International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
https://ijcjournal.org/index.php/InternationalJournalOfComputer/index

Defensive Cybersecurity Preparedness Assessment Model for Universities

William Kipkoech Too*

Email: wtoo@egerton.ac.ke

Abstract

Broadband and internet access has become readily available to citizens across the globe as a result the recent uptake of fiber connectivity. General Cyber Security threats like malware attacks, social engineering scams and financial frauds have increased. Though numerous security models have been advanced by NIST and ISO standards, but the frightening truth is that escalating cyber-attacks are still on the rise. This is because most existing security analysis tools focus mainly on detecting attacks. Despite the steady flow of security updates and patches, this scenario has led to a continued rise of attack surface in institutions of higher learning where students and staff sensitive information and valuable assets is of high stake. Therefore, the purpose of this study is to establish the factors for effective defensive cyber security in Universities. The study utilized a survey method to collect data from cyber security experts of the sampled universities. The study targeted 27 respondents (ICT experts) from 5 universities both public and private that were purposively sampled in Kenya. 23 questionnaires were returned translating to 85% response rate. This was very sufficient for the study. Correlation analysis was carried and the findings indicated a statistically significant relationship for human factors (87.7%), technology factors (83.5%), and policy factors (83.2%) on defensive cyber security preparedness. Multiple linear regression was also done to predict the extent of the effect of each independent variable on defensive cyber security preparedness. In conclusion, the study noted that, all the three cyber security factors were significant hence there was a need to enhance them so as to improve security against the advancing threat landscape across all sectors especially institutions of higher learning like universities.

Keywords: Fiber; Cybersecurity; cyber-attack; preparedness.

Received: 1/5/2025
Accepted: 3/28/2025
Published: 4/7/2025

---

* Corresponding author.

1. Introduction

Global connectivity and accessibility to information by users outside the organization increase risk beyond what has been historically addressed by IT general and application controls. Organizations' reliance on information systems and the development of new technologies render traditional evaluations of IT general and application controls insufficient to assure cyber security [1].

The Government of Kenya is promoting ICT usage to the government and the Kenyan public through undersea and terrestrial cable and network installations, increased availability of mobile/wireless technology, and a movement towards e-government services [2]. University education is one of the most rapidly expanding sub-sectors of the Education sector in Kenya. Demand for university education has continued to increase with many students who cannot be absorbed in Kenyan Universities seeking admission to institutions of higher learning outside the country [3]. Implementation of E-learning programs at Kenyan Universities as well as assessing the prerequisites and level of preparation of learners to attend E-learning environments too require extensive study and research [4].

As educational institutions are being targeted more frequently by cybercriminals, they are also contending with demands for increased digital capabilities from students and faculty. This has led to a growing number of devices and applications connecting to the network per person, thereby increasing the attack surface [5]. Seventy-two percent of students simultaneously connect two or more devices to campus networks, meaning schools have to balance defending against an influx of endpoints that they do not own with giving students and staff a seamless IT experience.

Additionally, bandwidth has been deployed to surrounding students' hostels to enable students the freedom to work from anywhere at any time. In this case, students connect their devices to the network, which leads to uncontrolled network growth. It is a common norm in the country with a high number of technology dependence that comes due to the several attack sites as every organization tends to go online in their services like cloud computing which is majorly practiced in the Kenyan institutions that embrace e-learning programs; these uncontrolled nodes/devices hooked to the network are avenues for cyber-attacks [6].

As public and private organizations migrate more critical functions to the Internet, studies reveal that criminals have more opportunities and incentives to obtain sensitive information through the Web application [7]. This is due to the expansion usage of their cutting-edge tools, where hackers attempt to break into their security by using the vulnerable security link or the less-informed computer user, therefore, universities are highly vulnerable to cyber-attacks occasioned by outsiders as well as insider students and staff who use their expertise to hack [8].

With the high percentage of internet users, it will be stressful that the number of security professionals will remain dismal and unable to match the entire population's percentage that uses the internet [9]. According to author [10] while working with users on hunt engagements, establish an average dwell time of 200-250 days in which an advanced adversary remains undetected in a victim's network before discovery. Advanced threat

hunting involves actively searching for compromises before alarm bells go off by carefully exploring networks and datasets to discover hidden threats.

As a result of frequent network threat analysis, institutions can get hold of evolving attacks before getting out of hand [10]. Therefore, since universities own valuable assets and information concerning students, staff, examinations, financials, and third-party engagements that need to be safeguarded against attacks, universities must employ effective defensive cyber security preparedness strategies to remain safe from advancing adversaries.

2. Problem Statement

To expand access to education, Kenya's government has implemented policies that have resulted in an unprecedented growth in the number of students compared to existing infrastructure, which includes ICT. As a result, Universalities has implemented a Bring Your Own Device (BYOD) policy to enhance current ICT infrastructure. Wi-Fi is commonly used to distribute bandwidth to adjacent student hostels, allowing students to do homework and research from the hostels. As students and employees connect their devices to the network, this scenario leads to uncontrolled network proliferation. Cyber-attacks can take advantage of uncontrolled nodes/devices connected to the network. Users with varying levels of cyber security expertise can connect to the nodes. These users pose a variety of threats to university information assets, including intruder and malware threats, putting universities at risk of cyber-attacks occasioned by outsiders as well as insider students and staff who use their expertise to hack.

Since ICT is critical in running the operations of universities, there is a need to adopt the use of a variety of defensive security technologies and mechanisms to safeguard valuable assets. NIST and ISO standards have proposed numerous security models. The frightening truth about escalating cyber-attacks is that most organizations/businesses, as well as the cyber security industry itself, are unprepared. This is because most existing security analysis tools focus mainly on detecting attacks. Despite the steady flow of security updates and patches, this scenario has led to a continued rise of attack surfaces in institutions of higher learning where students and staff's sensitive information and valuable assets are of high stake. The vast volume of data related to security not only makes these approaches too prone to error but also labor intensive while providing users with a “big picture” of their overall cyber situation. Cyber security metrics for Cyber Situational A, mission assurance analysis, and synchronized network defense are being overlooked by current systems hence there is a need to develop a defensive security model that will take into account the adequacy of security controls to assess the preparedness level among Kenyan Universities in averting the insider and outsider threats.

3. Objective of the Study

i. To establish the factors for effective defensive cyber security in Universities

4. Research Question

i. What are the factors for effective defensive cyber security in Universities?

5. Literature Review

5.1 The magnitude of threat existence in Universities

The speed at which technology evolves is magnified and the threat tempo is accelerating (Cilluffo, 2018). With IT systems that are open, permissive, and widely disseminated, educational institutions especially universities worldwide faces top risks such as account hacking, phishing, IP theft (piracy), ransomware, credit card fraud, harassment, and denial of service attacks. These systems have a big number of users and deal with highly sensitive and valuable data, making them ideal avenues for cyber criminals.

Consequently, the rise of mobile and the internet of things technology have enhanced access to information. Empowering the students of today especially in universities to create the world of tomorrow are increasingly moving away from paper books towards tablets and laptops [11]. Learning has been made easier with students learning at their own pace and accessing educational materials anywhere anytime. The majority of the students want to use their smart mobile devices more frequently, and especially in research.

While in university, students participate in much more than just academics. They socialize with their friends, join groups, network, and apply for employment and internships. Contact information, financial information, and personally identifiable information are all transferred during these processes. Everything may be saved, from addresses to relatives to emails. Furthermore, many students work on campus, which means that financial information is stored by colleges. Worse, many institutions collaborate with well-known corporations and government organizations. This indicates that staff or students have connections within those businesses.

Nonetheless, the consequences of these cyber security threats are of varied range. These include interruption to the functioning of a university network for general disturbance or targeted attempts to obtain valuable information from networks and their users. Universities also face an increasing challenge from advanced, persistent, and targeted threats that mirror the sector’s significant contribution to innovation and economic growth in the UK and beyond.

In 2018, for example, researchers found over 300 phony websites and login pages for 76 universities in 14 nations, including the United Kingdom. The email was most likely used to lure victims to fraudulent websites. Their credentials were stolen once they entered them into the bogus login page, and the victims were sent to the actual university website [12]. The false pages were frequently linked to university library systems, indicating the actors’ appetite for this type of material. Oxford, Warwick, and Greenwich universities are among many institutions of higher learning to have fallen victims to attack in recent years. The percentage increase in such attacks against the education sector in 2021 was 102%. The consequences for such attacks were significant as they disrupt critical operations like class schedules, assignment distribution, admission process, financial and staff across the institution.

In Africa, the use of cyber technology has increased, exposing the country's institutions to intentional security attacks with potentially serious implications. Insider assaults, as well as cybercriminals, have been known to target these institutions. Kenyan students rank fourth in Africa, behind Egypt, Morocco, and South Africa, in

terms of hacking school systems to alter grades and fees balance, according to research released during the Education Cyber Security Symposium by Cyberoam. For instance, Kenyatta University (KU) was faced with a legal battle that was launched in the year 2021 by Naomi (student) who failed to graduate with her classmates in December 2016 told the court that she was only ten days away from obtaining a Bachelor of Science degree in Foods, Nutrition, and Dietetics when the university slapped her with a suspension letter.

According to the university, Naomi had failed to explain before a disciplinary panel why five units in which she had scored D had been changed to A [13]. The fact that KU claimed that its systems had been hacked before the court raises questions over the number of such cases that go undetected, not just at the university in question, but across learning institutions in Kenya.

Ensuring effective management across every sector of organizations is becoming increasingly important to the success against the various threats, not just higher education. Considering the diversity of undertakings that university networks support, this study primarily centers on the challenge from more targeted attempts to attain potentially valuable information from universities [14]. The significance of developing effective methods to this challenge for universities is commensurate with the importance of digital data to their work.

Digital material is at the core of almost all of a university's undertakings and the safety and security of this information are important for a number of reasons:

First, Universities produce data as a primary intellectual asset that requires to be stored, accessed, and used appropriately to fully realize its academic or commercial value. This might include data produced for commercial contractors or which has commercial potential, through to politically sensitive data, such as economic or climate modeling [15]. Secondly, Universities rely on access to sensitive data from third-party organizations, such as patient-identifiable data or other clinical data that is provided from medical institutions. Universities may also rely on access to data provided by businesses or other bodies that are considered commercially, operationally, or personally sensitive [16].

Finally, Universities collect data associated with their enterprises, such as information about students, staff, or finances. Data might be considered sensitive by the law, the providers of data, or where it informs decision making, such as marketing and recruitment data, or potentially analytics from virtual learning environments. About 85 percent of colleges and universities need security training for faculty. These institutions, on the other hand, fail to inform students about the cyber security dangers. Students are generally aware of their privacy rights when it comes to their personal information, but many are not aware of how to spot scams.

Since digital information has grown, the need to ensure that data is secured from potential destruction, theft, or corruption is of great importance. However, security is a trade-off between the likelihood and potential impact of threats and the various costs that are incurred to defend against them in all organizations. Furthermore, different types of activity may involve different types of risks, management priorities, and associated security measures in the case of large, complex organizations like universities, [17].

5.2 Key factors for effective Cyber Security

Since the dawn of cyber threats, Companies have struggled with cyber security, but it is becoming more and more challenging as network infrastructure becomes more complex. In a climate-controlled data center, what used to be a rack (or ten) of servers tucked away in the building somewhere has evolved into a multi-cloud scenario or hybrid with applications, data, and servers spread across the country and around the world over the internet. At the same time, micro-services, containers, DevOps, and other developments in technology make the networks themselves more volatile and dynamic [18].

Though it's imperative for tools on cyber security and practices to adapt; not all threats can be detected with automated tools alone can address these rapidly evolving needs. These tools must be paired with trained threat analysts who have a deep understanding of their operating environment and the ability to ask the right questions. Threat analysts can make sense of complex data, develop hunting hypotheses, and test these hypotheses to better identify hidden threats [10]. Even with trained analysts using the right tools, ad-hoc hunting isn't enough; it must be standardized and measured. Advanced threat hunting requires implementing a repeatable process that's part and parcel of an organization's overarching security strategy. Visibility, context, and scalability are three fundamental things that are essential for effective cyber security regardless of the size of a business or what industry it's in [18].

One of the cyber security simplest truths is taking the protection of what can be seen. Assets and services connected to the network should have a perfect catalog to possibly discover vulnerabilities, identify configuration or other security issues, or detect suspicious or malicious activity on them, hence visibility is a fundamental cyber security strategy to protect network assets and information [19]. All security issues or vulnerabilities are not equal. The context is required for efficient use of resources and effective risk management. The severity of a vulnerability on a server in an internal development network is exponentially less critical than that on a server hosting an e-commerce website that opens to the public [20]. The exposure of assets and the potential security or compliance impact needs to be understood by IT teams to prioritize risk to allocate resources.

The ability to spawn resources and expand availability as demand increases and phase out unnecessary or unused resources when the need fades away is one of the characteristics or benefits of cloud computing, DevOps, and containers [21]. Moving on to cloud computing, instrumenting our networks becomes much more challenging. To ensure there are no gaps in security, and that security does not become a bottleneck that impedes network productivity and performance, cyber security tools need to be able to keep pace with the volatility of the cloud [22].

However, broader aspects were built upon the NIST Cyber Security Framework's purposes to promote a defense-in-depth security posture and manage cyber security risk. Ranking of the factors against known Advanced Persistent Threat (APT) tactics was done for effectiveness. Additional best practices and strategies will be needed to alleviate the new occurring tactics [23]. Any organization that seeks to improve its preparedness for cyber threats must seriously consider the following more factors to navigate through this increasingly large and complex cyber security threat landscape [24]. These factors includes:-

Update and upgrade software immediately: To effectively identify threats and protect an organization's assets, software need to be updated and upgraded immediately. The top management and cyber security professionals should automate the process to the extent possible, use an update service provided directly from the vendor, and apply all available software updates. Computerization is indispensable as the current reactive approach of patching known vulnerabilities is no longer tenable since hackers create exploits after studying patches, often soon after a patch is released. These "N-day" exploits can be as harmful as a zero-day [25]. Authentication of vendor updates must also be done, and to assure the integrity of the content, updates delivered over protected links should typically be signed. Threat actors can operate inside a defender's patch cycle if rapid and thorough patch application is not done. Hackers love low-hanging fruit and often use automated web crawlers to look for sites with unpatched applications. Keeping your website and backend software updated with the latest security patches is the single biggest (and often simplest) step an organization can take towards stopping an attack [26].

Defend privileges and accounts: The privileges should be identified and assigned to users defending on the requirement to maintain operations and risk exposure. Privileged Access Management (PAM) solution should be used to automate credential management and fine-grained access control that is related to the changes occurring during the evolution of the access control policy [27]. Tiered administrative access is another way to manage privilege in which each higher tier provides additional access, but is limited to fewer personnel. Generate ways that securely reset identifications such as tickets, passwords, and tokens. As threat actors continue to target administrator credentials to access high-value assets and to move laterally through the network privileged services and accounts must be controlled [23].

Enforce signed software execution policies*:* Signed software execution policies for scripts, executables, system firmware, and device drivers should be enforced by the use of a modern operating system. Maintain a list of trusted certificates to detect and prevent the use and injection of illegitimate executables. System integrity is ensured when execution policies are used in conjunction with a secure boot capability. To provide greater control, Application Whitelisting should be used with signed software execution policies. Threat actors establish persistence and can gain a foothold through embedded malicious code when unsigned software is allowed; thus Organizations should consider these technologies, particularly for centrally managed servers, desktops, and laptops, because of the relative ease in managing these solutions and the minimal additional cost [28].

Exercise a system recovery plan: Organizations should develop a comprehensive disaster recovery strategy that will ensure the restoration of data when compelled [29]. To ensure continuity of operations due to unexpected events, the plan must safeguard critical data, logs, and configurations. Backups should be encrypted, stored offsite, offline when possible, and support complete recovery and reconstitution of systems and devices for additional protection. Evaluate the backup strategy and perform periodic analysis. To accommodate the ever-evolving network environment, updating the plan is very necessary. A recovery plan is a needed mitigation for malicious threats, including ransomware as well as natural calamities.

Actively manage systems and configurations: To actively manage systems and configuration in an organization, software and network devices inventory should be taken. Do away with unwanted, unneeded, or unexpected software and hardware from the network. Beginning from a known standard establishes control of

the operational environment and minimizes the attack surface. When systems adapt to dynamic threat environments while scaling and streamlining administrative operations, active enterprise management is guaranteed.

Continuously hunt for network intrusions: Cyber security professionals should take proactive steps while continuously hunting for network intrusions. This enables them to detect, contain, and remove any malicious presence within the network. Enterprise organizations should assume that a compromise has taken place and use dedicated teams to continuously seek out, contain, and remove threat actors within the network. Tools such as Endpoint Detection and Response (EDR) solutions, logs, Security Information and Event Management (SIEM) products, and other data analytic capabilities for discovering malicious or anomalous behaviors are passive hence invaluable. Active hunts should also include hunt operations using well-documented incident response procedures and penetration testing to address any revealed gaps in security; for the biggest return, hunting and incident response needs to work together [30]. Using a continuous monitoring and mitigation strategy via established proactive steps will transition the organization beyond basic detection methods, thus enabling real-time threat detection and remediation.

Leverage modern hardware security feature: Secure Boot, Unified Extensible Firmware Interface (UEFI) Trusted Platform Module (TPM), and hardware virtualization should be leveraged as they offer modern hardware security features [31]. Older devices should be scheduled for a hardware refresh. Current hardware features increase the integrity of the boot process, support features for high-risk application containment, and provide system attestation. There's a need to focus on a risk-based approach, as it brings to the table an in-depth security analysis measure. This aids in the improvement of the ability for system protection, user credentials, and critical data from threat actors as a result of using a modern operating system on outdated hardware [32].

Segregate networks using application-aware defenses: Critical networks and services should be segregated to enhance cyber security using different architectures [33]. Restrict content and block improperly formed traffic, according to policy and legal authorizations by deploying application-aware network defenses. Obfuscation and encryption techniques are quickly decreasing in effectiveness for traditional intrusion detection based on known-bad signatures. Sophisticated, application-aware defensive mechanisms critical for modern network defenses are becoming essential as threat actors hide malicious actions and remove data over common protocols.

Integrate threat reputation services: Reputation services arising from a multi-sourced threat such as URLs, DNS, IPs, email addresses, and files should be leveraged [34]. These services aid in the discovery and deterrence of malicious activities; allowing prompt global responses to threats, a decrease in known threat vulnerabilities, and ensuring much larger access to threat analysis and tipping ability than an organization can afford by itself [35]. Evolving risks be it global campaigns or targeted, take place faster than most organizations can handle, resulting in poor coverage of new threats. A more timely and effective security posture against dynamic threat actors is achieved through information sharing services and multi-source reputation [36].

***Transition to multi-factor authentication*:** Prioritize the protection for accounts with remote access, higher privileges, and/or used on high-value assets. Since Knowledge-based factors such as PINs and passwords are

inadequate, physical token-based authentication systems are necessary to fill any gaps. Organizations should move away from single-factor authentication, such as password-based systems that result in poor user selections and are subject to theft, credential forgery, and reuse across multiple systems [37].

6. Conceptual Framework

A conceptual framework gives direction to the study and provides a researcher's position on the problem. Through the conceptual framework, the researcher can be able to show the relationships of the different constructs that he wants to investigate apart from displaying the direction of the study. The conceptual framework articulates the relationship of the variables (independent and dependent variables) in the study as shown in figure 1 below.

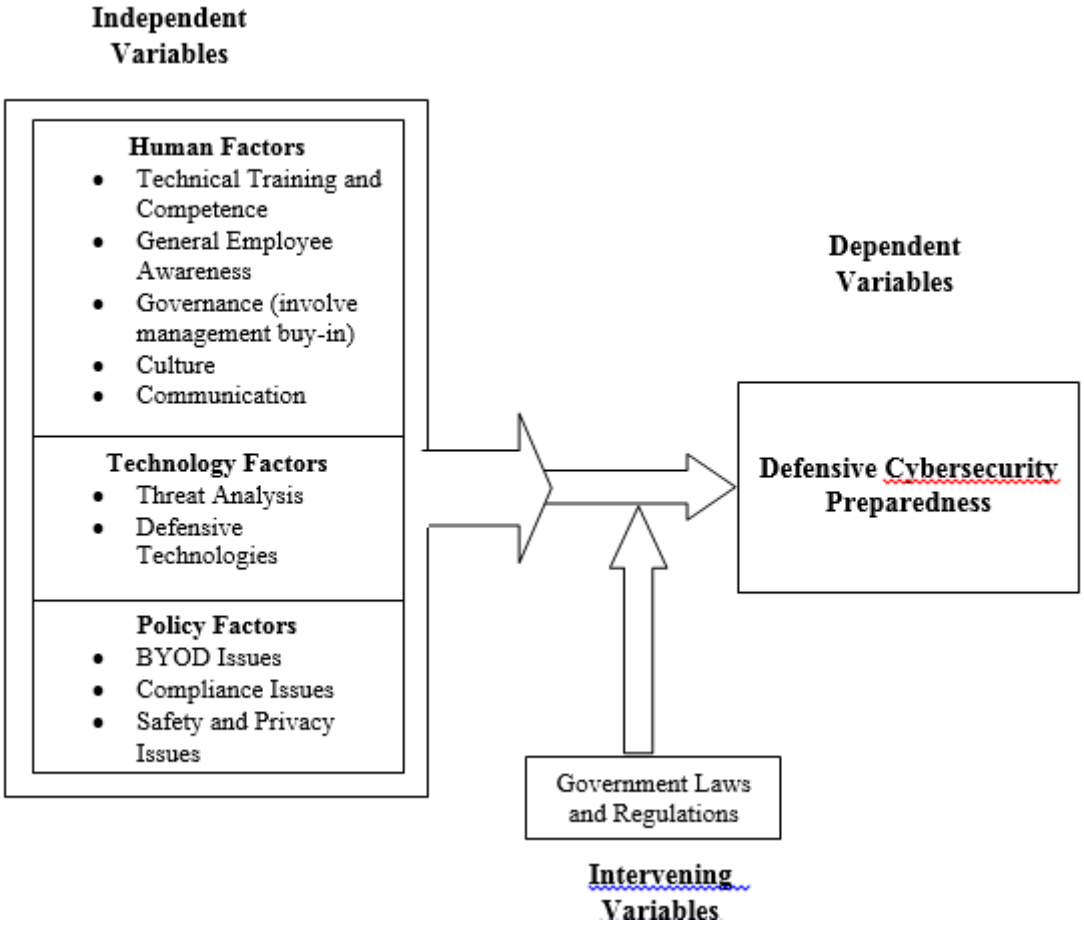

Figure 1: Conceptual Framework for Defensive Cybersecurity Preparedness in Universities.

7. Research Methodology

This study was achieved through a survey method where ICT experts were contacted to come up with relevant weights on factors for effective defensive cybersecurity preparedness in universities. In this study, data was collected to find out the need for a defensive cybersecurity preparedness assessment model.

7.1 Study Location, Population, Sampling, and Sample Size

The following section presents the study location, population sampling, and sample size of the study

7.1.1 Study Location

The study was conducted in selected fully chartered public and private Universities in Kenya. Fully chartered private and public Universities make a suitable representation of universities in Kenya and provided the needed data. Using Mugenda and Mugenda formula of 10% and based on their proximity and accessibility, three public (Egerton, Jomo Kenyatta University of Agriculture and Technology (JKUAT) and the University of Eldoret) and two private (Kabarak and Mount Kenya) universities were purposively selected for the study.

7.1.2 Study Population

The population is defined as the total of elements, individuals, groups, or households that the researcher intends to study [38]. The study population targeted by this research constituted all ICT staff in the chartered universities under study. A list of all ICT staff who were in the universities payroll was obtained from each university to provide a sampling frame to be used during the sampling process.

7.1.3 Sampling Procedure and Sample Size

This study used a multi-stage sampling procedure. In the first stage, a sample of universities whose ICT staff participated in the study was determined using Mugenda and Mugenda [40], a sample size of between 10 and 30% is a good representation of the target population and hence 10 % is adequate for analysis. Therefore, 3 public universities (31 x 0.1) and 2 private universities (18 x 0.1) were considered making a larger population of 49 respondents. To select the five Universities, purposive sampling was used. The selection of the universities under study was informed by university's characterization such as type, location and size as well as the need for resource people who helped in finding informants hence saving much time and effort that could be brought by misunderstanding.

Determining the sample size in qualitative research is easy since there are no hard and fast rules to specify the number of participants. Qualitative studies can be carried out with a single participant or with as many as 60 or 70 participants representing multiple contexts. A sample of more than 20 is large enough [39,41]. Author [42] notes that research questions and objectives that do not require statistical estimation should have a sample smaller than 30 participants. The author [39] also notes that having more participants does not necessarily mean the study or its results will be more reliable or more useful. Preliminary information revealed that there are 112 ICT employees in the five selected universities. Therefore, determining the number of ICT staff from the 5 universities who participated in the study, was determined using Nassiuma's (2000), formula given as:

$$n = \frac{NC^2}{C^2 + (N-1)e^2}$$

Where

n = sample size

N = Population (112)

c = co-variance (30%)

e = standard error (5%)

$$n = \frac{112(0.3)^2}{((0.3)^2 + (112-1)(0.05)^2)}$$

n= 27

Substituting the values in the formula gives a sample size of 27 respondents were selected to participate in the study. To ensure each university is represented in the sample, proportionate stratified sampling was used as shown in Table 1. below.

Table 1: Sample Size

UNIVERSITY	NUMBER OF ICT STAFF	SAMPLE SIZE
Egerton University	**30**	**7**
Kabarak University	**9**	**3**
University of Eldoret	**18**	**4**
JKUAT University	**35**	**8**
Mt Kenya University	**20**	**5**
Total	**112**	**27**

Source: University ICT staff of the respective universities (2019)

To select the sample units from each university, purposive sampling was used. Hence, ICT staff who are considered better informed on cyber security were selected to participate in the study. The target respondents for this study as illustrated in table 2. mainly comprised of ICT Managers/Directors, IT Security Managers, System Administrators, Network Administrators, and IT Support Officers who were purposively picked in each university to enhance presentation of factual information and university coverage. The targeted experts of the university filled out the survey questionnaire after which the researcher collected and analyzed them later.

Structured questionnaires with open and closed-ended questions were used to enrich the value of research data that was obtained, ease of data analysis, and for effective conclusions.

Table 2: Representation of respondents

Selected Universities	**ICT Experts to be sampled**					
	ICT Manager/ Director	**IT Security Manager**	**System Admin**	**Network Admin**	**IT Support Officers**	**Total**
Egerton University	1	1	1	1	3	**7**
Kabarak University	1		1	1		**3**
University of Eldoret	1		1	1	1	**4**
JKUAT University	1	1	1	1	4	**8**
Mt Kenya University	1	1	1	1	1	**5**
Grand Total	**5**	**3**	**5**	**5**	**9**	**27**

Source: University ICT staff of the respective universities (2019)

7.1.4 Sampling Techniques

In the first stage, the 5 universities were selected from the sampling frame of the 31 public and 18 private chartered universities using a convenient sampling method.

In the second sampling stage, the number of respondents in each university of the 5 selected universities was first determined and categorized into job categories; ICT Managers/Directors, IT Security Managers, System Administrator, Network Administrator, and IT Support Officers. The proportionate sampling method was used to determine the number of respondents in each of the job categories in each of the selected universities. Individual respondents were then selected using purposive sampling method.

7.2 Data Collection Procedure

The data collection procedure involved the use of questionnaires for qualitative research. The researcher first got the introduction letter from postgraduate and then applied for a research permit. After receiving permission from the relevant authorities, the researcher proceeded to collect data from the selected respondents. The researcher visited the area of study before actual data collection for familiarization and acquaintance. During this visit, the researcher informed the universities management about the purpose of the study and booked appointments for

data collection. After familiarization, data was collected using the mentioned instrument.

For this study, semi-structured questionnaires were given to ICT experts of the chosen private and public universities. This included ICT Managers/Directors, IT Security Managers, System Administrators, Network Administrators, and IT Support Officers. This was for exploring the preparedness of cyber security. The questionnaire contained various items seeking different elements of the study variables from the targeted respondents.

7.3 Data Analysis Procedures

The data collected was qualitative as it attempted to collect data from members of a population in order to determine the status concerning one or more variables [40]. The completed questionnaires from the experts were evaluated for consistency, cleaned, and then coded, entered, and analyzed using the SPSS data analysis method and presented using tables and texts.

8. Results and Discussion

8.1 Descriptive analysis for defensive cybersecurity preparedness

The study sought to examine the defensive cybersecurity preparedness in the sampled population. The findings are presented in Table 3.

Table 1: Defensive Cybersecurity Preparedness

Statement	SD	D	N	A	SA
Has a cybersecurity plan or strategy that includes an organizational structure stretching beyond IT and/or security departments that outlines the roles and responsibilities related to cybersecurity and information protection	6.1%	27.3%	18.2%	30.3%	18.2%
Establishes criteria for assessing and prioritizing dependencies	24.2%	24.2%	18.2%	18.2%	15.2%
Considers cybersecurity requirements related to vendor relationships.	9.1%	21.2%	15.2%	39.4%	15.2%
Establishes policies to protect assets and sensitive information.	3.0%	30.3%	15.2%	33.3%	18.2%
Consolidates cybersecurity processes, procedures, and requirements in a dedicated component of an enterprise-wide risk-management strategy	9.1%	21.2%	21.2%	39.4%	9.1%
Assigns responsibility for cybersecurity reporting obligations to specific personnel.	15.2%	21.2%	21.2%	24.2%	18.2%
Employs a coordinated approach to cybersecurity that links response and recovery plans and policies to activities related to physical and cyber operating environment security.	9.1%	21.2%	33.3%	27.3%	9.1%

Employs a coordinated approach to monitoring and detection that includes documented detection processes and procedures which are informed by industry standards and/or guidelines, and communicated to employees	6.1%	36.4%	27.3%	21.2%	9.1%
Identifies alternate channels for communication in the absence of functional mainstream IT or communications technology	6.1%	30.3%	24.2%	18.2%	21.2%
Establishes a dedicated cyber incident response plan that identifies roles and responsibilities for specific personnel and includes response procedures for escalation, containment, and eradication of the threat, including requirements of a third-party vendor	12.1%	24.2%	21.2%	36.4%	6.1%
Develops formal plans for continuity and recovery that reflect specific restoration priorities and include reconstitution measures.	3.0%	24.2%	30.3%	21.2%	21.2%
Incorporates lessons learned and corrective actions from real events into continuity and recovery plans	12.1%	36.4%	24.2%	24.2%	3.0%

According to research findings, 48.5% of respondents agreed that they have a cybersecurity plan or strategy that includes an organizational structure stretching beyond IT and/or security departments that outlines the roles and responsibilities related to cybersecurity and information protection. Moreover, 54.6% and 51.5% agreed that they consider cybersecurity requirements related to vendor relationships and that they establish policies to protect assets and sensitive information.

Risk-management strategies are vehicles of cyber securities. The findings of the research showed that 48.5% agreed that they consolidate cybersecurity processes, procedures, and requirements in a dedicated component of an enterprise-wide risk-management strategy. Correspondingly, 42.4% of the respondents were of the opinion that they assign responsibility for cybersecurity reporting obligations to specific personnel. Likewise, 36.4% agreed that they employ a coordinated approach to cybersecurity that links response and recovery plans and policies to activities related to physical and cyber operating environment security.

The findings too disclosed that 39.4% agreed that they identify alternate channels for communication in the absence of functional mainstream IT or communications technology. Also, 42.5% affirmed that these organizations have established a dedicated cyber incident response plan that identifies roles and responsibilities for specific personnel and includes response procedures for escalation, containment, and eradication of the threat, including requirements of a third-party vendor.

According to the study, it was discovered that 42.4% agreed that they developed formal plans for continuity and recovery that reflect specific restoration priorities and include reconstitution measures.

Nonetheless, 48.4% disagreed that they had established criteria for assessing and prioritizing dependencies. Similarly, 42.5% also disagreed that they employ a coordinated approach to monitoring and detection that includes documented detection processes and procedures which are informed by industry standards and/or

guidelines and communicated to employees. Finally, the study noted that 48.5% also disagreed that they incorporate lessons learned and corrective actions from real events into continuity and recovery plans.

8.2 Inferential Analysis

8.2.1 t-test

During testing for differences in defensive cyber security preparedness between public and private universities, an independent sample t-test was run. The results are shown in Table 4.

Table 2: Independent sample t-test

				t-test for Equality of Means		
University Category	**N**	**Mean**	**Std. Deviation**	**t**	**df**	**Sig**
Public University	18	2.58	0.84	-3.369	21	.003*
Private University	9	3.72	0.61			

*. Correlation is significant at the 0.05 level (2-tailed).

The independent sample t-test revealed that the mean defensive cyber security preparedness between public and private universities were significantly different at 0.05, $t(21)= -3.369$; $p<0.05$. This means that private universities having a higher mean (*Mean*=3.72; *SD*=0.61) were more prepared to cyber security as compared to public universities.

8.2.2 Correlations

Pearson correlation analysis was utilized at 0.01 alpha (2-tailed) to determine the relationship between the independent and dependent variables.

Table 3: Pearson Correlations

		Defensive Cyber Security Preparedness
Human Factors	Pearson Correlation	.877**
	Sig. (2-tailed)	.000
	N	23
Technology Factors	Pearson Correlation	.835**
	Sig. (2-tailed)	.000
	N	23
Policy Factors	Pearson Correlation	.832**
	Sig. (2-tailed)	.000
	N	23

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

The results of the study indicated that there exists a statistically significant relationship between human factors and defensive cyber security preparedness ($r=.877:p<0.05$). Furthermore, there is evidence of a significant relationship between technology factors and defensive cyber security preparedness ($r=.835:p<0.05$). Finally, a significant relationship exists between policy factors and defensive cyber security preparedness ($r=.832:p<0.05$). This implies that when these factors (human, technology, and policy) are enhanced in an organization, cyber security preparedness also improves.

8.2.3 Regression Analysis (Model Development)

To predict the extent of the effect of each independent variable on defensive cyber security preparedness, multiple linear regression was used. The results are given in model summary, ANOVA, and the Coefficients tables.

Table 4: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.919[a]	.844	.819	0.39

a. Predictors: (Constant), Policy Factors, Technology Factors, Human Factors

The model summary table specifies that 81.9% in the variation of defensive cyber security preparedness can be explained in the variation of factors such as human, technology, and policy in the model with a standard error of 0.39.

Table 5: ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	16.307	3	5.436	34.175	.000[b]
	Residual	3.022	19	.159		
	Total	19.330	22			

a. Dependent Variable: Defensive Cyber Security Preparedness

b. Predictors: (Constant), Policy Factors, Technology Factors, Human Factors

The robustness of the model is explained by the ANOVA. This shows that the model is statistically significant at 0.05 alpha level, $r^2=81.9$, $F(3,19)=34.175$; $p<0.05$.

Table 6: Coefficients[a]

Model	Unstandardized Coefficients		t	Sig.
	B	Std. Error		
1 (Constant)	-.025	.338	-.074	.942
Human Factors	.476	.155	3.077	.006
Technology Factors	.383	.164	2.339	.030
Policy Factors	.089	.203	.441	.664

a. Dependent Variable: Defensive Cyber Security Preparedness

The finding showed that human factors significantly influence defensive cyber security preparedness (β=0.476;ρ=0.006). Furthermore, Technology Factors significantly influence defensive cyber security preparedness (β=0.383;ρ=0.030). Finally, policy factors loaded a Non-Significant Beta on cyber security preparedness (β=0.089;ρ>0.05).

The equation for the model is given below:

$$y = C + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \varepsilon$$

Where:

Y= defensive cyber security preparedness

C=Constant

$$x_1 = Human\ factors$$

$$x_2 = \text{Technology } factors$$

$$x_3 = \text{Technology } factors$$

$$\beta_1, \beta_2 \text{ and } \beta_3 = Coefficients$$

$$\varepsilon = standard\ error$$

Therefore:

Y= {-0.025}+{0.476 x_1}+{0.383 x_2}+{0.089 x_3}+{0.39}

9. Conclusion

The criticality of the three factors affecting cybersecurity which are human, technology, and policy were checked so as to achieve this research question. Respondents were asked to rank the three cybersecurity factors in terms of their importance to their institutions. According to the findings, human factors were the most important of the three cybersecurity aspects, followed by technology and policy. The study further recommended that, since all the three cybersecurity factors were significant, there was a need to enhance them so as to improve security against the advancing threat landscape across all sectors especially institutions of higher learning like universities.

References

[1]. GTAG. (2016). Assessing cybersecurity risk. Retrieved from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/gtag-assessing-cybersecurity-risk.

[2]. Ministry of ICT, (2014). National Cybersecurity Strategy

[3]. Ministry of Education, (2014). University Education and Research.

[4]. Shahmoradi, L., Changizi, V., Mehraeen, E., Bashiri, A., Jannat, B., & Hosseini, M. (2018). The challenges of E-learning system: Higher educational institutions perspective. *Journal of Education and Health Promotion*, *7*. https://doi.org/10.4103/jehp.jehp_39_18

[5]. Biddle, S. (2017, December 13). Three of the Biggest Cybersecurity Challenges Facing the Education Sector. Retrieved March 28, 2019, from Fortinet Blog website: https://www.fortinet.com/blog/business-and-technology/three-of-the-biggest-cybersecurity-challenges-facing-the-education-sector.html

[6]. Update, T. P. (2017). Reimagining the Role of Technology in Education :, (January).

[7]. Beniwal, S. (2015). Ethical Hacking: A Security Technique. *International Journal of Advanced Research in Computer Science and Software Engineering*

[8]. Neaimi, A. Al, Ranginya, T., & Lutaaya, P. (2015). *A Framework for Effectiveness of Cyber Security Defenses , a case of the United Arab Emirates (UAE). 4*(1), 290–301.

[9]. Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., ... & Shitanda, S. (2015). Kenya Cyber Security Report 2015. Serianu Limited

[10]. Messer, A., & Medairy, B. (2018). *The Future of Cyber Defense... Going on the Offensive*.

[11]. Salcito, A. (2018). *The growing role of education as the engine of economic change makes the work happening to transform our schools and classrooms fundamental to global progress.*

[12]. NCSC, (2019). The cyber threat to Universities. Published 18th September 2019

[13]. Aineah, A. (2018). Why research puts Kenyan students fourth on list of top hackers in Africa. Retrieved February 19, 2019, from The Standard website: https://www.standardmedia.co.ke/article/2001268939/why-research-puts-kenyan-students-fourth-on-list-of-top-hackers-in-africa

[14]. Universities Uk. (2013). *Cyber security and universities: managing the risk*.

[15]. Van den Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2018). Privacy and Information

Technology. In E. N. Zalta (Edition.), *The Stanford Encyclopedia of Philosophy* (Summer 2018). Retrieved from https://plato.stanford.edu/archives/sum2018/entries/it-privacy/

[16]. Harwich, E., & Lasko-Skinner, R. (2018). *Making NHS data work for everyone*.

[17]. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy006

[18]. Bradley, T. (2019). The Secret to Comprehensive, Scalable and Effective Cybersecurity. Retrieved March 28, 2019, from Forbes website: https://www.forbes.com/sites/ tonybradley/2019/02/11/the-secret-to-comprehensive-scalable-and-effective-cybersecurity/

[19]. Quade, P. (2018, February 19). You can't protect what you can't see. Retrieved June 3, 2019, from CSO Online website: https://www.csoonline.com/article/3256211/you-cant-protect-what-you-cant-see.html

[20]. Abomhara, M., & Koien, G. M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

[21]. Walker, J. (2015, June 29). Top 5 benefits of containerization. Retrieved June 3, 2019, from Monitis Blog website: https://www.monitis.com/blog/top-5-benefits-of-containerization/

[22]. Zimmerman, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center*.

[23]. NSA, (2018). Top10 cybersecurity mitigation strategies.

[24]. Bodeau, D., & Graubart, R. (2016). *Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms*. (15), 12

[25]. Cui, A. (2018). N-Days: The Overlooked Cyber Threat for Utilities | Energy Central. Retrieved June 7, 2019, from https://www.energycentral.com/c/iu/n-days-overlooked-cyber-threat-utilities

[26]. Schiff, J. L. (2016, November 7). 7 ways to protect your ecommerce site from fraud, hacking and copycats. Retrieved June 3, 2019, from CIO website: https://www.cio.com/article/ 3137222/7-ways-to-protect-your-ecommerce-site-from-fraud-hacking-and-copycats.html

[27]. Richard Hoesl, C. (2017). *Capability Framework for Privileged Access Management*. Retrieved from https://www.isaca.org/Journal/archives/2017/Volume-1/Pages/capability-framework-for-privileged-access-management.aspx

[28]. Sedgewick, A., Souppaya, M. P., & Scarfone, K. A. (2015). *Guide to Application Whitelisting* (No. NIST SP 800-167; p. NIST SP 800-167). https://doi.org/10.6028/NIST.SP.800-167

[29]. Otaishan, K. (2018). Exercising IT Disaster Recovery Plans - Disaster Recovery Journal. Retrieved June 7, 2019, from https://www.drj.com/journal/winter-2018-volume-31-issue-4/exercising-it-disaster-recovery-plans.html

[30]. Hosburge, M. (2017). *Offensive-intrusion-analysis-uncovering-insiders-threat-hunting-active-defense-128770*. Retrieved from https://pen-testing.sans.org/resources/papers/gcih/ offensive-intrusion-analysis-uncovering-insiders-threat-hunting-active-defense-128770

[31]. NSA, (2017). Ctr-Uefi Defensive Practices Guidance. Retrieved from https://www.nsa.gov /Portals /70/documents/what-we-do/cybersecurity/professional-resources/ctr-uefi-defensive-practices-guidance.

[32]. Ani, U. D., He, H. (Mary), & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32–74.

https://doi.org/10.1080/23742917.2016.1252211

[33]. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security* (No. NIST SP 800-82r2; p. NIST SP 800-82r2). https://doi.org/10.6028/NIST.SP.800-82r2

[34]. US-CERT. (2018). Using Rigorous Credential Control to Mitigate Trusted Network Exploitation .Retrieved June 9, 2019, from https://www.us-cert.gov/ncas/alerts/TA18-276A

[35]. Houser, B. M. (2016). *A model for real-time data reputation via cyber telemetry*.

[36]. Vaynbergh, B. (2019). Securing the NSA Way. Retrieved June 9, 2019, from https://www.mimecast.com/blog/2019/05/securing-the-nsa-way/

[37]. NIST, CI. (2017). Special Publication 800-63B. Retrieved June 9, 2019, from /sp800-63b.html

[38]. Cooper, R. & Schindler, P. (2003). Business Research Methods. Boston: McGraw-Hill.

[39]. Gay, L. R, Mills, G E., & Airrasian, P. (2009). Educational research: competencies for analysis and applications. London: Pearson Education.

[40]. Mugenda, A., & Mugenda, O. (2013). Research methods: Quantitative and qualitative approaches. Nairobi: ACTS Press.

[41]. Creswell, John W. (2009). Research design: qualitative, quantitative and mixed methods approaches. 3rd Edition. Los Angeles: Sage Publications

[42]. Sauders, M, Lewis, P and Thornhill A. (2003). Research Methods for Business student. England: Pearson Education