American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-10, Issue-6, pp-206-211
www.ajer.org
Research Paper Open Access

Strategic Approach based on Cybersecurity for National Educational System

Nadine Nibigira[1]|Vincent Havyarimana[2]|Zhu Xiao[3]| Thabo Semong[4]
[1]*Department of Computer Science| University of Burundi | Bujumbura |Burundi*
[2]*Department of Applied Sciences| Ecole Normale Superieure |Bujumbura |Burundi*
[3]*College of Computer Science and Electronic Engineering| Hunan University| Changsha| China*
[4]*Department of Computer Science and Information System| Botswana International University of Science and Technology (BIUST)| Palapye| Botswana*

Abstract
In an era in which technology is advancing at an incredible rate, the threat of cybercrime is bigger than ever. Government agencies, private corporations, and the general public are frequently adopting newer and more advanced technologies that do not always account for adequate security protection. This makes the nation vulnerable to new and constantly evolving cyberattack risks. Students use social media as tool to express their feelings, to provoke discussions, or to become known. Many people want to be the first to share an issue, they some sometimes ignore the authenticity, integrity and confidentiality of the presented information.
Current training programs rely on manual setup and configuration for hands-on activities, which is a tedious and error-prone task. Schools and government ministries may lack resources and facilities to implement cyber security in educational system.
This paper demonstrates the importance of cybersecurity readiness in educational institutions and student's level of understanding of the subject. To achieve this, we first examine how for instance Facebook users behave on their privacy information. According to the survey done in five sample universities, we found that cybersecurity is relatively not known 74.5% among students asked said that they were not aware that cybersecurity exists. To enlighten students in terms of cybersecurity importance and based on the collected information, this paper proposes that in national education system, cybersecurity could be a topic of discussion in the conferences or in different discussions. In addition, the inclusion of cybersecurity as a discussion topic in schools will ensure that students have the basis on cybersecurity.
Keywords: Social Media, Internet, Cyberattacks, Facebook

Date of Submission: 10-06-2021 Date of acceptance: 24-06-2021

I. INTRODUCTION

The internet and other advanced technologies have an influence on modern society covering a large spectrum of businesses, academic institutions, governments, and Information Technology (IT) sector [1]. Students use internet to look for information's related to their needs. Many of them use social media through internet as a tool to express their feelings, to provoke discussions, or to become known. Many people want to be the first to share information about something recent, in most cases ignoring whether the information presented is authentic or otherwise. In this era of technology and multimedia, knowledge of cybersecurity is also important for students because the use of internet is not only limited to adults.

The rapid technological changes results in new risks, that require new solutions. Teachers may face problems in developing their knowledge of the latest technology and thus ensuring students are safe. This is a major obstacle for teachers, as they lack access to learning materials and need to be sensitive to technological change. Early exposure and training for students at schools should be promoted through cybersecurity symposiums. The students who are trained on cybersecurity are expected to be their country's future personnel in cyber defense.

An educated computer security workforce is essential to building trustworthy systems. Issues about what should be taught and how it should be taught are being ignored by many university faculties that teach cybersecurity courses.

a. Previous Research on Cybersecurity

There is an urgent need for organizations to truly understand their cybersecurity status and where necessary take urgent remedial actions to rectify weaknesses. If there is no sufficient adoption of cyber security policies, organizations will not be able to manage cybersecurity risks and they will almost certainly suffer a breach [2].

Many past researches have been conducted on cybersecurity, in different areas, for example [3]- [9]. Few articles focused on the steps that need to be done particularly by schools in order to help cultivate cybersecurity awareness in detail. And many of those researchers believe that education or training is essential in protecting cyber users from cybersecurity threats. Education is important in addressing evolving cybersecurity threats, as all protection factors play an essential role in curbing them. Moreover, security awareness programs are one of the strategies that can promote cybersecurity education in school. The principles of cybersecurity awareness have been refined over many years of research in the social psychology area, but have been largely ignored by IT professionals when developing information security awareness programs. Social media is one of the most adopted ways that people now communicate with their friends, family and businesses. It's a place where people can create, share and exchange information with online communities. It has become a big part of our everyday lives. Today, 91% of adult's online use social media regularly, and 85% of internet users have Facebook accounts [16].

The main purpose for adopting the use of social media is to be social, not promotional. Facebook was created for users to connect with each other and discuss things they care about, and it is meant to be friendly, social and engaging.

Facebook is the world's largest social media network and continues to grow at an exponential pace, with over one billion users [16]. Facebook users are able to create brand pages and join the social conversation where their customers are already spending a large amount of their free time.

b. Previous Research on Facebook Privacy

The future of social networking is endless; Facebook may be the most popular social networking site currently, but eventually some new social networking site will come along with far greater features [11].

A study from the United Kingdom found that Facebook's security settings confuse its users [14]. Almost half of Facebook users are not keeping track of recurrent changes to their privacy and security settings [10]. Facebook has changed its privacy policies eight times, including changes that automatically tell the user about their current location, and a change that allows third parties to access users' telephone numbers and addresses. According to The Montreal Gazette [11], a University of British Columbia study exposed Facebook's security system when it failed to stop a large-scale intrusion in which personal information on Facebook users accounts were collected. Researchers said they collected 250 gigabytes of information from Facebook users by using bots, or computer-generated fake Facebook profiles controlled by programming. It took eight weeks for the bots to gather this information, first by sending friend requests [10].

The objective of cybersecurity education is to educate the users of the cyberspace technology on the potential risks they may face when using internet communication tools, such as social media, chat, online gaming, email and instant messaging.

II. CYBERSECURITY IN EDUCATION SYSTEM

In an era in which technology is advancing at an incredible rate, the threat of cybercrime is bigger than ever. Government agencies, private corporations, and the general public are frequently adopting newer and more advanced technologies that do not always account for adequate security protection. This makes the nation vulnerable to new and constantly evolving cyber-attack risks.

There is currently a skills gap in the field of cybersecurity, and both universities and the government are keen to fill it by offering cybersecurity master's degrees. With thousands of cybersecurity jobs on the market and the number of jobs projected to increase, now is the time to forge a new career in an expanding industry. A Master of Science in Cybersecurity degree could help develop this critical expertise [13].

In general, information technology is not yet adopted and utilized by some countries in the world, especially in Africa [15]. For instance, students who are studying courses that are not IT related should be encouraged to take some computer related courses. The use of computer science department to service other non-computing departments still has a little impact in Burundi [19-20]. This problem affects also the implication and adoption of cybersecurity courses, in most universities. Some universities do not yet practice the teaching of cybersecurity and cyberattacks at all. We hope that this scenario will change soon as teacher training for cybersecurity adoption is underway.

Furthermore, Facebook is the most used social media by students when compared to other platforms like WhatsApp, Twitter and Instagram. Students use Facebook to share their information according to their common interests in their groups or communities and also invite their friends to share or like their posts.

The next section reflects on data analysis and discussions on the results found during this research.

III. DATA ANALYSIS AND DISCUSSIONS

The role of the internet continues to be a central one in the lives of people in societies where Information and Communication Technologies (ICT) trends are set, like in the case of Burundi.

3.1 Dataset description

Our description is based on the social media analysis and we focus mainly on Facebook as most students use it. The data from the 5 private universities helped us to get the result related to our study.

3.1.1 Sample size

To start our data analysis, we visited the following universities; Summit International Institute (SII), International University of Equator (IUE), Bujumbura International University (BIU), Burundi University (BU) and Ecole Normale Superieure (ENS). We took samples of fifty (50) students from IUE, thirty (30) from BIU, twenty (20) from SII, sixty (60) from BU and forty (40) from ENS to be interviewed. We then evaluated the use of social media, their awareness and the understanding of cybersecurity based on their responses.

3.1.2 Data collection methods

The underlying need for data collection is to capture quality evidence that seeks to answer all the questions that have been posed. Through data collection, business or management can deduce quality information that is a prerequisite for making informed decisions.

To improve the quality of information, it is expedient that data is collected so that you can draw inferences and make informed decisions on what is considered factual.

The methods ranged from traditional and simple ones, such as a face-to-face interview, to some more sophisticated ways of collecting and analyzing data.

- Interview: We approached students and discussed with them how and what social media they used, as well as asking them if they know the impact of cybersecurity nowadays.
- Questionnaire: We use a survey questionnaire to collect the data which has been used in this study.

3.2 Data Analysis

Academic institutions are critical part of preparing and educating the cybersecurity workforce. Collaboration among public and private entities enable such institutions to determine common knowledge and skills that are needed. As a result, these institutions can then develop and deliver curriculum that is relevant. Let us take an example of International University of Equator which tried to bring a system of two specializations: Software Engineering and Telecommunications Networks, where students learn some concepts of cybersecurity.

We first analyzed the awareness and found that 74.5% among students asked are not aware of cybersecurity as shown in Figure 1.

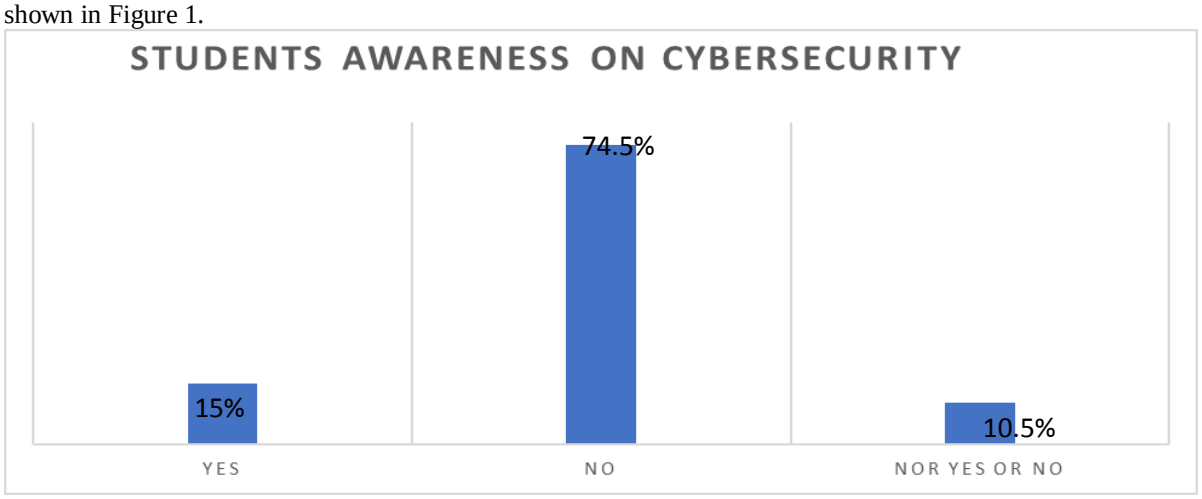

Figure 1: Students Awareness

As the number of students finding desired jobs in cybersecurity increases, more students will be attracted to cybersecurity programs as a pathway to a career.

Figure 2 below illustrates the percentage of students who showed interest on cybersecurity as their specialization. This figure can also be used to indicate the number of students who already have some basics knowledge on cybersecurity. More students in IUE want to specialize on cyber because they used to be

motivated by their lecturers teaching in network department through practical's. Also, they have access to ICT facilities within the university as the students wish to proceed for further studies which is not the case for students from BU.

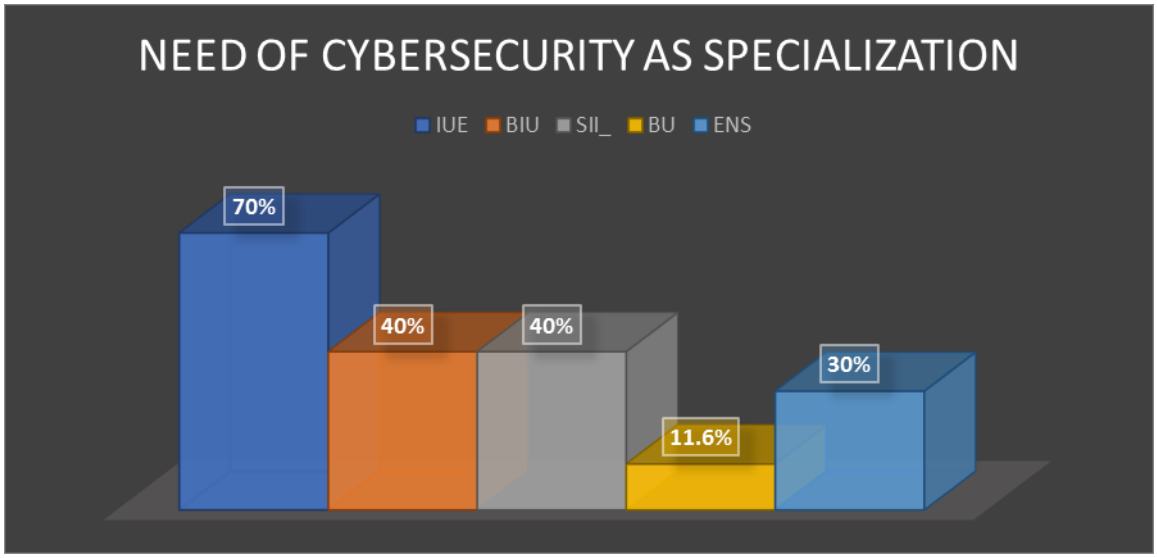

Figure 2: View on need of cybersecurity

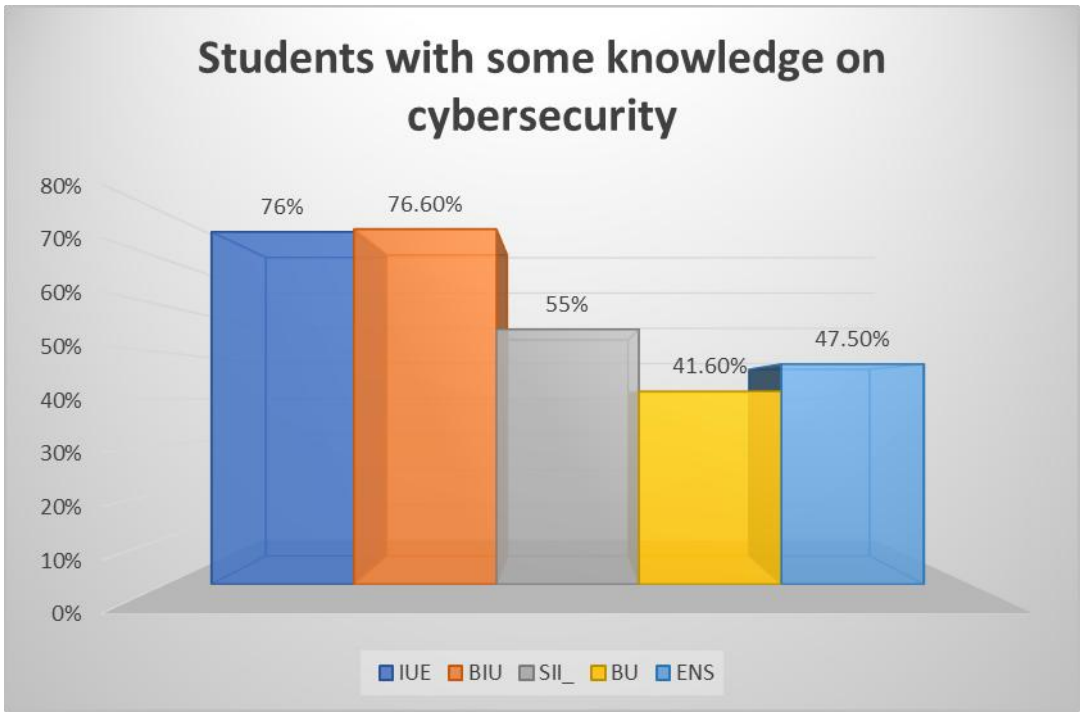

Figure 3: Students who have some knowledge on cybersecurity

Figure 3 indicates that 76% of students at IUE, 76.6% at BIU, 55% at SII, 41.6% at BU and 47.5% at ENS have some basic knowledge on cybersecurity. Few students from BU has little knowledge on cybersecurity due to lack of facilities relating to ICT as most of them come from low income families. Most of the students indicated that they really want to learn more about cybersecurity so that they can be prepared against the cyberattacks associated with using the cyberspace. They showed us that they really need to learn more computer skills to improve their cybersecurity knowledge in order to be able to teach others and boost interest on cybersecurity. Very few students prior to the study knew the basics about cybersecurity. Afterwards, most of them seemed to have understood what the field of cybersecurity involves and felt that they had gained some knowledge in this area

Universities should motivate for cybersecurity training in their respective schools so that they can inform the head of national education system about the importance of prioritizing it in Burundi higher education.

A As much as social media is highly used amongst the students, especially Facebook. We have realized that this platform can be exploited or infected through Distributed Denial of Service attack such as Phishing, social engineering and Trojan Horse [18]. 99% t of students interviewed use Facebook, and we are worried about their personal information security.

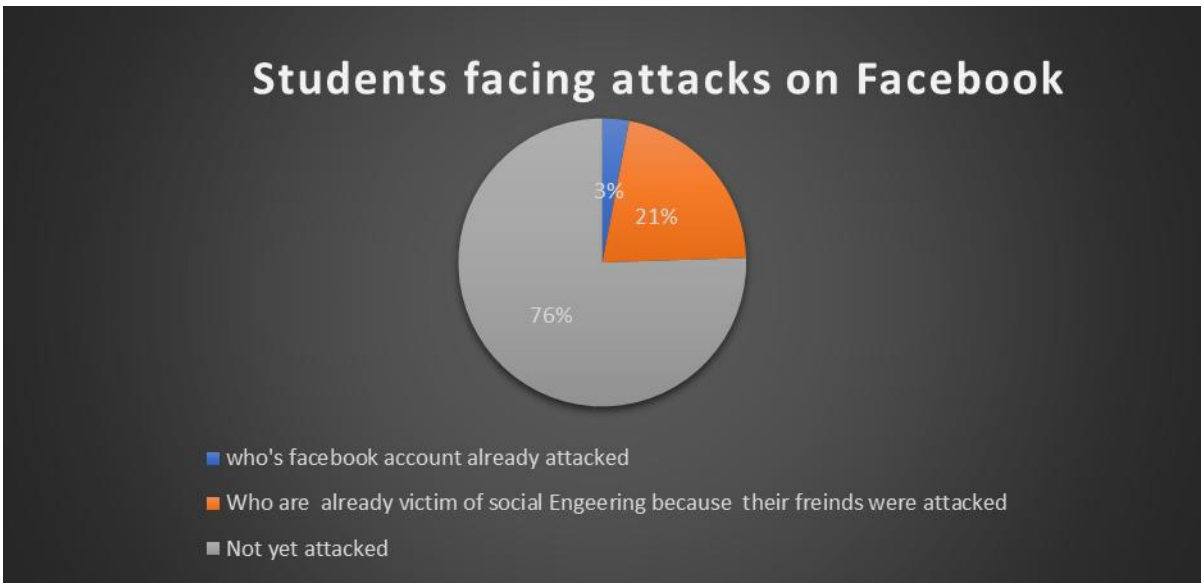

Figure 4: Students facing attacks on Facebook

Facebook allows users to communicate and share their information which is a matter of privacy for users. So users should be aware of limitations and disadvantages of using Facebook. The online privacy issues have been a real time problem, and however they are the main concerns for the experts to reduce the problems while sharing the kind of content that is allowed by the social media. There are issues that are general and the public need to oppose the privacy terms and conditions that expose their information. Among the students of the five universities where we did our research, 3% of students have been attacked before and 21% were victims due to their friends' previous attacks. The hackers used to send them messages pretending to be their friends, asking them to send money or airtime. Therefore, Facebook users who have left their security on a default setting have more frequently fallen victim to a virus or malware attack. The users of Facebook who have their privacy set to a custom setting are less likely to receive an attack on their profile.

Figure 4 deduce that 21% of student's interviews have already been attacked of social engineering.

Social engineering is when someone uses a compelling story, authority or other means to convince someone to handover sensitive information such as usernames and passwords [17]. With that number of victims of social engineering attacks among the students, we believe that it is imperative to organize conferences and discussions on cybersecurity for them.

We discover that 99.8% of students need conferences and 78.2% were keen for having many discussions on cybersecurity. Training on cybersecurity awareness will help the students to have the ability and knowledge of to recognize those types of attacks and avoid them.

3.3 Additional National cybersecurity actions

School administrators and teachers can discuss and organize school programs or activities about cybersecurity and share key information about the privacy issues or problems reported by social media users. Students should really be taught on how to keep themselves and their information safe from cyberattacks.

Every person who lacks cybersecurity awareness is as a result of not being informed of its importance and effects. Burundi's cybersecurity knowledge needs to be improved by including cybersecurity topics in national discussion. In addition, the safety aspects of cybersecurity can be taught through other subjects.

IV. CONCLUSION AND FUTURE WORKS

There are many benefits if a university can fully apply cybersecurity training. A survey on students from five universities on cybersecurity awareness indicates that students do not have knowledge on

cybersecurity to spend time in different conferences and discussions on cybersecurity. It is therefore crucial for schools to become cybersecurity training centers to educate the community on issues around cybersecurity.

Providing knowledge to students on cyber issues is one step that could be taken by schools to protect students from being victims of cybersecurity threats.

As future works, we plan to extend this research work by including teachers and schools' administrators on the survey to find out if they are aware of cybersecurity issues. This can also open discussions around how they planning to help student as they are the future employees of the schools. We will use Cyberattack model like intrusion Kill Chain which is a model of seven stages that an attacker inescapably follows to plan and carry out an intrusion. With the future works we will evaluate the applicability of our recommendations enumerate in the previous sections.

REFERENCES

[1]. Braun SK. Forensic evidence of copyright infringement by digital audio sampling analysis - identification - marking. *International Journal of Cyber-Security and Digital Forensics* (IJCSDF). 2014;3(3):170–182

[2]. Darko Možnik & Boris Guberina, Cybersecurity and cyber defence: national level strategic approach Darko Galinec,

[3]. C. S. Kruse et al., ―Cybersecurity in healthcare: A systematic review of modern threats and trends, ‖ Technology and Health Care, vol. 25, no. 1, pp.1-10, 2017.

[4]. P. Dong et al., ―A systematic review of studies on cyber physical system security, ‖ *International Journal of Security and Its Applications*, vol. 9, no. 1, pp. 155-164, 2015.

[5]. U. Franke and J. Brynielsson, ―Cyber situational awareness — *A systematic review of the literature*, ‖ Computers & Security, vol. 46, pp. 18-31, 2014.

[6]. N. H. A. Rahim et al., ―A systematic review of approaches to assessing cybersecurity awareness, ‖Kybernetes, 2015.

[7]. D. Mellado et al., ―A systematic review of security requirements engineering, ‖ *Computer Standards & Interfaces*, vol. 32, no. 4, pp. 153-165, 2010.

[8]. A. V. Herrera, M. Ron, and C. Rabadão, ―National cyber-security policies oriented to BYOD (bring your own device): *Systematic review*, ‖ in Proc. 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-4, 2017.

[9]. F. Mishna et al., ―Interventions to prevent and reduce cyber abuse of youth: A systematic review, ‖ *Research on Social Work Practice*, vol. 21, no. 1, pp. 5-14, 2011.

[10]. Investigation on Security Issues and Features in Social Media Sites (Face Book, Twitter, & Google+) Puneet Kumar Goud Kandikanti Governors State University

[11]. An Explore an Exploratory Study of a User y Study of a User's Facebook Security and Privacy Settings Brandon Charles Hoffmann Minnesota State University, Mankato

[12]. Addressing the challenges and opportunities in basic education, December 31, 2018 *public expenditure review*

[13]. https://findyourcontext.education/masters-degrees/cyber-security-masters-degree-online/

[14]. Information technology and developing countries,2014 J.F.Rada

[15]. Information Technology and the Challenge of Economic Development in Africa by T.W. Oshikoya and M. Nureldin Hussain African Development Bank

[16]. Step-by-step Facebook guide for LegalShield associates, https://meliafamily.com/wp-content/uploads/2014/07/Facebook.pdf available on 22nd/03/2021

[17]. https://en.wikipedia.org/wiki/Cyber_security_awareness,visited on 31st/03/2021

[18]. https://www.britannica.com/technology/denial-of-service-attack available on 28th/3/2021
ICT in Education in Burundi by Harry Hare , https://www.infodev.org/infodev-files/resource/InfodevDocuments_389.pdf
files/resource/InfodevDocuments_389.pdf

[20]. Developing the Use of Information and Communication Technology to Enhance Teaching and Learning in East African Schools: Review of the Literature Sara Hennessy, Brown Onguko, David Harrison, Enos Kiforo Ang'ondi, Susan Namalefe, Azra Naseem and Leonard Wamakote. Centre for Commonwealth Education & Aga Khan University Institute for Educational Development – Eastern Africa Research Report

Nadine Nibigira, et. al. "Strategic Approach based on Cybersecurity for National Educational System."*American Journal of Engineering Research (AJER)*, vol. 10(6), 2021, pp. 206-211.