RESEARCH ARTICLE

DOI: 10.34256/ajir2114

ASIAN JOURNAL OF INTERDISCIPLINARY RESEARCH

Cybersecurity: A Key Challenge to the Information Age in Sierra Leone

Ibrahim Abdulai Sawaneh [a,b,*], **Fatmata Kanko Kamara** [a,c], **Albert Kamara** [a,d]

[a] School of Technology, University of Management and Technology, Freetown, Sierra Leone.
[b] Ernest Bai Koroma University of Science and Technology, Makeni, Sierra Leone
[c] Sierra Leone Peacekeeping and Law Enforcement Academy, Sierra Leone.
[d] School of Postgraduate Studies, Cyprus International University, North Cyprus.
*Corresponding author Email: ibrahim.sawaneh@unimtech.edu.sl
DOI: https://doi.org/10.34256/ajir2114

Received: 20-12-2020
Revised: 07-02-2021
Accepted: 07-02-2021
Published: 10-02-2021

Abstract: Humans' growing desire to continuously interact with each other through the internet has both negative and positive consequences, especially if users tend to use it maliciously. The advent of social networking sites has broken the traditional barriers to communication. It is a cost-effective way of communicating using text-messages, video-messages, and voice-notes as it happens from a source (sender) to the audience (receivers). Anyone can participate if they have a mobile phone with internet facilities, and now, everyone is an online journalist and a reporter. Unfortunately, although social media platforms have numerous merits, these platforms still face critical challenges, especially in controlling and policing content post by users. The revolution in information technology and social networking platforms have provided a NEW NORMAL for online fraudsters and criminals. Fake news, hate speech, and political propaganda/rhetoric has created a confusing world, especially during the Covid-19 pandemic situation. Therefore, our paper presented some of the challenges and solutions to cybercrime.

Keywords: Cybersecurity, Information Age, Cybercrime, Fake News.

1. Introduction

Cybersecurity relates to several issues such as cybercrimes, countermeasures, cyber education, etc., to protect confidentiality, integrity, and availability of digital and information technologies against attacks and threats (Goodman and Herbert, 2007; O'Brien, & Marakas, 2011). Information refers to data processed to produce meaning to the person who receives it or the computer processing it (Dinesh Thakur, 2020). Confidentiality prevents unauthorized access to view, share and use information (Julian Jang-Jaccard and Surya Nepal, 2014). Information integrity is the act of avoiding data manipulation/deletion with malicious intent (Julian Jang-Jaccard and Surya Nepal, 2014). Availability assures that information is readily available when needed and those who need them. The growing appetite of the present generation's dependence on the internet and its related technologies has raised considerable concern on cybersecurity issues (e.g., cyber-attacks) due to the limited security features offered by these devices and websites (Zhao *et al*,, 2010), which cyber criminals might easily hack. Cyber-attacks are easily committed compared to physical attacks, as they are cheaper, convenient, and less risky (Julian Jang-Jaccard and Surya Nepal, 2014). Cybercrimes operate in boundaryless cyberspace, and their identities are hard to detect because of the anonymous nature of the internet. Cybercrimes such as cyber-attacks and security breaches on the internet are the order of the day (Arora, Nandkumar, & Telang, 2006; Hans de Bruijn,

Marijn Janssen, 2017). A breach in any cybersecurity leads to some form of financial and non-financial losses to the victim organization and its clients; thus, the purpose of cybersecurity is to protect against these breaches (Hussain Bhat and Alam Khan, 2015).

According to the Cybercrime Magazine Report, cybercrime is a great challenge human had faced and has an enormous impact on the global community (Steven Morgan, 2020). The Cybersecurity Ventures (2016) predicted that cybercrime would cost USD 6 trillion annually in 2021 compared to USD 3 trillion in 2015 (Steven Morgan, 2020). These cybercrimes may include damage done data, email and internet fraud, identity fraud, theft and sale of corporate data, identity theft, ransomware attacks, crypto-jacking (where hackers mine cryptocurrency using resources they do not own), financial fraud, cyber espionage, and cyber extortion (demanding money to prevent a threatened attack) (Kaspersky, 2020), and a host of others. The Cybercrime Magazine report also indicates that 3.5 million unfilled cybersecurity jobs in 2021 compared to the previous one million jobs in 2014. Statistical data (Oleg Kupreev *et al.,* 2020) for 2018/2019 further indicate that cyber-attack increased exponentially (Steven Morgan, 2020). The coronavirus pandemic has forced many workers to work remotely at home globally. Cybersecurity professionals' advice remotes employees to beef up their awareness and knowledge of phishing scams, the fastest-growing type of cybercrime, many of which are now playing on fears of the coronavirus. The growing spread of misinformation and disinformation will confuse the public and undermine the scientific response (UNODC, 2020). According to Herb Stapleton of the FBI Cyber Division Section Chief, scammers usually prey on vulnerable online users during national disasters and tragic events when people are distracted and let their guards. Stapleton notes COVIT-19 is worse and has spurred more cybercrime because of its global. The IC3 (2020) receives around 1,000 complaints per month, and now that figure is nearly 3,000. Another example includes the WannaCry ransomware attack in 2017 that affected roughly 150 countries, attacking 230,000 computers resulting in USD 4 billion in financial losses globally (Kaspersky, 2020).

We deluge colossal information through the internet, especially on social media platforms or websites in our daily activities. Therefore, it is crucial to ensure that Sierra Leoneans know how to secure their online activities, requiring a better understanding of security awareness and countermeasures. Cybersecurity should be taught as a component in specific ICT and its related courses in senior secondary schools, colleges, and universities in Sierra Leone. Therefore, only a few percentages of the student population offering information and communication technology and its related courses have cybersecurity awareness and know the critical preventive countermeasures. Thus, the author presents a brief overview of cybercrime, its causes, and preventive countermeasures in Sierra Leone.

2. Methodology

The research deploys a descriptive approach, which includes questionnaires and Internet searches. It evaluates the effects of cybersecurity on the information age in Sierra Leone. Forty questions were designed due to the limited time and made available online. There were 112 respondents among internet users in Sierra Leone gathering first-hand information on the causes of cybercrime and cybersecurity in the post-COVID-19 era.

2.1 Overview of Cybercrime

Cybersecurity has become a hot research topic globally (Steven Morgan, 2020) because of cyberspace's hash hostility. Cyberspace is the vast boundaryless space serving as the internet terrain. Cybersecurity involves a wide range of issues, including security tools and concepts, policies, standard security guidelines, risk management approaches, training, and technologies that would protect cyberspace (people and assets) (Ibikunle Frank and Eweniyi Odunayo, 2013). Cybersecurity endeavors to preserve and protect people and assets against malicious behavior in cyberspace. With the drive to formulate cybersecurity policies and legislations in Sierra Leone, the economic vitality and national security domains will depend on multiple interrelated infrastructures such as the critical networks, information systems, services, and other cyberspace resources. Therefore, standard security procedures are needed to protect infrastructure, systems, services, and data. However, security awareness and education are not entirely addressed by present technologies,

making organizations rely on their workers' security knowledge (Jama *et al.,* 2014). Lacking the essential knowledge can lead to threats and attacks from internal or external actors (Kortjan & von Solms, 2014; PCI Security Standards Council, 2014).

Cybersecurity and information security are interwoven. Information security awareness, including security knowledge and training, is essential for internet users (PCI Security Standards Council, 2014; Antwi-bekoc & Nimako, 2012), not only to protect sensitive information systems assets but as well to safeguard the sustainability of the organization. Information security education focuses on providing a better understanding and awareness of information security documents using theoretical delivery methods (Amankwa *et al.,* 2014). On the other hand, awareness focuses on creating employees' security consciousness when handling relevant information security documents (Bulgurcu *et al*., 2010; Mejias & Harvey, 2012). Just as awareness of an epidemic can reduce the risk of infection (Shang, 2013), awareness of information security documents can also mitigate security incidents. Employees' understanding of handling sensitive organizational and personal information is crucial to an organization's success (PCI Security Standards Council, 2014).

Sierra Leone is faced with a considerable task to safeguard its people from cyber-attacks since most lack the awareness of the preventive countermeasures regarding cybersecurity and cybercrime (Jama *et al.,* 2014). Unfortunately, the country has a weak legislature to protect internet users, and there are only a few educational institutions offering cybersecurity courses in the country.

2.1.1 Cybercrime definition

Cybercrime is a major threat globally, even to the most technologically advanced countries like the U.S (Laura, 1995). Cybercrime is any activity that aims to extract or steal confidential data, money, or unethical hacking (Shipra *et al.,* 2016).

According to McConnell International, cybercrime is a destructive act committed from or against a computer or network, differing in four perspectives from most terrestrial crimes. It can be easily used to commit crimes, need limited resources relative to the impending damages caused, anonymously use to commit cybercrime anywhere without physically being there, and are often legal. The Director of Computer Crime Research Centre (CCRC), in an interview in 2004, stated that cybercrime (computer crime) is any illegal behavior directed using electronic operations that aims at the security of computer systems and the data processed by them. In principle, it is a crime committed in cyberspace. It contains billions of information about people, objects, facts, events, phenomena, or processes denoted by the mathematical, symbol, or others and transmitted through local and global networks.

The INTERPOL defined cybercrime as crimes done against computers and information systems to gain illegal access to an electronic device or deny access to a legitimate user (Cybercrime and punishment, 2000). The above narrations indicate that cybercrime knows no borders and evolves fast, affecting critical services, businesses, and individuals. The effects of cybercrime cost trillions of U.S. dollars globally every year and inflict untold damages, and threatens national security. According to the President and consultant of the Cyber Laws, Mr. Pavan Duggal, in a report, stated the numerous categories and types of cybercrimes (Daniel J Solove & Chris Jay Hoofnagle, 2002).

2.1.2 Cybercrimes against persons

Cybercrimes committed against persons are becoming increasingly devastating. Crimes committed using cyberspace with the aid of a computer against an individual known as cybercrimes against persons. Examples include harassment via mail, cyberbullying, child pornography, credit/debit card fraud, phishing, to name a few.

The posting of offensive languages and videos on the internet, such as pornographic materials, hate speech, highly political rhetoric and blackmails, and cyberbullying, constitutes critical cybercrime components. They channeled them through social media platforms, including Facebook, Twitter, WhatsApp, WeChat, and others that instantaneously reach millions.

Therefore, if strong laws and policies are not enacted to mitigate Sierra Leone's effect, it will undermine the necessary foundation of peace (security). Such a security issue was evident by the

Melissa virus (Berkley Joseph P and Liu, 2003) that surfaced in 1999, affecting numerous computer systems in the United States and Europe. The damage caused by Melissa was to the tune of 80 million U.S. dollars worldwide. The increase in cybercrimes, such as the high-profile ransomware operations in recent times, leaked personal data on a massive scale, making the victims vulnerable to fraud and placing many lives at risk and services. It affected the NHS and many other organizations globally.

Cyberstalking and cyberbullying are distinctive cybercrime that does occur through cyberspace. Examples of cyber harassment include sexual, racial, religious, tribal, and others. Cyberstalking is a crime that violates a citizen's privacy, which is a significant crime globally. No citizens would like their valuable data to be invaded by someone either over the internet or other means (Goodman Symour E and Herbert S., 2007).

2.1.3 Cybercrimes against property

This category includes all cybercrimes done against property, such as computer vandalism (destruction of others' property), transmitting harmful programs (malicious links and software).

2.1.4 Cybercrimes against government

They constitute any cybercrimes perpetrated against nations. They include cyber-terrorism, cyber espionage, cyber warfare, intellectual property crimes, trade secrets, denial-of-service, etc. Today's cyberspace is highly polarized as the U.S. is abandoning major international regulatory bodies. For instance, the Intermediate-Range Nuclear Forces Treaty of 1987, the Paris Agreement of 2015, the Trans-Pacific Partnership of 2016, the U.N. Human Right Councils of 1946, the U.N. Educational Scientific and Cultural Organization (UNESCO) of 1945, World Trade Organization (threatened to pull out), NATO (questioned), NAFTA (renegotiated and await Congress to ratification) (treaties and agreements, 2019). If international solidarity fails, individual and hostile nations will perpetuate havoc to weaker countries and institutions. Therefore, the world needs leaders who can work together and draft strong international laws to safeguard global cyberspace.

The recent denial-of-service attacks eclipsed by the COVID-19 pandemic have dramatically increased because all activities and operations are conveyed via the internet. The U.S Department of Health and Human Services (HHS) website was under attack by hackers trying to disable it in mid-March 2020. They aimed to deprive citizens of access to official data on the COVID-19 pandemic and countermeasures. Also, unknown cyber actors spread misinformation in social networks and via text and email about introducing a nationwide quarantine in the U.S. The attempt failed: the HHS website continued to function, despite the increased load.

Furthermore, similar attacks occurred in France, Germany, the Netherland, the U.K., and other parts of the world to spread fake news and misinformation to the public (Oleg Kupreev *et al.,* 2020). Also, similar misinformation spread by unpatriotic Sierra Leoneans based in the Diaspora on the coronavirus spread misinformation in Sierra Leone through Facebook, Twitter, and WhatsApp.

2.2 Other Forms of Cybercrimes

Cybercriminals pursue to abuse human or security vulnerabilities to steal passwords, data, or money. The most common cyber threats include:

Phishing: Phishing attacks generally occur daily by attackers inserting malware into someone's machine through the internet (Kaspersky, 2020). An online user can stop it by practicing standard preventive measures. Phishing attacks are most successful because people click on malware when downloading a file or software on the internet and redirects them to another webpage before downloading begins. It mostly a bogus email requesting security and personal information. For example, customers at Lloyds bank were hit by a phishing scam of about 100 clients (Alex Scroxton, 2020). Bank clients warned of emails and SMS messages that direct them to a fake site and then request account log-in details

Denial-of-Service (DoS): A DoS attack is when a cybercriminal tries to make a machine or network inaccessible to its legitimate users by temporarily or indefinitely disrupting the services of a host linked to the internet. DoS attacks are usually caused by "flooding" the resource with many requests (Anand Kumar Shrivastav and

Ekata, 2013), limiting the server to reply to some or all authorized rights. Authorized users using the pool of resources denied access to those resources. A distributed denial of service (DDoS) attack is made against websites – often accompanied by extortion (Kaspersky, 2020).

Hacking: It is the unlawful access to an electronic device to view, copy, or create data intending not to destroy the data or damage the target device. Today, billions of electronic devices are hacked to the internet, making them prone to attack. Unfortunately, no system is 100% secure on the internet, and some internet users make it easy for hackers to infiltrate their networks. A security hacker uses his/her knowledge to break into a computer system and are sometimes called crackers (Lee, 2015). Typically, they steal Email passwords, credit card information, and social media account details resulting in substantial financial loss. They infect devices connected to the internet with malware to steal valuable information, search for the systems' vulnerability, or use a victim's computer to make even a substantial gain; they must first get the user to do something maliciously, like executing a code (Taylor *et al.,* 2015). Generally, two skill levels among hackers:

- **Expert Hackers:** These are hackers who develop software scripts and codes to exploits their victims. They are usually mastering many skills and will often create attack software and share it with others.
- **Script Kiddies:** These constitute hackers of limited skill and use expert-written software to exploit a system. They do not usually fully understand the systems they hack into:

Pirated software: An unauthorized software that copies disseminates, and transfers sensitive information belonging to individuals, organizations, and government. It usually contains malicious scripts and links, infected files, and computer viruses that target someone's' computer. Examples include the ransomware attack that hijacked critical files and holds them to ransom.

Cyber Attackers: Cyberattack is a menace facing the global community today. Recent studies indicated a surge in hacks and breaches globally during the COVID-19 pandemic as many people relying on the internet to do their daily activities. It further showed that many organizations failed to protect their data due to poor cybersecurity practices making them vulnerable to data theft (Saroj Mehta & Vikram Singh, 2013).

Cyber Bullying: Using electronic communications to intimidate or bully online users by communicating intimidating or threatening messages to oppressed victims (Richard Donegan, 2012).

Identity Theft: The act of stealing or gathering enough information about someone's details such as email address, date of birth, name, place of birth, residential address to commit identity fraud. Identity theft may occur for both the living and the dead person.

Cracking: Cracking is the unauthorized permission granted to online criminals to inflict damage to a computing system.

Email Spoofing: The act of falsifying email messages to gain access to someone's email. The criminal launches an attack when the recipient completes the challenge.

Spam: Spam is an unsolicited commercial Email - while many consider spam a joke, somewhat an attack but emerging as a vector for some online attacks.

Other types of Cybercrimes

According to Kamini (2011), the other types of cybercrimes include:

1. Unauthorized access to computer information - 8002 crimes
2. Creating, using, and distributing malware, spyware, or machine carriers with such programs1079.
3. They are violating computer best practices, computer systems, or networks-11.
4. They are violating copyrights and computer related-security issues- 528.

Causes of Cybercrime

The following are some of the causes.

1. Capacity to store mega-sized data in comparatively small space
2. Complexities of the computer software and programs engender human errors

3. Human negligence on cybersecurity creates easy access for cybercriminals
4. Cybercrime is associated with the loss of evidence as data is routinely destroyed, making it difficult to apprehend offenders.

Iwarimie-Jaja, (2012), opined that computer crimes flourish as a result of the following factors.

1. The potential gain is greater than the risk.
2. Managers disassociate themselves from operations.
3. Computer security is lax.
4. People with little skills easily accomplish certain types of computer crimes.
5. Obtaining the necessary evidence may be difficult.
6. They can sometimes refer to it as an error rather than a crime.

Furthermore, within the Sierra Leone context, the following causes are identifiable:

1. No laws regarding cyber and information security in the country
2. Rapid urbanization
3. Increasing youth unemployment
4. Lack of educational institutions to enroll cybersecurity into their curriculum.
5. Quest for wealth, values for materialism, and negative role models.
6. Public awareness of cyber-related activities by the government and the print media
7. Weak implementation of cybercrime laws and inadequately equipped agencies
8. Lack of or no formal knowledge on cybersecurity-related issues among those charged to police the cybercriminals' activities.

2.3 Solutions to Cybercrime

No computing system is 100% secured, even though numerous global authorities attempt to mitigate cybercriminals' threats. What is considered cybercrime in one jurisdiction might not necessarily be a crime in another. The lack of global solidarity in having a unique and stringent international law makes the fight against cybercrime challenging to fight. Therefore, the government should create cyber awareness among its citizens through formal education and sensitizations. When citizens are aware of cybercrime implications, they will follow the best practice to prevent such attacks. Also, organizations should always involve cybersecurity experts in making organizational' policies.

Furthermore, the individual nation should draft effective cybersecurity legislation that would eradicate cybercrime. Cyber education possibly prevents cybercrime from occurring. Another means to eliminate cybercrime is to harmonize international cooperation and law, which goes for the greed motivated and cyber-terrorists. They cannot be fought by education alone but by legislating new laws, adjusting the global legislatures, and enhancing full cooperation between national law enforcement agencies.

Some of the best practices to secure online activities include the following:

1. Install the Operating System/software update regularly.
2. Run genuine antivirus software and avoid free ones.
3. Prevent identity theft by not disclosing information that will help cybercrimes to steal sensitive credential, including:
    - Financial account numbers.
    - Social security numbers.
    - Driving license numbers;
    - Immediately report any abnormalize to the appropriate authority;
4. Beware of phishing scams;
5. Always turn on the firewall by check the computers' security settings for a built-in personal firewall.
6. Avoid downloading spyware and adware, as they might affect the computer functionality.
    - Spybot/Ad-Aware for removing spyware/adware from the computer.
    - Read software terms before installing free software.
    - Be cautious of invitations to download software from unknown internet sources;
7. Use strong passwords, making it challenging to guess by mixing upper- and lower-case letters, symbols. Follow tips like:

- Changing it at least every 72 hours;
- Never repeat passwords;
- Should not contain anything related to its owner;
- Avoid short passwords, at least eight characters long;
- Do not write passwords down;
- Do not share it with anybody;
- Use two-factor authentication;
- Avoid saving passwords on web browsers;

8. Backup important files.
9. Do not open attachments in spam emails.
10. Do not give out your personal information unless secure
11. Contact companies directly about any suspicious requests.
12. Be mindful of which website URLs you visit Keep an eye on your bank statement.

3. Results and Discussion

Cybercrime is increasingly growing in Sierra Leone as most youths use the internet daily, especially during the coronavirus pandemic.

For instance, the Sierra Leone Commercial bank (SLCB) published a cyber-attack report in January 2020 by an unknown person, though the bank said none of its customers' information was unaffected.

Table 1 indicated that Asia has a higher percentage of 50.9% as of May 2020, followed by Europe, with 15.7%, Africa with 11.3%, Latin America/Caribbean accounting for 10.0%, North America 7.5%, the Middle East 3.9%, and Oceania/Australia 0.6% of the global Internet usage. Also, Asia has the most significant Internet users in the World and Europe second.

Cyber defamation and cyberbullying have become a significant concern for many Sierra Leoneans. Most unpatriotic Sierra Leoneans living abroad use social media platforms to cause political chaos in Sierra Leone. The majority of Sierra Leoneans are illiterate and probably may not know the difference between authentic and unauthentic information posted over the internet.

Figure 1. shows that Asia again with the highest Internet users globally. Second to Europe and Africa third. Figure 2. indicates that North America has the highest Internet penetration rates (94.6%), followed by Europe with 87.2%, Latin America/Caribbean (70.5%), the Middle East (69.2%), Oceania (67.4%), Asia (53.6%) and Africa with 39.3%.

Table 1. World Internet Usage and Population Statistics 2020 Year-Q1 Estimates as of 31 May 2020

World Regions	Population (2020 Est.)	Population % of world	Internet Users 31 May 2020	Penetration Rate (% Pop.)	Growth 2000-2020	Internet World %
Africa	1,340,598,447	17.2 %	526,710,313	39.3 %	11,567 %	11.3 %
Asia	4,294,516,659	55.1 %	2,366,213,308	55.1 %	1,970 %	50.9 %
Europe	834,995,197	10.7 %	727,848,547	87.2 %	592 %	15.7 %
Latin America / Caribbean	658,345,826	8.5 %	453,702,292	68.9 %	2,411 %	10.0 %
Middle East	260,991,690	3.3 %	183,212,099	70.2 %	5,477 %	3.9 %
North America	368,869,647	4.7 %	348,908,868	94.6 %	223 %	7.5 %
Oceania / Australia	42,690,838	0.5 %	28,917,600	67.7 %	279 %	0.6 %
WORLD TOTAL	**7,796,949,710**	**100.0 %**	**4,648,228,067**	**59.6 %**	**1,187 %**	**100.0 %**

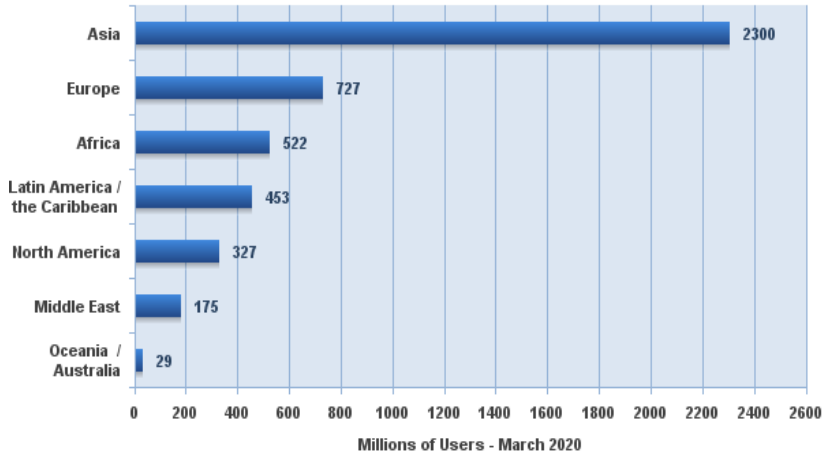

Figure 1. World Internet Users by Geographic Region – 2020 Q1 Report

Source: Internet World Stats (2020)

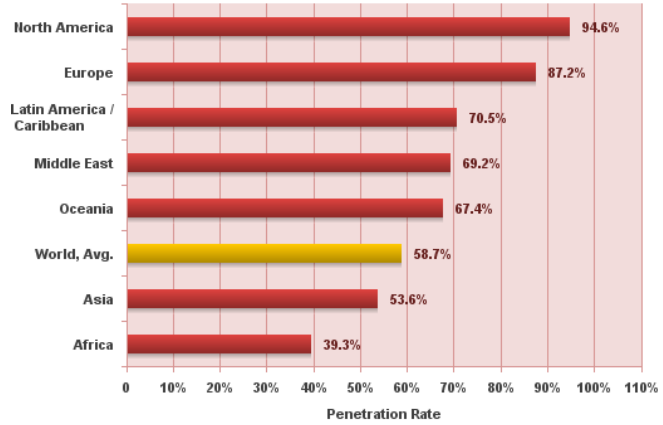

Figure 2. Internet world Penetration Rates by Geographic Region – 2020 Q1 Report

Source: Internet World Stats (2020)

It further indicates that Africa has the lowest Internet penetration rates even though it came third for the population percentage of the world in terms of Internet usage with 17.2%. Azeez Nureni Ayofe and Barry Irwin (2010) highlighted the following technological, economic government, and social-demographic viewpoints relating to cybersecurity issues:

Technology Viewpoint

1. Innovations in high-tech telecommunications devices and software, computing devices, and other essential technologies create new opportunities for online criminals, new kinds of cybercrimes, and new law enforcement challenges.
2. Lack of international legislation on cybersecurity and cybercrime.
3. Lack of global technological organization to monitor all countries.

Economy Viewpoint

1. Possible upsurges in consumer debt may affect bankruptcy filings.
2. Deregulation, economic growth, and globalization are shifting the volume and nature of unchallenged behavior.
3. The unification of the world economy is increasing opportunities for criminal activity.

4. The effect of the global pandemic is forcing the world into a recession, such as a coronavirus pandemic.

Government Viewpoint

1. Criminal and civil justice issues go beyond national boundaries, requiring full cooperation among the international communities, and involve treaty obligations, multinational environment, trade agreements, and other foreign policy concerns.
2. It is always a big challenge, as governments worldwide continuously fail to act as one body when sensitive to national security issues.

Social-Demographic Viewpoint

1. Internet users will continue to increase among the world population, making them highly crime-prone. For instance, about 61.6% of Sierra Leone people used the internet daily.
2. Also, social media has become the source of misinformation and fake news globally.

4. Conclusion

Cyber education, legislating and enforcing stringent cyber laws, and creating public awareness can prevent cybercrime from happening. Cybercrime can be stopped or mitigated with all shareholders' collective participation (state actors, civil society organizations, telecommunication companies, corporations, academics) and individuals' online users. Furthermore, law enforcement authorities are unaware of these online crimes due to the complex nature of evolving cybercrime. Therefore, creating public awareness, legislating effective cyber laws to replace the Public Order Act of 1965, and cyber-related curricula in schools, colleges, and universities will help understand the nature of cybercrime and subsequently mitigate its effects in Sierra Leone. Reliable and effective cyber laws should be legislated to punish cyber criminals. However, the study did not account for a detailed analysis of all the possible cybersecurity countermeasures as Sierra Leone is in its first technological evolution stage.

Recommendations

The following approaches are recommended to the government of Sierra Leone to help curb the effects of Cybercrimes:

Legislative approach

1. Laws should apply to cybercrime—the government of Sierra Leone Parliament is the principal organ to legislate strong laws on cybersecurity and information security, as done in most countries around the world;
2. Review the 1965 public order act to tackle this increasing cyber activity that would address the dynamic nature of cybersecurity challenges;
3. Harmonize national cyber legislatures with international laws, treaties, and conventions;
4. Enhance continuous capacity building programs state security forces;
5. Everyone should support the nation in fighting online crimes, especially the fourth estate and universities.

Security approach

1. Streamlining and improving the coordination regarding information security processes at the state and global platform;
2. Safeguarding citizens information and outline the best security standards that would protect the information security, network security, data privacy, making a safer society;
3. Collaborate with global partners in fighting cybercrimes;
4. Installing firewalls in all governmental departments and agencies;
5. Conducting routine training on information security features and processes;
6. Continuously update existing systems to meet the present circumstances.

Education/Research approach

1. The Parliamentary Committee on Education should enshrine the constitution to make higher education institutions mandatory for teaching cyber-related programs.
2. Formalize the coordination and prioritization of cybersecurity research and development

activities; disseminate vulnerability advisories and threat warnings.

3. Implement an evaluation/certification program for cybersecurity systems and product;
4. The Information and Communication Ministry and the National Telecommunication Commission (NATCOM) should create awareness on cybersecurity and information security issues continuously, thereby creating a culture of a secured cyber environment.

References

Alex Scroxton, (2020). Top 10 Cybercrime Stories of 2020. Available online: https://computerweekly.com/news/252493515/Top-10-cyber-crime-stories-of-2020 (accessed on 5 February 2021)

Amankwa, E., Loock, M. & Kritzinger, E., (2014), A Conceptual Analysis of Information Security Education, Information Security Training and Information Security Awareness Definitions, In The 9th International Conference for Internet Technology and Secured Transactions (ICITST -2014). London: IEEE, pp. 248–252. https://doi.org/10.1109/ICITST.2014.7038814

Anand Kumar Shrivastav, Ekata, (2013). ICT Penetration and Cybercrime in India: A Review, International Journal of Advanced Research in Computer Science and Software Engineering, 3: 414-419.

Antwi-bekoe, E. & Nimako, S.G., (2012), Computer Security Awareness and Vulnerabilities: An Exploratory Study for Two Public Higher Institutions in Ghana, International Journal of Science and Technology, 1(7), pp.358–375.

Arora, A., Nandkumar, A., & Telang, R., (2006). Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. Information Systems Frontiers, 8(5), 350–362. https://doi.org/10.1007/s10796-006-9012-5

Azeez Nureni Ayofe, & Barry Irwin, (2010). Cybersecurity: Challenges and the Way Forward, GESJ: Computer Science and Telecommunications, 6 (29): 56-69.

Berkley Joseph P, Liu, (2003). The DMCA and the regulation of scientific research, Technology Law Journal, 18(2):501-537.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010), "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", MIS Quarterly, 34(3), 523.

Cyber Crime and Punishment? Archaic Laws Threaten Global Information. Pg. 1 December 2000. http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf

Daniel J. Solove and Chris Jay Hoofnagle (2002). A model regime of privacy protection. University of Illinois Law Review, 7:1083-1167.

Dinesh Thakur. (2020) What is the difference between Data and Information? Available online: https://ecomputernotes.com/fundamental/information-technology/what-do-you-mean-by-data-and-information

Goodman Symour E and Herbert S. (2007) National Research Council and National Academy of Engineering, Toward a Safer and More Secure Cyberspace, Washington, DC: The National Academies Press. https://doi.org/10.17226/11925

Hans de Bruijin, Marijn Janssen (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1- 7. https://doi.org/10.1016/j.giq.2017.02.007

Ibikunle Frank, Eweniyi Odunayo (2013). Approach to cyber security issues in Nigeria: challenges and solution. International Journal of Cognitive Research in Science, Engineering and Education 1(1).

Internet World Stats (2020). Usage and Population Statistics. https://internetworldstats.com/ (accessed on 5 February 2021)

Iwarimie-Jaja (2012). Criminology: The Study of Crime. Owerri: Springfield Publishers.

Jama, A.Y., Siraj, M., & Kadir, R., (2014), Towards Metamodel - based Approach for Information Security Awareness Management, In 2014 International symposium on biometrics and security technologies (ISBAST). pp. 316–321.

Julian Jang-Jaccard, S. Nepal (2014). A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences, 80: 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Kamini, D., (2011). Cyber Crime in the Society: Problems and Preventions, Journal of Alternative Perspectives in the Social Sciences 3(1): 240-259.

Kaspersky, (2020) Tips on how to protect yourself against cybercrime. Available online: https://me-en.kaspersky.com/resource-center/threats/what-is-cybercrime (accessed on 5 February 2021)

Kortjan, N., & von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA, SACJ No. 52, pp. 29- 41. Available at: https://sacj.cs.uct.ac.za/index.php/sacj/article/download/201/95 (accessed on: 14/07/2015).

Laura, A., (1995): Cyber Crime and National Security: The Role of the Penal and Procedural Law, Research Fellow, Nigerian Institute of Advanced Legal Studies., Retrieved from https://nials-nigeria.org/pub/lauraani.pdf (accessed on 5 February 2021)

Lee, M., (2015). The evolution of Cybercrime: From Julius Caesar and Prince Philip to state-sponsored malware, International Business Times. https://ibtimes.co.uk/evolution-cybercrime-julius-caesar-prince-philip-state-sponsored-malware-1514552 (accessed on 5 February 2021)

Mejias, R. J., & Harvey, M. (2012). A case for information security awareness programs to protect global information, innovation and knowledge resources, International Journal of Transitions and Innovation Systems, 2, 302–324.

O'Brien, J.A. & Marakas, G.M., (2011). Management Information System, tenth edition, McGraw-Hill Company Inc, ISBN: 978-0-07- 122109-2.

Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov (2020). DDoS attacks in Q1 2020 https://securelist.com/ddos-attacks-in-q1-2020/96837/ (accessed on 5 February 2021)

PCI Security Standards Council (2014). Information Supplement: Best Practices for implementing a Security Awareness Program, Security Awareness Program Special Interest Group PCI Security Standards Council. Available at: https://pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf (accessed on 5 February 2021)

Richard Donegan (2012). Bullying and Cyberbullying: History, Statistics, Law, Prevention, and Analysis, The Elon Journal of Undergraduate Research in Communications, 3: 33-42.

Saroj Mehta & Vikram Singh, (2013), Study of Awareness about Cyber Laws in the Indian Society, International Journal of Computing and Business Research, 4(1).

Shang, Y., (2013). Discrete-time epidemic dynamics with awareness in random networks, International Journal of Biomathematics, 6(2):13500071-7. https://doi.org/10.1142/S1793524513500071

Shipra, R.K, Sumam, A.Y., Smita, S., & Akansha, S., (2016). Recommendations for Effective Cyber Security Execution. 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016).

Steven Morgan, (2020). Cybercrime to cost the world $10.5 Trillion annually by 2025. https://cybersecurityventures.com/hackerpocalypse-original-cybercrime-report-2016/ (accessed on 5 February 2021)

Tahir Hussain Bhat & Afaq Alam Khan (2015). Cybercrimes, Security and Challenges, Published in International Journal of Advanced Research in Computer and Communication Engineering, 4(5): 2319-5940. https://doi.org/10.17148/IJARCCE.2015.45108

Taylor, R.W., Fritsch, E.J., & Liederbach, J., (2015). Digital crime and digital terrorism. (3rd ed.). Upper Saddle River, NJ: Pearson.

UNODC (United Nations Office on Drugs and Crime). Available online: https://unodc.org/documents/Advocacy-Section/UNODC - CYBERCRIME AND COVID19 - Risks and Responses v1.2 - 14-04-2020 - CMLS-COVID19-CYBER1 - UNCLASSIFIED BRANDED.pdf

Zhao, J. J., Zhao, S. Y., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. Government Information Quarterly, 27(1), 49–56. http://dx.doi.org/10.1016/j.giq.2009.07.004.

Acknowledgments: The authors would like to thank all those who participated in the survey for their valuable inputs. Gratitude goes to Assistant Professor Brima Sesay of the School of Economics at the Wuhan University of Technology for his comments and suggestions. We also like to thank Professor Dr. Paul Kamara and Dr. (Mrs.) Abie Paula Kamara, the Chairman, Board of Trustee, and the Pro-chancellor, University of Management and Technology, Freetown Sierra Leone, for their supports

Does this article screened for similarity: YES

Funding: NIL

Conflict of Interest: NIL

About the License