
**ISSN Print:** 2394-7500
**ISSN Online:** 2394-5869
**Impact Factor:** 8.4
IJAR 2023; 9(10): 46-50
www.allresearchjournal.com
Received: 11-07-2023
Accepted: 19-08-2023

**Patrick Omondi Kwanya**
Department of Information Technology, Kibabii University, Nairobi Kenya

**Dr. Alice Nambiro**
Department of Information Technology, Kibabii University, Nairobi Kenya

**Dr. Anthony Luvanda**
Department of Information Technology, National Defence University-Kenya, Nairobi Kenya

**Corresponding Author:**
**Patrick Omondi Kwanya**
Department of Information Technology, Kibabii University, Nairobi Kenya

# A computer systems cybersecurity challenges encountered by secondary schools in Kenya, a case study of west Pokot county

**Patrick Omondi Kwanya, Dr. Alice Nambiro and Dr. Anthony Luvanda**

**DOI:** https://dx.doi.org/10.22271/allresearch.2023.v9.i10b.11301

**Abstract**
The education sector over time had experienced numerous computer cybersecurity challenges. These challenges made them became an easy target for the cybersecurity criminals. Nowadays, most of the secondary schools in Kenya had been equipped with computers and computing devices. Most of these schools had internet connectivity too making them vulnerable to cyber-attack. The vulnerability was also as a result of them lacking resources and attention to cybersecurity due to cybersecurity challenges they experienced. They had weak application security systems, weak endpoint security systems, and weak patch cadence. The study aimed at establishing the computer systems cybersecurity challenges in secondary schools in Kenya. The study was done in West Pokot County. From the finindgs- staffs were allowed to carry their computing devices to the schools, and they connected them to the schools' network in order to access internet; there was no segmentation of network to allow staffs have their own separate network access; some schools had IoT devices with no network segmentations; most schools lack data recovery plan, means to provide endpoint security, means to provide mobile security and means to provide website security. Lack of finance and budget, IT personnel, and user awareness contributed largely to these challenges. By establishing the computer systems cybersecurity challenges encountered, the secondary schools therefore, will find a solution to address them especially by looking at the contributors to the aforementioned challenges.

**Keywords:** Cybersecurity, targets, secondary schools, cyber-attacks, security systems, vulnerability, West Pokot, Kenya

## 1. Introduction
Most of the education institutions are nowadays equipped with computers as a way of integrating ICT in their education system. Focussing on Secondary schools in Africa, a report provided by UNESCO Institute for Statistics indicates that computers are more frequently available for secondary education [1]. As at the time of the report, learner to computer ratio in a few selected Africa counties were as follows: Gambia 37:1; Rwanda 40:1; Mauritius 19:1 and Botswana 17:1 [1]. With the growth of internet connectivity, most of the schools in the surveyed countries above are connected. As [1] noted, schools in Botswana and Mauritius are all virtually connected. The internet connectivity in these schools and the use of computer devices is what makes them vulnerable to the cyberattacks.

By 2017, a total of 1,609 secondary schools out of the total 7500 schools were equipped with ICT equipment [2]. By that time, a tender to supply other remaining secondary schools had already been advertised. To this end, most of the secondary schools in Kenya do have computers. It has been made possible due to government and donor funding [3].

Internet connectivity in secondary schools in Kenya has been on rise since the year 2014. As [4] reports, by the beginning of April 2014, Zuku had already rolled out a pilot project to cover 150 schools. The project was to cover 2000 public and private schools in Nairobi County and later extends to schools in other counties all over Kenya. Through another initiative, Communication Authority (CA) connects 899 secondary schools to high speed internet [4]. Any device connected to the internet is vulnerable to cyberattack. The vulnerability translates into the cybersecurity challenges of the computer systems in the secondary schools' set up. The growth of WiFi had allowed the creation of devices to connect to the internet or transfer data which at the end has a downside [5].

As [6] puts it, schools have a lot of data that is worth protecting. But they have security vulnerability and cybersecurity challenges; they lack resources and attention to cyber security. They have weak application security, endpoint security, patching cadence, and this makes hackers more likely to target schools and their data [6]. Furthermore, schools in developing countries face challenges of cybersecurity skills, structural capabilities, social integration and economic resources in relation to cybersecurity in education [7].

Schools rely so much on online applications for registration, data collection and making of payments, thus making their data all the more enticing to hackers [6], thus their need of application security. Application security is using software, hardware, and technical approaches to defend applications from exterior intimidations [8]. Endpoint devices used in schools such as IP- enabled and CCTV cameras, can have vulnerability too. These vulnerabilities could be weaknesses in hardware systems, weaknesses in software and application system or weaknesses of the user themselves. Zero-day and weakness in policy as well as procedures can too be considered as vulnerabilities [9]. This explains the need of the endpoint security in the secondary schools. Endpoint security is any device that connects to the network, from servers to desktops, fixed function to mobile devices, and-increasingly-any device that is network-enabled [10].

In their article, [11] stated three possible reasons why schools can have difficulty in using computer security system as; lack of IT personnel in schools, use of older computers and lack of cybersecurity expertise. On his part, [6] added lack of money and resources as some of the challenges faced by the schools in using computer security system. In their research, [12] established that Kenya faces shortage of ICT technicians in Secondary schools. The shortage of IT experts leaves the secondary schools to be at the mercy of outsiders who aim to make the end meets, as long as they make sales on their security systems.

Additionally, existences of old computers in secondary schools have made it difficult to provide computer security systems. As [13] noted, the reason older devices pose a risk is that manufacturers tend to phase out their technical support over time. As a result, security upgrades cease on those devices. The notion is supported by [14], who reported that the recent "WannaCry" attack was made possible by a flaw in the 15-year-old Windows XP operating system. Furthermore, lack of cybersecurity experts makes it even more serious. Secondary schools are not able to tell whether they have been attacked or not due to lack of know-how. The shortage of cybersecurity expert is not only in secondary schools but within the county as a whole. According to [15], "Kenya has too few cybercrime professionals despite the country being one of the most advanced countries in information and communication technology (ICT) on the continent."

By the year 2022, Kenya had over 10,463 secondary educational institution, including both private and public schools with over 2.94 million students [16]. There are students' data, employee's data, financial records and other sensitive information worth protecting. In spite of this, secondary schools have been noted to have weak cybersecurity in their systems or none at all. As [6] suggested, the schools have weak application security, endpoint security, patching cadence. Additionally, education sectors have a lot of users leading to larger network and cyber-attacks to schools may lead to attacks on other government ministries and agencies. The secondary schools have more cybersecurity challenges on their computing systems than meets the eye. The only way to find out about this was through this research study. To protect the schools computing systems and their data, the challenges had to be established. That was the aim of the study.

## 2. Materials and Methods

The descriptive survey design was used in the study. Descriptive research design describes the characteristics of the population or phenomenon that is being studied [17]. The research study was conducted in West Pokot County. The researcher used convenience sampling to pick on the location. As [18] puts it, convenience sampling is a sampling method where the selection of research location is due to its easier of accessibility. The researcher was familiar with the county and its set up, thus could easily and immediately develop a good rapport with the respondents. Additionally, [19] said that, the ideal location for any research study is that which directly relate to the researcher interest, can be accessed easily and allows an immediate rapport with the respondents. The study targeted teachers in charge of ICT from the sampled secondary schools in West Pokot County. These individuals interacted with schools' computer systems, the network and the policies. By the year 2021, when the study was carried out, West Pokot County had 112 registered public secondary schools. A sample size of 88 secondary was used in the study for the quantitative data, which was arrived to using Yamane formula. Each sampled school produced one teacher in charge of ICT to participate in the study.

The sampling techniques used were stratified sampling, simple random sampling and purposive sampling. Stratified sampling was used to subdivide the schools into different categories, i.e. the National secondary schools, Extra County Secondary schools, County Secondary schools and Sub-county Secondary schools. The schools in these categories were further picked using the purposive and simple random sampling. The researcher used questionnaires for data collections. Questionnaires were administered to teachers in charge of ICT. The generated data was analyzed and presented though tables. The analysis and interpretation were done using descriptive statistics.

## 3. Results

The study sought to establish the challenges encountered in applying the cybersecurity to the computer systems in secondary schools in Kenya.

### 3.1 General Cybersecurity challenges

The study aimed to establish from the general cybersecurity challenges from the participants. The analysis was as shown in table 1.

From table 1, the data was collected from 6 items with an aim of knowing the general cybersecurity challenges. The Likert scale of 1-5, where 1 was the minimum and 5 was the maximum. IoT devices having their own separate network had a mean score of 1.8636 and a standard deviation of 0.8865, meaning that there was a general disagreement that the secondary schools have a separate network to connect their IoT devices. In other words, IoT devices share the same networks with other computing devices.

**Table 1:** General Cybersecurity Challenges

| Items | Min | Max | Mean | Std. Dev. |
|---|---|---|---|---|
| IoT (CCTV camera, Smart TV and smart printer) devices in my school have their own separate Local Area Network | 1 | 5 | 1.8636 | 0.8865 |
| Staffs are allowed to connect their computing devices (laptops, tablets and phones) to the school's network. | 1 | 5 | 3.0341 | 1.236 |
| Staffs are allowed to access school's resources while in school's network. | 1 | 5 | 2.9659 | 1.1885 |
| Staffs are allowed to access school's resources while in a different network (Away from school's network). | 1 | 5 | 3.0227 | 1.1445 |
| Availability of a mechanism to ensure data confidentiality i.e. only authorized people are allowed to access the school's data | 1 | 5 | 3.1477 | 1.3002 |
| Availability of a mechanism to ensure data integrity i.e. no modification to school's data. | 1 | 5 | 3 | 1.1744 |

Likewise, the issue of staffs being allowed to connect their own computing devices (laptops, tablets and phones) to the school's network scored a mean of 3.0341 and a standard deviation of 1.236, showing that secondary schools allows their staffs to connect their computing devices to the school's network. Majority of the respondents agreed with this. Additionally, the issue of staffs allowed to access school's resources while in a schools network had a mean score of 2.9659 and a standard deviation of 1.1885, indicating that staffs do access the school's resources while in schools compound. Also, on the issue of whether staffs are allowed to access the school's resources away from the school's network, majority of the respondents agreed with a mean score of 3.0227 and a standard deviation of 1,445. Therefore, most of the staffs can access the school's resources even at home or in cybercafé. Consequently, the schools had mechanisms to ensure data confidentiality and data integrity with a mean score and standard deviation of 3.01477; 1.3002, and 3.000;1.1744 respectively.

### 3.2 Application systems security challenges

The study aimed to establish the cybersecurity challenges on the application systems used in secondary schools from the participants.

**Table 2:** Application systems security challenges

| Items | Min. | Max. | Mean | Std. Dev. |
|---|---|---|---|---|
| Use of email security to secure the access and data of an email account. | 1 | 5 | 3.59 | 1.18 |
| Use of endpoint security system to protect school's network from being accessed by remote devices such laptops and other wireless devices | 1 | 5 | 2.43 | 1.13 |
| Use of wireless security system to protect a school's wireless network from intruders and cyber attackers. | 1 | 5 | 2.06 | 0.9 |
| Use of mobile device security to protect your school's network from mobile devices accessing it. | 1 | 5 | 1.97 | 0.82 |
| Use of web security system which controls web use by denying access to malicious websites. | 1 | 5 | 1.9 | 0.8 |
| Use of disaster recovery plan and protection strategies to help in avoiding data loss. | 1 | 5 | 1.83 | 0.81 |

Table 2 shows the results of the challenges on the security systems of applications. The Likert scale of 1-5 was used, where 1 was the minimum value and 5, the maximum value. The use of email security to secure the access and data of email account had a mean score of 3.59 and standard deviation of 1.18, indicating that secondary schools have a way of ensuring email security. Likewise, the use of the endpoint security system had a means core of 2.43 and a standard deviation of 1.13, showing that majority of the schools do not use endpoint security systems to protect their network. Additionally, the use of wireless security systems had a mean score of 2.06 and a standard deviation of 0.9, indicating that most secondary schools do not use wireless security to protect schools wireless network. Similarly, the use of mobile device security had a mean of 1.97 and a standard deviation of 0.82, showing that secondary schools do not use mobile security to protect the school's network from the mobile devices accessing it. Also, the use of web security systems had a mean of 1.9 and a standard deviation of 0.8, showing that most of the secondary schools do not use web security systems to deny access to malicious websites.

### 3.3 Factors contributing to the challenges

The study aimed to establish from the participants the factors contributing to the cybersecurity challenges on the computer systems in secondary schools in Kenya.

**Table 3:** Factors contributing to the challenges

| Items | Minimum | Maximum | Mean | Std. Deviation |
|---|---|---|---|---|
| Shortage of IT personnel | 1 | 5 | 2.9148 | 0.76177 |
| Finance and Budget | 1 | 5 | 2.3551 | 0.78393 |
| User Awareness | 1 | 5 | 3.3440 | 0.67179 |
| Age of the computer | 1 | 5 | 3.2188 | 0.76734 |

Table 3 shows the factors that contributes to the cybersecurity challenges. The shortage of IT personnel had a mean score of 2.91148 and a standard deviation of 0.76177, showing that some schools have IT personnel to and others not, since its mean score is at the section of undecided respondents. Consequently, finance and budgeting had a mean score of 2.3551 and a standard deviation of 0.78393, showing that secondary schools lack finance to address the issues of cybersecurity. Likewise, user awareness had a mean score of 3.3440 and a standard deviation of 0.67179, indicating that there is user awareness on cybersecurity issues to the staffs of the majority of secondary schools. Finally, the age of computer had a positive response with a mean score of 3.2188 and a

standard deviation of 0.76734. This shows that majority of computers used in secondary schools are between 0-5 years old and thus easy to maintain and upgrade.

From the findings and the analysis, secondary schools have a mechanism to ensure data confidentiality and data integrity. However, most of the secondary schools lack network segmentation (separate network) to connect IoT and end user devices. Also, the school allows staffs to access school's resources while on a different network, i.e. when away from the schools network.

Additionally, the findings indicate that the secondary schools use email security to secure the access and data of their email accounts. However, majority of the schools lack endpoint security which protects schools from being accessed by the remote devices, they lack wireless security which protects wireless network from intruders and cyberattacks, they lack mobile devices security which protects the schools network from rogue mobile devices, and they lack website security which controls web use by denying access to malicious websites. Finally, shortage of IT personnel, the finance and budget contributes to the challenges. User awareness and the age of the computers does not affect the use of cybersecurity on the computer systems in the schools.

## 4. Conclusions

The study sought to establish the computer systems cybersecurity challenges in the secondary schools in Kenya. From the findings, it is therefore concluded that: schools lack network segmentation or separation which would have promoted the security of their network; staffs in the schools are allowed to access schools resources in a different network to that of schools, which would promote an attack vector to the schools computing devices and the network as a whole; the schools lacked endpoint devices security, which would protect their network from connections through unauthorized endpoint and remote devices; schools lacked wireless security which would protect the their wireless network from intruders as cyberattacks; schools lacked mobile devices security which would help in protecting their network from rogue mobile devices; schools lacked website security to allow them protect themselves through the control of web use and denying of access to the malicious websites. Further, finance and budget, and the shortage of IT personnel were identified to be contributing to the cybersecurity challenges. Without proper budget and financing of the IT departments in the secondary schools, the security application would not be possible. These security applications must be purchased. Likewise, without a knowledgeable IT personnel, it would not be possible to do the installation and maintenance of the security applications, both hardware and software.

## 5. References


1. Trunaco M. Surveying ICT use in education in Africa worldbank.; c2015. org.https://blogs.worldbank.org/edutech/surveying-ict-use-education-africa
2. Ministry of Education, Supply and delivery of computers to public secondary schools (2016/2017); c2017. Retrieved from https://www.education.go.ke/index.php/tenders/file/248-supply-and-delivery-of-computers-to-public-secondary-schools-2016-2017
3. Merireng S. Effect of Computers in Management of Secondary Schools in Kenya a Case of West Pokot County, Kenya, M. S. Thesis, University of Nairobi, Nairobi, Kenya; c2013. [Online]. Available. http://erepository.uonbi.ac.ke/handle/11295/56339
4. Kenya Education Network (KENET), KENET connects Kenyan schools to internet; c2020. kenet.or.ke. https://www.kenet.or.ke/node/392 (accessed Mar. 2, 2020.
5. Aidinyantz N. GlobalSign Blog. 31 Cybersecurity Tips for Business, globalsign.com; c2016. https://www.globalsign.com/en/blog/cybersecurity-tips-for-business/ (accessed Mar. 2, 2020)
6. Winan N. Hackers have begun targeting schools across the country; c2019. medium.com, https://medium.com/@nwinans/a-hackers-next-victim-your-childs-school-61b543c3228a (accessed Mar. 2, 2020)
7. Catota FE, Morgan MG, Sicker DC. Cybersecurity education in a developing nation: The Ecuadorian environment, Journal of Cybersecurity; c2020. p. 1-19. doi:10.1093/cybsec/tyz001,
8. Srinivasan J, Simna S. Disaster recovery, an element of cyber security-a flick through. International Journal of Management (IJM). 2020;8(4):125-133. https://www.researchgate.net/publication/320244744_Disaster_recovery_an_element_of_cyber_security-a_flick_through
9. IT Governance, "Types of cyber threat in 2020," itgovernance.co.uk, 2020 https://www.itgovernance.co.uk/cyber-threats (accessed Mar. 17, 2020)
10. Howarth F. Network and endpoint security; c2020. bloorresearch.com, https://www.bloorresearch.com/technology/network-and-endpoint-security/ (accessed Mar. 19, 2020)
11. CCSI Team. School districts remain vulnerable to cyber-attacks; c2019. securityboulevard.com https://securityboulevard.com/2019/10/school-districts-remain-vulnerable-to-cyber-attacks/ (accessed Mar. 18, 2020)
12. Ndegwa L, Githui P, Njoka J. Evaluation of ICT Preparedness in Public Secondary Schools: A Comparative Study of Public Boarding and Day Secondary Schools in the South Rift Region in Kenya, African Journal of Education, Science and Technology. 2023;7(3):628-636. https://doi.org/https://doi.org/10.2022/ajest.v7i3.891
13. Geffner M. Why your old computer poses security risks?; c2015. bankrate.com, https://www.bankrate.com/finance/mobile/old-computer-poses-security-risks.aspx (Mar. 19, 2020)
14. Parkinson S. Are public sector organizations more at risk from cyberattacks on old computers? gcn.com; c2017. https://gcn.com/articles/2017/05/17/legacy-it-vulnerabilities.aspx (accessed Mar. 19, 2020).
15. Tubei G. Kenya is a sitting duck in Cybersecurity as the country boasts too few cybercrimes professionals despite having a big name in African ICT circles," pulselive.co.ke. https://www.pulselive.co.ke/bi/strategy/kenya-is-a-sitting-duck-in-cybersecurity-despite-boasting-big-name-in-ict/nvcd12h (accessed Mar. 19, 2020)

16. Faria J. Number of secondary educational institutions in Kenya 2013-2019, statista.com; c2021. https://www.statista.com/statistics/1237217/number-of-secondary-educational-institutions-in-kenya/ (accessed Apr. 20, 2021)
17. Bhat A. Descriptive research: definition, characteristics, methods, examples and advantages, questionpro.com; c2020. https://www.questionpro.com/blog/descriptive-research/ (accessed Mar. 22, 2020, from)
18. Nikolopoulou K. "What Is Convenience Sampling? | Definition & Examples," scribbr.com; 2022 Dec 01. https://www.scribbr.com/methodology/convenience-sampling/ (accessed Feb. 21, 2023,)
19. Singleton R, Straits B, Straits M. Approaches to Social Research, Oxford, New York; c1993.