American Journal of Humanities and Social Sciences Research (AJHSSR)
e-ISSN : 2378-703X
Volume-08, Issue-05, pp-95-115
www.ajhssr.com
Research Paper Open Access

CYBER SECURITY ENHANCEMENT IN NIGERIA. A CASE STUDY OF SIX STATES IN THE NORTH CENTRAL (MIDDLE BELT) OF NIGERIA

Gavou, Thomas Pam (Ph.D)[1,] John Iliya (Ph.D)[2,]
Ekomaru Chinyere Ihuoma (Ph.D)[3,] Associate Prof. Joseph N. Gusen (Ph.D)[4]

[1]Senior Lecturer, Home Economics Education, Department of Science and Technology Education, Faculty of Education, University of Jos, Plateau State, Nigeria

[2]John Iliya (Ph.D) Deputy Director, Plateau State Ministry of Education, Headquarters, Jos, Nigeria. Department of Science and Technology.

[3]Ekomaru Chinyere Ihuoma (Ph.D) Senior Lecturer, Home Economics, Alvan University of Education Owerri, Imo State, Nigeria.

[4]Corresponding author: Associate Prof. Joseph N. Gusen (Ph.D) Reader in Computer Science Education, Department of Science and Technology Education, Faculty of Education, University of Jos, Plateau State, Nigeria,

ABSTRACT: Security plays an important role in human life and endeavors. Securing information and disseminating are critical challenges in the present day. This study aimed at identifying innovative technologies that aid cybercrimes and can constitute threats to cybersecurity in North Central (Middle Belt) Nigeria covering its six States and the FCT Abuja. A survey research design was adopted. The researchers employed the use of Google form in administering the structured questionnaire. The instruments were faced validated by one expert each from ICT and security. Cronbach Alpha reliability Coefficient was employed and achieved 0.83 level of coefficient. The population of the study was 200, comprising 100 undergraduate students from computer science and Computer/Robotics Education, 80 ICT instructors, technologists and lecturers in the University and Technical Colleges in the Middle Belt Nigeria using innovative technologies for their daily jobs and 20 officers of the crime agency such as: Independent Corrupt Practices Commission (ICPC) andEconomic and Financial Crimes Commission (EFCC). Three research purposes and questions as well as the hypothesis guided the study on Five (5) point Likert scale. Data collected were analyzed using mean and standard deviation for the three research questions while three hypotheses were tested using t-test at 0.05 level of significance. Major findings revealed that serious steps are needed to better secure the cybers against cybercrimes. Motivation, types, threats and strategies for the prevention of cybercrimes were identified. The study recommends that government, organizations and individuals should place emphasis on moral development, regular training of its employees, regular update of software, use strong password, back up data and information, produce strong cybersecurity policy, install antivirus soft and security surveillance (CCTV) in offices in order to safeguard its employees and properties from being hacked and vandalized.

***KEYWORDS**: Cybersecurity, cybercrime, cyberattack, cybercriminal, computer virus, Virtual Private Networks (VPN).*

I. INTRODUCTION

Cybersecurity is seen as the protection to defend internet-connected devices and services from malicious attacks by hackers, spammers, and cybercriminals [1]. The rate of cybercrime is viewed as a business which is boosting the economy [2]. Consequently, it is rising on daily basis. The growing number of attacks are putting lives at risk, costing companies, individuals, institutions of learning millions of money constituting the largest transfer of economic wealth in history and is stimulating job and cyber security salaries are high [3] andmore profitable than any legal business which is threatening national security[4].

II. LITERATURE REVIEW

This section reviews literature relevant to the topic under the following subheadings: major causes of cybercrimes, **r**anking of countries and their unique security issues, types of cybercrimes and cyberattack**,** Innovative Technologies use for Cybercrime,attack methods cybercriminals use for their operation,effect of cybercrime on business and individuals, methods of preventing/combating cybercrime attacks

2.1 Major Causes of cybercrimes

[5] pointed out the following as some of the major causes of cybercrimes that users of Internet must be acquainted with:(a) Easy Access System when security is compromised when skilled hackers can get unauthorized access by breaching access codes, retina images, voice recognition, etc. (b)The advent of computers that cybercrime came into existence and Storing Data in a Small Space are the biggest reasons behind cyberattacks which makes it easier for hackers to steal data in no time and utilize it for their own profit.(c)Complex Codings which are created with millions of codes are vulnerable to errors, these gaps can be easily exploited by the cyber-criminal making the operating system malicious for the users. (d)Negligence in ensuring the security of your system can bring you big troubles. (e)Loss of Evidence can become an important cause of cybercrime that can possibly paralyze your system and make it more vulnerable to cyber-attacks.(f) Evolution of Cyber Crime has been prevalent since computer technology's inception, dating back to the 90s

[4]pointed out the following as reasons why global attacks are rising factors fueling sustained growth in the field: (a) more devices(smart home devices, credit card readers, connected systems in your car) more points of vulnerability; (b)Rates of cybercrime are going up because of widespread adoption of digital technologies; (c)The Cloud computing platforms, like Amazon Web Services attend and Google Cloud, offer increased storage, empower remote collaboration and simplify file sharing which represent a new point of vulnerability; (d) More people work remotely such as distant learning and virtual meetings from home, shop from home and log in to medical appointments using computers and phones have created a digital landscape in which sensitive information flows over networks 24 hours a day;(e) Third-party relationships such as vulnerable organizations and agencies have created extended attack surfaces; (f)Outdated technology leaves data vulnerable as too many organizations, in an effort to save money and time, still use outdated legacy software that functions but is not as secure as newer applications and platforms;(g) The rapid transition to remote work and expanded cloud migration led to increased cybercrime rates, prompting organizations to beef up their digital security measures

[6] lamented that the economy inflation, the energy crisis and supply chain issues are affecting every industry. Inflation will increase the overall cost of cybercrime as preventive and remediation costs rise. Computer virus, also known as malware, is a malicious piece of software designed to infect a user's device, much as the same way a physical virus infects a person's body [7]. Other types of malware include spyware, rootkits, and worms. Malware-as-a-Service Since accessing malware services and kits has never been easier as attack rates are bound to rise substantially. Geopolitical conflict rising geopolitical tensions are already causing an increase in state-sponsored and politically driven attacks. Criminals target smaller organizations because they are starters, smaller targets usually have weaker security. Organizations cannot afford cyber insurance. They might be unable to afford cyber insurance, be declined coverage or experience significant coverage limitations as further pressure on businesses on the financial side in the event of a breach. Rapidly expanding attack surface as intruders may even reach corporate assets from a device connected to a home network where remote work occurs. Hacktivism rising. Hacktivism is a significant anti-establishment weapon promoting a diverse set of causes around the globe as environmental hacktivists targeting mining and oil companies.

[3] stated the following as six compelling reasons why you should study Cybersecurity because: (a) cyber security jobs are in high demand, (b) there is an increase in the number of Specialties;(c) It is a stimulating job;(d) you get to solve complex technical puzzles; (e) cyber security salaries are high (f) you get to play the Hero.

In the same vein, [8] pointed out 20 Frightening Cyber Security Facts & Stats that:(1)85% of people posting puppy photos are trying to scam you(2)Human error accounts for 95% of all data breaches(3)Every 39 seconds there is a cyberattack (4)43% of cyberattacks target small business(5)75% of cyberattacks start with an email (6)The global average costs of a data breach is $3.9 million across SMEs(7)Since COVID-19 and the increase in staff working from home, the Federal Bureau of Investigation (FBI) have reported an increase of 300% in reported cybercrimes (8)The worldwide information security market is forecast to reach $170.4 billion in 2022(9)Most companies take nearly 6 months to detect a data breach, even major ones (10)On average, only 5% of companies' folders are properly protected.(11)Data breaches exposed 36 billion records in the first half of 2020.(12)86% of breaches were financially motivated and 10% were motivated by espionage.(13)4 million files are stolen every day - that's 44 every single second (14)21% of files aren't protected(15)Cybercrime is quickly becoming more profitable than the illegal drug trade (16)Around 95% of cloud security failures are predicted to be the customer's fault (17)Word, PowerPoint and Excel (the Microsoft office formats) comprise the most prevalent group of malicious file extensions(18)Email is the primary entry point of 94% of malware attacks (19)Cybercrime is set to cost $6 trillion in 2021,twice what it was in 2015 and $10.5 trillion by 2025 (20)The Netherlands has the lowest cybercrime rate, whilst Russia has the highest.

Nigeria being a developing country is also affected as no one is entirely immune from Cybercrime. The Nigerian President of the Senate, Senator Godswill Akpabio, expressed these concerns in his remarks while declaring open a public hearing on the 2023 Cybercrime (Prohibition and Prevention) Act (Amendment) Bill, 2023 at the Senate Complex, Abuja, on Wednesday [9]. [9] decried the annual loss of approximately **$500 million** to various forms of cybercrime across Nigeria. This cybercrime applies to almost all forms of cybercrimes, including identification theft, fraudulent online transfers, payment-card frauds, network assaults, denial-of-service attacks by malicious networks of computers (botnets), ransomware, and malware attacks, among others [10]. According to [10]., some technology majors in Nigeria have fallen victim to cybercrimes because these attacks have become so organised, coordinated, and highly sophisticated that they can infiltrate the most elaborate firewalls of any organisation. The crime is characterized by an increased adoption of electronic devices such as computer systems, internet service and modern telecommunication systems, smart phones and social media devices like Facebook, WhatsApp and Instagram [11]. These technological and digital devices are used for downloading, storing and retrieving of unlimited access to information and saving of documents in our everyday activities at home, banking, teaching and learning, research, business transaction and for communication [12]. These digital devices are prone to cyberthreats, cyberattacks such as malware, denial-of-Service(DoS) attacks, phishing, spoofing, identity-based attacks, code injection attacks, supply chain attacks, insider threats, DNS tunneling, IoT-based attacks [13] which are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes,[1]. The more we use the Internet, network, World Wide Web (WWW) and smart phones, the more they intrude into our personal information and expose us to cyberattacks, cybercriminals, spammers, hackers, and exploiting us for their good. Therefore, Nigerians should be aware of what causes cyber-crimes and reasons why Cyber Crimes exist to find a solution to it. [14] stated that Nigeria ranked 16th in Federal Bureau of Investigation (FBI) global cybercrime victims report. Nigeria has been ranked 16th among the countries most affected by internet crime in the world in 2020**.** In its latest internet crime report, the US FBI said Nigeria received 443 complaints relating to internet crime in 2019. The last times the country featured in the annual reports were in 2016 (19th) and 2015 (3rd).The FBI said victims of such scams globally lost $4.2 billion in 2020, compared to $3.5 billion lost in 2019.

According to [15] Nigeria has embraced digital transformation and is witnessing a rapid increase in internet connectivity, as data breaches have intensified. For the uninitiated, a data breach occurs when an intruder usually a hacker, copies and leaks confidential user data such as names, email addresses, passwords, banking details and more without permission. According to a report [pdf] by IBM, the cost of a data breach averaged $4.35 million in 2022. A recent global studyreleased by Surfshark, an Amsterdam-based cybersecurity firm, ranks Nigeria as the 32nd most breached country in the first quarter of 2023. Per the report, Nigeria had 82,000 leaked accounts from January to March 2023, representing a 64% increase from the previous quarter. It adds that data breaches globally declined in Q1 2023, with 41.6 million accounts breached. This is almost 50% less than the nearly 81 million recorded in Q4 2022. Similarly, [16] stated that the Federal Government of Nigeria on Wednesday 2023 lamented the increase in cybercrimes in the country occasioned by the digital transformation witnessed in the country. This it noted had thrown up new types of crimes as well as aiding criminals to penetrate the traditional crimes using the new technologies. The Solicitor General of the Federation, Beatrice Jedy-Agba, disclosed this at the opening ceremony of a three-day cybercrime awareness programme organised by the Federal Ministry of Justice in collaboration with the US Embassy in Abuja on Wednesday 2023.

2.2 Ranking of countries and their unique security issues

[17] stated the following Bscholarly'sCybercrime Top 10 Rankings list of countries and their unique security issues:(a) **China** tops the list of countries with the highest rate of cybercrime and is third on the list of most breached countries in the world. In 2021, China recorded up to 5,000 cases of online gambling alone out of an estimated total of 65,000 cases relating to cybercrime in the same year. The major targets are usually defense, communications and technologies industries.(b) **Russia** in 2021 recorded over 500,000 crimes being fostered and committed with the aid of the internet space and telecommunication devices. (c) **India** in 2021 recorded more than 52,000 cases of cybercrimes. Cybercrime in India is principally regulated by the Information and Technology Act of 2000. (d) **Brazil** in the first six months of 2020 recorded over 320,000 cybercrime incidents. The nation ranks 5th in cybercrime target countries. Most of the targets are financing and banking. (e) **Iran** :has created a safe haven where cyber criminals acting for personal gain flourish and defendants like these are able to hack and extort victims, including critical infrastructure providers," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. Iran has the means, the technology and the manpower.(f) **Nigeria** loses over 0.8% of its Gross Domestic Product to internet fraud per annum. According to the FBI ranking, Nigeria is ranked 16th on victims of cybercrimes in the world.(g) **Germany** in 2019 recorded and handled over 300,000 cases of cybercrimes. The following year, records showed an 8% increase in the incidences of cybercrime. Germany loses up to 0.7% of its Gross Domestic Product to cyber fraud yearly. (h) **Vietnam,** according to the Vietnam National Security Centre, reported more than 1,300 attacks in January 2022 alone, for a 10% increase as compared to the previous year.(i) **Poland's** 2020 survey show3e that 29% of

businesses were victims of a cyberattack.(j).**United States** is the country recording the highest rate of breaches in the world. In the first half of 2022, more than 50 million U.S. citizens had been affected by cybercrimes.

[18] carried out a research on cybercrime in 10 countries. He collected survey data from 92 cybercrime experts, asking them to pick the top five cybercrime-producing nations in five different categories of crime: technical products and services; attacks and extortion; data and identity theft; scams; and cashing out or money laundering. For each nation, participants were asked to rate the nation on the impact of the crimes, the actors' professionalism, and their technical skill. The cost implication of each country are as follows: (a) Russia is $41.56. (b) Ukraine $31.37

Contributing, [19]have outlined the following key findings from the research into cybercrime(a)According to Ipsos, almost one in three Americans fell victim to online financial fraud in 2023 (Ipsos - 2023 Ipsos Poll (Wells Fargo))36% of people aged 35 to 54 have reported being a victim, compared to only 22% of Americans aged 18 to 34.(Ipsos - 2023 Ipsos Poll (Wells Fargo)$^{)}$(b)The total cost of cybercrime globally reached $8 trillion in 2023 and is predicted to hit $10.5 trillion by 2025(Ipsos - 2023 Ipsos Poll (Wells Fargo) (c)While there were fewer individual victims of cybercrime in 2023 (just over 350 million) compared to 2022 (over 425 million), there were over 1,400 more compromises in total(Identity Theft Resource Center - 2023 Data Breach Report)(d)The average amount of money lost by businesses as a result of cybercrime in 2023 was $1.3 million.[20] (e)Across all industries, the average cost of a data breach was $4.45 million, with the healthcare industry facing the highest average data breach cost at $10.93 million[20] It's estimated that the total value of the cybersecurity market in 2024 is close to $200 billion ES/B and this is forecasted to reach nearly $315 billion by 2029, according to Mordor Intelligence(Mordor Intelligence - Cybersecurity Market Size & Share Analysis - Growth Trends & Forecasts (2024-2029)).According to [21] Norton's Cyber Safety Insights Report, 77% of Americans have taken steps to protect their personal data online[21]

2.3 Motivation for the increase in cybercrime

[22] explain the following 10 reasons why cyber threats are on the increase at this staggering and exponential rates, thus:(a) cyber criminals are clever as organisations do not always do a good job monitoring their partners, suppliers and supply chain.(b) the numbers are not accurate anyway as far as many compromises go undetected(c) information security still do not get the respect it deserves as many organisations complacent about their security policy, data destruction and data protection laws.(d) lack of training on the effects of cyber security(e)lack of good leadership dedicated to information security(f) Insiders are the most costly and damaging threats as no organization have a programme in place to deal with the insider security threats(g) legalities as many organisations do not involve the law when cybercrimes are committed by insiders(h) service providers, consultants and contractors do not comply with privacy policies(i) Lack of talent as there is a shortage of experienced security professionals. The most skilled candidates are hired by bigger organisations. (j) connectivity as increases in attacks on connected consumer devices are being seen as they lack security safeguards.

[23] opined that the goal for many of these cyber crime organizations is personal information of the user credentials, social security numbers, driver's license numbers, credit card numbers, banking info, and other personal details fetch a hefty sum on the dark web where cybercriminals trade the spoils from data breaches and hacks. [24] outline 6 motivations of cybercriminals to include: money; entertainment; cause such as use of the Internet to promote a particular political, scientific or social cause; entrance to a social group; status through boosting of their skills and expertise in networks, operating systems, hardware, security and source credit. Other motives according to [25] are money, competition, and political motivation.. [23] stated that cybercriminals may target individuals, companies, and even governments with a motive of intentionally harming the reputation, causing physical, mental, or another type of harm, or using their equipment to form malicious networks (botnets).

[26] pointed out that a motivation involved in cybercrime depends on criminal's intent and need which are mostly motivated by financial gain, revenge, ideological beliefs, or the addictive nature of cybercrime, thus: (a) **Monetary Profit**: Cybercrimes are also motivated by the desire for financial gain.(b)**Political Motive**: Internet is used by extremist and radical groups for propaganda, to attack the websites and network of their opposite groups. (c)**Sexual Impulses**: People view porn sites to fulfill their immoral desires and needs. So, sexually deviant behaviour is illegal and is considered harmful. (d)**Entertainment**: Many cybercrimes are done for fun and enjoyment unlike other cybercrimes, in which internet is means to an end. For cyber criminals such as hackers, fun is both a means and an end. (e)**Emotional Motivators**: Cyber criminals who use anger as motivation are spurned lovers, fired employees, business associates or someone who feels cheated. [27] stated Four Reasons the Cybersecurity Field Is Rapidly Growing, thus: Hackers Are Getting Smarter, Everything Is Automated, Vulnerabilities Are Everywhere, Career Outlook for Cybersecurity Professionals

[28] outlined 8 Motives of CyberCrime as follows: (a)**Financial Gain**: Most of the hacker's primary motivation is Financial Gain. They are using a variety of methods such as phishing attacks to collect credit card or debit card details, banking account login details, etc. Once they gain credentials they login into your account

and transfer the money to their account. They also use attacks like Ransomeware on the entire organization for money. Some of the hackers use fake social media profiles to trap people and may collect money from them.(b)**Insider Threats**. This type of threat has occurred directly or indirectly by the person who is working in an organization with access to critical information. He may sell details to other organizations for personal gain or to damage the company's reputation in public. Sometimes the threat has occurred due to his negligence in using exposed passwords and easily guessable passwords for accounts as they identify these details and collect the required information.(c)**Recognition & Popularity**: In general, every human feels happy when everyone recognizes him. Hackers also do this activity for their recognition such as the hacker may hack the girlfriend's account to recognize his friend.(d)**State-Sponsored Hackers**: These hackers are either white hat or black hat hackers who steal information from foreign governments. Their targets are terrorists, foreign governments, and corporations. They may work for their governments. Such Government provides funds to these hackers. These hackers themselves treat as legitimate because they work for their government.(e)**Hacktivists**: Hacktivists are the hackers who protest the political and social ideas of organizations and governments by posting articles, videos, leaking sensitive information to stop their website services. These types of hackers come under the category of Gray Hat Hackers.The most famous Hacking Group is **Anonymous**. It fights for people against governments and organizations such as hacking governments' sites and leaks sensitive information and this group has a lot of fans. For in the Recent Ukrain War, hackers did a DDoS attack on Russia Government Websites and their sites were down due to this activity.(f) **Crackers:** Crackers are hackers who modify the programming in applications to use those applications for free. Some crackers crack the tools placed on websites like getintopc.com to earn money with ads and some of the hackers insert malicious code in these cracks to collect users' information using credit card links.(g)**Pornography**. Some hackers did hacking to produce pornography by hacking users' phones & Computers and collecting their personal information and blackmailing and uploading their videos porn sites. Etc Some stupid people did women trafficking by collecting their personal information and blackmailing them.(h)**Drugs**: Some Persons use their technical skills to do illegal activities like selling drugs etc. Most crimes have been done using the darknet. Darknet sites do not open by using normal browsers. They are using separate browsers like The Onion Router (TOR) which is **free and open-source software for enabling anonymous communication**. It directs Internet traffic via a free, worldwide volunteer overlay network that consists of more than seven thousand relays.

Competition. Getting into a manufacturers system can be valuable, whether for IP, blackmail, competitive intelligence, creating a PR nightmare (sabotage), or other reasons. This is especially risky given the (lack of) technical sophistication of systems across industries with complex intellectual property at their core, whether they be in technology, pharmaceuticals, high-tech manufacturing, resource extraction, general utilities, industrial systems or similar sectors [25].

Other motivating factors for engaging in cybercrime are:(a) cybercriminals are always on the lookout for ways to make huge financial gain (money) fun of breaching confidential information;(b) recognition & Achievement; (c)insider threats such as internal employees, vendors, a contractor or a partner;(d)political motivation to fund or further espionage and exploitation causes; (e) corporate espionage involves: (i)Acquiring property like processes or techniques, locations, customer data, pricing, sales, research, bids, or strategies(ii) Theft of trade secrets, bribery, blackmail, or surveillance [5], [29].

2.4 Types of cybercrime

Cybercrime in Nigeria like in other countries of the world seems to follow a pattern of highly sophisticated technologies in the form of emails scam, where the scammer(s) mail a letter via e-mail and with a scheme to extort money. Types of cybercrime like hacking, ransomware, and phishing email, identity theft, [30], botnet, Internet harassment, Customer Service Impersonation, Social engineering, Mirror Websites, Potentially Unwanted Programs (PUPs), Impersonation Scams, Sim Swapping, Viruses and malware attacks are all around us and their impact is global and crosses physical boundaries, [31]. [30] explains that: (a)Cybercrime encompasses a wide range of malicious activities exploiting digital technologies**,** affecting individuals, businesses, and governments globally. (b)Phishing scams, identity theft, and ransomware attacks are some of the most common types of cybercrime**,** with severe financial and psychological impacts on victims. Phishing is a scam where cybercriminals use fake emails or messages to trick people into sharing personal information. You can recognize it by looking for suspicious requests, urgent language, and unusual formatting in the message. Cybercrime is the flip side of cybersecurity, a huge spectrum of damaging and illegal activity carried out using computers and the Internet.

[32]and [33] share the same ideas on Malware attack, Social engineering attacks, Software supply chain attacks, Advanced persistent threats (APT), Distributed denial of service (DDoS), Man-in-the-middle attack (MitM), Password attacks, Cyber-threats actors as the main different types of Cybercrime and information security threats, thus:

1. **Malware attack**. This type of malware uses many methods such as asking you to click a link or open an attachment which are vulnerabilities in browsers or operating systems to install themselves without

the user's knowledge or consent to get malware into a user's device. Malware attacks include:(a)**Trojan virus:** Trojan virustricks a user into thinking it is a harmless file. A Trojan can launch an attack on a system and can establish a backdoor, which attackers can use.(b) **Ransomware.** Thistype of malwareprevents access to the data of the victim and threatens to delete or publish it unless a ransom is paid. (c)**Wiper malware:** Itintends to destroy data or systems, by overwriting targeted files or destroying an entire file system. Wipers are usually intended to send a political message, or hide hacker activities after data exfiltration.(d)**Worms:** This malware is designed to exploit backdoors and vulnerabilities to gain unauthorized access to operating systems. After installation, the worm can perform various attacks, including Distributed Denial of Service (DDoS). (e).**Spyware:** This malware enables malicious actors to gain unauthorized access to data, including sensitive information like payment details and credentials. Spyware can affect mobile phones, desktop applications, and desktop browsers. (f).**Fileless malware:** This type of malware does not require installing software on the operating system. It makes native files such as PowerShell and WMI editable to enable malicious functions, making them recognized as legitimate and difficult to detect.(g).**Application or website manipulation:** Open Web Application Security Project (OWASP) is a non-profit organization founded in 2001, with the goal of helping website owners and security experts protect web applications from cyberattacks outlines the top 10 application security risks, ranging from broken access controls and security misconfiguration through injection attacks and cryptographic failures. Once the vector is established through service account acquisition, more malware, credential, or APT attacks are launched

2. **Social engineering attacks**. Social engineering attacks work by psychologically manipulating users into performing actions desirable to an attacker, or divulging sensitive information. TheseSocial engineering attacks include the following:(a)**Phishing:** Phishing attackers send fraudulent correspondence that seems to come from legitimate sources, usually via email. The email may urge the user to perform an important action or click on a link to a malicious website, leading them to hand over sensitive information to the attacker, or expose themselves to malicious downloads. Phishing emails may include an email attachment infected with malware.(b)**Spear phishing:** This is a variant of phishing in which attackers specifically target individuals with security privileges or influence, such as system administrators or senior executives. (c).**Malvertising:** This is an online advertising controlled by hackers, which contains malicious code that infects a user's computer when they click, or even just view the ad. Malvertising has been found on many leading online publications. (d) **Drive-by downloads:** This is a situation whereattackers can hack websites and insert malicious scripts into PHP or HTTP code on a page. When users visit the page, malware is directly installed on their computer; or, the attacker's script redirects users to a malicious site, which performs the download. Drive-by downloads rely on vulnerabilities in browsers or operating systems. Learn more in the guide to drive-by downloads.(e)**Scareware security software:** Itpretends to scan for malware and then regularly shows the user fake warnings and detections. Attackers may ask the user to pay to remove the fake threats from their computer or to register the software. Users who comply transfer their financial details to an attacker. (f).**Baiting**: This occurs when a threat actor tricks a target into using a malicious device, placing a malware-infected physical device, like a USB, where the target can find it. Once the target inserts the device into their computer, they unintentionally install the malware.(g)**Vishing**: voice phishing (vishing) attacks use social engineering techniques to get targets to divulge financial or personal information over the phone.(h)**Whaling:** This type of phishing attack targets high-profile employees (whales), such as the chief executive officer (CEO) or chief financial officer (CFO). The threat actor attempts to trick the target into disclosing confidential information .(i)**Pretexting**: This occurs when a threat actor lies to the target to gain access to privileged data. A pretexting scam may involve a threat actor pretending to confirm the target's identity by asking for financial or personal data. (j).**Scareware,** a threat actor tricks the victim into thinking they inadvertently downloaded illegal content or that their computer is infected with malware. Next, the threat actor offers the victim a solution to fix the fake problem, tricking the victim into downloading and installing malware.(k).**Diversion theft** threat actors use social engineers to trick a courier or delivery company into going to a wrong drop-off or pickup location, intercepting the transaction.(l).**Honey trap:** This isa social engineer assumes a fake identity as an attractive person to interact with a target online. The social engineer fakes an online relationship and gathers sensitive information through this relationship.(m)**Tailgating or piggybacking:** This occurs when a threat actor enters a secured building by following authorized personnel. Typically, the staff with legitimate access assumes the person behind is allowed entrance, holding the door open for them.(n).**Pharming:** This is an online fraud scheme during which a cybercriminal installs malicious code on a server or computer. The code automatically directs users to a fake website, where users are tricked into providing personal data
3. **Software supply chain attacks**. A software supply chain attack is a cyberattack against an organization that targets weak links in its trusted software update and supply chain. **Types of software**

supply chain attacks (a)Compromise of software build tools or dev/test infrastructure (b)Compromise of devices or accounts owned by privileged third-party vendors (c)Malicious apps signed with stolen code signing certificates or developer IDs (d).Malicious code deployed on hardware or firmware components (e).Malware pre-installed on devices such as cameras, USBs, and mobile phones

4. **Advanced persistent threats (APT)**. When an individual or group gains unauthorized access to a network and remains undiscovered for an extended period of time, attackers may exfiltrate sensitive data, deliberately avoiding detection by the organization's security staff. **Common indicators of an APT presence include:(a) New account creation:** The P in Persistent comes from an attacker creating an identity or credential on the network with elevated privileges. (b).**Abnormal activity: L**egitimate user accounts typically perform in patterns. Abnormal activity on these accounts can indicate an APT is occurring, including noting a stale account which was created then left unused for a time suddenly being active. (c).**Backdoor/trojan horse malware:** Extensive use of this method enables APTs to maintain long-term access. (d).**Odd database activity:** This occur in a sudden increase in database operations with massive amounts of data. (e).**Unusual data files:** The presence of these files can indicate data has been bundled into files to assist in an exfiltration process.
5. **Distributed denial of service (DDoS)**. The DDoS is a variant of DoS in which attackers compromise a large number of computers or other devices, and use them in a coordinated attack against the target system. Their methods of DDoS attacks include**:** (a) **Botnets:** This— systems under hacker control that have been infected with malware. Attackers use these bots to carry out DDoS attacks. Large botnets can include millions of devices and can launch attacks at devastating scale. (b).**Smurf attack:** Itsends Internet Control Message Protocol (ICMP) echo requests to the victim's IP address. The ICMP requests are generated from 'spoofed' IP addresses. Attackers automate this process and perform it at scale to overwhelm a target system. (c).**TCP SYN flood attack:** This type of DDoSattacks flood the target system with connection requests. When the target system attempts to complete the connection, the attacker's device does not respond, forcing the target system to time out. This quickly fills the connection queue, preventing legitimate users from connecting.
6. **Man-in-the-middle attack (MitM)**. This occurs when users or devices access a remote system over the internet, they assume they are communicating directly with the server of the target system. The MitM attacks include the following**:** (a) **Session hijacking:** An attacker hijacks a session between a network server and a client. The attacking computer substitutes its IP address for the IP address of the client. The server believes it is corresponding with the client and continues the session. (b).**Replay attack:** A cybercriminal eavesdrops on network communication and replays messages at a later time, pretending to be the user. Replay attacks have been largely mitigated by adding timestamps to network communications. (c).**IP spoofing:** An attacker convinces a system that it is corresponding with a trusted, known entity. The system thus provides the attacker with access. The attacker forges its packet with the IP source address of a trusted host, rather than its own IP address. (d).**Eavesdropping attack:** Theattackers leverage insecure network communication to access information transmitted between the client and server. These attacks are difficult to detect because network transmissions appear to act normally. (e).**Bluetooth attacks:** Since Bluetooth is often open in promiscuous mode, there are many attacks particularly against phones, that drop contact cards and other malware through open and receiving Bluetooth connections. Usually this compromise of an endpoint is a means to an end, from harvesting credentials to personal information
7. **Password attacks**. This occurs by a hacker gaining access to the password information of an individual through 'sniffing' the connection to the network, using social engineering, guessing, or gaining access to a password database. An attacker can 'guess' a password in a random or systematic way. The Password attacks include the following**:** (a).**Brute-force password guessing:** This allowan attacker to use software to try many different passwords, in hopes of guessing the correct one. The software can use some logic to trying passwords related to the name of the individual, their job, their family, etc. (b).**Dictionary attack:** This isa dictionary of common passwords which is used to gain access to the computer and network of the victim. One method is to copy an encrypted file that has the passwords, apply the same encryption to a dictionary of regularly used passwords, and contrast the findings. (c).**Pass-the-hash attack:** This is an attacker that exploits the authentication protocol in a session and captures a password hash (as opposed to the password characters directly) and then passes it through for authentication and lateral access to other networked systems. In these attack types, the threat actor doesn't need to decrypt the hash to obtain a plain text password. (d).**Golden ticket attack: I**t is a golden ticket attack that starts in the same way as a pass-the-hash attack, where on a Kerberos (Windows AD) system the attacker uses the stolen password hash to access the key distribution center to forge a ticket-granting-ticket (TGT) hash. Mimikatz attacks frequently use this attack vector
8. **Cyber-threats actors.** It is veryimportant to understand who the threat actor is, as well as their tactics, techniques, and procedures (TTP). The common sources of cyberthreats include the following:

(a).**State-sponsored:** Any state-sponsoredcyberattacks by countries can disrupt communications, military activities, or other services that citizens use daily.(b)**Terrorists:** Terrorists may attack government or military targets, but at times may also target civilian websites to disrupt and cause lasting damage. (c).**Industrial spies:** This is anorganized crime and international corporate spies that carry out industrial espionage and monetary theft. Their primary motive is financial gain. (d).**Organized crime groups:** This type ofcriminal groups infiltrate systems for monetary gain. Organized crime groups use phishing, spam, and malware to carry out identity theft and online fraud. There are organized crime groups who exist to sell hacking services to others as well as maintaining even support and services for profiteers and industrial spies alike. (e).**Hackers:** There is a large global population of hackers, ranging from beginner "script kiddies" or those leveraging ready-made threat toolkits, to sophisticated operators who can develop new types of threats and avoid organizational defenses. (f).**Hacktivists:** Hacktivists are hackers who penetrate or disrupt systems for political or ideological reasons rather than financial gain.(g).**Malicious insider:** Insiders represent a very serious threat, as they have existing access to corporate systems and knowledge of target systems and sensitive data. Insider threats can be devastating and very difficult to detect.(h).**Cyber espionage:** This is a form of cyberattack that steals classified, or sensitive intellectual data to gain an advantage over a competitive company or government entity.

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual. At the other end of the spectrum is the growing crime of theft while at the midway along the spectrum lies transaction-based crimes such as fraud, trafficking in child pornography, digital privacy, money laundering and counterfeiting [34] these are specific crimes with targeted victims, but the criminal hides in the relative anonymity provided by the internet. Another part of this type of crimes involve individuals within corporations or government bureaucracies deliberating altering data for either profit or political objectives [35]. At the other end of the wave are those crimes that involve attempts to disrupt the actual workings of the internet. These range from span, hacking and denial of service attacks against specific sites to acts of cyber-terrorism that is, the use of the internet to cause public disturbances and even death. Cyber-terrorism focuses upon the use of the internet by non-state actors to affect a nation's economic and technological infrastructure. Some of the few types of cybercrime highlighted by this work are as follows: Hacking, Charity funds fraud, Bank verification Number (BVN), Data and Airtime (DAT), Theft from Service Providers, Cyber-plagiarism, Social-Hi-Jacking, Cyber-stalking, Intellectual property theft, Cyber-theft Banking fraud [36].

Cybercrime is considered as an epidemic which is borderless a menace. It cuts across religious faiths and political systems and affects young and old, male and female. Cybercrime is any criminal activity that involves a computer, network or networked device [2]. While most cybercriminals use cybercrimes to generate a profit, some cybercrimes are carried out against computers to directly damage or disable them. Cybercrimes nowadays include: Hacking, Malware, Identity theft, Social Engineering and Soft Privacy. Cybercrimes are considered a major risk because they can have devastating effects like financial losses, breaches of sensitive data, failure of systems and it can also affect an organization reputation.

Cybercrime sometimes targeted individuals, businesses, groups and even governments. Cybercriminal is a person who uses his skills in technology to do malicious acts and illegal activities known as cybercrimes. They can be individuals or groups. They are widely available in what is called the "Dark web" where they mostly provide their illegal services or products. Hacking is described as one of the cybercrimes but not every hacker is a cybercriminal because hacking activity is not considered a crime as it can be used to reveal vulnerabilities to report and batch them which is called "white hat hacker". Hacking can only be considered criminal act when its purpose has malicious and harmful activities and therefore it is called "black hat hacker or cyber-criminal". Some examples of cybercriminals include the following: Black hat hackers, cyber stalkers, cyber terrorists and Scammers [37].

However, it is worthy of note that cybercriminals take advantage of security holes and vulnerabilities found in systems and exploit them in order to take a foothold inside the targeted environment. The security holes can be a form of using weak authentication methods and passwords, it can also happen for the lack of strict security models and policies.

All over the world, many people have made cybercrime as a means of livelihood at the expense of other people's physical and mental wellbeing [38]. [39] affirmed that many have become rich through cybercrime while others have been caught by law. [37] states that educating young people would help decrease the risk of students in cyberspace. [40] posited that the level of education contributes significant difference to the student's perceptions of cybercrime.

2.5 Types of Cyberattacks.

[41] and [42] share similar ideas and presented the following types of cyberattack:

1. **DoS and DDoS attacks**. A denial-of-service (DoS) attack is designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests. A distributed denial-of-service (DDoS) attack on the other hand is similar in that it also seeks to drain the resources of a system. A DDoS attack is initiated by a vast array of malware-infected host machines controlled by the attacker. DoS and DDoS attacks are different from other types of cyber attacks that enable the hacker to either obtain access to a system or increase the access they currently have

2. **MITM attacks**. Man-in-the-middle (MITM) types of cyberattacks refer to breaches in cybersecurity that make it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers. It is called a “man in the middle” attack because the attacker positions themselves in the “middle” or between the two parties trying to communicate. In effect, the attacker is spying on the interaction between the two parties.

3**. Phishing attacks**. A phishing attack occurs when a malicious actor sends emails that seem to be coming from trusted, legitimate sources in an attempt to grab sensitive information from the target. Phishing attacks combine social engineering and technology and are so-called because the attacker is, in effect, “fishing” for access to a forbidden area by using the “bait” of a seemingly trustworthy sender.

4. **Whale-phishing attacks**. A whale-phishing attack is so-named because it goes after the “big fish” or whales of an organization, which typically include those in the C-suite or others in charge of the organization. These individuals are likely to possess information that can be valuable to attackers, such as proprietary information about the business or its operations.

5. **Spear-phishing attacks.** Spear phishing refers to a specific type of targeted phishing attack. These types of attacks are aptly called “spear” phishing because of the way the attacker hones in on one specific target. The attacker takes the time to research their intended targets and then write messages the target is likely to find personally relevant. The message will seem legitimate, which is why it can be difficult to spot a spear-phishing attack.

6. **Ransomware**. With Ransomware, the victim’s system is held hostage until they agree to pay a ransom to the attacker. After the payment has been sent, the attacker then provides instructions regarding how the target can regain control of their computer. The name "ransomware” is appropriate because the malware demands a ransom from the victim.

7. **Password attacks**. Passwords are the access verification tool of choice for most people, so figuring out a target’s password is an attractive proposition for a hacker. This can be done using a few different methods. Often, people keep copies of their passwords on pieces of paper or sticky notes around or on their desks. An attacker can either find the password themselves or pay someone on the inside to get it for them. An attacker may also try to intercept network transmissions to grab passwords not encrypted by the network. They can also use social engineering, which convinces the target to input their password to solve a seemingly “important” problem

8**. SQL injection attacks**. Structured Query Language (SQL) injection is a common method of taking advantage of websites that depend on databases to serve their users. Clients are computers that get information from servers, and an SQL attack uses an SQL query sent from the client to a database on the server. The command is inserted, or “injected”, into a data plane in place of something else that normally goes there, such as a password or login. The server that holds the database then runs the command and the system is penetrated.

9. **URL interpretation**. URL stands for Uniform Resource Locator(URL).With URL interpretation, attackers alter and fabricate certain URL addresses and use them to gain access to the target’s personal and professional data. This kind of attack is also referred to as URL poisoning. The name “URL interpretation” comes from the fact that the attacker knows the order in which a web-page’s URL information needs to be entered. The attacker then “interprets” this syntax, using it To execute a URL interpretation attack, a hacker may guess URLs they can use to gain administrator privileges to a site or to access the site’s back end to get into a user’s account..

10. **DNS spoofing**. The term DNS stands for Domain Name System(DNS).With DNS spoofing, a hacker alters DNS records to send traffic to a fake or “spoofed” website. Once on the fraudulent site, the victim may enter sensitive information that can be used or sold by the hacker. The hacker may also construct a poor-quality site with derogatory or inflammatory content to make a competitor company look bad.

11. **Session hijacking**. Session hijacking is one of multiple types of MITM attacks. The attacker takes over a session between a client and the server. The computer being used in the attack substitutes its Internet Protocol (IP) address for that of the client computer, and the server continues the session without suspecting it is communicating with the attacker instead of the client. This kind of attack is effective because the server uses the client's IP address to verify its identity

12. **Brute force attacks**. This type of attack gets its name from the “brutish” or simple methodology employed by the attack. The attacker simply tries to guess the login credentials of someone with access to the target system. Once they get it right, they are in.

13. **Web attacks**. This is the type of threats that target vulnerabilities in web-based applications. Every time you enter information into a web application, you are initiating a command that generates a response. For example,

if you are sending money to someone using an online banking application, the data you enter instructs the application to go into your account, take money out, and send it to someone else's account. Attackers work within the frameworks of these kinds of requests and use them to their advantage.

14. **Insider threats**. Sometimes, the most dangerous actors come from within an organization. People within a company's own doors pose a special danger because they typically have access to a variety of systems, and in some cases, admin privileges that enable them to make critical changes to the system or its security policies.

15. **Trojan horses**. This type of attack uses a malicious program that is hidden inside a seemingly legitimate one. When the user executes the presumably innocent program, the malware inside the Trojan can be used to open a backdoor into the system through which hackers can penetrate the computer or network. This threat gets its name from the story of the Greek soldiers who hid inside a horse to infiltrate the city of Troy and win the war.

16. **Drive-by attacks**. This sort of attack embeds malicious code into an insecure website. When a user visits the site, the script is automatically executed on their computer, infecting it. The designation "drive by" comes from the fact that the victim only has to "drive by" the site by visiting it to get infected. There is no need to click on anything on the site or enter any information.

17. **XSS attacks**. XSS also known as cross-site scripting. XSS attacks fall into one of three categories: reflected XSS, stored XSS, and Document Object Model (DOM) XSS. In this case, the attacker transmits malicious scripts using clickable content that gets sent to the target's browser. When the victim clicks on the content, the script is executed. Because the user has already logged into a web application's session, what they enter is seen as legitimate by the web application.

18**. Eavesdropping attacks**. This type of attack involves the bad actor intercepting traffic as it is sent through the network. In this way, an attacker can collect usernames, passwords, and other confidential information like credit cards. Eavesdropping can be active or passive. Both active and passive eavesdropping are types of MITM attacks

19. **Birthday attack**. The name "birthday attack" refers to the birthday paradox, which is based on the fact that in a room of 23 people, there is more than a 50% chance that two of them have the same birthday. In a birthday attack, an attacker abuses a security feature: hash algorithms, which are used to verify the authenticity of messages. The hash algorithm is a digital signature, and the receiver of the message checks it before accepting the message as authentic. If a hacker can create a hash that is identical to what the sender has appended to their message, the hacker can simply replace the sender's message with their own. The receiving device will accept it because it has the right hash.

20. **Malware attack**. Malware is a general term for malicious software, hence the "mal" at the start of the word. Malware infects a computer and changes how it functions, destroys data, or spies on the user or network traffic as it passes through. Malware can either spread from one device to another or remain in place, only impacting its host device.

2.6 Innovative Technologies use for Cybercrime

Innovative technologies like mobile phones that we have, the web can be surfed irrespective of location. Innovative technology is a new or improved product or process whose technological characteristics are significantly different from [35]. However, there are so many trending cyber issues today which include: 5G Network, Artificial Intelligence, Physical Biometrics,Hardware Authentication, Zero-Trust model, Cloud Computing, Block chain cyber security and Behavioral Analytics [43].These attack include: Malware, Denial-of-Service (DoS) Attacks, Phishing, Spoofing, Identity-Based Attacks, Code Injection Attacks, Supply Chain Attacks, Insider Threats, DNS Tunneling, IoT-Based Attacks [13]..

These Information Technology (IT) can be used to aid a number of activities including teaching and learning, combatting crime, games, tracking of cars, calls and individuals. These new technologies create opportunities for committing crimes [36], as the knowledge imported to learners during learning.[44] noted that what distinguishes cybercrime from traditional criminal activities, obviously is the use of the digital computers and other ICT tools to commit crime. And that technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not only need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity or violate someone's privacy, instead they need additional digital technological devices like mobile phones [45]. All those activities existed before the "cyber" prefix became inbiquitous. Cybercrime, especially involving the internet, represents an extension of existing criminal behavior alongside some novel illegal activities. Most cybercrimes are attacks on information about individuals, corporations or governments [46].

2.7 Attack Methods Cyber-criminals use for their Operation

Cybercriminals may target individuals, companies, and even governments with a motive of intentionally harming the reputation, causing physical, mental, or another type of harm, or using their equipment to form malicious networks (botnets). They may use social media, chat rooms, emails, forums, and text messaging to accomplish their tasks. [46] outline Top 10 Attack Methods Attackers Use for their criminal activities as follows:

1. Bait and Hook. This is one of the most widely used attack methods that phishers and social media scammers use. Attackers try to set up or create a situation where it seems natural, normal or helpful to provide requested information or to click the link that's displayed. Attackers carefully study and understand human psychology to craft phishing messages that are designed to get victims upset, curious, excited or anxious so that they fall for the bait and respond immediately.

2. Disguise and Conquer. Once the victim opens a phishing page, chances are it will be a very convincing imitation of the sender and its website. After all, anyone can grab the source code and graphics from a website to create a webpage that looks and feels like the original. There is a chance you will notice some formatting errors such as odd combinations of headers and footers or a font mismatch as the case may be. Google data saw a record-breaking 2 million phishing websites in 2020, a trend that accelerated following the beginning of the pandemic.

3. Hidden and Malicious Payloads. Even if victims don't provide the requested information on the phishing site, clicking the link can sometimes be good enough for cybercriminals to get a foot in the door. That's because malicious pages often try to automatically install malware (aka drive-by downloads) on unsecured and unpatched PCs. Drive-by downloads rely on "active content" to work on a web browser. Active content means there's code inside one or more objects on a webpage that gets triggered when a webpage is downloaded. Modern forms of active content are built into web browsers (such as HTML5 and JavaScript), while older forms of active content (such as Flash and ActiveX) require special browser add-ins although these are widely available for most browsers. When a browser downloads a webpage, it interprets hidden instructions inside active content, and this can provide unauthorized and unfettered access to bad actors.

4. Information Harvesting. Newer forms of cyberattacks harvest personally identifiable information (PII) prior to an actual attack. They use clever social engineering techniques to entice victims to provide information such as names, passwords, dates of birth and occupations. Gathering PII allows the attacker to take further action by, for example, disguising as a trusted source, compromising accounts or gaining full remote access to a computer.

5. Malvertising. Banner ads have come a long way since the days of brightly colored images. Today's ads are rich with Flash, JavaScript or other application code that provides a contextual experience to shoppers. Unfortunately, this has introduced an ability for attackers to inject malicious code into advertisements. Simply viewing a malware-laced ad can launch a drive-by attack as described earlier.

6. Webcam Hijacking. Once cybercriminals break into a machine, they have the option to take control over the computer's video camera to stealthily view and record anything that is going on or near the computer. Clever attackers can use this sensitive information to blackmail the victim or study the activities of whoever is in the room to chart a further course of attack.

7. Business Email Compromise. Business email compromise (BEC) is one of the most profitable forms of cybercrime. All the hacker does is break into a corporate email account of someone in a position of power like the CEO. The criminal then studies the habits and communication styles of the individual for weeks or months. The hacker will then masquerade as the individual — for example, sending out emails to instruct the CFO or payroll to execute a wire transfer or make payments to a third party. This technique is highly effective, as few people question the actions taken by a CEO. As such, almost half of cybercrime losses in 2019 were attributed to BEC scams.

8. Cryptocurrencies. The use of cryptocurrencies like Bitcoin is growing in popularity. As of March 2020, the value of all bitcoins in circulation was about $160 billion. Of course, attackers go where the money is, so they are known to target Bitcoin users and cyptocurrency exchanges. As the preferred mode of payment for all major ransomware attacks, cryptocurrency is virtually impossible to trace.

9. Bring Your Own Device. BYOD is the concept whereby employees use their own personal smartphones, tablets and laptops for their work instead of using company-provided equipment. This causes fresh concerns, as these devices are outside company control and its security perimeter. A user can easily plug their smartphone into their work computer and infect it with a virus or introduce malware or ransomware into the network. A STX Next survey (via Infosecurity Magazine) found that more than half of all global organizations do not carry a BYOD policy.

10. Internet of Things. With 5G on the horizon and smart devices going mainstream (light bulbs and sockets, speakers, home appliances, security cameras and home alarm systems, etc.), hackers are breaking into such devices and reprogramming them for nefarious purposes. Most IoT devices have weak security and authentication mechanisms, which attackers exploit to their advantage. According to Nokia (via Help Net Security), IoT devices now make up roughly 33% of all infected devices globally.

Cybersecurity is all about risk management, and the only way you can truly decrease your risk is by deconstructing the motives, means and methods that cybercriminals use. Once these attack vectors are understood well, you can begin building appropriate defenses.

2.8 Effect of Cybercrime on Business and Individuals

[47] has explained that Cybercrime can devastate businesses and individuals alike as shown below.

1. **Effects of cybercrime on businesses**. Businesses and organizations that fall victim to cybercrime may experience the following:(a)**Financial consequences:** Cybercrime can result in direct financial impacts for businesses, including theft of funds, ransom payments and costs associated with incident response. The financial repercussions are significant across businesses of all sizes.(b)**Operational disruption:** Downtime, data loss and potential halts in critical services can disrupt business operations. There are thousands of examples of businesses experiencing operational disruptions due to cyber incidents, impacting productivity and revenue streams.(c)**Data breaches and privacy concerns:** Data breaches compromise sensitive customer information, leading to privacy concerns and potential legal consequences for failing to protect valuable data.(d)**Reputation damage:** Businesses can suffer severe reputation damage due to cyber incidents, eroding trust among customers, partners and stakeholders. High-profile breaches often lead to long-term damage to a company's brand and credibility.(e)**Intellectual property theft**: Theft of intellectual property (IP) is a significant consequence, affecting a company's competitiveness and market position. Cybercriminals targeting proprietary information can compromise a business's innovative edge.(f)**Regulatory compliance issues:** Failing to protect customer data in accordance with regulations like GDPR can result in legal ramifications and financial penalties, further impacting a company's reputation and bottom line.(g)**Supply chain disruption:** An attack on one part of the supply chain can cause disruptions across multiple businesses, affecting the delivery of goods and services and creating a domino effect of financial and operational consequences.(h)**Increased cybersecurity costs:** Businesses often incur increased costs post-attack, investing in enhanced cybersecurity measures, employee training and incident response capabilities to mitigate future risks.
2. **Effects of cybercrime on individuals**. Cybercrime can also have a severe impact on individuals in the following ways:(a)**Financial losses:** Individuals can suffer direct financial losses due to cybercrime, including online fraud, identity theft and unauthorized access to financial accounts, impacting personal finances and credit.(b)**Identity theft:** Cybercriminals steal personal information for identity theft, leading to the opening of fraudulent accounts and various forms of financial fraud against individuals.(c)**Privacy breaches:** Cybercrime violates personal privacy, with leaked private information causing potential embarrassment, harassment or even extortion for affected individuals.(d)**Emotional distress:** People may experience anxiety, stress and feelings of vulnerability when personal information is exposed, impacting their mental well-being. Information in the hands of the wrong people can lead to bad outcomes like online abuse, blackmail, stalking or cyberbullying.(e)**Reputation damage:** False information online, doxxing incidents or compromising content shared without consent can damage an individual's reputation, affecting personal and professional life.(f)**Career and professional impact:** Compromised online profiles, leaked sensitive information or false accusations online can significantly impact an individual's career prospects and professional standing.

2.9 Methods of Combating Cybercrime Attacks

Experts in the field of cybercrime, cybersecurity and cyberattacks such as:[41], [42] [43] and [30] share similar ideas on methods of presenting/combating cybercrime, thus:

1. To prevent DoS and DDoS attacks, one should use a firewall that detects whether requests sent to your site are legitimate
2. To combat Man-in-the-middle (MITM) types of cyberattacks, computer users should use strong encryption on access points or to use a virtual private network (VPN
3. For phishing attack one should one should think carefully about the kinds of emails you open and the links you click on. One should pay close attention to email headers, and do not click on anything that looks suspicious. It is advised that one should check the parameters for "Reply-to" and "Return-path."
4. To prevent whale-phishing attack, take the same kinds of precautions to avoid phishing attacks, such as carefully examining emails and the attachments and links that come with them, keeping an eye out for suspicious destinations or parameters
5. In order to combat Spear phishing attack, users can carefully check the details in all fields of an email and making sure users do not click on any link whose destination cannot be verified as legitimate
6. Strategy to prevent Ransomware attack, use a next-generation firewall (NGFW) that can perform deep data packet inspections using artificial intelligence (AI) that looks for the characteristics of ransomware
7. In order to prevent Passwords attack, users should set up a lock-out policy. With a lock-out policy, the attacker only has a few tries before they get banned from access. This locks out access to devices, websites, or applications automatically after a certain number of failed attempts.
8. To solve the problem of Structured Query Language (SQL) injection, allow the CEO to be kept from accessing areas of the network even if they have the right to know what is inside. You can also apply a least-privileged policy that can prevent not just bad actors from accessing sensitive areas but also those who mean well but accidentally leave their login credentials vulnerable to attackers or leave their workstations running while away from their computers.

9. To prevent URL interpretation attacks from succeeding, computer users should use secure authentication methods for any sensitive areas of your site. This may necessitate multi-factor authentication (MFA) or secure passwords consisting of seemingly random characters

10. In order to prevent Domain Name System (DNS) spoofing, computer uses should make sure their DNS servers are kept up-to-date. Attackers aim to exploit vulnerabilities in DNS servers, and the most recent software versions often contain fixes that close known vulnerabilities

11. To prevent session hijacking, computer users can use a VPN to access business-critical servers. This way, all communication is encrypted, and an attacker cannot gain access to the secure tunnel created by the VPN.

12. In order to prevent brute-force attacks, have lock-out policies in place as part of your authorization security architecture. After a certain number of attempts, the user attempting to enter the credentials gets locked out. This typically involves “freezing” the account so even if someone else tries from a different device with a different IP address, they cannot bypass the lockout

13. In the case of Web attacks, computer users should inspect their web applications to check for and fix vulnerabilities. Another way to patch up vulnerabilities without impacting the performance of the web application is to use anti-CSRF tokens. Use a token to exchange between the user’s browser and the web application. Before a command is executed, the token’s validity is checked. So if it checks out, the command goes through, if not, it is blocked. You can equally use SameSite flags, which only allow requests from the same site to be processed, rendering any site built by the attacker powerless

14. One of the best ways to prevent insider threats in organizations is to limit employees' access to sensitive systems to only those who need them to perform their duties. For the select few who need access, computer users should use MFA, which will require them to use at least one a password they know in conjunction with a physical item they have to gain access to a sensitive system.

15. To prevent Trojan attacks, computer users are instructed not to download or install anything unless its source can be verified. Also, NGFWs can be used to examine data packets for potential threats of Trojans

16. To protect against drive-by attacks, computer users should make sure they run the most recent software on all their computers, including applications like Adobe Acrobat and Flash, which may be used while browsing the internet. It also important to use web-filtering software, which can detect if a site is unsafe before a user visits it

17. One of the most straightforward ways of preventing XSS attacks is to use a whitelist of allowable entities. This way, anything other than approved entries will not be accepted by the web application. You can also use a technique called sanitizing, which examines the data being entered, checking to see if it contains anything that can be harmful.

18. To prevent Eavesdropping attacks, computer users can encrypt their data, which prevents it from being used by a hacker, regardless of whether they use active or passive eavesdropping.

19. In a birthday attack, use longer hashes for verification. With each extra digit added to the hash, the odds of creating a matching one decrease significantly

20. To prevent malware attack, install software on the target device. In addition to using firewalls that can detect malware, users should be educated regarding which types of software to avoid, the kinds of links they should verify before clicking, and the emails and attachments they should not engage with

21. Generally, computer users should keep software up-to-date and by avoiding opening suspicious emails such as attachments or links that can infect your devices.

22. Computer users should use anti-virus and anti-malware installed on their computers that will significantly reduce their vulnerability because as long as users are connected to the web, it is impossible to have complete and total protection from malware.

23. Computer should use a VPN to privatize their connections that will encrypt their connection and protect their private information, even from their internet service provider.

24. Computer users should double check on a hyperlinks before they click. On most browsers, users can see the target Uniform Resource Locator (URL) by hovering over the link.

25. Computer users should regularly update their passwords and using passwords like howsecureismypassword.net to find out how secure their passwords are that combine special characters, upper and lowercase letters, and numbers can help protect their accounts. Do not be lazy with your passwords. Put more effort into creating your passwords by using a tool.

26. Computer users should disable their Bluetooth when they do not need it. Devices can be hacked via Bluetooth and subsequently their private information can be stolen. If there is no reason to have their Bluetooth on kindly turn it off.

27. Computer users should use Enable 2-Factor Authentication to keep their accounts more secure.

28. Computer users should remove adware from their machines by using AdwCleaner to clean adware and unwanted programs from their computer to maintain their privacy. This is because Adware collects information about you to serve you more targeted ads.

29. Computer users should Double-check for Hypertext transfer protocol secure (HTTPS) on websites before they give away personal or private information. HTTPS is the primary protocol used to send data between a web browser and a website
30. Computer users should not store important information in non-secure places that cannot be accessed by unauthorized users.
31. Computer users should scan their external storage devices for viruses before accessing them as external storage devices are just as prone to malware as internal storage devices. If users connect an infected external device to your computer, the malware can spread.
32. Computer users should avoid using public networks. When you connect to a public network, you are sharing the network with everyone who is also connected. Any information you send or retrieve on the network is vulnerable. Stay away from public networks or use a VPN when you are connected to one.
33. Computer users should avoid the "secure enough" mentality. Big companies like Facebook invest a fortune into security every year but are still affected by cyberattacks. Unless you're completely isolated from the rest of the world, otherwise being "secure enough."
34. Computer users should invest in security upgrades when they are available. This is because it is better to eat the costs of security than pay for the consequences of a security breach!
35. Users should back up their important data. To make sure they are prepared to restore data once it is lost, they should ensure their important information is backed up frequently on the cloud or a local storage device.
36. Organisations and institutions of learning should train their employees. The key to making cybersecurity work is to make sure their employees are well trained, in sync, and consistently exercising security practices. This is because an improperly trained employee can cause an entire security system to crumble.
37. Computer users should use HTTPS on their website. Having an SSL certificate installed and HTTPS enabled on their website will help encrypt all information that travels between a visitor's browser and your web server.
38. Institutions of learning and organization should employ a "White Hat" hacker. These are hackers who expose security risks for the sake of helping others improve their cybersecurity by keeping them aware of security flaws and patching them. Not all hackers are bad. It might benefit you to hire one to help you find risks you never knew you had.

STATEMENT OF THE PROBLEM

The innovation of technology has over the time gone through several advancements and made daily works easy to carry out. In the ever-evolving landscape of digital innovation, the surge of emerging technologies brings both unprecedented opportunities and formidable challenges, particularly in the realm of cyber security. While cyberattacks themselves are becoming more sophisticated, the rapid growth of emerging technologies such as 5G, robotic process automation and, of course, generative AI, means there are even more opportunities for cyberattacks and data breaches to occur [47]. Academic, legal and practitioner responses to cyber threats have been predominantly reactive, punitive, and deterrence-based, with limited attention given to the motives underlying computer criminals' behaviors. Cybercriminals use a variety of techniques to gain unauthorised access to sensitive information using different types of computer virus (malware) such as Trojans, spyware, phishing, adware, botnets structured language query (SQL) injection, denial-of-service attack, man-in-the-middle attack and ransomware attacks [48], [14].The consequences of these attacks can be devastating, including loss of data, financial damage, reputational harm, erode customer trust and loyalty, leading to a decline in customer base and revenue which give rooms for legally, businesses might also be sued over the data breach. The increased costs for borrowing and greater difficulty in raising more capital, destruction of a major radios, telephone and Internet switching centre might result into cut off from the rest of the world [48], [49].

It has been noticed that the more the innovative technology, the more cybercrimes committed and the more cybersecurity strategies needed to combat it. Uncountable, cybercrimes committed in the country especially in North-central Nigeria and the FCT are all affected. This is as a result of high knowledge in innovative technologies acquired by individuals who are criminals. Studies have shown that, there is no specific strategies to combat the menace that has gone ubiquitous.

[50] stated that by the end of the coming year (2025), the cost of cyberattacks on the global economy is predicted to top $10.5 trillion. The author observed that this staggering amount reflects the growing need for cyber security to be treated as a strategic priority on an individual, organizational and governmental level. He pointed out that as in every other field of business and technological endeavor, artificial intelligence (AI) will have a transformative impact on both attack and defense. Its impact will be felt across every one of the trends [50]. [50] explain that a shortage of professionals with the skills needed to protect organizations from cyberattacks continues to be a running theme throughout 2024. [50] emphasize that the situation appears to be getting worse, research indicates that a majority (54 percent) of cyber security professionals believe that the impact of the skills shortage on their organization has worsened over the past two years. He contended that organization or individual can expect efforts to rectify this situation to include a continued increase in salaries

paid to those with the necessary skills, as well as greater investment in training, development and upskilling programs.

Therefore, this study seeks to find out the innovative technologies that aid cybercrimes, cybersecurity threats, causes of cybercrime, consequent of cybersecurity and strategies to be adopted to reduce cybercrimes.

III METHOD AND PROCEDURE

The study adopted a descriptive survey design. The area of the study was the North-central (Middle Belt) of Nigeria and the FCT Abuja (Niger, Nasarawa, Kwara, Kogi, Benue, Plateau and FCT) and was carried out in Nigerian Public Universities within the zone. The population for the study was 210 ICT users made up of 110 Computer Science and Computer Robotics Education Students, 80 ICT cyber instructors, technologists and lecturers in Universities and Technical Colleges and 20 Officers of Security agencies like ICPC and EFCC. The entire population was used. Closed ended structured questionnaire were developed by the researchers and used for data collection. The questionnaire was divided into two sections, A and B. Section A contains items that sought the demographic information from the teachers and lecturers while section B consists of a total of 30 items. 10 sought for innovative technologies that aid in cybersecurity threats in North central and the FCT Abuja, 10 sought for cybercrimes committed using innovative technologies and 10 sought for the consequent cybersecurity strategies to be adopted to combat cybercrimes in the North-central Nigeria and the FCT Abuja. Five (5) point Likert rating scale was used such as Strongly Agree (SA), Agree (A), Undecided (UD), Disagree (D), Strongly Disagree (SD) with corresponding value of 5,4,3,2 and 1 respectively. The instruments were faced validated by two (2) experts. One from the Computer Science Education, Department of Science and Technology Education, Faculty of Education, University of Jos while the other one is from the Economic and Financial Crime Commission (EFCC office).

The expert's observations and suggestions were considered and effected to make the work better. The data was collected by administrating the questionnaire directly on the respondents by the researchers with some research assistants. Data collected was analyzed using Statistical Product and Service Solutions (SPSS) version 27.0. The statistical tools employed were mean and t-Test. Mean was used to answer the research questions while t-Test was used to test the three hypothesis at 0.05 level of significance. Any item with mean value of 3.50 and above was considered agreed upon while any item with a mean below 3.50 as disagreed.

PURPOSE OF THE STUDY

The purpose of the study is to determine innovative technologies that support cybercrimes and can generate cybersecurity threats in Nigeria.

The study specially aims to

1. Identify innovative technologies that can aid cybersecurity threats in the North-central Nigeria and the FCT Abuja.
2. Identify the cybercrimes committed using innovative technologies in North-central Nigeria and the FCT Abuja.
3. Identify the cybersecurity strategies adopted towards reducing cybercrimes in North-central Nigeria and the FCT Abuja.

RESEARCH QUESTIONS

The following research questions were answered by the study:

1. What innovative technologies can aid cybersecurity threats in the North-central Nigeria and the FCT Abuja?
2. What type of cybercrimes are committed using innovative technologies in North-central Nigeria and the FCT Abuja?
3. What type of cybersecurity strategies could be adopted toward reducing cybercrimes in North-central Nigeria and the FCT Abuja?

RESEARCH HYPOTHESES

The following null hypotheses were developed to guide the study and were tested at 0.05 level of significance.

Ho1. There is no significant difference in the mean responses of the University lecturers and officers of crime agencies in North-central Nigeria on the innovative technologies that can aid and constitute cyber security in North-central Nigeria and the F.C.T. Abuja.

Ho2. There is no significant difference between the mean responses of the students and the officers of crime agencies on the cybercrimes that are committed using innovative technologies in North-central Nigeria and the F.C.T. Abuja.

Ho3. There is no significant difference between the mean responses of students and the officers of crime agencies on the consequent of cybersecurity strategies to be adopted to reduce cybercrimes in North-central Nigeria and the FCT Abuja.

PRESENTATION OF RESULTS

Table 1. Mean and t-Test analysis of the innovative technologies that can aid and constitute to cybersecurity threats in Middle Belt Nigeria and the FCT Abuja.

S/N	Items statements	X	SD	Decision	Sig	Ho
1	5G Network	2.66	0.87	D	0.69	NS
2	Artificial Intelligence	3.63	0.75	A	0.10	NS
3	Physical Biometrics	2.67	0.87	D	0.99	S
4	Embedded Hardware Authentication	2.21	0.81	D	0.56	NS
5	Hardware Authentication	3.84	0.86	A	0.06	NS
6	Zero-Trust model	4.53	0.71	SA	0.32	NS
7	Cloud computing	3.82	0.81	A	0.08	NS
8	Block chain cybersecurity	4.56	1.07	SA	0.08	NS
9	Anti-spyware	3.63	0.75	A	0.11	NS

Note: X = Grand mean, SD = Standard Deviation, HO = Null Hypothesis, NS = Not Significant, SA = Strongly Agreed, A = Agree, U = Undecided, D = Disagree and SD = Strongly Disagree.

Data presented in the Table 1 shows that seven items had their mean values ranging from 3.63 – 4.53 which is above the cut-off point of 3.50. This means that the university lecturers and officer of the crime agency in Nigeria that the items 2,5,6,7,8, and 9 are innovative technologies that aid in cybersecurity threats. Also three items in serial Nos 1,.3, and 4 have their mean value ranging from 2.07 – 2.66 which is below the cut-off point of 3.50. This implies that the university lecturers and the officer of the crime agency in Nigeria did not agree that the items are innovative technologies that aid in cybersecurity threats. Therefore, the null hypothesis which stated that there is no significant difference in the mean responses of the university lecturers and officers of the crime agency in Nigeria is accepted.

Table 2: Mean and t-test analysis of the cybercrimes that are committed using innovative technologies in North-central Nigeria.

S/N	Items Statements	X	SD	Decision	Sig	Ho
1	Hacking	3.78	0.59	A	0.55	S
2	Charity funds fraud	4.28	0,81	SA	0.30	S
3	Bank Verification Number (BVN) Scams	3.72	0.60	A	0.31	S
4	Data Airtime (DAT) Theft from service providers	3.52	0.62	A	0.47	S
5	Cyber-plagiarism	3.57	0.88	A	0.86	S
6	Social hijacking	2.19	0.76	D	0.08	NS
7	Cyber pornography	2.26	0.76	D	0.32	NS
8	Cyber-stalking harassment and Blackmailing scam	3.92	0.82	A	0.46	S
9	Intellectual Property Theft	3.86	0.75	A	0.31	S
10	Cyber-Theft/ Banking Fraud	3.60	0.69	A	0.10	S

Source: Researchers' Field Work, 2024

Note: X = Grand mean, SD = Standard Deviation, HO = Null Hypothesis, NS = Not Significant, SA = Strongly Agree, A = Agree, U = Undecided, D = Disagree, SD = Strongly Disagree.

Data presented in Table 2 shows that enlightens had their values ranging from 3.52 – 4.28 which is above the cut-off point of 3.50. This implies that the students and the officers of crime agency agreed that the items in serial Nos 1,2,3,4,5,8,9.10 are crime committed using innovative technologies in North-central Nigeria. Also, two items in serial Nos 6 and 7 had their mean values ranging from 2.19 – 2.26 which are below the cut-off point of 3.50. This implies that the students and the officers of crime agency response did not agree that there are crimes committed using innovative technologies in North-central Nigeria.

Table 2 also shows that all the 10 items had their significant value to be greater than 0.05 (p>0.05). This indicated that there was no significant difference between the mean responses of students and the officers of crime agency on crimes committed using innovative technologies in North-central Nigeria. This means that the hypothesis which stated there is no significant difference in the mean response of male and female students on the crimes committed using innovative technologies in North-central Nigeria.

Table 3: Mean and t-test analysis of the consequent cybersecurity strategies to be adopted to reduce cybercrimes in North-central Nigeria.

S/N	Items Statement	X	SD	Decision	Sig	Ho
1	Raising awareness	3.70	0.59	A	0.55	S
2	Use strong password	4.29	0.82	SA	0.31	S
3	Working with invested partner	3.19	0.77	D	0.09	S
4	Strategic assessments of cyber threats and vulnerabilities	3.53	0.63	A	0.48	S
5	Crises and incident response planning and exercising	3.57	0.89	A	0.86	S
6	Network segmentation	3.73	0.60	A	0.31	S
7	Cyber-theft/Banking fraud	2.27	0.76	D	0.32	NS
8	Keep up to date on major security breaches	3.91	0.83	A	0.46	S
9	Training and education security personnel	3.86	0.76	A	0.32	S
10	Implementing a response plan	3.61	0.70	A	0.11	S

Source: Researchers' Field Work, 2024

Note: X = Mean, SD = Standard Deviation, HO = Null Hypothesis, NS = Not Significant, SA = Strongly Agreed, A = Agreed, U = Undecided, D = Disagree, SD = Strongly Disagree. Data presented in Table 3 indicates that eight items in serial Nos 1,2,4,5,6,8,9 and 10 had their mean values ranging from 3.53 to 4.29 which is above the cut-off point of 3.50. This implies that the students and the officers of crime agency agreed that the items are the consequent of cybersecurity strategies to be adopted to reduce cybercrimes in North-Central Nigeria. Also, one items in serial Nos. 3, 7 had their mean values ranging from 3.19 to 2.27 which is below the cut-off point of 3.50. This implies that the students and the officers of crime agency did not agree that the items are the consequent of cybersecurity strategies to be adopted to reduce cybercrimes in North-Central Nigeria. Table 3 shows that all the items their significant values to be greater than 0.05 (p>0.05). This shows that, there was no significant difference between the mean responses of the students and the officers of crime agency on the consequent cybersecurity strategies to be adopted to reduce cybercrimes in North-Central Nigeria. Therefore, the null hypothesis which stated that there are no significant differences in the mean response of the students and the officers of crime agency on the consequent of cybersecurity strategies to be adopted to reduce cybercrimes in North-Central Nigeria was accepted.

IV. DISCUSSION OF FINDINGS:

The data from Table 1 indicates that innovative technologies that aids cybersecurity in North-central Nigeria includes: hardware authentication, zero-trust model and cloud computing. This is in line with [44] who stated that many terrorists around the world had resorted to the use of some innovative technologies like artificial intelligence and anti-spyware to commit their heinous crimes. This finding also support [46] who stated that many hackers now adopted new methods of accessing and stealing people's sensitive and personal data online for obnoxious reasons.

Table 2 revealed that 8 items listed are the cybercrimes committed using innovative technologies in North-Central Nigeria. Some of these crimes include: hacking, charity funds fraud and Bank Verification Number (BVN) scams. This finding is in line with [40] who pointed out that most youths in Nigeria have resorted to the use of ICT tools in committing crimes such as cyber-theft/Bank fraud and intellectual property theft. [46] supported this assertion when he stated that cyber-attackers use the following methods of attacks: Bait and Hook, Disguise and Conquer, Hidden and Malicious Payloads, Information Harvesting, Malvertising, Webcam Hijacking, Business Email Compromise, Cryptocurrencies, Bring Your Own Device and Internet of Things which has increasethe rate of cyber-plagiarism and cyber-pornography since the inception of innovation technological development in the 21st century. However, the findings in Table 3 indicates that strategic network segmentation, assessments of cyber threats and vulnerabilities, and crisis/incident response planning and exercising are some of the consequent cybersecurity strategies adopted to reduce cybercrimes in North-central Nigeria. This is in line with [46] who posited that cybercrimes can be reduced by implementing a response plan and training/education of security personnel on the best way to handle situations of cybercrimes. This finding is also in line with [30] who pointed out that organizations and individuals should use the following tools (a) Wireshark, (b) Nagios (c)Nessus Professional(d) Acunetix (e)Snort to detect, mitigate cyber threats, terrorism and to prevent, cybercrime. This finding also support what [41] posited as Cybersecurity Tips and Best Practices for Your Business such as Keep software up-to-date**,** Avoid opening suspicious emails, Keep hardware up-to-date, Use a secure file-sharing solution like TitanFile, Use anti-virus and anti-malware installed on your computers, Use a virtual private network (VPN) to privatize your connections, Double check on a hyperlinks before you click, Regularly updating your passwords, Disable Bluetooth, Enable 2-Factor Authentication to keep your accounts more secure, Remove adware from your machines by using AdwCleaner, Double-check for Hypertext transfer protocol secure (HTTPS) on websites, Do not store important information in non-secure places, Scan external storage devices for viruses, avoid using public networks, Avoid the “secure enough” mentality, Invest in security upgrades when they are available, Back up important data,Train employees, Use HTTPS on your website, and employ a “White Hat” hacker to combat cybercrimes.

V. CONCLUSION

This study comes to conclusion that cybercrime has extraordinary implications for individuals, organizations, societies, and governments. By exercising common sense and following security best practices, users can protect themselves against phishing attacks, ransomware, malware, identity theft, scams, and some of the other most common types of cybercrime. There are several innovative technologies that can constitute cybersecurity threats. As such, the responsibility for cybersecurity does not just fall on companies and national leaders; it also rests on individuals and societies. All hands must be on deck in preventing cyberattacks, requiring a comprehensive approach that includes technical measures, awareness, and adherence to robust security policies. As individuals, we have the power to significantly bolster our own cyber defenses through a few key actions with the appropriate strategies and innovative technologies, cybercrimes can be checked and a strong cybersecurity system can be built as there are some innovative technologies that can be introduced to check youth’s involvement in committing cybercrimes. Therefore, combating cybercrime requires a comprehensive approach, including the use of threat intelligence solutions, antivirus software, VPNs, and security awareness training, backed by a robust legal framework and professional cybersecurity expertise. It is therefore paramount that we approach cybersecurity with utmost seriousness, adopting a proactive stance to shield our online presence. This proactive approach encompasses implementing robust password practices, routinely updating our software and systems, educating ourselves and our teams about prevalent cyber threats, and investing in cutting-edge security technologies.

VI. RECOMMENDATIONS

From the literature, the results of the study, discussion of findings, and conclusion made, irrespective of how much we prepare to protect sensitive data, it is not possible to completely eradicate cybercrime and ensure complete internet security. Cyber criminals always find ways to navigate security and hack our systems. However, this does not mean we cannot protect our systems from the impact of cybercrime. Therefore the following are a few cybercrime precautions, suggestions and recommendations that, if put in place, organizations, institutions of learning and individuals can effectively reduce cybercrime risks or even stop cyber criminals from targeting their systems by adopting the following strategies: .

1. Adopt strong authentication protocols by using a strong password with combine special characters, upper and lowercase letters, and numbers to securely generate and store complex, long passwords whether on work or personal accounts
2. Consider using a Virtual Private Networks (VPN) to provide encryption and secure connections, particularly on networks where trust is questionable, such as public Wi-Fi in cafes, hotels, or airports. Include VPN that often includes tools like password managers, assisting in meeting robust authentication standards and managing your passwords more securely.
3. Update all your software regularly. Software updates and patches are designed to address known vulnerabilities in operating systems, applications, and other software components. Cybercriminals often exploit vulnerabilities in outdated software to gain unauthorized access or deploy malicious code. Organizations can significantly reduce the risk of such exploits by staying current with software updates.
4. Being vigilant could protect you and inform yourself about the latest scam tactics to avoid becoming a victim
5. Report any suspicious online activities to appropriate authorities so as to detect and respond to breaches more quickly According to IBM’s report, it takes organizations an average of 204 days to identify a data breach, followed by an additional 73 days to contain it.

6. Produce a good cybersecurity policy that will contain:(a)methods to harden the system(b) social media usage guidelines(c)firewall rules(d) use of antivirus(e)handling of restricted and classified information(g)handling of a cyber security breach
7. Develop **a s**trong Password policy to ensure that you maintain multiple strong passwords for different accounts to avoid becoming an easy target. Also, ensure you do not write them down anywhere, as this makes it all the more easier for cybercriminals to get their hands on and exploit the same. Equally, ensure you keep changing the passwords frequently to avoid becoming an easy target.
8. **Protect Your Storage Data:** It is important that you encrypt all your data to prevent any and every kind of attack on your system or database, as this could prove fatal to your privacy.
9. **Secure your phone/ system:** Make sure your operating systems are always up to date to enable you download your software and tools from trusted and reliable sources as phones and computers are prone to malicious viruses and malware attacks.
10. **Use security software:** Make sure you have the right security software protection of phones and computers in place to avoid any and every security-related complication to prevent and protect resources from any kind of invasion.
11. Create cybersecurity incident response plans to support these policies and procedures.
12. Use multifactor authentication (MFA) apps or physical security keys.
13. Activate MFA on every online account when possible.
14. Verbally verify the authenticity of requests to send money by talking to a financial manager.
15. Scrutinize all email requests for transfer of funds to determine if the requests are out of the ordinary.
16. Train employees on cybersecurity policies and procedures and what to do in the event of a security breach as key part of defense.
17. Keep websites, endpoint devices and systems current with all software release updates or patches.
18. Back up data and information regularly to reduce the damage in case of a ransomware attack or data breach.
19. There should be strategic assessments of cyber threats and vulnerabilities to be conducting regularly
20. Use Antivirus software to serve as a key defense against cybercrime. It scans programs and files for any threats, compares them to a database of known malware, and neutralizes potential threats. While no antivirus solution is entirely effective against all threats, regularly updated antivirus software can provide essential protection. However, users should also be aware of potential downsides, such as system slowdowns, false positives, and frequent advertisements or upselling

REFERECES

[1] Kelley, K.(2023).What is Cybersecurity & Importance of Cyber Security**.** Retrieved from:https://www.simplilearn.com › *tutorials › what-is-cyber-s...*

[2] Brush, K., & Cobb, M. (2021).What is cybercrime? Definition from SearchSecurity. Retrieved from: *https://www.techtarget.com › searchsecurity › cybercrime*

[3] Bay Atlantic University - Washington, D.C.(2023). 6 Compelling Reasons Why You Should Study Cyber ...Retrieved from: https://bau.edu › blog › why-study-cyber-security

[4] The University of Tulsa(2023). 8 Reasons Demand for Cybersecurity Professionals Will keep raising. Retrieved from: https://online.utulsa.edu › blog › reasons-demand-for-cy...

[5] UNext Learning(2022).Major Causes of Cyber Crimes You Must Be Aware Of. Retrieved from: https://u-next.com › blogs › cyber-security › major-caus...

[6] Security Intelligence (2023). 7 Reasons Global Attacks Will Rise Significantly in 2023. Retrieved from: https://securityintelligence.com › articles › 7-reasons-glo

[7] Mathews, I.(2023). Cyber Crime Definition, Types & Statistics – Lesson. Retrieved from: https://study.com › academy › lesson › what-is-cyber-cr..

[8] Databasix(2023). 20 Frightening Cyber Security Facts & Stats. Retrieved from: https://www.dbxuk.com › statistics › cyber-security

[9] Alechenu,J. (2023).Cybercrime: Senate decries $500m annual loss, threats to digital ...Retrieved from: https://www.vanguardngr.com › 2023/11 › cybercrime-s.

[10] BusinessDay (2023). Nigeria recorded a 174% increase in cybercrimes in six months. Retrieved from: https://businessday.ng › news › article › nigeria-recorde...

[11] Deborati, & Jaishankar (2017). Computer experience, school support and computer anxieties; Educational psychology, 17(3), 267-284.

[12] Gusen, J.N. (2019). SWOT Analysis of ICT Across the Curriculum. Jos. Byang Printing Press

[13] Baker, K.(2023).10 Most Common Types of Cyber Attacks Today - CrowdStrike. Retrieved from: https://www.crowdstrike.com › cybersecurity-101 › most

[14] Asadu, C. (2021).Nigeria ranked 16th in FBI global cybercrime victims report. Retrieved from: https://www.thecable.ng › nigeria-ranked-16th-in-fbi-glo...

[15] Oloruntade, G.(2023).Nigeria is witnessing a disturbing surge in data breaches. Retrieved from: https://techcabal.com › 2023/05/23 › nigeria-is-witnessi...

[16] Odeniyi, S. (2023).FG decries rising cybercrimes, EFCC secures 1084 ...Retrieved from: https://punchng.com › fg-decries-rising-cybercrimes-efcc...

[17] Kass D.H.(2023).Cybercrime Top 10 Rankings: China is No. 1 While U.S. Records Highest Rate of Security Breaches..Retrieved from: *https://www.msspalert.com › news › cybercrime-top-10-r...*

[18] Lemos R.(2024).Nigeria, Romania Ranked Among Top Cybercrime Havens. Retrieved from**:** https://www.darkreading.com › cybersecurity-analytics

[19] Punjwani,M.and Campbell,S.(2024).Cybersecurity Statistics in 2024. Retrieved from: https://www.usatoday.com › blueprint › business › vpn

[20] IBM Security - Cost of a Data Breach Report 2023. InPunjwani,M. and Campbell,S. (2024). Cybersecurity Statistics in 2024. Retrieved from: https://www.usatoday.com › blueprint › business › vpn

[21] Norton's Cyber Safety(2023), Insights Report, 77% of Americans have taken steps to protect their personal data online. In Punjwani,M. and Campbell,S. (2024). Cybersecurity Statistics in 2024. Retrieved from: https://www.usatoday.com › blueprint › business › vpn

[22] Shred-it UK Stericycle solution(2015).10 Reasons Why Cyber Threats Are on the Increase. Retrieved from: https://www.shredit.co.uk › breaches-damage-control › 1..

[23] Lukic, D.(2022).Cyber Criminals and Motivation for Cyber Crime. Retrieved from: https://www.idstrong.com › SENTINEL › Security Tips

[24] Robb,B (2016),6 motivations of cybercriminals | PPT. Retrieved from: *https://www.slideshare.net* › **Technology**

[25] Tanny,J. (2018).Cyber Criminals: Who They Are and Why They Do It. Retrieved from: https://www.vircom.com › blog › cybercriminals-who-th...

[26] StudeerSnel, B.V (2024). Theoretical Framework Cybercrime Cyber crime ...Retrieved from: https://www.studocu.com › university-of-calicut› theor.

[27] Tulane University School Of Professional Advancement(2024). Four Reasons the Cybersecurity Field Is Rapidly Growing Retrieved from: https://sopa.tulane.edu › blog › four-reasons-cybersecurit.

[28] HackerNet (2022).Best of 2022: 8 Motives of CyberCrime – Hackers World. Retrieved from: https://securityboulevard.com › 2022/12 › 8-motives-of.

[29] CoreTech Staff(2022).6 Motivations of Cyber Criminals. Retrieved from: https://www.coretech.us › blog › 6-motivations-of-cyber...

[30] Borges E.(2024).Guide to Cybercrime Types: Prevention & Impact. Retrieved from: https://www.recordedfuture.com › cyber-threats › types.

[31] Barthel Legal (2024).Cybercrime | Definition, Statistics, & Examples. Retrieved from: https://www.britannica.com › topic › cybercrime

[32] Cassetto, O. (2023).Cybersecurity Threats: Everything you Need to Know. Retrieved from:info@exabeam.com.

[33] Kings, N.(2023). 10 Different Types of Cybercrime in 2023 (Best Explained). Retrieved from: tps://www.nwkings.com › Blog

[34] Banerjee, S. B., Gulas, C. S., & Lyer, E. S. (2015). Shades of green: A multidimensional analysis of environmental advertising. *Journal of Advertising*, 24, 21-31.

[35] Bradley, G. & Rusell, G. (2018), Computer technology application and vocational education. A review of literature and research. *European Journal of Social Sciences*, 14(4), 645-651.

[36] Can, G., & Cagiltay, K. (2016). Turkish prospective teacher's perceptions regarding the use of computer games with educational features. *Educational Technology and Society, vol. 9,* no. 1, pp 308-21

[37] Chawki, M. (2015). A critical look at the regulation of cybercrime. ICFAIJ. Cyber law, 3:1-55.

[38] Adler, J. (2015), Environmentalism at crossroads. Washington, DC: Capital Research Center.

[39] Tade, O., and Aliyu, I. (2017). Social organization of internet fraud among University undergraduates in Nigeria. *International Journal of Cyber Criminology, 5(2),* 860-875

[40] Asokhia, M., (2019). Enhancing national development and growth through combating cybercrime internet fraud. A comparative approach. *Journal of Social Sciences* 23(5), 13-19

[41] Titanfile.com (2024). 21 Cybersecurity Tips and Best Practices for Your Business. Retrieved from: https://www.titanfile.com › blog › cyber-security-tips-bes...

[42] Fortinet Staff(2024).Top 20 Most Common Types Of Cyber Attacks. Retrieved from: *https://www.fortinet.com › resources › cyberglossary*

[43] Coursera (2024). 10 Common Types of Cyberattacks and How to Prevent Them. Retrieved from: https://www.coursera.org › ... › Networks and Security

[44] Park, J., Cho, Y., & Martinez, D. (2016). ABIM and AWB Integrated Mobile Robot Navigation System for indoor Position Tracking Applications. *Journals of Constructional Engineering Project Management. 6*, 30-39.

[45] Karoaglan, B., & Kisla, T. (2019). A study on Science Teachers attitudes towards information's and communication technologies in education. *The Turkish online Journal of Educational Technology – TOJET, 8(2)*, 20-32.

[46] Forbes Technology Council (2021).Deconstructing Cybercrime: Top 10 Attack Methods Use...Retrieved from: https://www.forbes.com › Innovation.

[47] ID Agent (2024). What is Cybercrime? Types, Effects, Protection Tips. Retrieved from: https://www.idagent.com › Blog

[48] ODoherty, C. (2024).Emerging Technologies and their Impact on Cyber Security. Retrieved from: https://www.metacompliance.com › blog › emerging-tec

[49] Lusher, C. (2023).The current state of cybercrime; the role of AI in cybersecurity. Retrieved from: https://www.continent8.com › the-current-state-of-cyberc...

[50] Sterling, B.(2024).Cybercrime | Definition, Statistics, & Examples. Retrieved from: https://www.britannica.com › topic › cybercrime.

[51] Marr, B. (2024).The 10 Biggest Cyber Security Trends In 2024 Everyone must be ready for Now..*https://www.forbes.com › Innovation › Enterprise Tech*