A SURVEY ON THE PERCEPTIONS AND AWARENESS OF CYBER SECURITY IN NIGERIA

John Adinya Odey
University of Calabar
29 PUBLICATIONS **41** CITATIONS
SEE PROFILE

Prince Ana
Cross River University of Technology
20 PUBLICATIONS **23** CITATIONS
SEE PROFILE

A SURVEY ON THE PERCEPTIONS AND AWARENESS OF CYBER SECURITY IN NIGERIA

John Adinya Odey[1], Iwinosa Agbonlahor[1], Prince Ana[2]

[1]: Department of Computer Science, University of Calabar, Nigeria.
[2]: Department of Computer Science, Cross River University of Technology, Calabar, Nigeria.

ABSTRACT

A rapidly expanding and evolving field; cyber security has indeed become an ever present factor in every aspect of computing. Recent advances in technology and the proliferation of digitization technologies and paradigms like cloud, mobile and personal computing devices has enabled a lot of global crimes now to be committed over cyber space. Consequently, it has become imperative that cyber security practices become integrated into the very fabrics of everyday use of computing technologies. This paper investigates cyber security perceptions in Nigeria to unveil the factors that influence people's perception of different threats in cyber space. The systematic literature review method was used to review relevant publications from reputable journals and conferences. Also a primary exploratory data analysis survey through questionnaires was administered online on General Knowledge, Industry Specific and Personal perceptions of Nigerians on Cyber Security. The results bring to light the current awareness level of cyber security in Nigerian which shows a general lack of interest and awareness of respondents on the three primary areas of survey. This research can be used by authorities to implement safe practices in the Nigerian cyber space to curbing the fast-growing menace of cyber-crimes in the society.

Keywords: Cyber-Security in Nigeria, Cybercrime perception, Nigerian cyberspace.

1.0 INTRODUCTION

It is in the human nature to hold opinions and perceptions about relatable concerns. These perceptions could be justifiable or relative, based on inexhaustible list of factors, which could be categorized base on facts available like cultural norm, personal desire/bias or even popular opinion. These factors that affect perception are not with exception as they borders on sensitive issues like cyber security. Cyber security is the practice of protecting systems, networks, and programs from digital attacks.

In this age of internet evolution and digital systems, cyber security stands as a very important subject for every individual, corporation and government who seeks to operate efficiently and under minimal risk. Information and Communication Technology (ICT) has impacted significantly on institutional operations, processes and products such that Cyber Security now stands a necessity for every organization. This significant influence calls for the need of ensuring protection of properly functioning ICT systems, which we call cyber security.

Cyber-security however is not merely a function of employing a few tools and personnel that would manage the ICT systems; it is rather a culture that should be interwoven into the fabrics of all organizational processes of concerned individuals and institutions.

There is the gap between perception and reality which needs to be addressed for more objective and accurate security stance to be measured. Beyond the optimistic desire to feel safe, what standard should be the informed yardstick to judge cyber security preparedness remains a challenge for developing countries like Nigeria with evolving cyber security awareness. Even so is the lack of internationally-recognized standards on safe practices and adequate law enforcement methods, even among seasoned professionals.

As ICT have gradually crept into our daily lives and businesses featuring its prominence and value to individuals, corporations and government alike, we have all been inducted into this virtual world as our new reality. So as much as security is a necessity in physical world, much more, it has become a necessity in the virtual. Knowledge of people's perception towards risk and cyber threat becomes necessary because we are faced with safety and security challenges every time we go online.

Individuals play as different actors in the cyber world and they in their portfolio hold unique perception to cyber security. These perceptions and opinions whether accurate or not must be investigated, understood, constructively spelt out and then a mental model of a more accurate knowledge-based notion/ideation of cyber security can be designed and communicated. These and the need to ascertain user's online behaviour as it regards to ensuring security of their data underscore the aim of this study.

2.0 LITERATURE REVIEW

Due to proliferation of internet and ICT enabled services, more people interact with computing devices such as servers through smart phones, smart watches, laptops, etc. These devices can be exploited or compromised by attackers using various malicious programs or techniques. As a result, cyber security professionals have their hands full patching and plugging holes across a huge variety of devices and systems and checking to make sure each type of device is fully patched, not being compromised or leveraged as a pivot-point in an attack (Gilheany, 2017). Cyber security has been a resounding subject in the world of internet technology and computer usage. Cyber security refers to any activity carried out to ensure integrity, confidentiality and availability of information systems (Chai, 2021). Cyber security is everybody's concern as much the same way as security in the physical space is everybody's business. A number of polls and studies carried out by (Kostyuk & Wayne†, 2019) (Furman S, et.al, 2012), and other security enthusiasts have shown erroneous behaviour towards cyber security.

As is widely reported in the media, cyber-attacks are increasing in quantity and sophistication (Fossi et al., 2011). In most cases, it is the weakest link in cyber security (the human element) that is the target for the increasing number of online criminals who are perpetrating an ever-greater variety of cybercrimes. The need for cyber security awareness (CSA) campaigns is thus undisputed, as these remain the first line of defense in providing employees and stakeholders with the know-how to interact safely online (Chandarman & Van Niekerk, 2017).

Most individuals believe cyber security is the responsibility of governmental organizations or security applications and tools like (antivirus, firewalls, etc), some corporate individuals believes it is the duty of the I.T. department to handle security. This may not be very accurate as some studies have proven (Nurse et al., 2011), but it is the persisting mindset among some nonetheless. The human factor have been the weakest link through which several successful cyber-crimes have the perpetuated (Huang, Rau & Salvendy, 2010). Yet this erroneous perception exist among a host of internet users.

Another yet disturbing perception is the belief that, Yes, cyber threat is real, but "I will not fall a victim". They believe other more sensitive institutions like banks, governments, and high-profile individuals should be more concerned about cyber security (Smith, 2017). Even with low knowledge on cyber security some still believe they are well secured by their limited security practices. Some others don't preview cyber threat as much of a deal to be prioritized because it does not inflict physical harm, as other catastrophic societal threats and they underestimate the probability of its occurrence (Lawson et al., 2016), seeing only cyber operations that disrupts or degrades governments and corporations systems are published in the media, and such events seldom occurs.

A majority of users feel unsusceptible to threats; the reason for this mindset is quite varied among individuals. Some believes the hackers target the financially stable and those with political interest not regulars (Smith, 2017). Some believe that cyber-attacks are more channeled towards luxurious gold mines, national infrastructure, terrorism or violent crime. Some hold an optimistic judgment that they can't fall victim probably because they have never fallen victim, this confidence is not based on any technical security setup put in place, but sheer optimism.

Some users don't see cyber-crime as a threat they could have assured security over (Ghosemajumder, 2017), this drives the belief that if the government and skilled professionals cannot attain 100% security, there is no need fussing over what is beyond control. Then security is a thing of fate and not so much of deliberate actions. (Jang-Jaccard & Nepal, 2014) believe stressing much on security can cost even more than they intend to secure and would be penny wise, pound foolish to effect. This belief sponsors the idea that security consciousness will cause so much limitation to our online activities (Acquisti, Brandimarte & Loewenstein, 2015). They believe to glide freely on the cyberspace you should be ready to allow some compromise on security or an alternative is to avoid participation or suffer skeletal service on the cyberspace. Some others believe it is the duty of online systems administrators to preserve their privacy and bank agency to secure their online transactions.

Some users generally just play down on the impact cyber risk could pose as they prefer to give credence/ attention to risks that is in their judgment have great dread and prominence as emphasized in the media space (Slovic, 2014), for example terrorism, violent crimes. Since the impact of cyber threat is not often reported and the pain not as visible as physical injuries, although cyber threat could have catastrophic effects on victims, it is just not perceived as such. Some individuals believe they are in complete control of their cyber activities (Slovic, 2014), because of the belief that they control the devices, sites visited and set their password; they are non-susceptible to the risk of cyber threat. They believe their vulnerability lies in their lack of control.

In (Huang, Rau & Salvendy, 2010), the study aims to supply knowledge as to the several actors in the cyber space, the roles in defining cyber security, and their perceptions towards cyber security. A lot of actors play sensitive roles to ensure cyber security of information systems. Although it has earlier been thought that the security cyber space was the sole call of a few skilled IT security experts, this ideology has steadfastly been discarded as research in the socio-technical security sector has been on the increase. It has become imperative due to the increasing count of cyber-attack that exploits the human factor (social engineering and phishing) for studies to be carried out that appreciate the place of the human element in ensuring the security of information systems. As a matter of fact, some security experts considers humans as the weakest link in the security chain. (Nurse et al., 2011) considers that cyber security information must be properly communicated for acceptance and appropriate necessary action to be taken to effectively guard against its occurrence. Considering the broad interplay of factors that can influence human perception and judgment, the study categorized human perception based on the roles the different actors play in the cyber space.

(Tony Bradley, 2017) asserts that most company executives and security professionals have a reasonable understanding of cyber security. Even if they don’t fully understand the mechanics under the hood, they at least realize that there is a vast and aggressive threat landscape out there, and that their networks are under virtually constant siege from attackers. However (Tony Bradley, 2017) further surmise that “When you ask how they feel about their security, though, and how confident they are in their ability to successfully detect and block attacks, the response shows a startling disconnect between reality and their perception”.

3.0 SURVEY METHODOLOGY

In keeping with this study’s subject of literature surveys and general perception of cyber security, various literatures were reviewed as shown in the previous section using systematic Literature Survey (SLRs) methodology in software engineering (M. A. Babar and H. Zhang, 2009). Also consistent with the objectives of this study to investigate Nigerians perception of cyber security to unveil factors that influence these perceptions of different threats to the cyber space and what cyber practices were in common use, the study tried to answer such questions as “What does cyber security mean to people?”, “How much do they know about cyber security?”, “What are their experiences, thoughts and opinions about the concept?”. With the population in focus being the Nigerian populace, a primary exploratory survey adopted and data acquired through questionnaire (Roopa S. and Rani MS, 2012) administered online. Data was collected using several open-ended and close-ended questions. Survey questions were framed on cyber security issues like malware, phishing and other such attacks as well as cyber hygiene practices within and without the workplace.

A high-level outline of the questionnaire was segmented into three parts as follows: General Knowledge, Industry/Organization Specific and Personal Assessment had questions on user knowledge, experiences and practices and was thrown open to internet users across several industries. This was in order to get a broad range of responses not solely restricted to certain particular industries. Through this, a keen understanding of internet users’ behaviors was obtained and utilized appropriately. The questions were in part also set in the form of a benchmarking exercise aimed at assessing the current situation of Nigeria against the Global Cyber- security Index (GCI). A total of 40 respondents participated in this survey and the results analyzed are shown in the preceding sections.

4.0 RESULTS AND DISCUSSIONS

The comprehensive results of the survey conducted are presented below. Graphs and charts are summarily discussed and interpreted accordingly.

4.1 PERSONAL ASSESSMENT

A total of 40 respondents participated in this survey and a summary of the results are presented below; as shown in Figure 1, 97.5% agree to the use of antivirus software on their computer systems used for daily responsibilities. However, only 45% agreed they use paid versions of the antivirus software as against 55% of the population who use free security software (Figure 2). Also, 42.5% update their security software regularly enough as required.

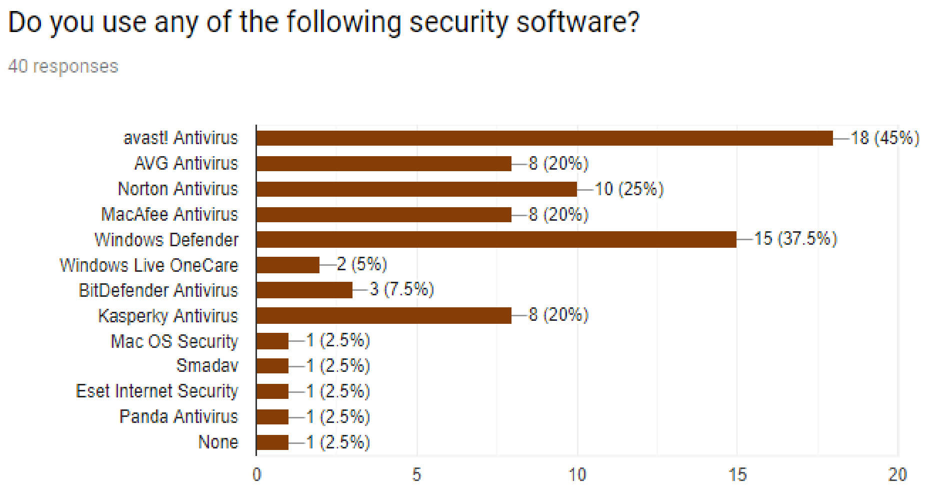


Figure 1*: Usage statistics of various anti-virus Software.*

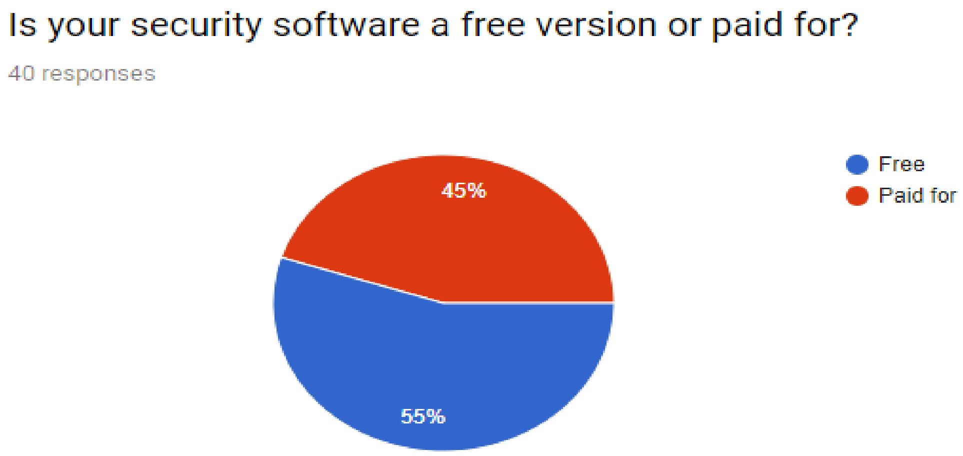


Figure 2: Statistics of respondents who paid for anti-virus software.

Also from the survey, 45% of the respondents regularly visit between 4 – 10 websites that requires passwords. 22.5% of respondents visit over 10 sites and 32.5% visited less than 4 sites that require passwords. Of this population, 22.5% used a single password for all sites visited while 25% had a maximum of 2 passwords for websites.

75% of the surveyed population admitted that internet security is a big deal, and 45% of these populations were aware that in keeping their devices safe, they were helping keep other devices safe as well. 32% of the respondents were always careful about what and where they downloaded over the web (Figure 3), and 42.5% respondents were usually very cautious about opening email attachments (Figure 4).

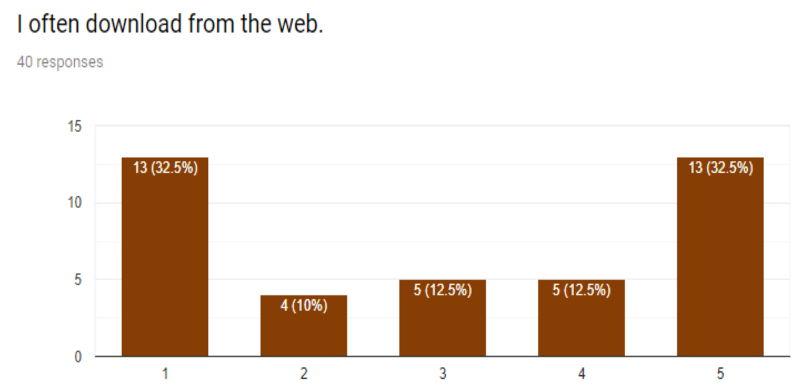


Figure 3: *Statistics of respondents on internet downloads.*

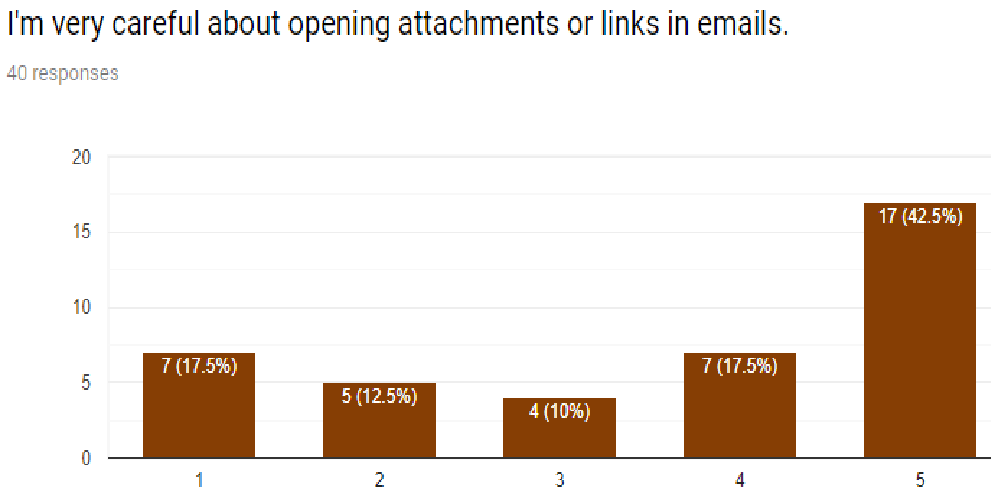


Figure 4: *Statistics of respondents on opening email attachments*

The survey on the interest of respondents to attend a 2-hour cyber security seminar, 75% of respondents would only attend the training if the event was free (Figure 5). 15% would not mind paying for the training, while 10% of respondents are not interested in the training, whether paid or free. It can be deduced that for a paid security event, only 15% of the population would be in attendance.

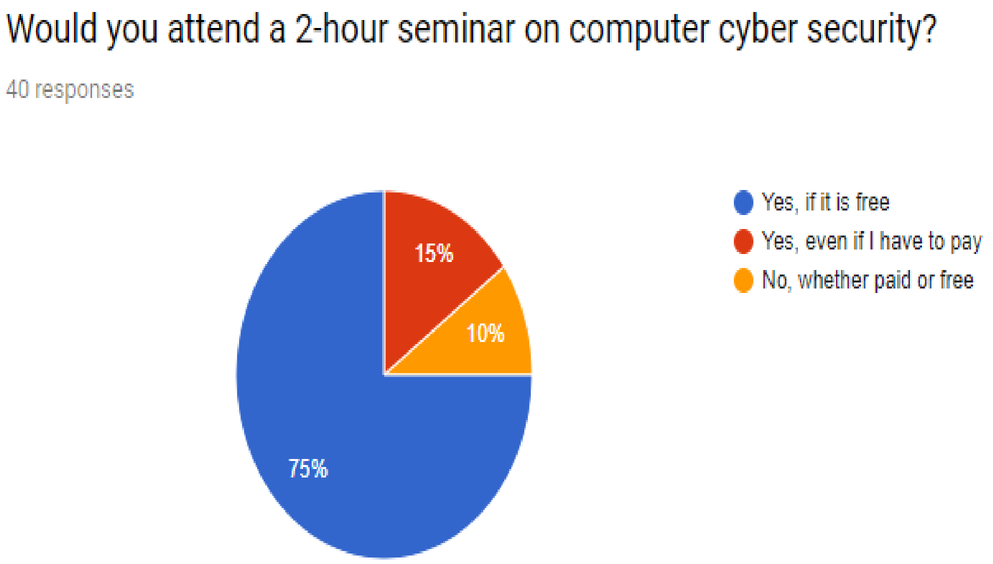


Figure 5: *Statistics of attendance of respondents to a paid cybercrime seminar.*

4.2 INDUSTRY/ORGANISATIONAL AWARENESS

In this survey, responses were obtained from various organizations. The respondent population was made up of 67.5% full-time employees, 5% part-time employees and 3% partners. The contractor, volunteer, student, CEO and unemployed populations were equally 2.5% each. 52.5% had a cyber/computer security team, 42.5% did not, while 5% was not sure whether or not such a team was in place (Figure 6).

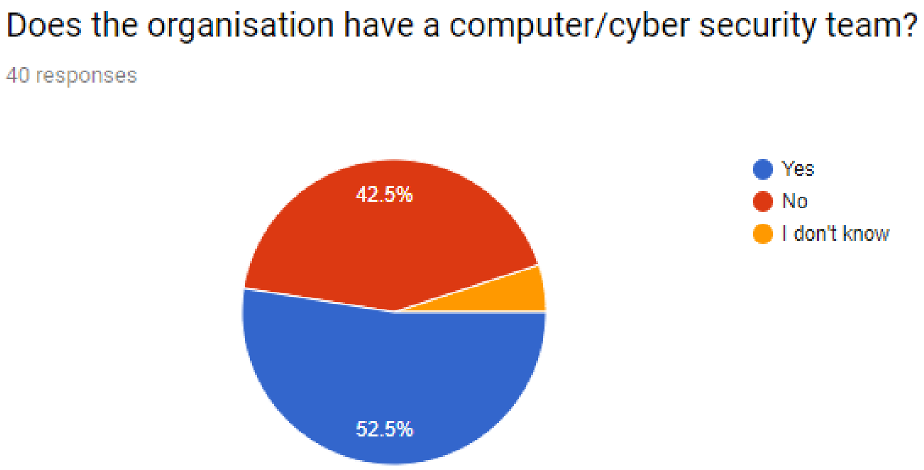


Figure 6: statistics of respondent organization with cyber security team at work.

65% of respondents admitted to having had their work computer corrupted by a virus or Trojan, while 30% of the respondents have never had any encounter with Virus or Trojan. Also 5% did not know what a virus or Trojan was. 42.5% of the surveyed population also did not know how to identify a compromised system. 22.5% said they share their work passwords and 37.5% never changed their work passwords (Figure 7).

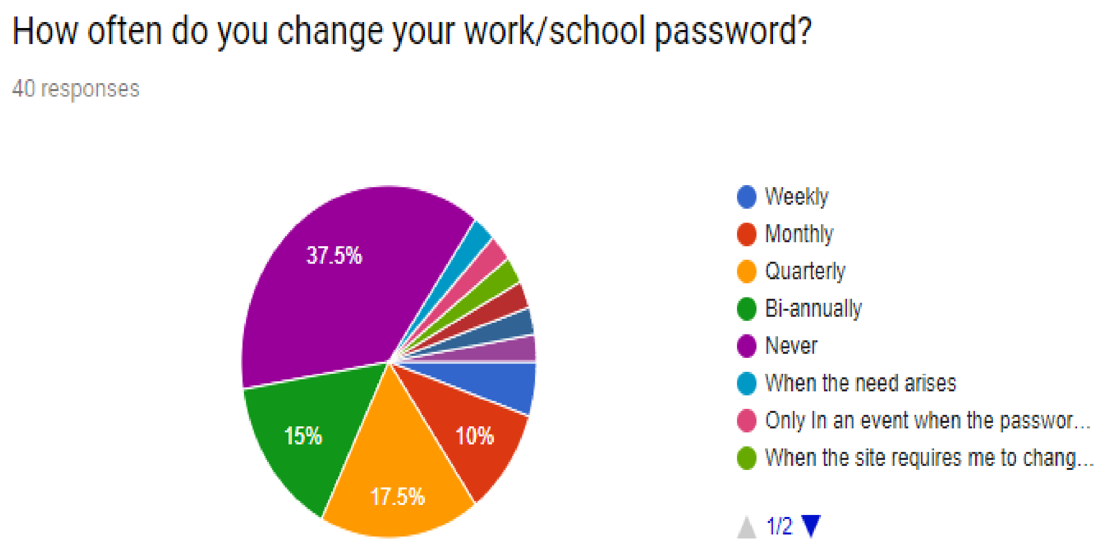
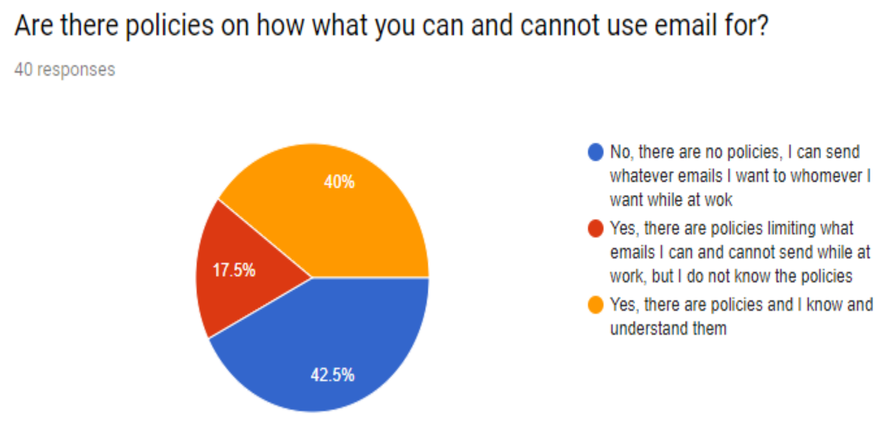


Figure 7: Statistics on the frequency of changing password.

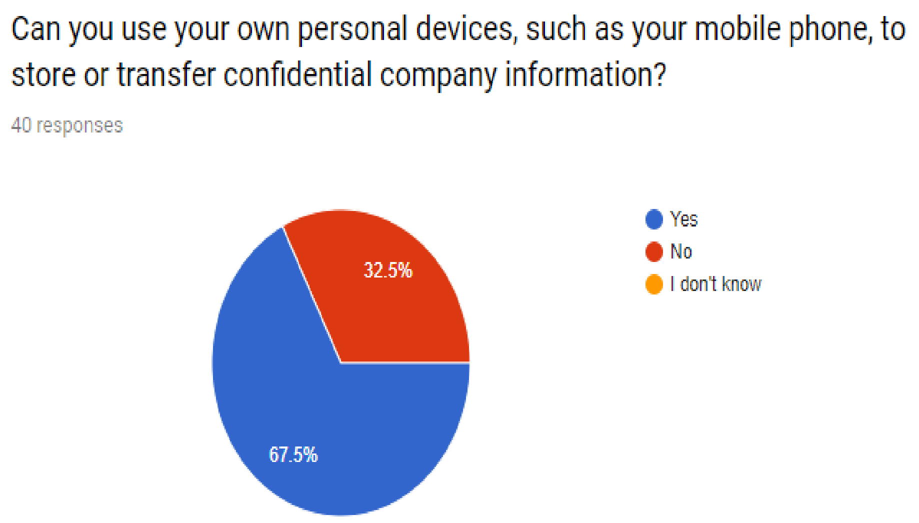
55% of the respondent population believes erasing a hard disk means losing the information forever while 57.5% had no clue what a phishing attack is. 32.5% of the population said there were no policies on what websites could be visited on their organizations network and 42.5% said there were no restrictions on what their work emails could be used for (Figure 9).



5

Figure 8: *Perception of respondents on company policies on e-mail use.*

On using personal devices such as mobile phones to store or transfer confidential company information (Figure), 67.5% said they could and do. 32.5% did say they were very confident about their organization's security posture. On barriers that inhibit their organizations from adequately defending against cyber threats, 60% admitted it was the lack of cyber security awareness amongst personnel.



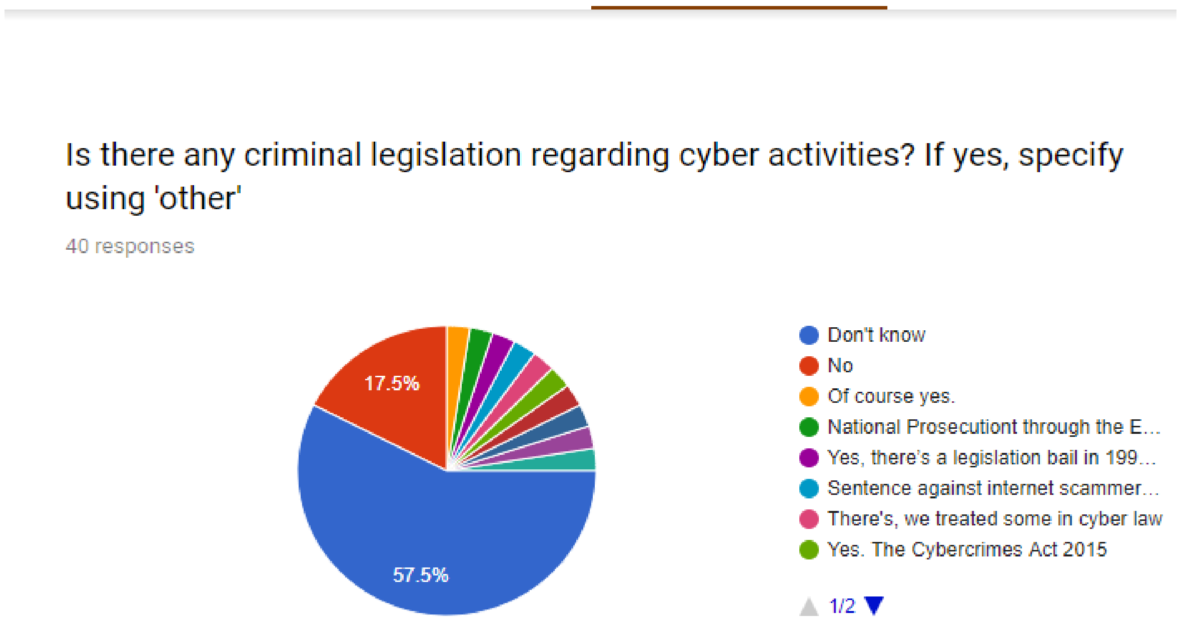
Can you use your own personal devices, such as your mobile phone, to store or transfer confidential company information?

40 responses

Figure 9: Statistics of respondents on the use of personal mobile.

4.3 GENERAL KNOWLEDGE

On the existence of criminal legislation regarding cyber activities, 57.5% were not aware of any, 17.5% opined there was none and 2.5% said it was the jurisdiction of the Economic and Financial Crimes Commission (EFCC).

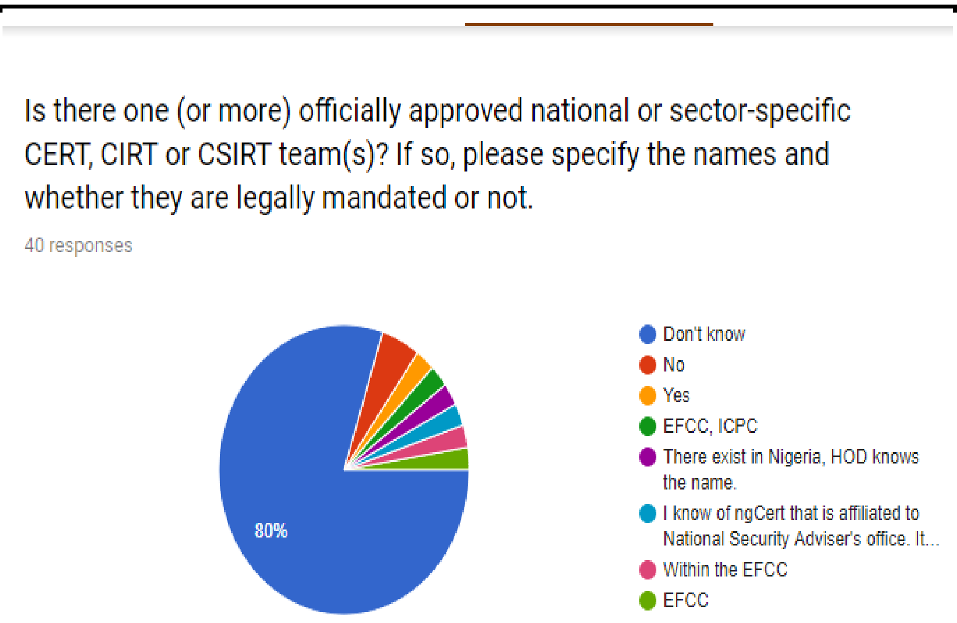


Is there any criminal legislation regarding cyber activities? If yes, specify using 'other'

40 responses

Figure 10: Statistics of respondents on criminal legislations

On regulations on Cyber security and compliance requirements, 72.5% were not aware of any registration on Cyber Security while 17.5% of the respondents were of the opinion that no such legislation exists. Asked if there were any officially approved national or sector-specific CERT, CIRT or CSIRT team(s) legally mandated in the country, 80% had no idea, 5% said there was none and 2.5% believed the teams were EFCC and Independent Corrupt Practices and other related offences Commission (ICPC) (Figure 11).



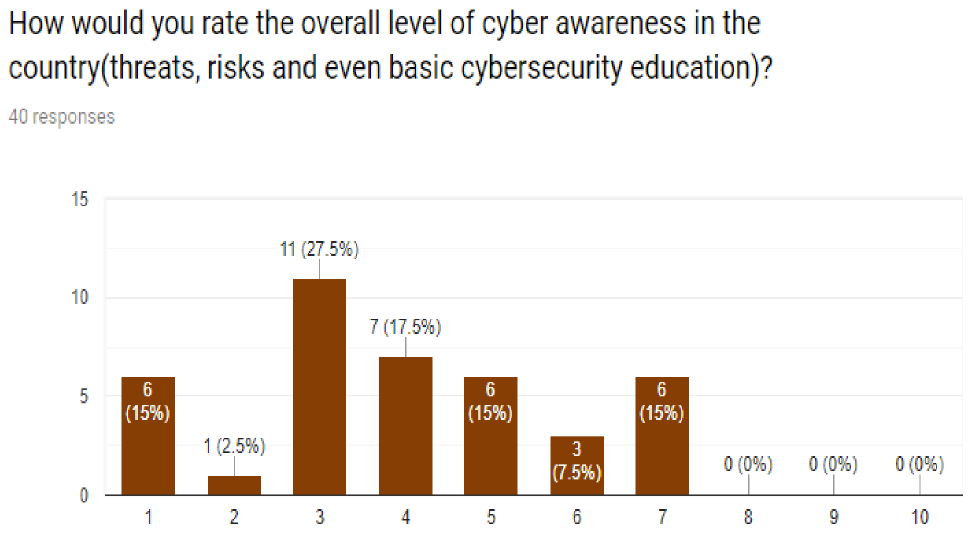
Is there one (or more) officially approved national or sector-specific CERT, CIRT or CSIRT team(s)? If so, please specify the names and whether they are legally mandated or not.

40 responses

80%
● Don't know
● No
● Yes
● EFCC, ICPC
● There exist in Nigeria, HOD knows the name.
● I know of ngCert that is affiliated to National Security Adviser's office. It...
● Within the EFCC
● EFCC

Figure 10: Statistics of respondents on criminal legislations

On if the current level of cyber awareness in the country will suffice given the current rate of cybercrimes worldwide, 42.5% of the respondents believed it would not.



How would you rate the overall level of cyber awareness in the country(threats, risks and even basic cybersecurity education)?

40 responses

Figure 10: Statistics of respondents on cyber security Awareness.

These results indicate clearly that a lot needs to be done in the way of cyber Security awareness in the country, even amongst company executives. It also shows why cybercrime is so prevalent in the country; the populace is mostly unaware of the existing cyber laws and sanctions in the country. As a result, they are quite convinced they can perpetrate all sorts of cybercrimes and get away with them. More disturbing however, is that some cyber criminals are actually not aware that their use of cyber space is indeed criminal and subject to punishment. Another angle to it is the fact that people (victims) have no idea who to report these crimes to or even how to access such authorities.

5.0 CONCLUSION

It is obvious from the results obtained from this study, that while a decent population of

Nigerians is aware of basic security issues, the larger populace has barely any knowledge of cyber security and its larger implications. This lack of knowledge can be seen as expressed in various areas of their internet practices and overall cyber hygiene. The study has also exposed how unaware Nigerians are of the existence of agencies responsible to handling issues of cyber security in the country, same for knowledge of the 2015 Cyber Security Act.

The implication of these findings is that the responsible agencies or relevant cyber security authorities in the country should increase general education and awareness training of the Nigerian population to the threats, laws and general hygiene of cybercrimes. This absolute lack of cyber security awareness should be a wakeup call to all those tasked with the responsibility of defending the country's cyber borders and space. The current hike in global cyber-crime/wars is enough for persons and agencies responsible for defending the Nigerian cyber space to wake up to the responsibilities of ensuring a healthy Nigerian cyberspace , given the numbers reflected in this study.

6.0 RECOMMENDATIONS

As indicated by the results of the study, it is quite apparent that the issues with cyber security perception in Nigeria are lack of awareness among the citizenry and lack of law enforcement/appropriate prosecution of cyber-crimes. Cyber Security enforcement Agencies and organizations should endeavor to regularly organize trainings for staff and carry out awareness campaigns on issues and trends in cyber security. The infusion of cyber security in the national educational curriculum starting from basic education would also help create awareness from the grass roots up.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. doi: 10.1126/science.aaa1465

CERT. (2008). Full Statistics of cert.org. Available from http://www.cert.org/stats/fullstats.html [accessed 11/01/2008]

Chai, W. (2021). Confidentiality, integrity and availability (CIA triad). Retrieved 14 September 2021, from https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Chandarman, R., & Van Niekerk, B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal Of Information And Communication*, (20), 133-155. doi: 10.23962/10539/23572

Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., & Adams, T. et al. (2011). Symantec Internet Security Threat Report trends for 2010. Retrieved 6 September 2021, from http://www.securityprivacyandthelaw.com/uploads/file/Internet%20Security%20Threat%20Report.pdf

Furman, S., Theofanos, M., Choong, Y., & Stanton, B. (2012). Basing Cybersecurity Training on User Perceptions. *IEEE Security & Privacy Magazine*, *10*(2), 40-49. doi: 10.1109/msp.2011.180

Ghosemajumder, S. (2017). You Can't Secure 100% of Your Data 100% of the Time. Retrieved 28 September 2021, from https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time

Huang, D., Rau, P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221-232. doi: 10.1080/01449290701679361

James Carder (2018). 2018 Cybersecurity: Perceptions & Practices, A Benchmark Survey of Security Professionals in the U.S., U.K., and Asia-Pacific Regions. Retrieved on September 3, 2019 from https://www.jassolution.com/document/LogRhythm/LogRhythm_Cybersecurity

_Practices_and-Attitudes_Benchmark_Study_2018.pdf

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal Of Computer And System Sciences*, *80*(5), 973-993. doi: 10.1016/j.jcss.2014.02.005

Kostyuk, N., & Wayne†, C. (2019). Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats. *UNIVERSITY OF MICHIGAN LIBRARY ONLINE JOURNAL*. Retrieved from http://www-personal.umich.edu/~nadiya/communicatingcybersecurity.pdf

Lawson, S., Yeo, S., Haoran Yu, & Greene, E. (2016). The cyber-doom effect: The impact of fear appeals in the US cyber security debate. *2016 8Th International Conference On Cyber Conflict (Cycon)*. doi: 10.1109/cycon.2016.7529427

Maisikeli, S. (2020). UAE Cybersecurity Perception and Risk Assessments Compared to Other Developed Nations. *2020 3Rd International Conference On Information And Computer Technologies (ICICT)*. doi: 10.1109/icict50521.2020.00075

Muhammad Ali Babar and He Zhang, 2009, "Systematic literature reviews in software engineering: Preliminary results from interviews with researchers" Conference: Proceedings of the Third International Symposium on Empirical Software Engineering and Measurement, ESEM 2009, October 15-16, 2009, Lake Buena Vista, Florida, USA. DOI:10.1145/1671248.1671281. https://www.researchgate.net/publication/221495038_Systematic_literature_reviews_in_software_engineering_Preliminary_results_from_interviews_with_researchers. Accessed on 12th June, 2021.

Nurse, J., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. *2011 1St Workshop On Socio-Technical Aspects In Security And Trust (STAST)*. doi: 10.1109/stast.2011.6059257

Pranas Zukauskas , Jolita Vveinhardt and Regina Andriukaitienė, Exploratory Research, Management Culture and Corporate Social Responsibility, Edition: 1st,Publisher: IntechOpen, April 2018,DOI: 10.5772/intechopen.70631.

Roopa S. and Rani MS, "Questionnaire Designing for a Survey" The Journal of Indian Orthodontic Society 2012, 46(4): 273-27, DOI: 10.5005/jp-journals-10021-1104. Accessed on 14th June, 2021.

Sjoberg, L., 2000. Factors in risk perception. Risk Analysis, 20, 1–11. A report on https://www.fbi.gov/news/stories/2015/october/national-cyber-security-awareness

Slovic, P. (2014). *The perception of risk*. Abingdon, Oxon: Earthscan from Routledge.

Smith, A. (2017). What the Public Knows About Cybersecurity. Retrieved 7 September 2021, from https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/

Sonali Shah (2014, March). Cyber Security Risk: Perception vs. Reality in Corporate America Retrieved on September 3, 2019 from https://www.wired.com/insights/2014/03/cyber-security-risk-perception-vs-reality-corporate-america/

Tom Gilheany (2017, March). It's Time to Change Your Perception of the Cybersecurity Professional. Retrieved on September 3, 2019 from https://www.securitymagazine.com/articles/ 87833-its-time-to-change-your-perception-of-the-cybersecurity-professional

Tony Bradley (2017, March 9). Exploring the Gap between Cybersecurity Perception and Reality. Retrieved on September 3, 2019 from https://www.forbes.com/sites/tonybradley/ 2017/03/09/ exploring-the-gap-between-cybersecurity-perception-and-reality/#59db39d8172a

X. Liu, Y. Zhang, B. Wang, and J. Yang, 2013 "Mona: Secure multi owner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191