descriptive statistics was used to determine the frequencies of the most common risks and associated harms to LMS. The chi-square test was used for determination of significant associations between among, and between the independent and dependent variables. Summary statistics were used to summarize and present the quantitative data. Likewise, summary tables of themes/sub-themes were used to summarize and present qualitative data. By utilizing numerous analytical techniques, it aids in the creation of population-level generalizations. Many different sampling procedures are employed in order to select random samples that accurately represent the population [17].

According to the words of Thompson [16], "better honor the reality to which the researcher is ostensibly trying to generalize" which explains why multivariate methods like the multiple regression analysis has gained more respect. It is against this background, the multinomial logistic regression analysis (MLRA) for multinomial associations of variables adjusted for confounding effect, was used to determine the among the identified risks, which was contributing most to the harms to the LMS in this study. The "main effects" method, stepwise, single rule entry method to automatically chose each predictor at a time was used to model to model multinomial outcome variable where the log odds of the outcomes were modeled as a linear combination of the predictor variables. The model fitting information of the -2 log likelihood difference of the final model (chi-square value) and statistical significance was used to determine the "goodness of fitting" of data of the model. The β and Expo(β) value and associated 95% lower and upper confidence intervals

were used to interpret the results of the MLRA. The MLRA was chosen because of its strength to select for inclusion only those variables contributing a certain amount to the outcome. Thus, eliminating the need for model diagnostics and assumption checking.

For qualitative analysis, this study used the versatile thematic analysis as the technique for analyzing the data and interpreting the qualitative results. It was used to identify themes or chunks of similar ideas or the most common ideas that are the broad groups of data that are shared by many participants. Both quantitative and qualitative analysis were integrated and interpreted simultaneously.

3.1 Data Summarization and Presentation.

The quantitative analysis results were presented using summary tables of frequencies. The results of qualitative analysis were summarized and resent using summary tables of themes and sub-themes. The quantitative, qualitative findings and feedbacks from respondent validation were used to inform as well as guide the development of the risk assessment framework. The resultant risk assessment framework was summarized and presented in a schematic diagram or figure as shown in Figure 4.1. This study specifically adopted the approach of Hadullo et al [18] to develop the risk assessment framework. Some of the benefit of employing metric scales to develop an assessment framework includes making them more accurate and dependable when it comes to measuring the underlying theme they were intend to evaluate [19]. However, scale development requires a significant amount of work and study [20]. In particular, the pre-testing of the questions, conducting the survey, lowering the number of tools' items, and determining how many aspects the scale captures are all steps in the scale-construction process.

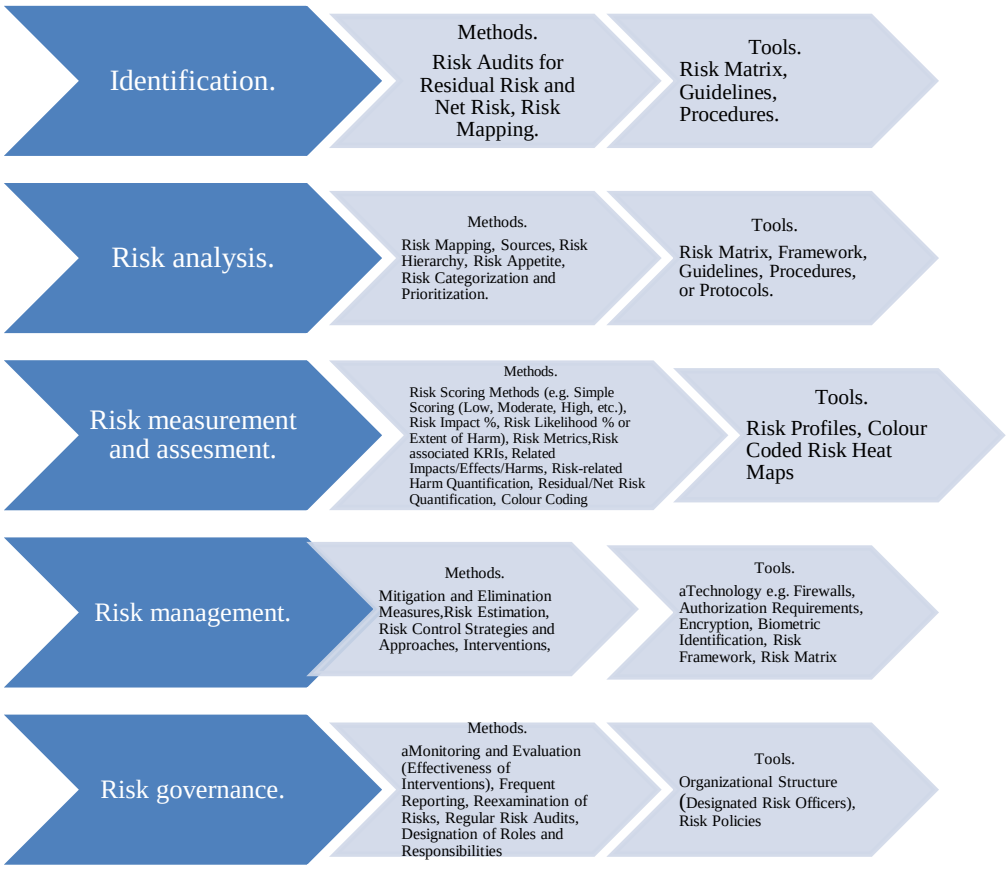
Table 4.3: LMS Risks Profile.

Risks	**Likelihood/Probability (%)**	**Impact/Associated Risk**	
Lack of safeguards	25.3%	Low likelihood.	
Skills gap	51.7%	Moderately likely.	
Technology challenge	39.6%	Moderately likely.	
Poor infrastructure	41.8%	Moderately likely.	
Human error	42.9%	Moderately likely.	
Harm	57.7%	Moderately likely.	

Table 4.4: LMS Risk Associated Harms Profile

Harms	**Consequences**				
	Insignificant	**Minor**	**Moderate**	**Major**	**Disastrous**
Lack of safeguards	★				
Skills gap				★	
Technology			★		
Poor infrastructure				★	
Human error			★		
Harm					★

Figure 4.1: Proposed risk assessment framework.



3.2 Results and Discussion

The Table 4.1 summarizes the characteristics of the 15 participants who were selected from the DCI headquarters, cybercrime department for key informants' interview. The key informants were selected based on the following factors; since they were forensic investigators, also dealing with cybercrimes, and based on their characteristics that was relevant not just to this study, but also to the wider population. In particular, the key informants comprised of 9 males and 5 females with an average age of 36.9 (±6.8), had training in ICT, computer science, software engineering, data science, cyber security, etc. Generally, these are the trainings you will find in the staff working in the ICT departments, and thus dealing with the LMS in the public universities in Kenya. The context of this study and the aforementioned aspects are crucial for the transferability of the findings from this study to other settings as well as to the wider population.

Likewise, Table 4.2, is a summary of the most common risks to LMS identified in this study. According the Table 4.2, the risks facing the LMS varied in their frequency in the following order; skill gap 51.7%, poor infrastructure 41.8%, human error 42.9%, technology challenge 39.6%, harm 57.7% and lack of safeguards at 25.3%. Chi-square analysis was carried out among the variables and contributed to the model with skill gap with of Beta (-21.082) and significance (<0.01). The multinomial logistic regression analysis (MLRA) identified among the identified most common risks to LMS, only 2 variables as having the most influence on the harm. In other words, the 2 were the most important contributors to the harm to the LMS and included; poor infrastructure (β = 18.605) as well as technology challenges (β = -14.983). Additionally, Table 4.3 is a summary of the consequences of the identified risks associated harm to the LMS. The Table 4.3. summarizes the consequences of the harm associated from the identified risks. Overall, the harm was rated as "disastrous", implying that suitable mitigation measures were required. As for specific risks, the consequences of skills gap and poor infrastructure on LMS were rated as "major", while, technology and human error were rated as "moderate". Surprisingly, the consequences from the risks of lack of safeguards for LMS Was insignificant.

The participants responded well to the interview and made various comments and suggestions in reference to risks of LMS. Based on the study objectives, the interview responses were coded into three main and several sub-themes. Notably, two emergent themes of "increased cybercrimes" and "evolution of cybercrimes" were identified. The results of the thematic analysis, with associated relevant direct quotes have been summarized in the Table 4.4. To choose the relevant direct quotes for the Table 4.4, the most illustrative and representative participants quotes of the findings related to a theme or a sub-theme, were selected. The interviewees acknowledged not only the rise of cybercrimes in Kenya, but also how it has affected all sectors including academic institutions. They reported that cases from institutions of higher learning such as universities had risen tremendously especially during the COVID-19 pandemic. Notably, this was a period when most of the institutions adopted online learning so as to comply with health restrictions such as

lock-downs and regulations. The key informants also indicated that loss of data, manipulation of information and poor performance of the systems supporting online learning were some of their findings in their investigations. The hitherto mentioned findings were linked to factors such as technology, lack of awareness and lack of comprehensive framework to manage the risks of occurrence of such crimes.

The Figure 4.1 is schematic diagram of the proposed risk assessment framework (RAF) and its workings. It indicates a step by step processes, methods and procedures to be followed as well as the tools to be used on how to not only identify, analyze, measure and assess risks, but also to manage them, govern, monitor as well as evaluate effectiveness of the risk mitigation interventions. In summary, essentially it is an "all in one" framework on how handle risks when encountered. The first step is to identify the risk through finding, recognizing and describing risks, checking for threats and security breaches such as loss of data and change of passwords, risk management plans, audits etc. The second step is analysis by mapping of the events constituting risks, risk through determining sources, their potential consequences and areas of impacts. The third step is measurement and assessment of the risk by determining the level of risk, extent of damages and likelihood of occurrence using the composite risk indices (CRI) for risk quantification. The fourth step is the risk management, through a risk management plan, risk treatment plan, security controls and risk evaluation as well as prescription of a suitable mode of action of the risk; Lastly is the risk governance through assigning roles, responsibilities and accountabilities, development of policies and strategies for reporting of risks, monitoring and evaluating the effectiveness of mitigation measures applied, such as changes of the software in the system or installing modern anti-viruses, training of users, putting up a governance structure that will see through implementation of policies related to cybercrimes as well as conducting regular risk audits.

3.3 Discussion of the Results.

After administering a total of 120 questionnaires in the cross sectional survey, 91 were available for analysis. This translates to a 75.5 % response rate, which is adequate enough to avoid the issue of low response or non-response bias. The participants for the survey consisted of ICT staff from the selected 12 public universities in Kenya. For the qualitative phase of this study, a total of 15 cybercrime detectives from DCI of Kenya, Nairobi headquarters and Kianyaga branch were also interviewed on crimes related to LMS risks, as key informants.

According to quantitative findings of this study, the three most common risks to LMS were identified as the skills gap (51.7%), human error (42.9%) and poor infrastructure (41.8%). This was supported by qualitative findings from the key informant interviews. As such, recurrent themes of inadequate safeguards, technological challenges and need for mitigation measures, such as increased investments in training and infrastructure, were identified and summarized in Table 4.4. In line with this, 2 interviewees said that ***"Without immediate mitigation measures, the situation might get worse".*** More agreements were provided by the responses from two participants who specifically stated that ***"Stakeholders should take an initiative to create enough awareness about the cybercrimes"***. More importantly, feedback from respondents' validation was also in agreement that the safeguards currently in use were not adequate enough to counter cyber-attacks and the goals of the online learning may be sabotaged, if cybercrimes are not effectively tackled. Indeed, they recommended not only creation of more awareness about the cybercrimes, but also encouragement of knowledge sharing and transfer about the same. It has been reported by many researchers that the human link is the weakest in information security [21].

Another key finding of this study is that although the use of technology in learning such as online learning had increased steadily over the past fifteen year, with the increase being experienced during the COVID-19 pandemic. This was due to stringent restrictions put in place to control the spread of the outbreak such as the lock-downs, social and physical distancing. Notably, this had also led to sharp rise in cybercrimes. Although inn agreement on the rise in cyber-attacks, feedback from the respondents' validation was that the increase mainly affected academic institutions. Therefore, although the increased usage of online learning has improved outcomes, it has also created a significant threat to the LMS in the form of cybercrime [22]. According to this study, in the majority of public institutions, there have been numerous documented incidences of cyber-attacks, notably of their LMS.

In the overall, the increased adoption and integration of technology in learning such as online learning by use of LMS, thus an associated increase in risks to the system, was an important observation relevant to this study. Notably, in all the studied 12 public universities each one of them was using a form of e-learning. The e-learning theory, which claims that using audio-visual aids in instruction improves student understanding explains this observation. Similarly, connectivism principle, which contends that students should synthesize ideas, theories, and general knowledge in a beneficial way while utilizing technology relates very well with the observation. From the identified most common risks, the most important influencers of harm to the LMS were; poor infrastructure, technology challenges and availability of framework, in that order. This implies that the security and privacy of LMS and associated data might be vulnerable, thus needing more safeguards. The findings of this study concur with those of Salazar & Woodward's [23] and Tablante's[24] on security of LMS that contends that learner's data privacy as well as security must be maintained at all costs.

The ultimate goal of this study was to develop a comprehensive risk assessment framework for risks to LMS. According to the findings of this study, although the respondents reported that they were using some form of a framework such as the internet service provider (ISP)-based, quality management system (QMS) and risk association procedures, the current ones in use were not comparable to the one from this study. For instance, the reported frameworks currently in use by the studied institutions were general in scope, not-LMS specific, or aligned to LMS, thus inadequate to effectively the increasing evolving nature of cybercrimes. The workings of the current frameworks were also fundamentally different from this one. For instance, the QMS framework which is the most comprehensive among the current frameworks in use, though it applies the process approach and risk-based thinking for addressing both risks as well as opportunities, is still deficient. Profoundly, unlike the RAF developed in this study that outlines more extensive risk management methodologies, the QMS based one does not include formal methods for risk management or risk management processes [25]. Again, it is not specific for risks and associated harms to LMS. Therefore, since not all processes of a QMS have the same level of risks and given that the nature of risks, effects of the risks, opportunities encountered may not be the same for all organizations or systems, the QMS may not be the most suitable framework

for LMS [26]. Similarly, the workings of the IPS-based and risk association procedures frameworks are not as extensive, comprehensive and as elaborate as the RAF developed in this study.

In support, this study reported that the current crime has become more sophisticated and now using high technology to perpetrate the crime. Another key finding in this study is the involvement of students who are "technology survey" as perpetrators of the cybercrime. The support for this is provided by the direct quotation of two key informant responses; ***"Students will target examination material in systems of academic institutions, and "Their targets vary depending on their intentions".*** This was corroborated by the feed-backs from the respondents' validation who were of the opinion that ***"Cybercrime perpetrators change their means of attacks mainly to hide their identity and cause more harm"***. All these suggests an urgent need for a paradigm shift in our thinking about cybercrime and the current ways we view as well as handle the same. Too, a common and recurrent theme in the key informant interview was not only the increased cybercrimes post-COVID-19 pandemic, evolution or sophistication of cybercrime, inadequacy of LMS safeguards and security, but also the need for more effective frameworks, increased awareness of the risk and investment in training and technology. This was well captured in the two direct quotes from the respondents to the effect that; **"*There has been a steady rise of cybercrimes" and* "*With increasing literacy, perpetrators also gain new knowledge of conducting cybercrimes".***

The ongoing COVID-19 epidemic is not just a significant factor in the global media spotlight, but has led to rapid shift to online teaching by institutions of higher learning. In addition, the development of ICT has had an impact on every element of life in the modern world [27]. As such, the majority of global sectors use internet communications and networking to do business, including governments, businesses, and transactions. Consequent to this, a rise in different illegal actions aimed at online users has been brought on by this greater reliance on online activities. When it comes to cyberspace, criminals use the internet as a tool to find and access security flaws in the systems of internet users, giving them the opportunity to hurt those individuals through theft and other illicit actions. To combat COVID-19 online, a number of fresh strategies and rules have been put into place [28].

According to Abood [29], schools provide online classes so that everyone can learn. And thus students from all over the world not only communicate and share knowledge, but also learn together. However, the students themselves have now become risk threats and are now causing stakeholders to fear them almost as much as they fear professional crooks breaking into schools' computer systems. This underscores the need for an effective framework for risk assessment and management. The usefulness of such a framework suggested by the fact that careful planning and use of effective tools is essential to reduce hazards. As it is a particularly sensitive topic that requires knowledge, Dimitrijevic, [30] stated that higher education institutions needed a framework for risk assessment. However, their proposed framework was based on working processes, assets that were at risk, and mitigation methods. In contrast, the framework (Figure 4.1) developed in this study, provides much more than this by outlining the most common identified risks/hazards specific to the LMS of e-learning, step by step process of risk assessment, measurement, management, monitoring and governance with associated method and tools to use, in a single graphical illustrative summary. This RAF is expected to serve as a guide for educators who are trying to assure LMS security for the widespread conversion of education to the online mode. For instance, operational hazards may result from faculty members' lack of LMS experience, outdated technology, or inadequate infrastructure. Hence, by bringing in all the users and stakeholders such educational technologists to implement safe procedures, this might be lessened [31].

According to this study's finding public universities should invest more resource in terms of time, technology, infrastructure and well trained human resource. An increase in the awareness of threats, risks and harm to LMS is needed, as recommended by the feedbacks from the respondents' validation. This is by ensuring that the LMS users such as e-tutors, e-learners, manager (Chairmen of departments), system administrators, educational technologists, guest users and other support staff were not only properly trained, but also equipped with basic skills, knowledge to conduct risk assessments, as well as manage them in an organized, efficient manner [32. The study has effectively incorporated the key dangers for each player identified by Singh [33] as well as the levels of risk and their protective methods categorized by other studies into our proposed framework. From the experiences of COVID-19 pandemic-imposed restrictions on the use of digital platforms, there is a need for energetic counter measures of potential threats or risks employing a variety of techniques [34]. In agreement with the aforementioned studies, this study has also demonstrated the need for institutions of higher learning to increase their investments of resources including time and money for developing faculty members' as well as learners'/students' competencies. This is in order to not only assess, but also reduce hazards in daily tasks, then incorporate them into e-learning processes. From the results presented earlier in chapter four and discussed in this chapter, it is clear that the all study objectives set were achieved and the asked research questions answered.

3.4 Implication of the study.

Since the internet and LMS are some of the main platforms for e-learning implementation, they are subject to multiple criminal activity and security risks. So, the environment for online learning is inescapably exposed to a wide range of security risks, threats, assaults, and vulnerabilities The e-learning is susceptible to security, especially cyber security, because it is a multi-user environment with shared information that is almost certainly accessed through the internet [35]. It seems the. An important difference in the interviewees' responses was the reporting by 3 interviewees of the increased in cybercrimes and participation of students as perpetrators of cybercrimes, targeting institutional systems. In particular, the participants said that **"*There has been a steady rise of cybercrimes".*** The systems targeted by the students were not just the LMS, examination management systems to access examination in advance, but also financial systems, to change their financial details. This was a notable deviant case or contradictory evidence that warrants further investigation to confirm it.

Some of the limitations of this study included;

- The studying of only 12 out of the 32 initially selected public universities

- Use of purposeful sampling method to select the key informants for interviewing and associated potential of selection bias.
- Direct involvement of the researcher in the interviewing of the key informants, which might have introduced potential interviewer's bias.

However, despite the above mentioned limitations of the study, some of the notable strengths of this study that may have countered their effects, include;

- The use of mixed methods approach and a hybrid research design which not only enriched the study, but also increased confidence and acceptability of the findings.
- Triangulation of data from multiple sources.
- Respondents' validation by involving a few relevant stakeholders for their feedback and opinion.
- A detailed description of the participants' characteristics, context of the research, documents and other sources of data used, to support transferability of the findings to the wider population or other settings.

4.1 Summary, Conclusion and Recommendation.

In summary;

- The most common risks to LMS in public universities in Kenya that were identified by this study included skills gaps, technology challenges, poor infrastructure, human error and lack of safeguards.
- The most influential identified risks to the harm to LMS are the skills gap, technology challenge and availability of framework, in that order.
- A number of public institutions studied used a form of framework. However, they were not only inadequate but also not specific for LMS.

4.2 Conclusions

From the study findings, it is clear that there is a real threat of risks and potential harm to LMS of public universities that need to addressed. The most influential identified risks to the harm of LMS are dependent variables (their effect on harm does not depend on any other predictor variable) that requires a broader spectrum or blanket and comprehensive intervention measures, as opposed to targeted ones. By developing a comprehensive risk assessment framework, this study has contributed to the fields of e-learning and forensic science, by providing an essential tool not just for LMS, but that may also be used for forensic investigation of cybercrimes. There is a clear need for a more comprehensive risk assessment framework that is not only aligned to the LMS, but also that take into account the evolving nature of cybercrime.

4.3 Recommendations.

This study makes a number of recommendations to the relevant stakeholders, including;

1. Given that cybercrime has not only increased, but also has become more sophisticated, a paradigm shifts by all the relevant stakeholders in how we currently perceive, handle or manage cybercrimes, is urgently required.
2. Increased investment by learning institutions in technology, infrastructure and training of man power (all the users of LMS) on the risks and harms to LMS. Increased use by learning institutions and other interested stakeholders of risk assessment frameworks such as the one developed in this study, not just to manage risks, but also informing decision making and policy formulation.
3. Further studies focusing on the evolving nature of cybercrimes and involvement of students as perpetrators as well as its implication on the systems or institutions.

5.0 References

1. Fatma, S. F. (2013). E-learning trends issues and challenges. International journal of economics. Commerce and research, 3(2), 1-10.
2. Communication Authority of Kenya (CAK) Annual Report Financial Year 2020-2021; https://www.ca.go.ke/document/annual-report-financial-year-2020-2021/
3. Sabbah, Y. W. S. (2012). Proposed models for secure e-examination system. Cairo university.
4. Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: new concern cyber security issues of critical cyber infrastructure. Applied sciences,11(10), 4580.
5. Desai, V. P., Oza, K. S., & Kamat, R. K. (2021). Preference based e-learning during covid-19 lockdown: an exploration. The online journal of distance education and e-learning, 9(2).
6. Alexei, l. A., & Alexei, a. (2021). Analysis of iot security issues used in higher education institutions. International journal of mathematics and computer research, (5), 2277-2286.

7. Kibuku, R. N., Ochieng, D. O., & Wausi, A. N. (2020). e-Learning Challenges Faced by Universities in Kenya: A Literature Review. *Electronic Journal of e-Learning*, *18*(2), pp150-161.
8. Esteban-Navarro, M. Á., García-Madurga, M. Á., Morte-Nadal, T., & Nogales-Bocio, A. I. (2020, December). The rural digital divide in the face of the COVID-19 pandemic in Europe—recommendations from a scoping review. In Informatics (Vol. 7, No. 4, p. 54). MDPI.
9. Alwi, N. H. M., & Fan, I. S. (2010). E-learning and information security management. International Journal of Digital Society (IJDS), 1(2), 148-156.
10. Tong, A., Sainsbury, P., & Craig, J. (2007). Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups. *International journal for quality in health care*, *19*(6), 349-357.
11. Babalola, E. O., Otunla, F. L., & Omolafe, E. V. (2023). Undergraduates' level of acceptance and utilization of Moodle platform for learning during Covid-19 pandemic. Indonesian Journal of Multidiciplinary Research, 3(1), 31-40.
12. Ali, R., & Zafar, H. (2017). A security and privacy framework for e-Learning. International Journal for e-Learning Security
13. Pei, L., & Wu, H. (2019). Does online learning work better than offline learning in undergraduate medical education? A systematic review and meta-analysis. Medical education online, 24(1), 1666538.
14. L. Haven, T., & Van Grootel, D. L. (2019). Preregistering qualitative research. Accountability in research, 26(3), 229-244.
15. Findley, M. G., Kikuta, K., & Denly, M. (2021). External validity. Annual Review of Political Science, 24, 365-393.
16. Taherdoost, H. (2016). Sampling methods in research methodology; how to choose a sampling technique for research. How to choose a sampling technique for research (april 10, 2016)?
17. Thompson, J., Gusev, P., & Burke, J. (2019, September). Ndn-cnl: A hierarchical namespace api for named data networking. In Proceedings of the 6th ACM Conference on Information-Centric Networking (pp. 30-36).
18. Hadullo, K., Oboko, R., & Omwenga, E. (2017). A model for evaluating e-learning systems quality in higher education in developing countries. International journal of education and development using ict, 13(2).
19. Gehlbach, H., & Hough, H. J. (2018). Measuring Social Emotional Learning through Student Surveys in the CORE Districts: A Pragmatic Approach to Validity and Reliability. Policy Analysis for California Education, PACE.
20. McIver, J., & Carmines, E. G. (1981). Unidimensional scaling (Vol. 24). sage.
21. Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. Educational Planning, *27*(2), 23-39.
22. Peng, M. H., & Hwang, H. G. (2021). An empirical study to explore the adoption of e-learning social media platform in Taiwan: An integrated conceptual adoption framework based on technology acceptance model and technology threat avoidance theory. Sustainability, 13(17), 9946.
23. Salazar, M., & Woodward, B. (2017). WITH GREAT DATA, COMES GREAT RESPONSIBILITY: UNIVERSITY STUDENTS'PERCEPTIONS ON DATA PRIVACY. Issues in Information Systems, 18(1).
24. Tablante, C. B., & Fiske, S. T. (2015). Teaching social class. Teaching of Psychology, 42(2), 184-190.
25. ISO. 2015. Quality Management System Requirements, 5th Edition, Geneva, Switzerland. www. iso.org.
26. KEBS. 2015. Kenyan Standards, Quality Management System Requirements. 5th Edition, Nairobi, Kenya. www.kebs.org.
27. Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., ... & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. International journal of information management, 55, 102211.
28. Alqahtani, A. Y., & Rajkhan, A. A. (2020). E-learning critical success factors during the covid-19 pandemic: A comprehensive analysis of e-learning managerial perspectives. Education sciences, 10(9), 216.
29. Abood, H., & Abu Maizer, M. (2022). Strategies to Address Cheating in Online Exams. International Journal of Technology in Education, 5(4), 608-620.
30. Ruzic-Dimitrijevic, L., & Dakic, J. (2014). The risk management in higher education institutions. Online Journal of Applied Knowledge Management, 2(1), 137-152.
31. Roos, S. (2018). Chatbots in education: A passing trend or a valuable pedagogical tool?
32. Dhawan, S. (2020). Online learning: A panacea in the time of COVID-19 crisis. Journal of educational technology systems, 49(1), 5-22.

33. Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ism) practices: Lessons from select cases from India and Germany. Global Journal of Flexible Systems Management, 14, 225-239.
34. Lara Nieto-Márquez, N., Baldominos, A., Iglesias Soilán, M., Martín Dobón, E., & Zuluaga Arévalo, J. A. (2022). Assessment of COVID-19's Impact on EdTech: Case Study on an Educational Platform, Architecture and Teachers' Experience. *Education Sciences*, *12*(10), 681.
35. Topham, L., Kifayat, K., Younis, Y. A., Shi, Q., & Askwith, B. (2016). Cyber security teaching and learning laboratories: A survey. Information & Security, 35(1), 51.

Appendices.

Participants Profile/ Workplace/Department	Age	Gender	Education/Professional Training	Documents Used	Other Data Sources
Cybercrimes department	43	Male	ICT	Cybercrime database.	ISO 9001: Quality Standards
Cybercrimes department	30	Male	Computer science	Active cases.	
Cybercrimes department	28	Male	Software engineering	Active cases.	Reported cases.
Cybercrimes department	34	Female	Data science	Cybercrime database.	
Cybercrimes department	39	Female	ICT	Prosecuted cases.	Undercover investigations.
Cybercrimes department	48	Male	Computer programming.	Cybercrime database.	
Cybercrimes department	32	Female	Computer science	Prosecuted cases	INTERPOL
Cybercrimes department	33	Male	Software engineering	Active cases.	
Cybercrimes department	35	Male	ICT	Cybercrime database.	
Cybercrimes department	50	Female	ICT	Prosecuted cases	
Cybercrimes department	31	Male	Cyber security	Active cases.	National Intelligence Service.
Cybercrimes department	43	Female	ICT	Cybercrime database.	
Cybercrimes department	41	Female	Software engineering	Active cases	
Cybercrimes department	36	Male	Computer science	Prosecuted cases	
Cybercrimes department	34	Male	Computer engineering	Prosecuted cases	

	Main Themes/Sub-themes	Participant or Group of Participants	Related Direct Quote	Modification based on Feedback
Theme 1	**Inadequacy of LMS Safeguards**	**Interviewee 4, 7,12 (DCI)**		Safeguards currently in se are not adequate enough to counter the cyber-attacks.
Sub-theme 1	Awareness of Risks and Harms	Interviewee 6, 8 (DCI)	*"Stakeholders should take an initiative to create enough awareness about the cybercrimes".*	
Sub-theme 2	Education of Student and Lecturers	Interviewee 9, 11 (DCI)		The goal of educating students through online may not be achieved if cybercrimes are not tackled.
Sub-theme 3	Lack of Framework	Interviewee, 7,9, 10(DCI)		

	Main Themes/Sub-themes	**Participant or Group of Participants**	**Related Direct Quote**	**Modification based on Feedback**
Theme 2	**Technology Adoption post- Pandemic**	**Interview ee1, 4, 7 (DCI)**	***"Sudden shift to use of technology for learning in academic institutions encouraged more cybercrimes in academic institutions".***	
Sub-theme 1	Sudden Uptake of Online Learning	Interviewee 6, 12 (DCI)		
Sub-theme 2	Technology- driven increase in Cyberattacks	Interviewee 3, 5, 7 (DCI)	"*Cyberattacks become more sophisticated with new technology".*	
Theme 3	**Need for Mitigation Measures**	**Interviewee 8, 14 (DCI)**	***"Without immediate mitigation measures, the situation might get worse".***	
Sub-theme 1	Need for More Awareness	Interviewee 1, 7,,13,(DCI)		Those who are already aware should be encouraged to inform anyone close to them who is not aware.
Sub-theme 2	Need for more Investments	Interviewee 2, 6,14 (DCI)		
Theme 4	**Increased Cyber Crimes post-pandemic**	**Interviewee 1, 10 (DCI)**		It majorly affected academic institutions.
Sub-theme 1	Cybercrime Targets e.g. Banks, Academia (Hacking of Examinations and Data Loss)	Interviewee 4, 7,(DCI)	*"Their targets vary depending on their intentions. Students will target examination material in systems of academic institutions".*	
Theme 5	**Evolution of Cyber crimes**	**Interviewee 3, 8, 13(DCI)**	**"*There has been a steady rise of cybercrimes".***	
Sub-theme1	Sophistication of cybercrime e.g. New targets and Methods E.g. Learning Institutions LMS, Changing Exam Results, Accessing Exam Materials Upfront, Changing Student's Financial details	Interviewee 9, 13 (DCI)		Cybercrime perpetrators change their means of attacks mainly to hide their identity and cause more harm.
Sub-theme 2	Skilled Perpetrators (Students and Civilians)	Interviewee 4, 13 (DCI)	"*With increasing literacy, perpetrators also gain new knowledge of conducting cybercrimes".*	
Sub-theme 3	Use Latest Technology for the Crime	Interviewee 3,15, (DCI)		