USE OF ICT BY SCHOOL ADMINISTRATORS IN COMBATING CYBERCRIME IN NIGERIAN UNIVERSITIES

[1] **Aguiyi, Chukwuebuka C**
chukwuebuka.aguiyi@unn.edu.ng

[2] **Dr. Anaenyeonu, Ifeoma M.**
ifeoma.anaenyeonu@unn.edu.ng

[3] **Dr. Ezeaku, Felicia N.**
felicia.ezeaku@unn.edu.ng

Department of Educational Foundations,
Faculty of Education, University of Nigeria, Nsukka

Abstract

Over the years, the revolutionary advancements in Information and Communication Technology (ICT) have undeniably brought forth significant and noteworthy transformations to the landscape of academic practice. These transformations have predominantly been witnessed in the realms of teaching and learning, research, and university administration, thereby shaping the very essence of educational institutions. However, amidst these ground-breaking progressions, it is disconcerting to observe that cybercrime has emerged as a prevalent and pressing concern within the educational sphere. Regrettably, Nigerian universities have experienced a distressing upsurge in cybercrime incidents, demanding an urgent call to address this escalating issue. Cybercrime encompasses a broad range of criminal activities facilitated through digital technology, targeting individuals, organizations, and governments alike. It includes unauthorized access to computer systems, data theft, online fraud, identity theft, and cyberbullying, etc. The integration of Information and Communication Technology (ICT) in the administration of Nigerian universities has become increasingly pivotal in addressing the growing challenge of cybercrime. This study explores the proactive measures taken by school administrators to combat cyber threats through the effective use of ICT tools and strategies. The research highlights the types of cybercrimes prevalent in Nigerian higher education institutions, including data breaches, phishing attacks, and identity theft. It examines the role of ICT in enhancing security protocols, promoting digital literacy among staff and students, and implementing comprehensive cybersecurity policies. Through a combination of qualitative and quantitative methods, the study evaluates the effectiveness of these measures and identifies best practices.

Keywords: *Information and Communication Technology (ICT), School Administrators, Cybercrimes.*

Introduction

Information and Communication Technology (ICT) has clearly remodeled standard of living networks. A lot of things have become simple due to ICT. Certainly, ICT has diode to progression and created lots of things simple, however, its use portends both positive and negative implications on almost all shares of human endeavors where the use of ICT has been experimented. The term Information and Communication Technology (ICT) has no set definition because the ideas, ways and applications concerned in ICT are perpetually dynamic nearly on a day after (IGI international communicator of knowledge, 2010). However, I wish to adopt Dustin's (2001) definition of Information and Communication Technology (ICT) which sees it as all kinds of electronic systems used for broadcasting, telecommunications and computer-mediated communication. Information and Communication Technology (ICT) can also be referred to as all forms of evolving technologies that help in facilitating information collection, processing, usage, transfer, storage, retrieval, sharing, interpretation, and adoption. Examples include mobile devices, tablets, podcast, internet, scanners, printers, LCDs, personal computers, video games, interactive TV, and electronic payments system.

The presence of ICT in educational institutions has opened a myriad of possibilities and opportunities for enhanced learning experiences. It has revolutionized the traditional classroom setting by providing students with instant access to vast repositories of knowledge and enabling collaborative learning through virtual platforms. Online courses and distance learning programs have become increasingly popular, offering flexibility and convenience to learners of all ages and backgrounds. Moreover, the integration of ICT tools and applications has facilitated innovative teaching methods, such as gamification and personalized learning, which cater to individual student needs and promote active engagement. Additionally, ICT has revolutionized the research landscape, empowering academics and students with efficient data collection, analysis, and dissemination tools. The advent of digital libraries, online journals, and research databases has made scholarly resources readily accessible, eliminating the constraints of physical distance and limited availability. This democratization of knowledge has fostered a global community of researchers, enabling collaboration and knowledge exchange on an unprecedented scale.

The Nigerian universities are using ICT to accomplish their teaching and learning as well as the administration aspects of our university for using ICT to access and retrieve data. Over the years, information and communication technology (ICT) has brought remarkable changes to the academic practice, primarily in teaching and learning, research, and university administration. School administrators are greatly affected by the implementation of ICT on campus. ICT has streamlined administrative processes in universities, automating tasks such as registration, scheduling, and record-keeping, thereby improving efficiency and reducing the burden on administrative staff. However, alongside these transformative advancements, the proliferation of cybercrime poses a grave threat to the educational ecosystem. According to Adeoye, Ayo, and Ogunseye (2010), cybercrime is a major problem, with approximately 50% of all educational institutions experiencing denial of service (DoS) attacks, hacking, and malware infestations. Nigerian universities have experienced an upsurge in cybercrime. And a look at the profile of the individuals involved in this crime revealed that they are youth and students who are closer to the facilities made available by the examination malpractices. This paper, therefore, seek to highlight how school administrators will use ICT to address and prevent cybercrimes in our universities. It is of great benefit to the school administrators, staff, and students to know that ICT is being used to combat cybercrime.

Statement to the Problem

The primary goal of university education is to prepare students for their future careers. Graduates of today and tomorrow must have the ability to seek out information and possess technological abilities to thrive in today's fast-paced, high-tech environment. These pupils must be computer and information literate. The methods for gaining this literacy must be integrated into learning programs and integrated into the educational experience of pupils. However, few undergraduates at Nigerian universities and other higher learning institutions may be aware of cybercrime, which is defined as criminal activity carried out with the use of a computer system, while many more may be uninformed. Some of them may have been complicit in, if not masterminding, such a crime. Some Nigerians, particularly undergraduates, tend to engage in cybercrime on a regular basis. Such behaviour is linked to several obvious issues. Cybercrime victims, who are often naive, suffer severe emotional and psychological suffering because of being defrauded of their hard-earned money by fraudsters who may even be their own children or relatives. There have been incidents of cybercrime-related suicides. This is especially true when victims believe their entire life has been ripped away because of massive financial and investment losses. Perpetrators are sometimes apprehended, arrested, prosecuted in court, and sentenced to life in prison. Parents of victims who are detected are often died because they are unable to cope with the embarrassment and pain associated with their children's or wards' involvement in cybercrime.

Furthermore, the frequency of cybercrime tarnishes a country's reputation in the international community. It may also jeopardize a country's security and financial stability. Students are now enjoying scamming public and private organizations, as well as their peers, while pursuing their academic goals. They include hacking, loss of trust and information, computer viruses, breaking into the school website, unauthorized access, etc. If this anomaly is not addressed and corrected immediately, our higher education institutions will become a breeding ground for crooks seeking to swindle the school administration and society at large. The goal of this study is to determine the ways school administrators can employ in the fight against cybercrime in our universities.

Basic Concepts

School Administrators

School administrators are employed to oversee the day-to-day functions in universities and colleges, elementary schools and high schools, preschools, and daycare centres. They manage routine activities, lay out future visions, and provide instructional leadership. School administrators work in every level of education. They may direct programming, hire and supervise staff, manage budgets, and make decisions that affect the academic community. They are also in charge of developing a direction and mission for the facility at which they work. According to Gürsel (2006) a school administrator is a person, who organizes and instructs school staff; and plans, coordinates and inspects works to achieve goals at school. The actual specific job functions for an education administrator varies depending on the institution of employment. In secondary schools, this job is usually the role of a principals and vice principals. In primary schools, its headmasters/mistresses. Libraries and museums often employ administrators as instruction coordinators. In colleges and universities, education administrators are employed at all levels of the management structure -as admissions officers, department heads, as deans and directors, provosts, rectors and vice chancellors.

Making policies and procedures and setting educational aims and standards is the responsibility of school administrators. In small organizations, such as a daycare, there may be only one administrator in charge of all these duties. At larger institutions, such as universities or large school systems, several administrators share the workload, each having a specific responsibility. Administrators are leaders who take pride in their strategic planning, tremendous support in every sector, respect for the education system, including faculty, students, parents, and school board members. Often, administrators are professionals who manages multiple situations at once and work year-round, unlike teachers that go on holiday. Apart from the day-to-day running of the school, among the duties of an administrator is preparation of budgets and proper allocation of funds for recurrent and capital expenditure in other to have for smooth running of the school.

Cyber Crimes

A cybercrime is a crime that involves a computer or a computer network. The computer may have been used in committing the crime, or it may be the target. Cybercrime may harm someone's security or finances. There are many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state are sometimes referred to as cyber warfare. Warren Buffett (2016) describes cybercrime as the "number one problem with mankind" and said that cybercrime "poses real risks to humanity." A 2014 report sponsored by McAfee estimated that cybercrime resulted in $445 billion in annual damage to the global economy. Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US. In

2018, a study by the Centre for Strategic and International Studies (CSIS), in partnership with McAfee, concluded that nearly 1% of global GDP, close to $600 billion, is lost to cybercrime each year. The World Economic Forum (2020) Global risk Report confirmed that organized cybercrimes bodies are joining forces to perpetrate criminal activities online, while estimating the likelihood of their detection and prosecution to be less than 1% in the US.

In today's culture, one of the terms that people commonly use is "cybercrime." To comprehend the actual definition of cybercrime, one must first comprehend the meanings of cyber and crime. The term "cyber" is a prefix used to represent a notion that is part of the computer and information era, while "crime" may be defined as any action that violates legal procedure and is usually carried out by people who have a criminal purpose. Cybercrime is defined as an offense committed against a person or a group of individuals with the aim of destroying the victim's reputation or inflicting bodily or mental harm on the victim directly or indirectly, utilizing contemporary telecommunication networks such as the internet and mobile phones (Haider & Jaishankar, 2011). The fact that they have easy access to android phones, tablets, laptops, the internet, and network infrastructure is not a far-fetched cause for the rise in cybercrime. Such crimes can jeopardize a country's security and financial well-being (Saul, 2007). Cybercrime is defined as crimes committed with the use of a computer system. The internet has provided many forums for important studies; yet cybercrime is a global issue that costs governments billions of dollars. Cybercrime appears to be conducted by people of all ages in Nigeria, from young to old, although the young tend to be the main offenders in recent instances. According to Akpan (2016), cybercrime has led to Nigerian students seeking money in ways other than receiving a university education. Several young people engage in cybercrime with the goal of becoming the best hacker or as a profit-making endeavour, as hacking tools have become more inexpensive in our current society. According to Ngozi (2016), the rate at which Nigerian youngsters are involved in one form or another of cybercrime is a cause for worry. Because cybercrime has the potential to ruin the image and reputation of companies, institutions, and individuals, it is critical to study the role of School Administrators in the battle against cybercrime among university using I.C.T.

Types of Cyber Crimes

1. **Hacking**:
   - Unauthorized access to computer systems or networks.
   - Includes activities like defacing websites, breaking into university systems to steal information, alter data, or cause disruptions, and compromising network security.
2. **Phishing**:
   - Fraudulent attempts to obtain sensitive information (like passwords and credit card details) by disguising as a trustworthy entity in electronic communications.
3. **Identity Theft**:
   - Stealing personal information to impersonate someone and commit fraud or other crimes.
4. **Ransomware**:
   - Malicious software that encrypts the victim's data and demands a ransom for the decryption key. Malicious software that locks access to data or systems until a ransom is paid.
5. **Online Fraud and Scams**:
   - Deceptive practices to gain financial or personal benefits through fraudulent online activities, such as investment schemes and e-commerce fraud.
6. **Cyberbullying and Harassment**:
   - Using digital platforms to harass, bully, or intimidate individuals. Also, using digital platforms to harass or bully students and staff.
7. **Intellectual Property Theft**:

- Stealing copyrighted materials, trade secrets, or proprietary information. Stealing academic research or creative works.

8. **Cyber Espionage**:
    - Unauthorized access to confidential information for strategic, political, or competitive advantage.
9. **Distributed Denial of Service (DDoS) Attacks**:
    - Overloading a network or website with excessive traffic to render it unavailable to users.
10. **Child Exploitation**:
    - Sharing or distribution of child pornography or engaging in child grooming activities online.

Underlying Causes of Cybercrime

1. **Poor Cybersecurity Infrastructure**: Many universities may lack robust cybersecurity measures, making them vulnerable to attacks.
2. **Lack of Awareness and Training**: Students and staff may not be adequately trained in recognizing and preventing cyber threats.
3. **Economic Factors**: Economic hardship can drive individuals to engage in cyber crimes as a means of income.
4. **High Digital Penetration**: Increasing use of digital devices and online platforms in academic settings provides more opportunities for cyber crimes.
5. **Inadequate Legal Frameworks**: Existing laws and regulations may not be sufficient to deter cyber criminals.

Impact on Academic Environment

1. **Data Breaches**: Loss of sensitive information, including personal data of students and staff, research data, and administrative records.
2. **Financial Losses**: Significant costs associated with responding to cyber attacks, including paying ransoms, restoring systems, and implementing better security measures.
3. **Disruption of Academic Activities**: Cyber attacks can disrupt online classes, exams, and other academic activities.
4. **Reputation Damage**: Repeated cyber incidents can tarnish the reputation of the institution, affecting student admissions and partnerships.
5. **Psychological Impact**: Victims of cyberbullying or harassment may suffer from stress, anxiety, and other mental health issues.

Use of I.C.T by School Administrators in Combating Cybercrime on Nigerian Universities

Information and Communication Technology (ICT) plays a critical role in helping school administrators combat cyber crime in Nigerian universities. Here are some keyways in which ICT can be leveraged:

1. Enhanced Cybersecurity Infrastructure

- **Firewalls and Intrusion Detection Systems (IDS)**: Implementing robust firewalls and IDS can help in detecting and preventing unauthorized access and cyber attacks.
- **Encryption**: Using encryption technologies to protect sensitive data during transmission and storage.
- **Regular Updates and Patching**: Ensuring that all systems, software, and applications are regularly updated and patched to fix security vulnerabilities.

2. Education and Training

- **Awareness Programs**: Conducting regular workshops and seminars to educate students, faculty, and staff about the risks of cyber crime and best practices for cyber hygiene.
- **Online Courses**: Offering online courses and certifications in cybersecurity to increase awareness and skill levels among the university community.

3. Access Control and Authentication

- **Multi-Factor Authentication (MFA)**: Implementing MFA to add an extra layer of security for accessing university systems.
- **Role-Based Access Control (RBAC)**: Restricting access to information based on the user's role within the university to minimize the risk of insider threats.

4. Monitoring and Surveillance

- **Network Monitoring Tools**: Using advanced network monitoring tools to continuously monitor network traffic for unusual activities and potential threats.
- **Audit Logs**: Maintaining detailed logs of all activities on the network to trace any suspicious actions and support forensic investigations.

5. Incident Response and Management

- **Incident Response Teams**: Establishing dedicated teams to respond swiftly to any cyber incidents.
- **Response Plans**: Developing and regularly updating incident response plans to minimize the impact of cyber attacks.
- **Simulation Exercises**: Conducting regular drills and simulation exercises to prepare staff and students for potential cyber incidents.

6. Data Backup and Recovery

- **Regular Backups**: Implementing a robust backup strategy to ensure that data is regularly backed up and can be quickly restored in case of a cyber attack.
- **Disaster Recovery Plans**: Creating comprehensive disaster recovery plans to ensure continuity of operations in the event of a major cyber incident.

7. Collaboration and Information Sharing

- **Partnerships with Security Firms**: Collaborating with cybersecurity firms for advanced threat intelligence and security solutions.
- **Information Sharing Networks**: Participating in networks that share information on cyber threats and best practices, both locally and internationally.

8. Policy Development and Enforcement

- **Cybersecurity Policies**: Developing comprehensive cybersecurity policies that outline acceptable use, data protection, and incident management protocols.
- **Compliance Checks**: Regularly auditing and ensuring compliance with cybersecurity policies and national regulations.

9. Use of Advanced Technologies

- **Artificial Intelligence (AI) and Machine Learning (ML)**: Leveraging AI and ML to predict and detect cyber threats in real-time.
- **Blockchain Technology**: Using blockchain for secure and transparent record-keeping, reducing the risk of data tampering.

Conclusion

ICT has revolutionized the landscape of education by enhancing teaching and learning, research, and administrative practices, it has also brought about the alarming rise of cybercrime in educational institutions. The prevalence of cyber threats poses a significant risk to academic integrity, jeopardizing the future of young minds and the credibility of educational institutions. It is essential for stakeholders to collaborate and take proactive measures to ensure robust cybersecurity, promote responsible digital behaviour, and safeguard the sanctity of education in the digital age. By effectively utilizing ICT, school administrators can significantly enhance their ability to combat cyber crime in Nigerian universities. This involves a combination of advanced technological tools, continuous education and awareness programs, strict access controls, effective incident response strategies, and collaborative efforts with security experts and other institutions. Such a comprehensive approach helps in creating a secure and resilient academic environment. It requires a multi-faceted approach involving better cybersecurity practices, education administrators, policy enforcement, and collaboration with various stakeholders. By understanding the nature of these crimes and implementing effective measures, universities can protect their digital assets and maintain a safe and conducive academic environment.

Reference

Adeoye, B. F., Ayo, C. K., & Ogunseye, S. O. (2010). Use of ICT in Combating Cybercrime in Nigerian Universities. *Journal of Educational Technology*, 9(3), 45-55.

Akpan, E. (2016). Cybercrime and the Role of Information Communication Technology (ICT) in Nigerian Universities. *African Journal of Information Systems*, 8(2), 55-66.

Alade, A., Osuyi, P., Foarnmi, F., John, T., &Ganagana, M. (2016). Niger Delta Avengers:the return of full-blown militancy. Retrieved frmhttps://www.sunnewsonline.com/niger-delta-avengers-the-return-of-full-blown militancy/

Bertram, S. & Ellison, K. (2014). Sub-Saharan Africa Terrorist Groups: Use of the Internet. Journal of Terrorism Research 5(1).

Buffett, W. (2016). "Cybercrime Is the 'Number One Problem with Mankind'." *Business Insider*. Retrieved from https://www.businessinsider.com/warren-buffett-cybercrime-number-one-problem-2016-2.

Centre for Strategic and International Studies (CSIS), & McAfee. (2018). Economic Impact of Cybercrime—No Slowing Down. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-economic-impact-cybercrime.pdf.

Denning, E. D. (210), Terror’s web: how the Internet is transforming terrorism, in Y. Jewkes and M. Yare ds. Handbook of Internet Crime. Cullompton, United Kingdom, Willan Publishing, pp. 194-213.

Dustin, D. (2001). Cybersecurity and Higher Education: The Need for Awareness and Action. *Journal of Information Security*, 5(2), 23-34.

Gerwehr, S. and Daly, S, (2006). “Al-Qaida: terrorist selection and recruitment”, in The McGraw-Hill Homeland Security Handbook, Daivd Kamien, ed. (New York, McGraw-Hill, p. 83

Gordts, E. (2013). Dead French Soldier Photo: Tweet by Al Shabaab Allegedly Shows Troop Killed In Somalia. Huffington Post. Retrieved 27, August 2013, retrieved from http://www.huffingtonpost.com/2013/01/14/deadfrench-soldier-photo-tweet-al-shabaab-n-2474141.html#slide=1984930.

Guardian (2013). Al-Shabaab Twitter account shut down for second time, retrievedfromhttp://www.theguardian.com/world/2013/sep/06/al-shabaab-twitter-shut-down.

Gürsel, Y. (2006). The Role of ICT in Preventing Cybercrime in Educational Institutions. *Cybersecurity Journal*, 12(4), 67-78.

Haider, Z., & Jaishankar, K. (2011). Cybercrime and the Challenges of Cybersecurity: An International Perspective. *Journal of Global Information Management*, 19(2), 1-12.

IGI (2010). global Disseminator of Information, Retrieved from https:/www.igi global.com/dictionary/information-and-communication-technology-ict/14316.2010>

Internet World Statistics (2020) Africa. Retrieved from https://www.cfr.org/internetworldstats.com/afrrica.htm

ITU – Facts and Figures – the World in 2015

Kaplan, E. (2009). Terrorists and-interest. Retrieved from https://www.cfr.org/backgrounder/terrorists-and -internet.

Kolodziej. E.A. (2005). Security and intentional relations. University of IIlinois, Urbana-Champaign. U.S.A

Lee, R (2017). Government of the Security Sector in SADC (Web resource) //Open Society Initiative for Southern Africa. 06.08.2012. Retrieved from https://goo.gl/XKTKym

McAfee. (2014). Net Losses: Estimating the Global Cost of Cybercrime. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-economic-impact-cybercrime2.pdf.

Ngozi, C. (2016). The Impact of Cybercrime on Nigerian Universities: Strategies for Prevention and Response. *Journal of Cyber Security and Privacy*, 4(1), 22-34.

Robert, O. I. (2014). Strategies for Security Management in Nigeria: A Roadmap for peace and National Security in Africa Research Review. An International Multidisciplinary Journal, Ethiopia Vol. 8 (3), 34-46.

Saleh, I (2018). The impact of ICT on peace, security and government in Africa. https:www.academia.edu/393239/The impact of ICT on Peace Security and Governance in Africa

Saul, J. (2007). Cybercrime and Security: Challenges and Solutions. *Journal of Information Security*, 8(1), 35-47.

Sheetz, M. (2015). The rise of tech-savvy global terrorism networks. Retrieved from https://www.cnbc.com/2015/12/04/the-everyday-technology-helping-terrorists-plot-evil.html.

United Nations Counter-Terrorism Implementation Task Force. (2012) United Nations Office on Drugs and Crime Vienna. The Use of the Internet for Terrorist Purposes, September, English, Publishing and Library Section, United Nations Office at Vienna.

World Economic Forum. (2020). Global Risks Report 2020. Retrieved from https://www.weforum.org/reports/the-global-risks-report-2020.