International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
http://ijcjournal.org/

Defensive Cybersecurity Preparedness Assessment Model for Universities

William Kipkoech Too[a]*, Simon Maina Karume[b], Nelson Bogomba Masese[c]

[a,b,c]*Kabarak University, P.O. Box Private Bag, Kabarak, 20157, Kenya*
[a]*Email: wktoo@kabarak.ac.ke*
[b]*Email: smkarume@gmail.com*
[c]*Email: nmasese@kabarak.ac.ke*

Abstract

With the recent uptake of fiber connectivity, broadband and internet, access has become readily available to citizens all over the world. General Cyber Security threats like malware attacks, social engineering scams and financial frauds have increased. NIST and ISO standards have proposed numerous security models, but 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 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 develop a web-based model for assessing cybersecurity preparedness in universities. This was achieved through design science methodology and engineering design process. The model provides the overview of the university's preparedness level and the appropriate recommendations that need to be considered to remain cyber ready at all times.

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

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 provide assurance over cyber security [5].

---

* Corresponding author.

The Government of Kenya is promoting ICT usage to both the government and the Kenyan public through an undersea and terrestrial cable and network installations, increased availability of mobile/wireless technology, and a movement towards e-government services [12]. 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 are unable to be absorbed in Kenyan Universities seeking admission in institutions of higher learning outside the country [11]. 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 [19].

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 [2]. Seventy-two percent of students connect two or more devices to campus networks at the same time, 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. This scenario results in uncontrolled network expansion as personal devices are hooked to the network by students. Though 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 tend to go online in their services like cloud computing which is majorly practiced in the Kenyan institutions that embrace e-learning programmes; these uncontrolled nodes/devices hooked to the network are avenues for cyber-attacks [20].

As public and private organizations migrate more of their critical functions to the Internet, studies reveal that criminals have more opportunity and incentive to gain access to sensitive information through the Web application [1]. 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 stand at great risk to cyber-attacks occasioned by outsiders as well as insider students and staff who use their expertise to hack [15].

With the high percentage of internet users, it will be quite stressing that the number of security professionals will remain dismal and unable to match the entire population's percentage that uses the internet [8]. According to Messer and Medairy (2018) 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 through networks and datasets to discover hidden threats.

As a result of carrying out 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 with respect to students, staff, examinations, financials and third-party engagements that need to be safeguarded against attacks, universities must employ effective defensive cyber security preparedness strategies.

2. Problem Statement

In order 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 personal 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 are able to 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 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, but 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 surface in institutions of higher learning where students and staff sensitive information and valuable assets is of high stake. The huge amounts of data related to security not only make these approaches too prone to error but also labor intensive while providing users a “big picture” of their overall cyber situation. Cyber security metrics for CSA, mission assurance analysis and synchronized network defense are being overlooked by current systems hence there is need to develop a defensive security model that will take into account 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 develop model to assess defensive cyber security preparedness in Universities

4. Research Question

i. How can a model to assess defensive cyber security preparedness in Universities be developed?

5. Limitations of the Study

The proposed defensive cyber security model was developed and was intended to be easily adaptable across entire universities. It may not be possible to implement out the study due to the knowhow constraints, and therefore the model was made customizable and learnable.

6. Literature Review

6.1 The evolving threat landscape

Following an interconnected and more open nation supported by the aggressive advancement in technology has offered adversaries avenues for exploiting computer networks in Kenya. The frequency of cyber attacks and the probability of success over time are continuously increasing and to a great extent faster than cyber defenses [12]. An attack progression from 1980-2014 is provided in Figure 1 below. The hacktivists pursuing publicity of political views, terrorist groups pursuing to cause financial or political harm, criminal organizations seeking financial gain, and security organizations advancing their own economic or national security aims or from state-sponsored intelligence are key architects of these cyber-attacks. Many attacks involve social engineering techniques and extremely sophisticated technological methods; insider threats remain a danger regardless of low-technology penetrations. The evolving threat landscape is summarized in Figure 1 below by the Ministry of ICT (2014).

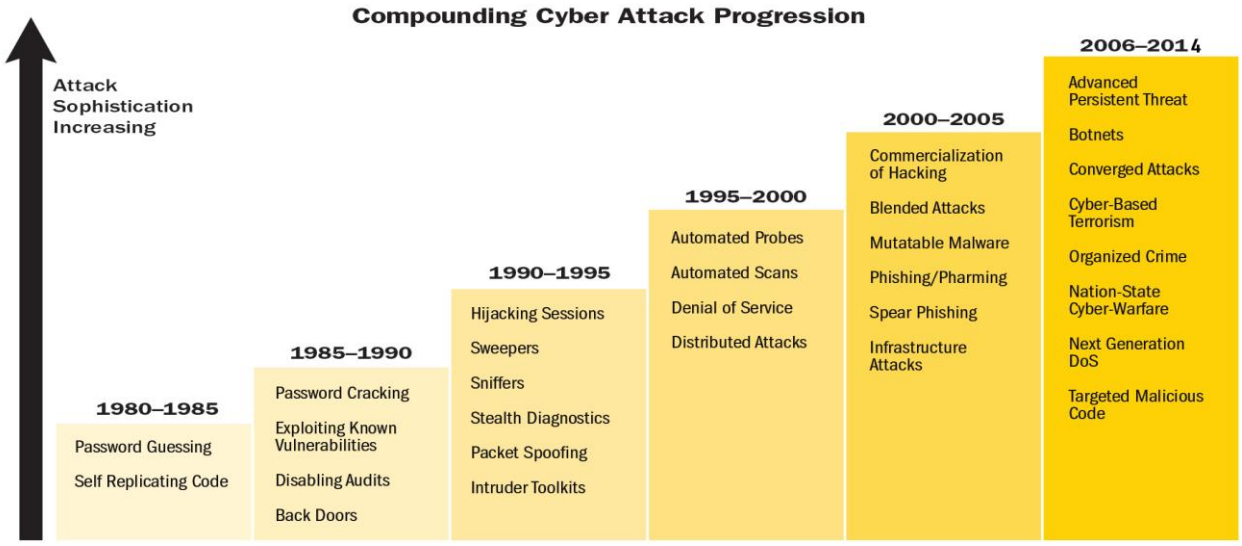


Figure 1: Sophistication of Cyber-attack Progression from 1980-2014

Source: (Ministry of ICT, 2014)

6.2 The magnitude of threat existence in universities

According to Cilluffo (2018), the speed at which technology evolves is magnified and the threat tempo is accelerating. With IT systems that are open, permissive, and widely disseminated, educational institutions especially universities across the globe faces top risks like 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 targets 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 [16]. Learning has been made easier with students learning on their own pace and access educational materials anywhere anytime. Majority of the students wants 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. This is according to RSI Security (2019).

6.3 Existing models guiding defensive cyber security

Theoretically, numerous models to the management of cyber security have been advanced. This study will use the Business Model for Information Security by ISACA, the ISO/IEC 17799 Information Security Management and the EMC Corporation's Intelligence Driven Information Security Model to get more insights into the theory of cyber security management.

1 The business model for information security

Conceptually the Business Model for Information Security is best depicted as an adaptable, three dimensional, pyramid formed structure made up of four components connected up by six element interconnections. The dynamic interconnections go about as strains, applying a push and draw constraints in response to changes in the venture, permitting the model to adjust as required. The four components of the model are: organizational strategy and design, processes, people and technology. The interconnections are governance, culture, enabling and support, emergence, human factors, and architecture. This is well explained by ISACA (2009).

2. ISO/IEC27001 Standard

The International Electro-technical Commission (IEC) and the International Organization for Standardization (ISO) are two international bodies that formulate standards for best practice in different fields worldwide. ISO and IEC joint technical committees (JTC) work together in fields of reciprocal interest [17]. ISO/IEC 27001 is an international standard that was published in 2005 as ISO 27001:2005 and revised in 2013 by the JTC as ISO 27001:2013. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature [21].

Basically, the ISO/IEC 27001 standard was developed to provide protection to the assets in the organization and therefore it is a good starting point when developing information security. The standard provides the requirements for establishing, implementing, maintaining, and continually improving the Information Security Management system (ISMS), and can be applied to all types of organizations ranging from government agencies to non-profit organizations, to commercial enterprises [13]. The purpose of the ISMS is to provide tools,

processes, and ways of working in order to improve the level of information security within organizations that implement it. It uses IEC/ISO 27002 to specify appropriate controls for information security contained by the ISMS [13].

However, organizations are free to select and implement other controls as they see fit Annex A since IEC/ISO 27002 is merely a guideline rather than a certification standard [7]. The standard incorporates a summary of controls and contains actual requirements part from IEC/ISO 27002 in Annex A, which catalogs a set of 133 controls grouped into 11 clauses from which an organization can choose through a process called Statement of Applicability (SOA). The eleven clauses are; A.5 Security Policy, A.6 Organization of Information Security, A.7 Asset Management, A.8 Human Resource Security, A.9 Physical and Environmental Security, A.10 Communications and Operations, A.11 Access Control, A.12 System Acquisition, Development and Maintenance, A.13 Information Security Incident Management, A.14 Business Continuity Management, and A.15 Compliance [6].

3. NIST Framework

The NIST cyber security framework (CSF) takes a more holistic approach than the ISO/IEC 27001standard as depicted by its implementer's view in figure 2 provided below. However, the NIST Cybersecurity Framework is a risk-based approach to managing cyber security risk and is composed of three parts: **The Framework Core, the Framework Implementation Tiers, and the Framework Profiles** [14]**.**

The Framework Core consists of five concurrent and continuous functions namely **Identify, Protect, Detect, Respond and Recover** [9] as provided in Figure 3 The **Framework Implementation Tiers** provides context on how an organization views cyber security risk and the processes in place to manage that risk. The Tiers characterize an organization's practices over a range from **Tier 1: Partial, Tier 2: Risk-Informed, Tier 3: Repeatable & Tier 4: Adaptive**

Finally, the **Framework Profile** represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories [3]. Profiles can be used to identify opportunities for improving cyber security posture by comparing a "**Current" Profile (**the **"as is"** state**)** with a **"Target" Profile** (the "**to be**" state). **Therefore, NIST** is generally viewed as a comprehensive and living framework. It will change along with the changing risk and regulatory environments. It brings in **Best Practices** from **ISO 27001:2013, COBIT 5, NIST SP 800-53 and ISA 62443-2009** standards [3].

	ISO/IEC 27001	NIST CSF
Orientation	Process-oriented	Outcome-oriented
Action drivers	Risk-driven control requirements	Focused on risk mitigation
Approach	Prescriptive, management system Rule-based	Adaptive, risk-driven
Mantra	**"What you have to do"**	Open to prioritization, improvise **"What you want achieved"**

Figure 2: Implementer's View

Source: (DiMaria & Tse, 2018)

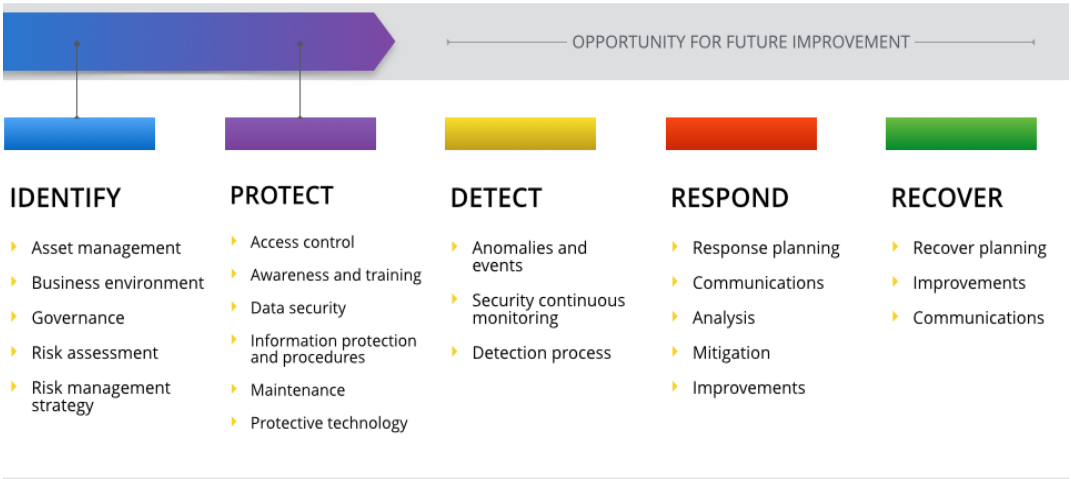


Figure 2: NIST Mitigation Framework

Source: (Kumar, 2014)

7. Research Gap

According to the literature reviewed, the researcher noted that very little had been done concerning cyber preparedness in education sector especially in universities. Though ISO 27001 and NIST cyber security frameworks have both laid the foundations but little has been done in institutions of higher learning as compared to other sectors such as financial and health institutions. This attributed to the evolving nature of cyber-attacks. Few years ago attackers majorly focused on financial and health institutions such as banks and hospitals but lately learning institutions especially Universities have fallen victims of cyberattacks. The table 1 below provides a summary of the identified gaps that the researcher intended to provide a solution:

Table 1: Research Gap Summary Table

Author	Year	Title of the research	Existing Gap
Ikovo V. Ngundi	2018	Cybersecurity Preparedness Toolkit	Only focus on SMEs and their top management Does not lay emphasis on training and sensitization Lacks adequate reporting mechanisms and relies only on NIST and CERT frameworks
Melissa Hathaway *et al*	2015	Cyber Readiness Index 2.0: A Baseline and an Index	The cyber security readiness index measures a country preparedness and commitment to cyber security in its infrastructure. The only downfall to this methodology is that it focuses on country's infrastructure in general and does not narrow down to specific organizations such as institutions of higher learning like universities.
Maina P. King'ori	2014	Assessment of awareness and preparedness of cyber café internet users to deal with threats of cyber crimes	It centers on knowledge, attitude, and exposure issues of users without looking on the safeguards in place to determine how prepared they are It noted lack of sufficient cyber security knowledge and does not provide adequate policies or rules on organizational culture stating how employees are expected to behave
Serianu limited	2017	Africa Cyber Security Report: Demystifying Africa's Cyber Security Poverty Line	The study reveals a lot of gaps both exposed to private and public companies relating to limited visibility of database activities, compromised administrator accounts, very inadequate patch management, trainings and awareness done after an incident, Tool analysts IT teams and board members relying on standard audit reports to understand the security posture of the organizations
Messer & Medairy	2018	The Future of Cyber Defense...Going on the Offensive	The study talks of a good approach that pairs best-in-class Cyber Defense tools with trained threat analysts who have a deep understanding of their operating environment and an ability to ask the right questions. Though it's a great step in advancing the issue of advance threat hunting, the study does not clearly indicate how the process will be achieved
Too W. Kipkoech	2019	A model to assess defensive cybersecurity preparedness in universities	From the reviewed literature, most of the research that has been conducted are centered on Healthcare and Financial sectors. There is little research conducted in higher learning institutions, especially universities. The researcher filled the existing gaps from the reviewed literatures by designing a model for assessing defensive cyber security preparedness as a web application by incorporating the 3 elements of cyber security in an organization namely: Human factors, Technology factors and Policy factors, in conjunction with the client's current security posture, to offer a proactive, defense in-depth solution focused on finding malicious actors. The assessment model will be available online and also provide relevant recommendations thus solving the downfalls of the existing models.

7. Research Design

The model development was achieved using design science approach to serve as a solution for assessing defensive cybersecurity preparedness in universities. The design science paradigms is given in the figure below.

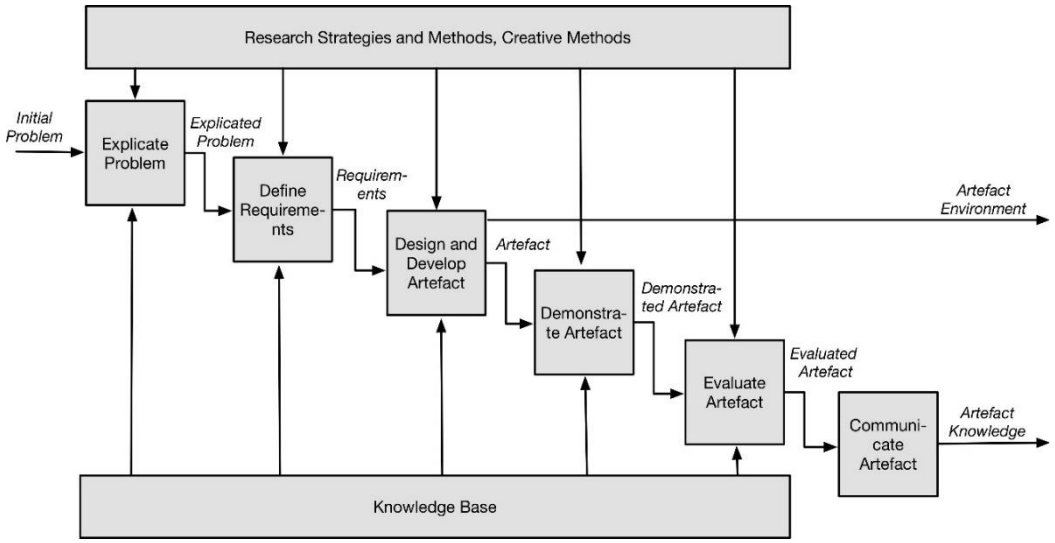


Figure 4: A Model Development using Design Science

Source: Johannesson & Perjons (2014).

8. Software Engineering and Design

The model's software engineering and design were accomplished with the PHP programming language for controls, the MySQL database engine for storing system data, JQuery and Javascript for adding responses to the system, and CSS3 for styling the model's layout. This section explains how the various components of the model for assessing defensive cybersecurity preparedness were created

9. Implementation of Regression Equation

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

The regression equation was provided as and utilized in model development; where:

Y= defensive cyber security preparedness

C=Constant

$x_1 = Human\ factors$

$x_2 =$ Technology $factors$

$x_3 = \text{Technology } factors$

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

$\varepsilon = standard\ error$

Therefore, the above formula from analysis was then coded as is into the model as shown below:

```
<? php

{user_id = $_SESSION ('admin');

$ sql = "SELECT ROUND (100 * (( -0.025 + sum( user_score * weight)) (0.025 + (-0.025 + sum(5*(weight))),
1) FROM Prepareness_assessment WHERE user_id='$user_id'";

$result = mysqli_query($conn,$sql);

$data = mysqli_fetch_array($result);

$defn = $data[0];

if ($defn = =0) {

Echo 0;

}

}

?>
```

10. Results and Discussion

The developed model demonstrated the prototype which contained various modules as under:-

i. User Module – to enable new users to register so as to access other system functionalities
ii. Login Module – to strictly allow authorized users to access the system functionalities after providing correct credentials
iii. Assessment Module – to allow users the assessment queries where the results will be stored in the database for use in computing the preparedness index
iv. Reports Module – to allow the users to view their scores and recommendations of the submitted assessments

The prototype model for implementation is as shown in the figure below:

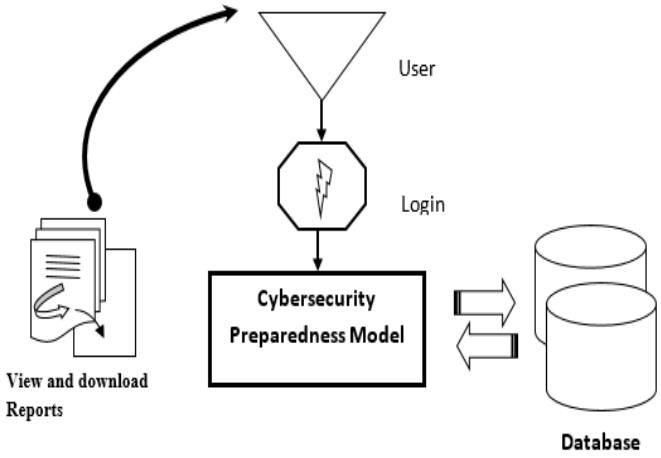


Figure 3: Model Implementation Framework for Defensive Cybersecurity Preparedness in Universities

Source: (Researcher, 2019)

i. Registration module

The registration module acts as the platform's entrance point. To gain access and perform defensive cybersecurity preparedness assessment, any respondent must first register to the platform. This procedure entails providing information such as the user's name, email address, institution, username, and strong password to the system that will be utilized to get access to the system on subsequent logins.

Figure 6: User Registration Form

Source: Researcher (2021)

ii. Login module

This is the part where only registered authorized users are allowed to access and carry out system functions. Basically, users who supply the system with the right login credentials will be given access rights to perform

system functions while denying the unauthorized ones.

Figure 7: Login Form

Source: Researcher (2021)

iii. Dashboard

This is the part that leads the user to the homepage upon successful login. When active assessments are in place, the user can get a fast overview of their cybersecurity assessment statistics. This includes the overall percentage index indicating their preparedness in terms of defensive cybersecurity. The dashboard is denoted by 0 when no new user records thus indicating no active assessments. The system dashboard for a new user with active assessments is given in figure 7 below. Still at the dashboard, all active assessment average scores and recommendations of actions required for optimum preparedness can be obtained for all signed-in users.

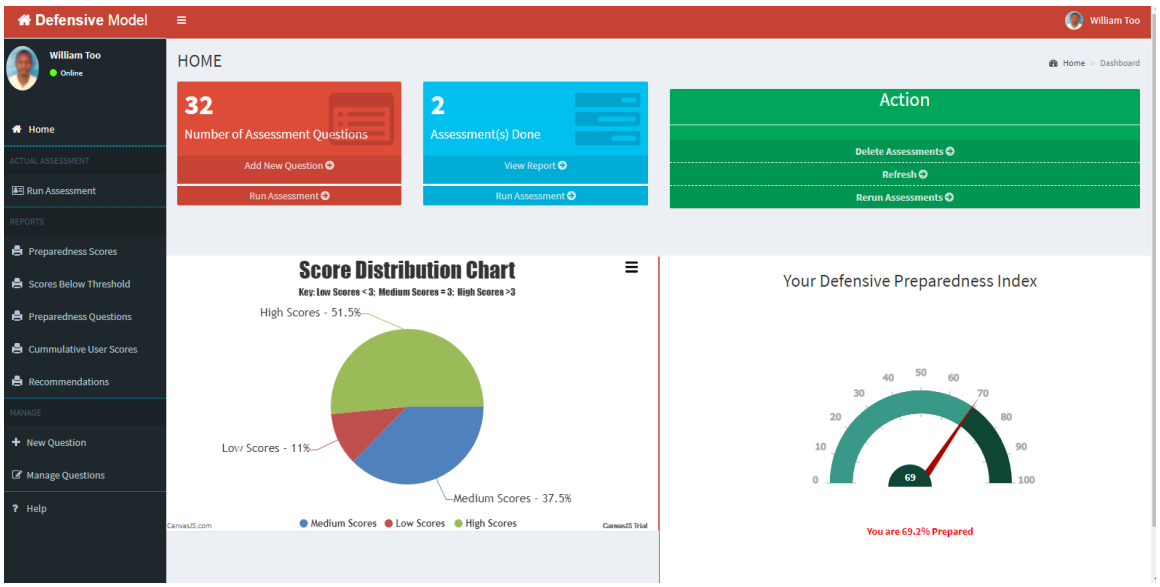


Figure 8: Dashboard with two Active Assessments for the logged-in user

Source: Researcher (2021)

iv. Cybersecurity preparedness assessment

This module extracts the defensive cybersecurity preparedness assessment questions from the database and presents them in a likert scale between 1 to 5 and where they can make appropriate choice.

The defensive cybersecurity preparedness assessment module also allows the users to choose the most appropriate responses to each preparedness assessment statements and to submit their dully-filled form to the database.

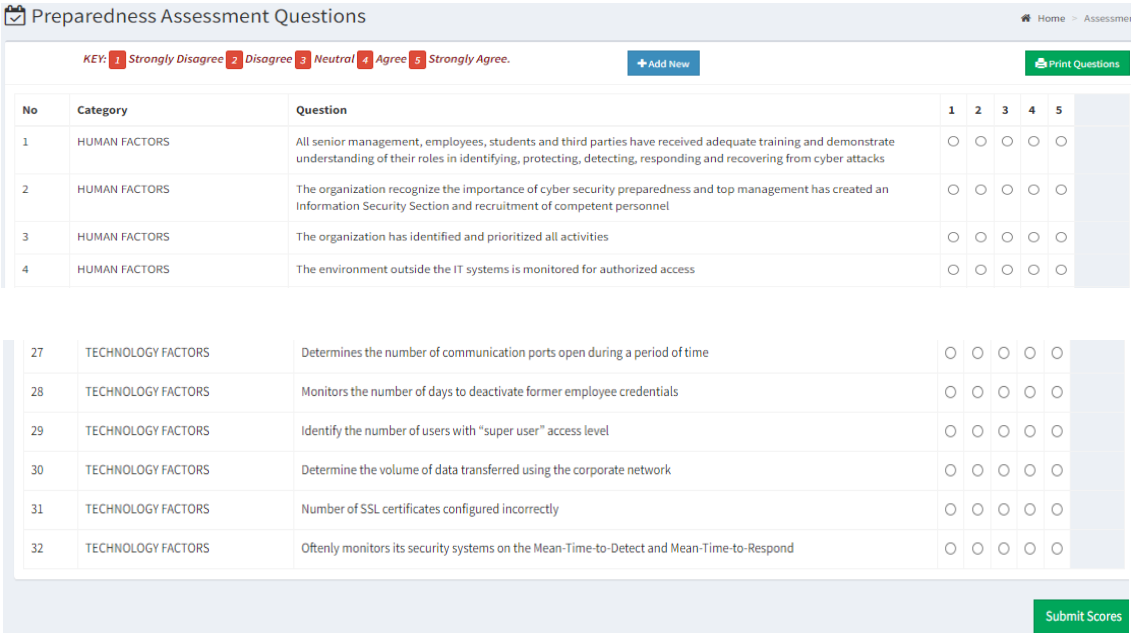
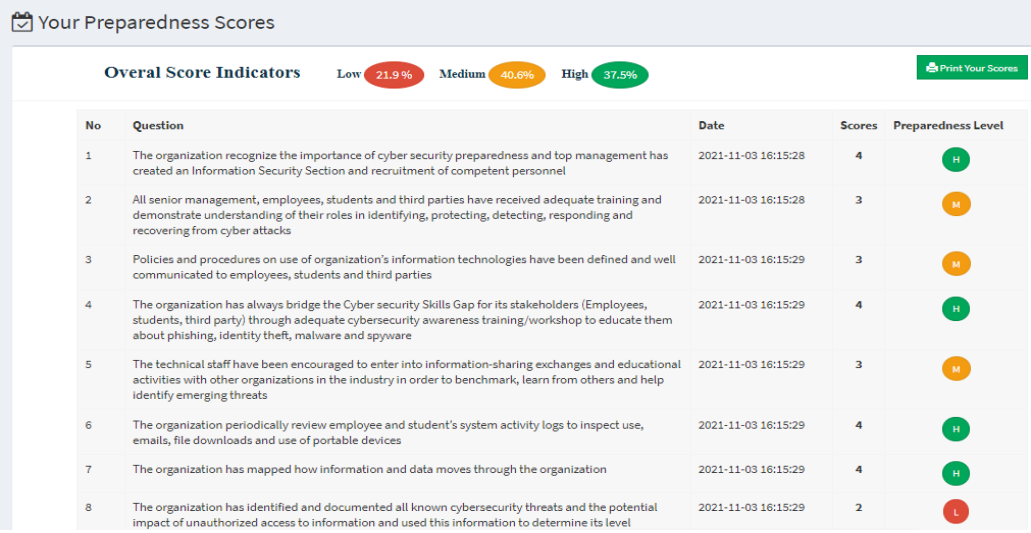


Figure 9: Preparedness Assessments Page

Source: Researcher (2021)

v. Cybersecurity Preparedness Scores

This component was created to capture and return to the user the cybersecurity readiness assessment scores stored in the database. This was deemed necessary for customers to go back over their past assessments and check how they scored various cybersecurity preparedness claims. The module was designed to filter the scores of the currently logged-in user while avoiding accessing or interfering with the records of other users. Users can only access their assessment results, which are listed and categorized by the dates of the cybersecurity readiness exams. This module allows users to see the cores for all of their cybersecurity preparedness exams, regardless of how many times they completed them. As a result, the user can read the scores in HTML format, print them out, or download them as a portable document (pdf).



Your Preparedness Scores

Overal Score Indicators Low 21.9 % Medium 40.6% High 37.5%

Print Your Scores

No	Question	Date	Scores	Preparedness Level
1	The organization recognize the importance of cyber security preparedness and top management has created an Information Security Section and recruitment of competent personnel	2021-11-03 16:15:28	4	H
2	All senior management, employees, students and third parties have received adequate training and demonstrate understanding of their roles in identifying, protecting, detecting, responding and recovering from cyber attacks	2021-11-03 16:15:28	3	M
3	Policies and procedures on use of organization's information technologies have been defined and well communicated to employees, students and third parties	2021-11-03 16:15:29	3	M
4	The organization has always bridge the Cyber security Skills Gap for its stakeholders (Employees, students, third party) through adequate cybersecurity awareness training/workshop to educate them about phishing, identity theft, malware and spyware	2021-11-03 16:15:29	4	H
5	The technical staff have been encouraged to enter into information-sharing exchanges and educational activities with other organizations in the industry in order to benchmark, learn from others and help identify emerging threats	2021-11-03 16:15:29	3	M
6	The organization periodically review employee and student's system activity logs to inspect use, emails, file downloads and use of portable devices	2021-11-03 16:15:29	4	H
7	The organization has mapped how information and data moves through the organization	2021-11-03 16:15:29	4	H
8	The organization has identified and documented all known cybersecurity threats and the potential impact of unauthorized access to information and used this information to determine its level	2021-11-03 16:15:29	2	L

Figure 10: Cybersecurity Preparedness Scores in HTML output

Source: Researcher (2021)

vi. Recommendations

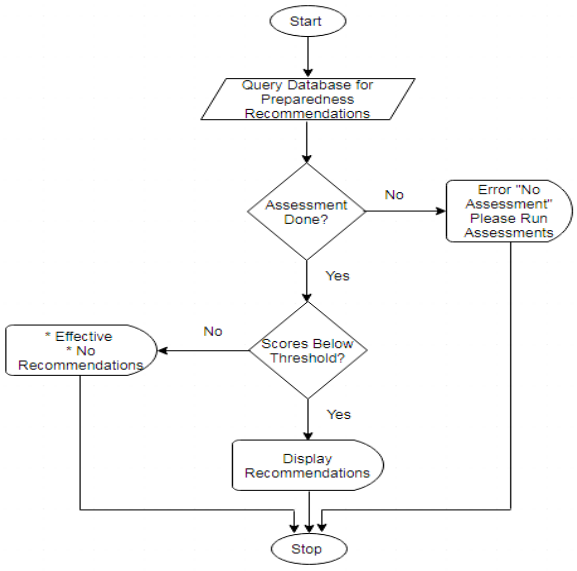
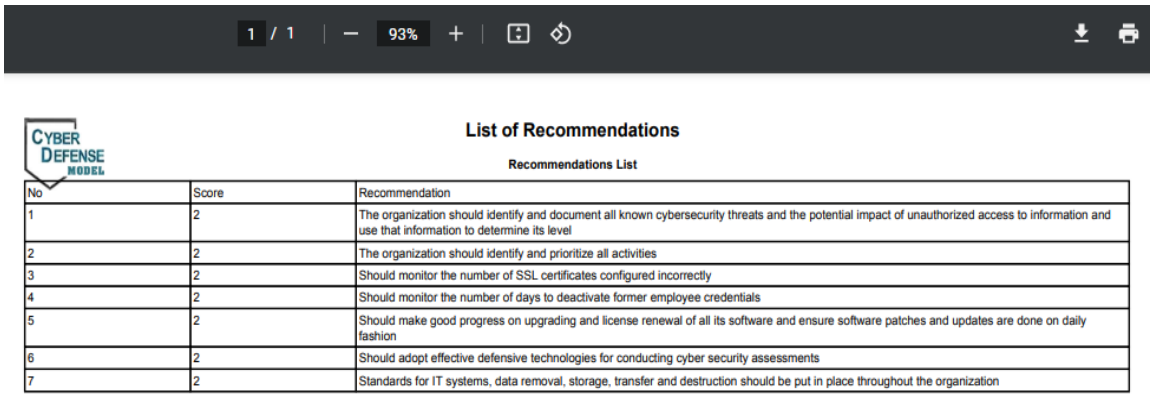


Figure 11: Cybersecurity Preparedness Recommendation Flowchart

This is a results-display module whose output is based on the active preparedness assessmentts of logged-in users. The system verifies if the logged-in user has completed cybersecurity preparedness assessments, and the results are saved in the database as shown in figure 9. If no such records exist, the system instructs the user to conduct a new assessment and submit the results to the database. Otherwise, the system compares the logged-in user's database preparedness scores to the associated threshold scores. If the scores fall below the threshold, the system generates a list of conditions that must be met in order to achieve optimum preparedness. The

cybersecurity readiness suggestions are available in pdf format, which the user can download or print. The PDF result of the cybersecurity preparedness recommendation module is shown in Figure 10.

Source: Researcher (2021)



No	Score	Recommendation
1	2	The organization should identify and document all known cybersecurity threats and the potential impact of unauthorized access to information and use that information to determine its level
2	2	The organization should identify and prioritize all activities
3	2	Should monitor the number of SSL certificates configured incorrectly
4	2	Should monitor the number of days to deactivate former employee credentials
5	2	Should make good progress on upgrading and license renewal of all its software and ensure software patches and updates are done on daily fashion
6	2	Should adopt effective defensive technologies for conducting cyber security assessments
7	2	Standards for IT systems, data removal, storage, transfer and destruction should be put in place throughout the organization

Figure 12: Cybersecurity Preparedness Recommendation PDF

Source: Researcher (2021)

11. Conclusions and areas for further research

The defensive cybersecurity model was developed by employing mathematical concept. A regression analysis was carried immediately after the correlation was done between the defensive cybersecurity preparedness and each of the three factors (human, technology and policy). The model was developed as a web-based and made to appear friendly to all users who can register to use the system.

Once an assessment is done, preparedness level will be displayed and ICT experts will be able to gauge the effectiveness and areas of its system that need improvements in terms of countermeasures. In addition, the recommendation that will be gathered from the system gives proper opportunity to the ICT experts to provide sound advice to the management and other stakeholders on the right way to go without compromising its valuable information assets. A study on secure and trustworthy defensive cyber security systems that can scale identity management and traceback techniques for tracking down adversaries should be considered in future research.

References

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

[2] 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

[3] Cybersecurity. (2014). *Framework for Improving Critical Infrastructure*

[4] DiMaria, J., & Tse, R. (2018). *Case Study - The Business and Regulatory Value of Third Party Certification to the NIST Cybersecurity Framework*.

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

[6] Irwin, L. (2019, March 18). ISO 27001: The 14 control sets of Annex A explained. Retrieved June 13, 2019, from IT Governance Blog website: https://www.itgovernance.co.uk /blog/iso-27001-the-14-control-sets-of-annex-a-explained

[7] Kalechava, B. (2017, January 4). Information Security Management System (ISO/IEC 27000 Series). Retrieved June 10, 2019, from The ANSI Blog website: https://blog.ansi.org/2017/01/ information-security-management-system-isoiec/

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

[9] Kumar, D. (2014). NIST Cybersecurity Framework v1.0: Key Takeaways

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

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

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

[13] Mutai, J. (2017). *Assessing Security Risk Exposure in Kenyan Savings and Credit Cooperative Societies using a Web Based Model to Compute Security Risk Exposure Index*. *2*(1), 11.

[14] Mwambe, O. O., & Echizen, I. (2016). *Security modeling tool for information systems: Security Oriented Malicious Activity Diagrams Meta Model Validation*.

[15] 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.

[16] 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.*

[17] Schweizerische, S. V. (2013). Information technology-Security techniques-Information security

management systems-Requirements. ISO/IEC International Standards Organization

[18] Serianu, (2017). Kenya CyberSecurity Report 2017: *Demystifying Africa's Cyber Security Poverty Line*

[19] 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

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

[21] Weiss, M. M., & Solomon, M. G. (2016). *Auditing IT infrastructures for compliance* (2nd Edition). Burlington, MA: Jones & Bartlett Learning.