International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 255-260 www.ijaem.net ISSN: 2395-5252

Preventive Measures for Office Cybercrime among Tertiary Institutions

Vincent Tamaramiebi D.[1], Samson, Isobo D.[2], Apere, Tonubari[3]

Computer Science Department, Isaac Jasper Boro College of Education, Sagbama, Bayelsa, Nigeria.
Mathematics Department, Isaac Jasper Boro College of Education, Sagbama, Bayelsa, Nigeria.
Computer Science Department, Isaac Jasper Boro College of Education, Sagbama, Bayelsa, Nigeria.

Date of Submission: 10-01-2024 Date of Acceptance: 20-01-2024

ABSTRACT: The internet and electronic devices are great assets for knowledge acquisition and sharing globally. Tertiary institutions use this platform to perform several activities to advance their relevance in the education sector (i.e. online advertisements, online fee payment, online admission, online results, digital certificates, electronic meetings, e-learning, e-library, etc.). Hence tertiary institution networks, databases, infrastructures and electronic devices are not immune to cyber attacks. Cyber attacks can originate from anywhere and launched by anybody targeting sensitive institutional data. Hacking, cyber-theft, malware attack, spamming, financial fraud (credit card theft, ATM fraud), identity theft, extortion, phishing, cyber harassment, cyber laundering, website cloning, website defacement, lottery scam, spoofing, spyware, beneficiary of a will scam, online charity, web browser exploits (public and private), next of kin scam, instant messaging abuse, intellectual property theft, bogus cashier's check, internet service time theft, stolen hardware, password sniffing, system infiltration, document forgery and counterfeiting etc. as common cybercrime trends in tertiary institutions' cyberspace. This paper attempts to provide detailed preventive measures that tertiary institutions can adopt to secure institutional data and reduce cybercrime occurrences at various office levels.

KEYWORDS: Cybercrime, Cyber Security, Tertiary Institution, Preventive Measures,

I. INTRODUCTION

Globally cybercrime is a household name affecting every sector of human endeavor wherever information and communication technology is applied. Cybercrime has no geographical constraints thereby creating a climate of unending cybercrime and fraudulent activities against technology users.Technological advancement is growing geometrically leading to more sophisticated digital devices, applications and the internet. The internet acts as a bedrock unifying this growing ICT advancement and cybercrime also evolves and increases with the current innovative trends [6].These advancements have created a new dimension as perpetrators of cybercrime activities now make it look attractive to society and penetrate every organization (especially tertiary institutions) in disguise. [4] listed ATM Jackpotting, Malware-only ATM Attacks, Endpoint vulnerabilities, Biometric Hacking, Gaming as a Cyber Attack Launch Pad, Multi-Vector Dark Web Attacks, Cryptojacking, Internet of Things (IoT) device threats, Geopolitical risks, Cross-site scripting, Mobile malware as emerging online cyber security threats.

[9] defined Cybercrime as a combination of information, financial and personal security threats.This implies that personal, organizational and institutional data are the main target of cybercrime. [1] noted that while institutions apply advanced technology to upgrade their security measures and implement strict cyber security policies to reduce cybercrime risk, so also are malicious hackers who now use sophisticated tools to advance their course. If any tertiary institution leaves its data security to chance, the astronaut impact resulting from a cyber breach will be unimaginable. Data breaches in an institution can cause reputation damage, revenue loss, operational disruption, loss of data, etc.

II. CYBERCRIME AT TERTIARY INSTITUTION OFFICES

Tertiary institutions are organized in different levels of offices for effective administrative purposes. every office in an institution holds sensitive information resulting from daily data processing activities. These data

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 255-260 www.ijaem.net ISSN: 2395-5252

processing activities involve the use of internet sophisticated applications (media platforms, social networking sites, electronic mail, World Wide Web, electronic banking, etc.) and electronic devices (networks, desktops, laptops, tablets, notebooks, palmtops, etc.) to provide the needed service for the tertiary institution [2].

Services such as sales of admission forms, online advertisements, online fee payment, online admission, electronic meetings, academic board meetings, online call for journal papers, open access scholarly communication and general online publications are all facilitated by internet technology [3]. The internet also provides further services such as online universities' e-learning institutions, online educational programmes at certificate, diploma and degree levels, learning management systems, automation of library routines and digitization of print materials especially grey literature in libraries and development of institutional repositories to tertiary institutions [5]. These various online services tertiary institutions embark on are spearheaded at the office level. Murugiah& Karen (2013) noted that where the internet and electronic devices are used for data processing cybercrime attacks are inevitable.

[5] listed Hacking, Cyber-theft, Malware attacks, Spamming, Financial fraud (Credit Card theft, ATM fraud), Identity theft, extortion, phishing, Cyber harassment, Cyber laundering, Website Cloning, website defacement, Lottery scam, spoofing, spyware, Beneficiary of a Will Scam, Online Charity, Web browser exploits (public and private) Next of Kin Scam, instant messaging abuse, intellectual property theft, The "Winning Ticket in a Lottery one Never Entered" Scam, Bogus Cashier's Check, Internet Service Time Theft, stolen hardware, password sniffing, system infiltration, document forgery and counterfeiting etc. as common cybercrime trends in tertiary institutions' cyberspace.

Every tertiary institution is a function of multiple small offices. If a cyber data breach is experienced it could lead to disaster. A cybercrime in a tertiary institution can be done by an insider (staff), student, or an intruder for selfish gains. Hence the need to apply strict preventive measures to secure institutional data at the office level is vehemently important. This research seeks to expose globally accepted and current practical measures on how to prevent office cybercrime at tertiary institutions.

III. IMPORTANCE OF CYBER SECURITY TO TERTIARY INSTITUTIONS

Cyber security is undoubtedly important to tertiary institutions because sensitive data and information are kept and accessed online. These institutional data may be financial information, intellectual property, copyright, personal (staff and students) information, unauthorized data (such as health, tax and results), etc. which might be accessed by cybercrime perpetrators [8]. Many staff easily trust people they meet online by sharing or storing institutional information unintentionally through social networks, browsers autosave and cloud storage which makes them vulnerable to activities of cybercrime. Since institutional data processing (online) is done at the office level staff must employ adequate safety measures to secure data at their unit

IV. CHALLENGES OF CYBER SECURITY AT TERTIARY INSTITUTIONS

[5] defined cyber security as the collection of "tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets".Tertiary institutions are concerned about securing computing devices, applications, data and information transmission, telecommunication and services in cyberspace. [8] noted that challenges can therefore arise from network security (unwanted access attacks), application security (computer and mobile device applications attacks), data security (securing data on network and applications), cloud storage security (cloud data protection), mobile security (login, chats, banking). Cyber security travails to secure institutional data within a cyber environment when effectively applied.

V. IMPORTANCE OF CYBER ETHICS AT TERTIARY INSTITUTIONS

Good ethical practice is a fundamental requirement within an institution. The daily use of the internet and electronic devices has created conflicts over privacy, accessibility, security, censorship, property, filtering and other issues [11]. Offensive, abusive and violent language, cyberbullying, content plagiarism, copyright infringement (materials, software, etc.), document forgery and counterfeiting, direct or indirect cyber crime involvement are common ethical

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 255-260 www.ijaem.net ISSN: 2395-5252

misconducts found in tertiary institutions' environment[8].[11] define cyber ethics or internet ethics as a branch of applied ethics that examines moral, legal, and social issues at the intersection of computer/information and communication technologies. Cyber ethics awareness among staff within an institution is of utmost importance because while using cyberspace, a user needs to be ethically correct. As data processing takes place at the office level everyone must understand their cyber citizen responsibility to practice good cyber ethics. This is a relatively important preventive measure to mitigate cybercrime.

VI. CYBERCRIME PREVENTIVE MEASURES AT TERTIARY INSTITUTIONS

Having a robust security solution for detecting, preventing and disrupting cyberattacks should be a priority for every tertiary institution [12]. Adopting effective and affordable measures to reduce electronic device attacks and its users' online risk is critical for any institution to protect its information base online. Basic preventive measures that should be taken are;

1. Encrypt institutional data: Data and information stored in plaintext format make it easy for hackers to access. Sensitive institutional data (financial records, tax returns, student results, health records, staff records, etc.) needs to be encrypted. Data encryption software helps to limit data access to unauthorized parties [10].
2. Secure institutional electronic devices: every office uses electronic devices (desktops, laptops, mobile devices) for data processing at the institution. It's therefore important for institutions to secure endpoints or entry points of end-users of these devices. These devices can be remotely accessed through network paths which implies that they can be maliciously exploited by cybercrime perpetrators [12]. Tertiary institutions need to apply endpoint protection (antivirus, full disk encryption, and patching) software to secure electronic devices and network access paths in institutional data.
3. Ensure Software and system updates on institutional devices and networks: cyberattacks often occur because most internet and electronic device users fail to install original software and update software regularly. This neglect weakens your system and network making it vulnerable to hackers' attack and exploitation to gain illegal access to your network and devices [1]. The use of updated software is crucial to digital and cyber security. Updated software version adds new features, fixes bugs and helps patch security flaws and vulnerabilities [10]. Ensuring that every device and network used for data processing at the institution periodically performs software and system updates is a proactive measure of securing institutional data.
4. Ensure Social-Media Savvy: Social media (Twitter, Facebook, MSN, YouTube, etc.) brings competitive advantages to an institution. The use of social media marketing, branding, communication, etc. is important to every institution. Social media is vulnerable and prone to cyberattacks, so institutions have to ensure that their social network profiles are set to private [10]. Be deliberate about security settings and be careful about information posted online. Having good savvy is key to protecting any institution's social media accounts.
5. Use Strong Passwords and regularly change passwords: [1], states that 80% of institutional data breaches result from weak passwords. A hacker does less work to gain access to a system once they identify a small gap in your password and exploit it fully to their advantage. Institutional data are extremely sensitive, have a strong password setup for devices, applications and networks to prevent unauthorized access [12]. Password cracking technology is immensely advanced therefore changing passwords regularly helps to maintain a high level of protection against internal and external cyber threats. [10], advised the use of the following when creating a password:
   i. All passwords should consist of 10 characters minimum.
   ii. It should contain alphanumeric (letters, numbers, special) characters.
   iii. It should not contain any personal information (date of birth, anniversary date, etc.).
   iv. It should not have any correctly spelled words.
   v. They should be unique and never used before.
   vi. Avoid auto-save on devices, browsers, and applications.
   vii. Safely store passwords in encrypted format
6. Use multi-factor authentication: [12] noted that institutions need to move from using simple passwords to more complex passwords by

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 255-260 www.ijaem.net ISSN: 2395-5252

deploying multi-factor authentication strategies to secure sensitive information and discourage cybercrime at the office level. A multi-factor authentication system (MFA) requires verifying a user's identity before granting them access to an account. It provides a much more reliable assured means of authenticating authorized users therefore reducing unauthorized access possibilities. Multi-factor authentication is more effective at protecting institutional systems than passwords [1].

7. Install Firewalls: Cyber threats have become sophisticated and advanced hacking techniques to access data are emerging daily. When a system (electronic device or network system) is online, a firewall is the first line of cyber defense. A firewall system protects from brute force attacks, blocks connections to unknown sites, keeps the system out from some types of viruses and hackers and prevents security incidents from irreversible damage [1]. Firewalls provide network traffic monitoring and help to identify suspicious activities that could compromise data integrity. It also prevents complex spyware from gaining access to your systems and promotes data privacy [12]. Institutions need to choose the right firewall that gives them full security control capabilities and application and network visibility to their cyber security infrastructure.
8. Internet Security & Antivirus: installing proper internet security and Antivirus applications on institution office systems helps to protect sensitive data both offline and online [8]. Internet security is designed to secure and protect systems and staff's activities while online such as web browsers, email, web apps, websites, and social networks. installing and regularly updating Antivirus prevents malware and spyware from infecting office systems.
9. System Access Management: Institutional data is handled by different levels of users at different office levels. Providing a preventive measure to ensure that various users access only the right resource at their level of trust is important. Granular policy settings can apply to control access to only authorized users for daily tasks. Monitor user's access permission and evaluate risks associated with each login. Step up user authentication when the user's content changes and risk association increases. Manage admin rights and block staff from installing unwanted applications and accessing certain data that are not beneficial to the security [12].
10. Physical System Access Control: Physical attacks on office systems are common practices in a work environment. Putting practical measures to control who accesses your electronic device and network is important [7]. For instance, a colleague can plug in a contaminated USB drive into your office system intentionally or unintentionally which could affect files on your device and network. Installing and setting a security perimeter is key to stopping such system breaks at the office. Many institutions focus on the digital part of cyber threats and entirely neglect their physical premises. Periodically conduct security assessments and determine if critical infrastructure is safe from security breaches. A situation can arise where institution data is safe online and a janitor can break into an office to obtain sensitive information, or go through garbage and obtain sensitive information. Use high-value systems and 2-factor authentication (biometrics and keycards) to protect restricted areas [1].
11. Protect office Wi-Fi: Wireless technology is growing daily and is used to connect multiple devices within the office environment. Any device connected to a network can be infected and if such an infected device is connected to an institution's network, that entire institution's system is at serious risk [7]. [10] stated that poorly secured Wi-Fi is vulnerable to attacks. Encrypting wireless devices might prevent unwanted access and system damage. Most Wi-Fi devices include wireless access points and are configured with default administrator passwords. Default passwords can be obtained online and they provide minimal protection. Changing Wi-Fi device default passwords may enhance device security. Tertiary institution staff must avoid using public Wi-Fi to conduct financial or corporate transactions on these networks and also secure wireless devices within its office space.
12. Regular staff Training: many institutions invest massively in cyber security infrastructure and tools but neglect the importance of staff training. Staff needs to be regularly trained on how to protect themselves and the institutional data and report cyber threats. According to [1], malicious hackers access databases through phishing emails sent to their employees. Emails contain dangerous malware in the form of links that hackers use to gain access to user personal data including login credentials. Statistically over 3.4 billion

phishing emails are sent to employees annually. Regular and proper staff training on cyber security awareness (i.e., verifying email addresses before replying to them and verifying links before clicking them)is vital to securing sensitive data in an institution. Also emphasizing the institution's cyber security policies on sensitive information sharing in any platform and among colleagues.

13. Regular Backup data: when disaster strikes (cyber-attack) only backup data can save you. [12], Keeping a regular backup is to avoid virus infection, unwanted access, data damage and loss, deletion, ransomware, financial loss, etc. Data backup means keeping a duplicate copy of sensitive information in another external drive. This activity helps the institutions to recover sensitive information when cyber attacks and natural disasters occur in an institution.
14. Create a Strong Cyber Security Policy: strong policies influence cyber security in an institution [1]. Stating clear data breach detection and prevention guidelines by an institution's Information Technology (IT) team is very important. The IT team should regularly conduct risk assessments, identify loopholes and perform penetration testing to provide robust cyber security policies and guidelines to the institution. Cyber security policies should include security testing, access control, access management, incident reporting and response plans, and disaster recovery plans.

VII. CONCLUSION

The use of the internet and electronic devices for daily data processing at tertiary institutions is growing geometrically and its associated cybercrime grows proportional. Sensitive institutional data such as personal data (staff and students), financial data, admission records, result data, certificates, databases, etc. are under cyberattacks daily. There is no absolute preventive measure or solution to cybercrime but tertiary institutions can adopt strict preventive measures as listed above to protect sensitive institutional data against cybercrime activities both offline and online. Cyber security in tertiary institutions should protect against all intentional and unintentional intrusions from both inside and outside systems. Cyber security policies at tertiary institutions should ensure the integrity, confidentiality and availability of institution data online and offline.

ACKNOWLEDGEMENT

This search was sponsored by Tertiary Education Trust Fund (TETFUND) Abuja, Nigeria.

REFERENCES

[1]. Axel Sukianto (2023).10 Ways to Reduce Cybersecurity Risk for Your Organization. https://www.upguard.com/blog/reduce-cybersecurity-risk. (19/12/2023)

[2]. Asiabaka, C.C. (2014). Imperatives of e-Government and the Future of Nigeria. Owerri: FUTO. www.softwareclubnigeria.org/.../FUTO%20VC%20E-Gov%20Imperatives%20.

[3]. Balogun, V.F. & Obe, O.O. (2014). E-Crime In Nigeria: Trends, Tricks and Treatment. The Pacific Journal of Science and Technology, 11 (1), 343 – 355. www.akamaiuniversity.us/PJST.htm

[4]. Gogwim, Joel Godwin (2020). Cybersecurity: Emerging Threats And Mitigation Strategies.https://nji.gov.ng/wp-content/uploads/2020/03/Joel-Presentation-@NJI-converted.pdf

[5]. Ibikunle, F. & Eweniyi, O. (2014) Approach to cyber security issues in Nigeria: challenges and solution. International Journal of Cognitive Research in Science, Engineering and Education. http://ijcrs

[6]. Igwe K. N. & Ahiaoma I. (2014). Imperative of Cyber Ethics Education to Cyber Crimes Prevention and Cyber Security in Nigeria. International Journal of ICT and Management, https://www.researchgate.net/publication/314213703

[7]. Leaf (2013). 10 Ways to Prevent Cyber Attacks.https://leaf-it.com › 10-ways-prevent-cyber-attacks.

[8]. Lubna T. (2020). Cybersecurity and Safety Measures. International Research Journal of Modernization in Engineering Technology and Science Volume:02/Issue:06 e-ISSN: 2582-5208. www.irjmets.com www.irjmets.com

[9]. Roman V. Veresh (2018). Preventive Measures against Computer Related Crimes: Approaching an Individual. Informatol. 51, 2018., 3-4, 189-199. https://doi.org/10.32914/i.51.3-4.7

[10]. Sudhir H, Prakash M., & Sandip B.(2019). 10 Cyber Crime Prevention Tips. https://pcpc.gov.in/files/1.pdf November, 2019

[11]. Sourajit K. B. & Arti V. (2022). Cyber Ethics: An Important Concept to Become a

Responsible Cyber Citizen. International Journal of Technical Research & Science. https://doi.org/10.30780/IJTRS.V07.I02.001

[12]. Tilly Kenyon (2021). Top 10 Ways to Prevent Cyber Attacks.https://cybermagazine.com/cyber-security/top-10-ways-prevent-cyber-attacks