The Defensive Cyber Security Readiness Model for Higher Education

William Kipkoech Too[1]; Alex Kibet [2]

[1]Department of Information Communication Technology, Egerton University, Kenya
[2]Department of Computing and Informatics, Laikipia University, Kenya

Publication Date: 2025/04/02

Abstract: Cybersecurity entails a variety of concepts, tools and practices that are closely related to those of security aligned to information and operational technology. Citizens worldwide now have easy access to the internet, broadband, and fiber connectivity due to recent technology adoption. Threats to general cyber security, such as financial fraud, social engineering schemes, and virus attacks, have grown. Despite the fact that numerous standards like NIST and ISO have came up with a number of security models, the majority of businesses and organizations, as well as the cyber-security industry itself, are ill-prepared for the growing number of cyberattacks. This is due to the fact that the majority of security analysis systems now in use are primarily concerned with attack detection. Because of this circumstance, the attack surface has been continuously expanding in institutions of higher learning where sensitive data and valuable assets are highly valued by staff and students. This study was to evaluate the defensive cyber security preparedness model for Universities. The study utilized a goal-based method to evaluate the model based on its functionality, usability, reliability, efficiency, and maintainability metrics. The evaluation results from the experts conducted indicate that the model is over 80% satisfactory. This study is very significant as universities will be able to ascertain their preparedness status as well responding to outlined recommendations that will ensure they stay safe from future evolving cyber threats.

Keywords: *Fiber, Cybersecurity, Cyber-Attack, Preparedness, Metrics.*

How to Cite: William Kipkoech Too; Alex Kibet (2025). The Defensive Cyber Security Readiness Model for Higher Education. *International Journal of Innovative Science and Research Technology*, 10(3), 1763-1771. https://doi.org/10.38124/ijisrt/25mar1158

I. INTRODUCTION

Global connectivity and users' access to information from outside the company raise risk beyond what general and application controls in IT have traditionally been able to handle. Traditional assessments of IT general and application controls are insufficient to provide assurance over cyber security due to organizations' dependence on information systems and the advancement of new technologies (GTAG, 2016). By installing terrestrial and underwater cables and networks, expanding the availability of mobile and wireless technology, and advancing e-government services, the Kenyan government is encouraging the use of ICT by both the government and the Kenyan populace (Ministry of ICT, 2014).

In Kenya, university education is one of the areas of the education system that is growing the fastest. Many students who cannot be accepted into Kenyan universities are applying to universities abroad, which has increased demand for higher education (Ministry of Education, 2016). E-learning program implementation in Kenyan universities and determining the requirements and readiness of students to participate in e-learning environments also call for a great deal of research and study (Shahmoradi *et al.*, 2018).

In addition to facing rising expectations from students and faculty for greater digital capabilities, educational institutions are also seeing an increase in hackers targeting them. The attack surface has increased as a result of this, as more gadgets and apps are connected to the network per person (Biddle, 2017). Given that 72% of students connect two or more devices to campus networks simultaneously, schools must strike a balance between providing a seamless IT experience for staff and students and protecting against an influx of endpoints that they do not own. In order to give students the flexibility to work from wherever at any time, broadband has also been installed in the nearby dorms. As students connect their personal devices to the network, this situation leads to unchecked network growth. Because every firm tends to go online for their services, such as cloud computing, which is primarily used in Kenyan institutions that embrace e-learning programmes, it is a prevalent standard in the nation with a high number of technological dependences brought on by several assault sites; these uncontrolled nodes/devices hooked to the network are avenues for cyber-attacks (Update, 2017).

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 (Beniwal, 2015). 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 (Neaimi *et al.*, 2015).

➢ *Problem Statement*

Kenya's government has enacted policies to increase access to higher learning especially the university education. This has in turn resulted in an unprecedented increase in the number of students joining universities in comparison to the infrastructure that is now in place, including ICT. In order to improve the current ICT infrastructure, institutions of higher learning has instituted a Bring Your Own Device (BYOD) policy and student and employees personal devices can now be easily connected to the university network. These connected devices pose a great danger to institution's sensitive data and valuable assets as threats to general cyber security, such as financial fraud, social engineering schemes, and virus attacks are advancing their threat landscape daily. Despite the fact that numerous standards like NIST and ISO have came up with a number of security models, the majority of businesses and organizations, as well as the cyber-security industry itself, are ill-prepared for the growing number of cyberattacks.

Therefore, in order to provide a solid model for the institution's competitive advantage, universities must regularly evaluate their cybersecurity posture to stay up with the rate at which threats are expanding their attack surface.

➢ *Objective of the Study*

- To evaluate the defensive cyber security readiness model for higher education.

➢ *Research Question*

- How to evaluate the defensive cyber security readiness model for higher education?

II. LITERATURE REVIEW

➢ *Metrics for Monitoring Defensive Cybersecurity Readiness*

The difference between a project that is useful and efficient and one that is a total waste of money can be determined by how well certain information security performance metrics are managed.

Despite the fact that managers have been using KPIs in information security for a while,,This phenomenon is rare and still evolving practice to track cyber security metrics (Cipher, 2017). To guarantee the effectiveness of security projects, several recommendations for cyber security metrics that can and should be monitored are covered here.

Based on the degree of automation implemented, there is a corresponding reduction in Mean-Time-to-Detect and Mean-Time-to-Respond (MTTR) and the ability for a defender to close more cases (Trull, 2017). Mean Time To Identify (MTTI) and Mean Time To Contain (MTTC) for US companies indicates that the Detect and Respond Phases are suffering. The MTTC in 2017 was 208 days and the MTTI was 52 days. At the same time, the likelihood of incurring a mean breach cost of $2.25M is almost 28% over the next 24 months for U.S. companies.

One of the main causes of breach expenses is subpar MTTI and MTTC performance. When assessing information security, these two KPIs ought to be your top priorities. For long-term improvement, CISOs can measure and present this KPI to their board. Enhancing these two KPIs should be a top priority for every member of the security team.

Continuous risk assessment that automatically recognizes and ranks cyber security threats, permits effective distribution of cyber security resources, and improves defense against contemporary cyberthreats is necessary for defending company networks (Lippmann & Riordan, 2016). The effectiveness of security projects can be ensured by following these recommendations for cyber security metrics that can and should be monitored.

A crucial cyber security indicator for assessing the risk your company faces is knowing how many assets in your environment are at risk.To guarantee that systems are kept current and less vulnerable to common vulnerabilities, all software patches and hardware updates must be completed on schedule. In order to prevent vulnerabilities that could be exploited in your environment, patch and update management is a complicated process (Lykou *et al.*, 2018).An asset-wide vulnerability check will show you what needs to be done to strengthen your company's security posture. Rather than being a polite gesture, a vulnerability management program is essential.It is crucial to ascertain the quantity of SSL certificates that are improperly setup.

It is possible to keep certificates out of the wrong hands and ensure that your company's digital identity is not used to steal user information by keeping an eye on each certificate's security requirements and making sure servers are installed correctly. There is an increase in data traffic on business networks. A new network design will be necessary for company success in the future (Molck-Ude, 2019). You can spot resource abuse if your employees have unfettered access to the internet via the workplace network by keeping an eye on traffic volume.

Users that download software, movies, videos, and applications may be opening the door for botnets and malware to infiltrate their environments. This is especially true if the downloads come from websites that are known to be harmful. One of the most important aspects of information security management best practices is having complete control over user access to company resources. Only the systems, information, and resources required for their job must be accessible to employees.Permitting users to use their own devices to connect to the network might cause chaos because it is hard for IT departments to regulate

(Poremba, 2017). All network users' access levels can be categorized so that you can prohibit any illogical administrators or superusers and change them as necessary.

When an employee leaves, it is not only crucial but also required to protect company data (Preston, 2019). You can determine whether IT teams and human resources are working together by keeping an eye on these cyber security metrics. Ideally, users who are fired from the company should have their access immediately revoked.Maintaining them in use poses a serious danger since it might result in compromised devices and the loss of private data. For security reasons, it's also important to keep an eye on how many communication ports are open at any given time. The two main categories of port scanning are horizontal and vertical scanning. While the more popular horizontal scans are used to identify hosts for a certain open port, vertical scans are used to identify open ports of a single host (Ring *et al.*, 2018). Generally speaking, you should not let NetBIOS inbound traffic (TCP 135-139 and 445, UDP 137 and 138). Keep an eye out for SSL (TCP 443) outbound traffic: a prolonged session may indicate an SSL VPN tunnel that permits bi-directional activity. For a considerable amount of time, any common ports for protocols that permit remote sessions, such as TCP 22 (SSH), TCP 3389 (RDP), TCP 23 (telnet), and TCP 20 and 21 (FTP should be watched.

In order for third parties to finish a project or activity, IT administrators typically allow them access to their networks.After developers and IT specialists, third-party vendors pose the second-highest safety risk to the company (Walsh, 2017).

It's critical to keep an eye on whether access is terminated at the conclusion of service delivery. If you don't, you put your surroundings at risk in case the third party returns to steal data or engage in other harmful activities. For example, they might work for a rival company. Even worse, you can put your network at risk if the third party's network is compromised. In the context of security, it is crucial to map out the company's vital systems and identify the users who have access to them.Both the use of third-party providers and the breaches linked to them are common (Francis, 2017).

Tracking efforts by unauthorized individuals to access servers or programs that shouldn't be accessible could reveal wrongdoing and attempts to compromise your environment. Even if cyberattacks are getting more frequent, the majority of firms admit that their defenses are insufficient (Levin, 2018). Monitoring the percentage of business partners with effective cyber security policies is important. You must maintain strict control and monitor the cyber security metrics of the companies that provide services for your business. Giving access to your environments to this outsourced company can be a huge risk if it does not have effective policies for its safety in the first place. It is not too much to say that if your company invests in security but has third parties connected to your systems that do not, you have no security at all.

- *Model Evaluation*

Model evaluation is a crucial step in the model creation process. In this study, the model was assessed in relation to the predetermined goals using the "Goal-based evaluation of IT systems as such" approach. This approach only requires the the involvement of the evaluator hence the end users are not involved. This means definition and specification of the systems requirements serve as the basis for the evaluation criteria that are employed (Cronholm & Goldkuhl, 2003).

The model was assessed based on user registration, which involved adding a user to the database so that the database server could validate it upon completion of a request. The authentication procedure ensured that unauthorized users were rejected and verified that the correct users could log in to the system without any issues. Additionally, to guarantee that service-choosing customers can obtain the appropriate services they need when they ask for them.

Program and acceptance testing criteria were used to evaluate the new model's functionality under a variety of conditions, including normal and peak loads. The evaluation was conducted by asking actual users of the finished model to rate how well it satisfies their needs and expectations, which include completeness, accuracy, reliability, consistency, efficiency, integrity, user-friendliness, maintainability, resilience, tracking, and performance measurement.

III. RESEARCH METHODOLOGY

This study was achieved through a goal-based method where 11 ICT experts were conducted to evaluate the defensive cybersecurity preparedness model for universities based on its functionality, usability, reliability, efficiency, and maintainability metrics.

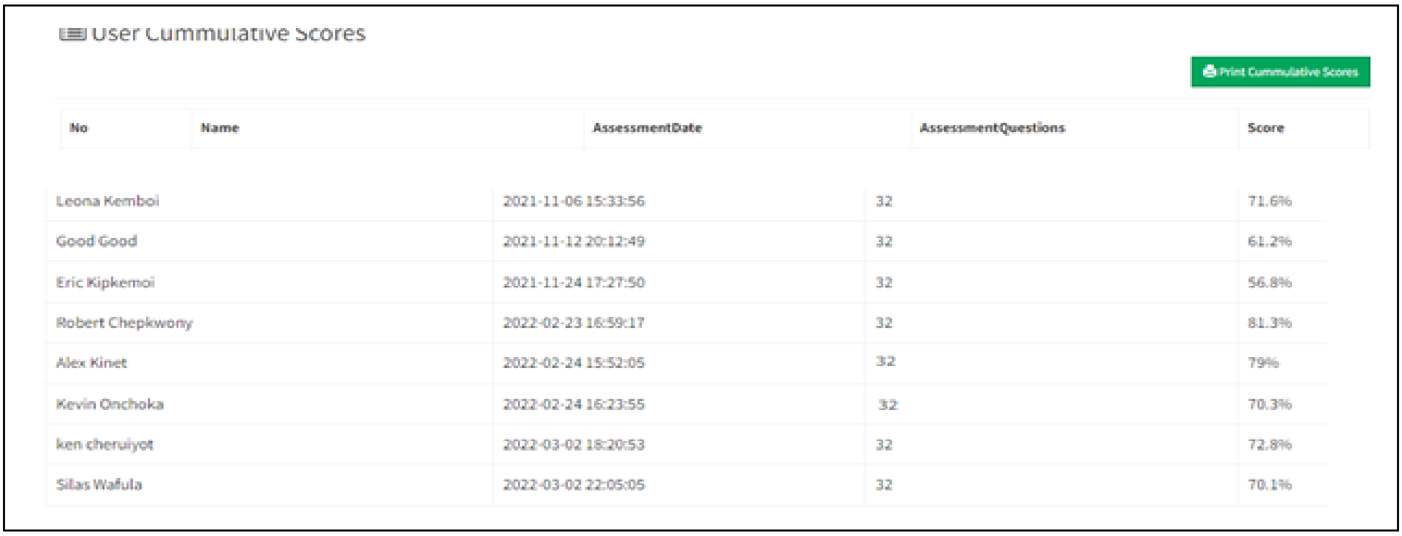
- *Evaluation of the Model Procedure*

After the design phase, the model was tested to see if it could accomplish the goals it was created for. The intended objectives were established prior to the design process and were utilized as a deliverables checklist for evaluation after the design was completed. Besides the designer’s objective evaluation, the model remote URL was sent out to as many (ICT experts) users as was possible to verify the model by registering as users, logging in, and performing cybersecurity preparedness assessments which was the primary purpose of the model. These experts (mainly ICT Managers/Directors, IT Security Managers, System Administrators, Network Administrators, and IT Support Officers) upon successful login and running assessments were expected to evaluate the model based on its functionality, usability, reliability, efficiency, and maintainability metrics as outlined in the model evaluation questionnaire that was provided to them. The delivered outcomes were reported alongside the desired aims in table 1 below. All of the objectives were met, as stated in the table. To summarize, the system performs the functions it was designed to do.

Table 1 Objective Assessment

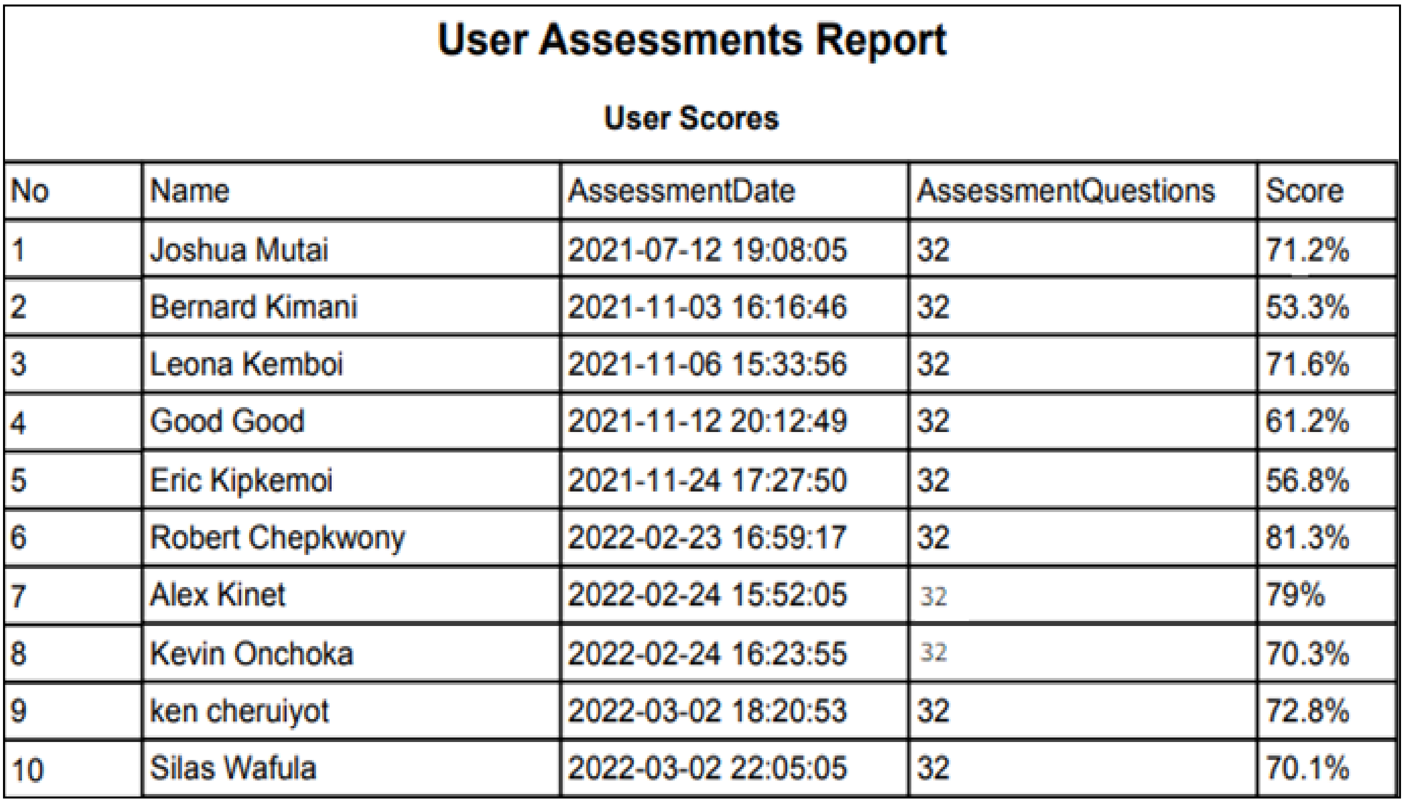
Evaluation Metric	Aims	Expert Evaluation Outcomes
Functionality	1. Check for data accuracy . Explore the suitability of the model Check for the model role compliance	The model outputs the correct results from the right user data input All the information provided by the model helps the user to effectively complete the available tasks. 3. All key model functionalities are working as expected
Usability	To check the model for: 1. Learnability 2. Efficiency 3. Errors 4. Memorability 5. Attractiveness 6. Subjective Satisfaction	The model is easy to learn and use with clear information displayed on the screen 2. Users can complete tasks provided quickly The model provides clear information on how to fix error problems when they occur It is easier to get re-established to the model even after a long period of not using it 5. The model user interface is user friendly The model comfort of use and overall performance is very satisfactory
Reliability	To measure the model reliability in terms of its: 1. Maturity 2. Recoverability 3. Availability	The model is complete and well designed with dashboard panels providing links to various other pages . Whenever an error is made, the model makes it easy to recover quickly The model is hosted online, easy to access and use by any registered user
Efficiency	To test the model efficiency by looking at its response to : 1. Time behavior 2. Resource utilization	The model performance is time responsive and satisfying. It gives quick statistics panels for assessment questions, active assessments, runs assessments, and delete assessments The model adequately utilizes all its supplied resources to help effectively perform specified tasks
Maintainability	To check how the model responds to its maintainability attributes such as: 1. Analyzability 2. Changeability 3. Testability	1. The model can be diagnosed to identify areas for improvement 2. The model can be modified to make it more resilient without compromising its goal The objectives of the model can effectively and efficiently be performed. For example, Cybersecurity preparedness scores can be posted to the database.

The evaluation was done by experts filling the questionnaire and submitting it after which their responses were analyzed and summarized in bar graphs as given in 7.1. In addition, figures 1 and 2 below presents the output of successful cybersecurity preparedness assessments for various users who logged in. To strictly preserve ethical standards of anonymity, users' institutions and their emails could not be displayed.


User Cummulative Scores

No	Name	AssessmentDate	AssessmentQuestions	Score
	Leona Kemboi	2021-11-06 15:33:56	32	71.6%
	Good Good	2021-11-12 20:12:49	32	61.2%
	Eric Kipkemoi	2021-11-24 17:27:50	32	56.8%
	Robert Chepkwony	2022-02-23 16:59:17	32	81.3%
	Alex Kinet	2022-02-24 15:52:05	32	79%
	Kevin Onchoka	2022-02-24 16:23:55	32	70.3%
	ken cheruiyot	2022-03-02 18:20:53	32	72.8%
	Silas Wafula	2022-03-02 22:05:05	32	70.1%

Fig 1 User Verification – Professional Analysis
Source: Researcher (2021)



User Assessments Report

User Scores

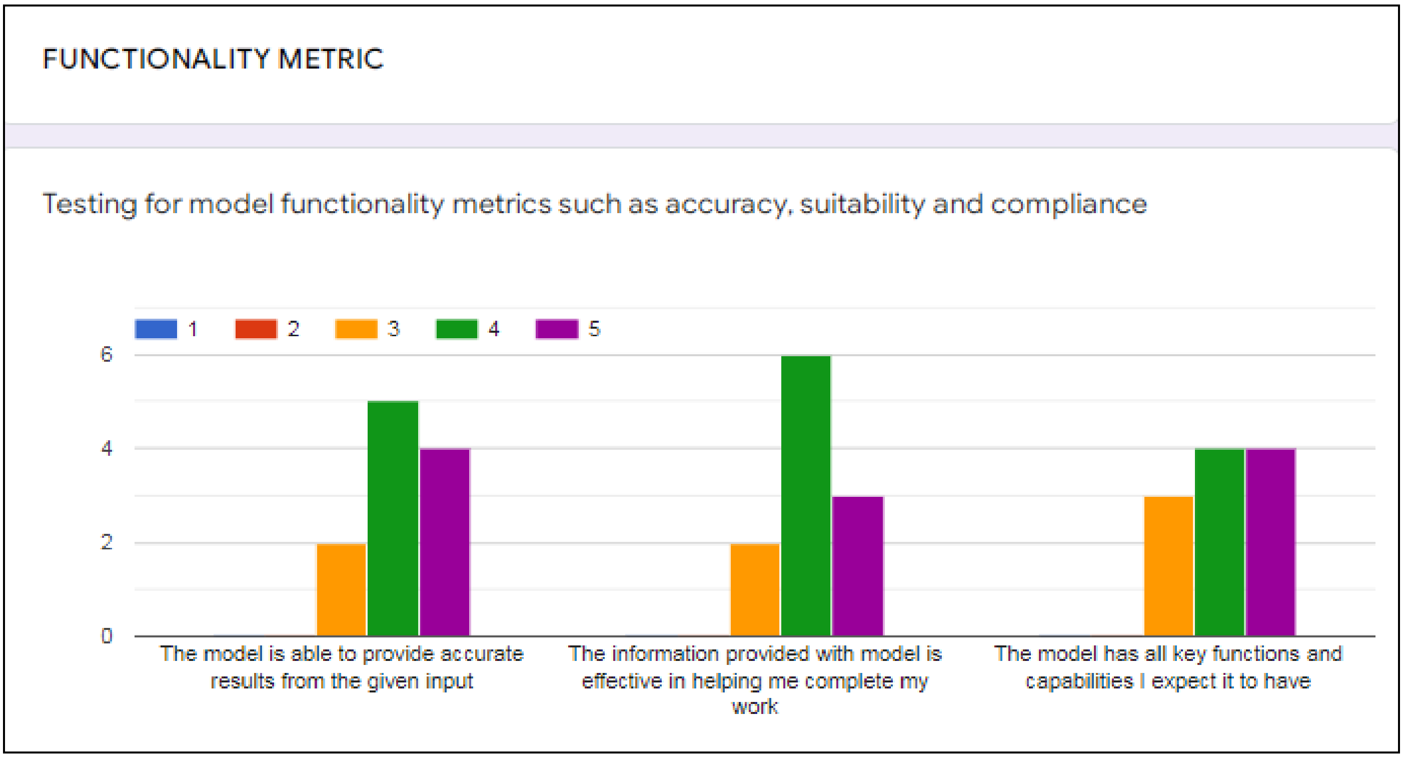
No	Name	AssessmentDate	AssessmentQuestions	Score
1	Joshua Mutai	2021-07-12 19:08:05	32	71.2%
2	Bernard Kimani	2021-11-03 16:16:46	32	53.3%
3	Leona Kemboi	2021-11-06 15:33:56	32	71.6%
4	Good Good	2021-11-12 20:12:49	32	61.2%
5	Eric Kipkemoi	2021-11-24 17:27:50	32	56.8%
6	Robert Chepkwony	2022-02-23 16:59:17	32	81.3%
7	Alex Kinet	2022-02-24 15:52:05	32	79%
8	Kevin Onchoka	2022-02-24 16:23:55	32	70.3%
9	ken cheruiyot	2022-03-02 18:20:53	32	72.8%
10	Silas Wafula	2022-03-02 22:05:05	32	70.1%

Fig 2 User Assessments Report
Source: Researcher (2021)

IV. RESULTS AND DISCUSSION

- *Model Evaluation Results*

The bar graphs below assess and summarize the extent to which the experts consulted to evaluate the model agreed on the measures under consideration. The bar graph Keys are rated on a Likert scale of 1 to 5, with 1 indicating Strongly Disagree, 2 indicating Disagree, 3 indicating Neutral, 4 indicating Agree, and 5 indicating Strongly Agree.

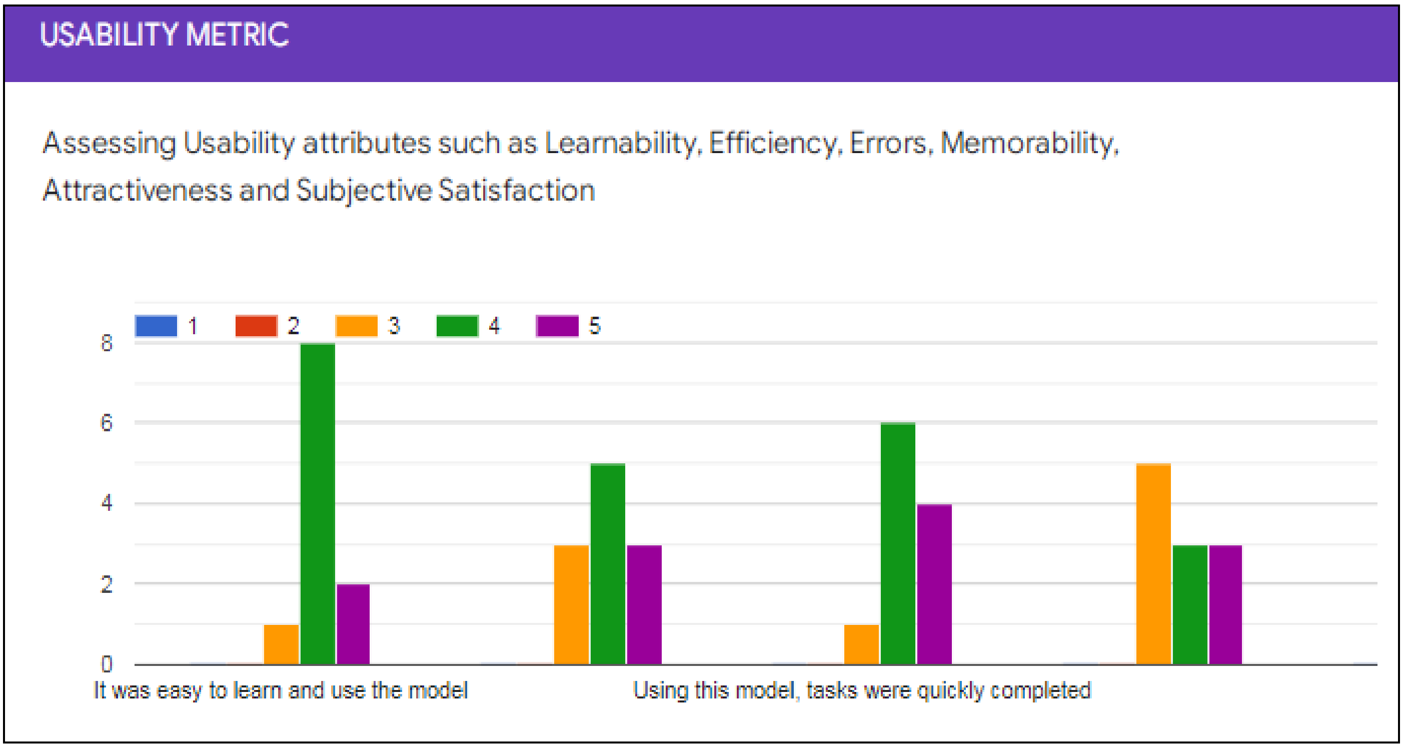


FUNCTIONALITY METRIC

Testing for model functionality metrics such as accuracy, suitability and compliance

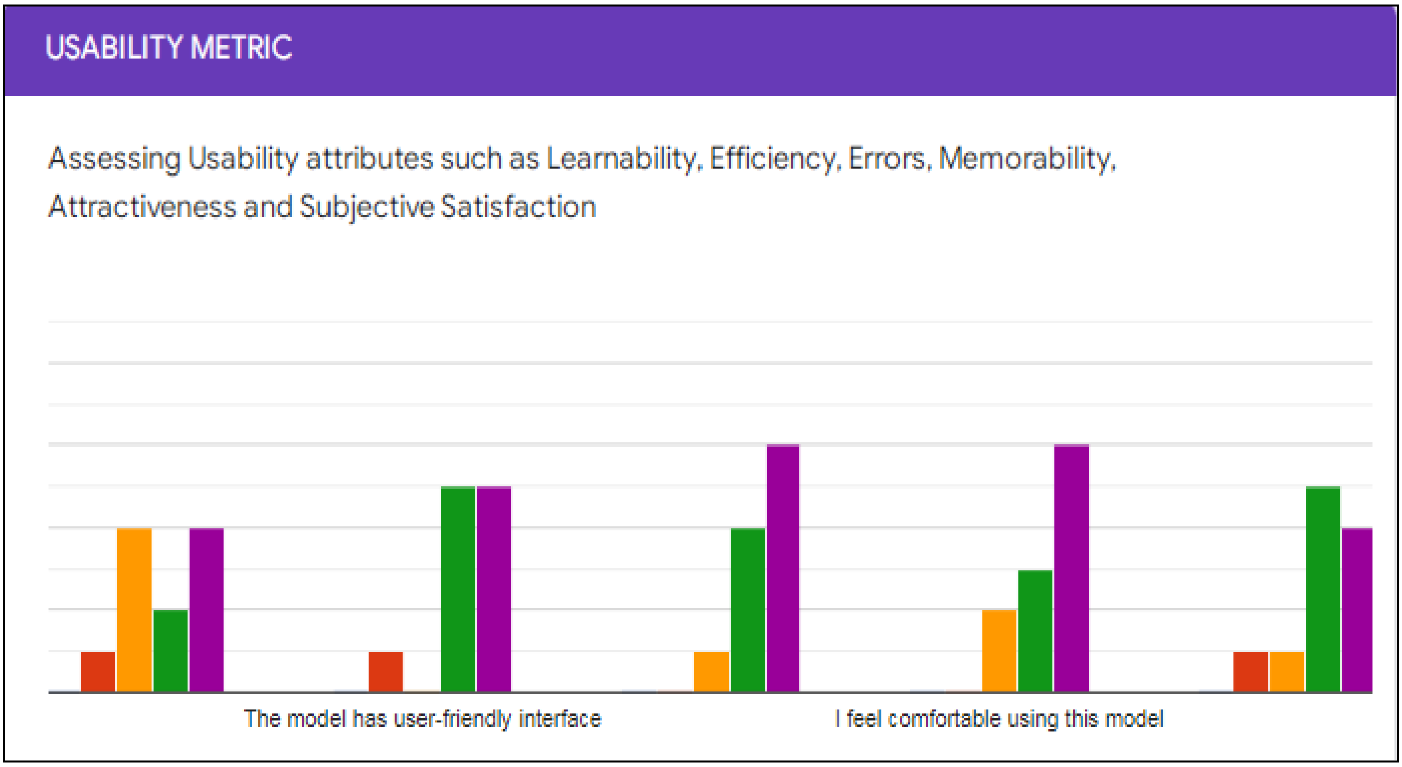
Fig 3 Functionality Metric

As shown on the graph above, it's noted that 9 respondents agree to the model accuracy and suitability functionalities with 8 respondents believing in its compliance. 2 respondents took a neutral position concerning the model accuracy and suitability while compliance remained neutral among the 3 respondents.


USABILITY METRIC

Assessing Usability attributes such as Learnability, Efficiency, Errors, Memorability, Attractiveness and Subjective Satisfaction

Fig 4 Usability Metric


USABILITY METRIC

Assessing Usability attributes such as Learnability, Efficiency, Errors, Memorability, Attractiveness and Subjective Satisfaction

Fig 5 Usability Metric

From the above graph, the general output displays that the model usability sub-metrics (learnability, efficiency, errors, memorability, attractiveness, and subjective satisfaction) were agreed upon by at least 7 to 10 respondents from a sample of 11 experts conducted. Only 1 respondent disagreed to the model memorability, attractiveness, and subjective satisfaction component.

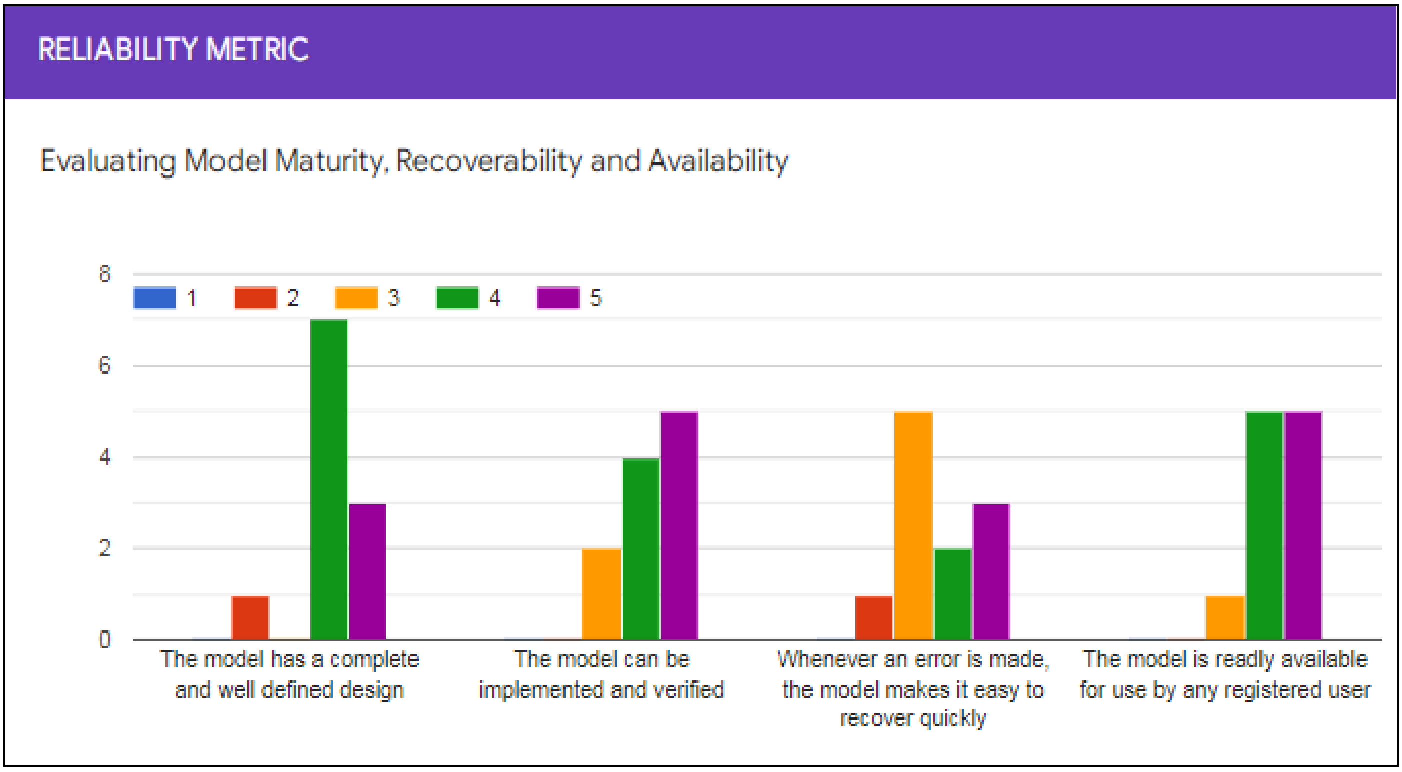


Fig 6 Reliability Metric

From the graph above, it was observed that at least 10 respondents agree to the model maturity and availability with 5 respondents believing in its recoverability. Only I respondent disagreed to its maturity and recoverability with 1 choosing neutral position concerning the model availability.

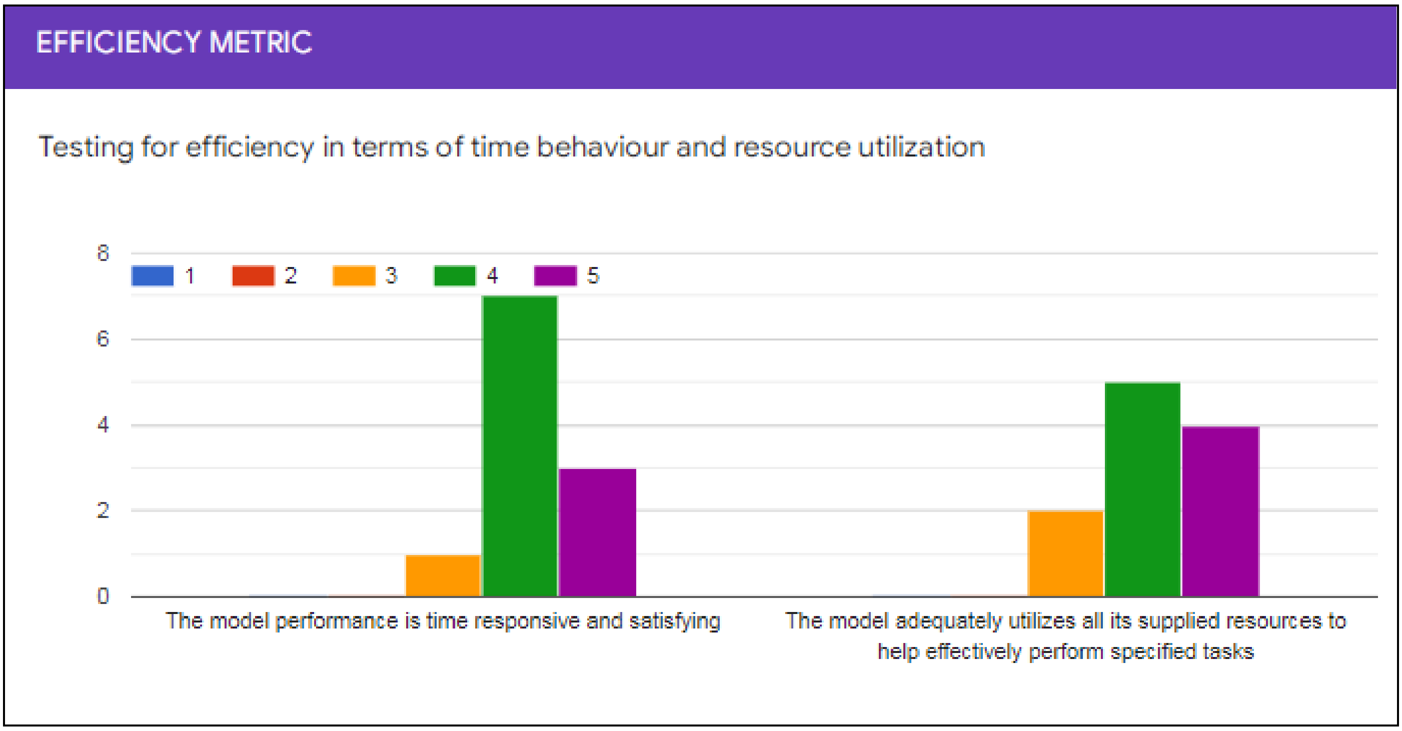


Fig 7 Efficiency Metric

As analyzed from the graph above, the efficiency of the model is agreeable by 10 respondents and 9 respondents in terms of time behavior and resource utilization respectively. Only I respondent took a neutral position on model time behavior and 2 respondents choosing neutral position resource utilization.

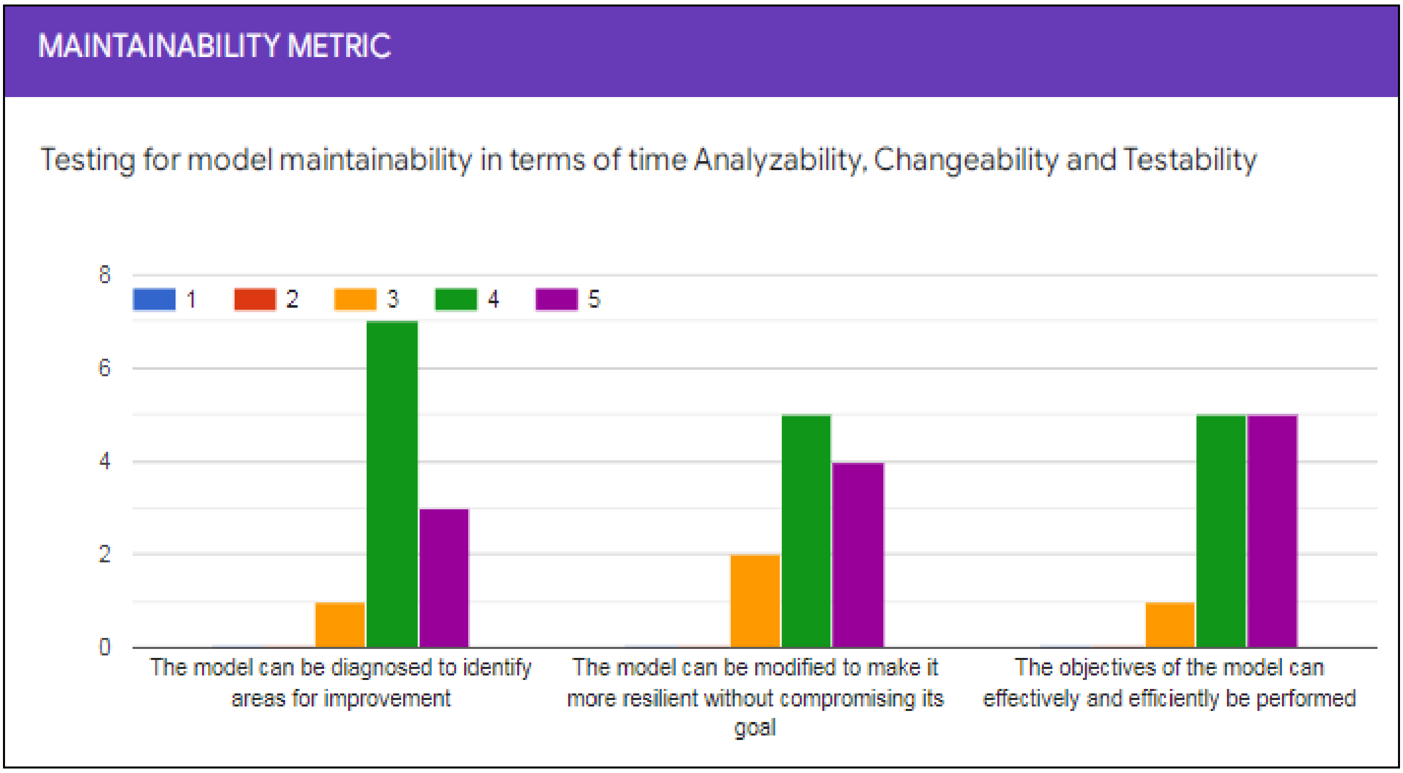


Fig 8 Maintainability Metric

From the graph above, it was observed that at least 10 respondents agree to the model maturity and availability with 5 respondents believing in its recoverability. Only I respondent disagreed to its maturity and recoverability with 1 choosing neutral position concerning the model availability.

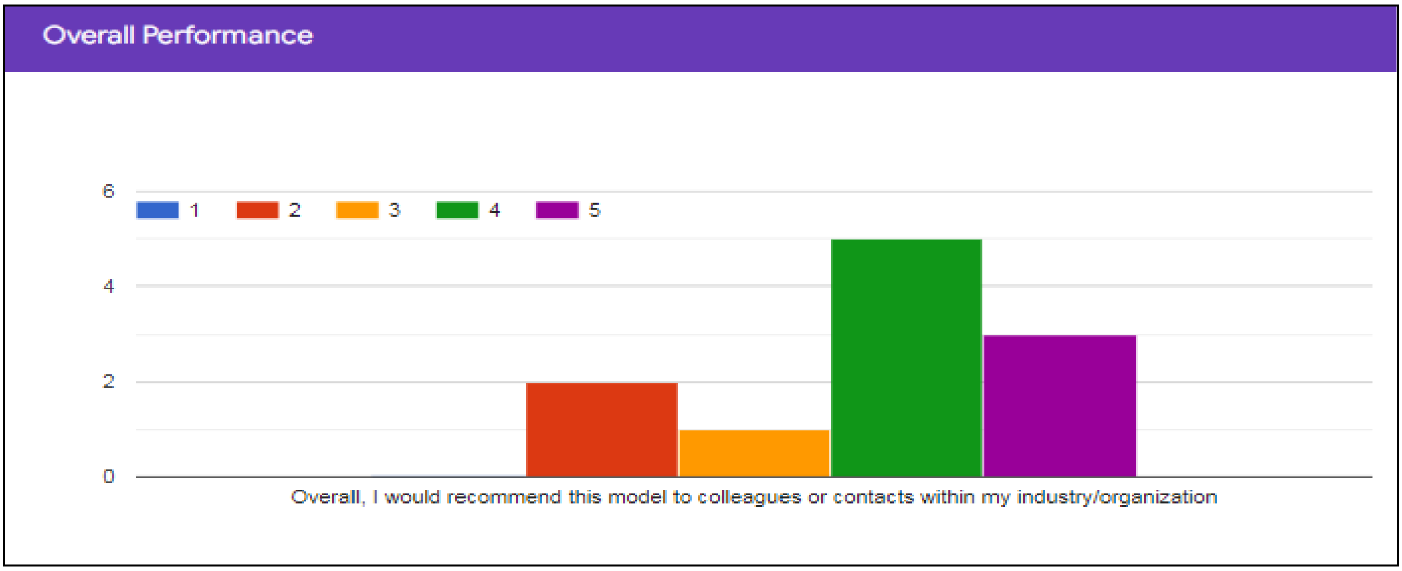


Fig 9 Overall Performance

In conclusion, 8 out of 11 respondents advocate the approach to their colleagues or contacts within their organization, with only one expert taking a neutral position and two others disagreeing.

V. CONCLUSION

After the model was developed, it was hosted to make it available online for users to access. Validation of the model was achieved by giving the URL to ICT experts who were first (new users) expected to register before logging into the system. When a registered user logs in with the right credentials, one will be permitted into the system and can perform system activities such as running assessments and submitting scores, managing questions, reading their preparedness status, viewing their scores and reports as well as retrieving recommendations. All these processes undergo system validation to ensure system goals and functionalities are working as expected. This activity of model evaluation is very critical to any organization as it provides insights both to developers, ICT security specialist, and institution management about their systems performance and areas that need attention.

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]. Cipher. (2017). 10 Cybersecurity Metrics You Should Be Monitoring. Retrieved April 4, 2019, from http://blog.cipher.com/10-cybersecurity-metrics-you-should-be-monitoring

[4]. Cronholm, S., & Goldkuhl, G. (2003). Strategies for Information Systems Evaluation- Six Generic Types. *Electronic Journal of Information Systems Evaluation*, *6*(2), 65–74.

[5]. Francis, R. (2017, May 5). Third parties leave your network open to attacks. Retrieved June 11, 2019, from Network World website: https://www.networkworld.com/article/3194832 /third-parties-leave-your-network-open-to-attacks.html

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

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

[8]. Levin, A. (2018, February 22). How Can 73 Percent of Companies Not Be Prepared for Hackers? Retrieved June 11, 2019, from Inc.com website: https://www.inc.com/adam-levin/more-than-70-percent-of-businesses-admit-theyre-unprepared-for-a-cyberattack.html

[9]. Lippmann, R. P., & Riordan, J. F. (2016). Threat-Based Risk Assessment for Enterprise Networks.

[10]. Lord, N. (2014, December 18). 101 Data Protection Tips: How to Keep Your Passwords,Financial & Personal Information Safe in 2019 [Text]. (2014, December 18). Retrieved June 11, 2019, from Digital Guardian website: https://digitalguardian.com /blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

[11]. Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors*, *19*(1), 19. https://doi.org/10.3390/s19010019

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

[13]. Ministry of Education, (2016). University Education and Research.

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

[15]. Molck-Ude, P. (2019). A corporate network is part of a company's IT strategy. Retrieved June 11, 2019, from https://www.t-systems.com/en/perspectives/networks/network-techniques/data-networks-375244

[16]. 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.

[17]. Poremba, S.M. (2017). Network Access Control: Controlling Access to Your Network and Data. Retrieved June 11, 2019, from https://www.esecurityplanet.com/network-security /network-access-control.html

[18]. Preston, W. C. (2019). Protecting Corporate Data When an Employee Leaves. Retrieved June 11, 2019, from https://www.druva.com/blog/protecting-corporate-data-employee-leaves/.

[19]. Ring, M., Landes, D., & Hotho, A. (2018). Detection of slow port scans in flow-based network traffic. *PLOS ONE*, *13*(9), e0204507. https://doi.org/10.1371/journal.pone.0204507

[20]. 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

[21]. Trull, J. (2017, August 3). Top 5 best practices to automate security operations. Retrieved June 3, 2019, from Microsoft Security website: https://www.microsoft.com/security/blog/2017 /08/03/top-5-best-practices-to-automate-security-operations/

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

[23]. Walsh, K. (2017, March 23). User Access Review Best Practices.. Retrieved June 11, 2019, from Reciprocity website: https://reciprocitylabs.com/user-access-review/.