SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL8 No2
JUNE 2024

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 8(2): 1 – 7 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

THE CYBER CRIMINOLOGICAL PERSPECTIVE OF PUBLIC VIGILANTISM CASES ON SOCIAL MEDIA CONCERNING THE RIGHT TO LIFE IN SOUTH AFRICA

Rantho Fortunate Dolly, Sithuga Ndivho Percy
Department of Criminal Justice. School of Law, University of Venda

ABSTRACT: Vigilantism is one of the most life-threatening events faced by people who are accused or suspected of committing crimes and witchcraft. The victims of vigilantism are mostly killed before the police can arrive to rescue them, violating their Constitutional right to life. Communities in South Africa resort to taking the law into their own hands because they feel that the justice system is failing them, and this is the only way they can protect themselves against crime and witchcraft. This article looks at the cyber criminological perspective of public vigilantism cases on social media concerning the Constitutional right to life in South Africa. This study estimates that Vigilantism will continue to be a problem if it is not addressed and people will continue to lose their lives, even innocent ones. This study applied the qualitative approach to collect data and aims to help community members to understand their shortcomings and assist them in coming up with solutions to avoid taking the law into their own hands.

KEYWORDS: *Vigilantism; Victims; Constitutional rights; vigilante, social media*

1.0 INTRODUCTION

Social media has now become one of the contributing factors towards public vigilantism in South Africa. The study focused on vigilantism at large and how social media is used to spread ideas of public vigilantism and its *modus operandi* which results in the violation of the constitutional right to life. In South Africa, many communities seem to believe that vigilantism is the only way to prevent crime and deter other criminals from committing crimes without having an understanding that this is a violation of the Constitution and a violation of the victim's rights, suspects are deemed not to have rights and are not given an ear to tell their side of the story even previously (Jung et al, 2020).

Vigilantism is not a practice that has just recently been practiced, but it has however existed for years and years from the 1930s to 1990s when certain structures were introduced to reduce the occurrence of crime, such as (Mapogo a Mathamaga, People against gangsterism "PAGAD", and the Makgotla (Cupido, 2021). These structures were established because people did not have faith in the Western Justice system back then and even today, mob justice occurs because the public does not have faith in the Justice system. Mob justice is a problem that is experienced by provinces all over South Africa (Geldenhuys, 2020).

According to Hunter, 2021, people who are usually victims of this public vigilantism are young men and women who in most cases are always accused of witchcraft and crimes such as theft, murder, rape, and gang involvement, furthermore, most of them are "nyaope" addicts (Hunter, M., 2021). Incidents of public vigilantism continued to escalate after apartheid; this was argued by a researcher, Cupido, 2021. During the apartheid era, the police focused more on protecting the white families, and at the same time, they were enforcing the apartheid policies and rules while ignoring the safety of black people."

Due to the lack of proper policing, it has resulted in an increased rate of gang-related crimes, murder, and theft because the criminals knew that there were very low "chances of them being caught and prosecuted (Cupido, 2021). This contributed to the occurrence of vigilantism even more because communities needed to protect themselves from crime, as the police were failing them. The victims are hunted down by the community based on the suspicion they have about committing the crime, and then

they are attacked, whereas some are caught in the act, and they are attacked on the spot (Kucera & Mares, 2015).

South Africa is now known to be one of the most violent countries in Africa and in the World due to the figures of crime reported. In 2017-2018, South Africa reported 20 336 murders, of which 849 of them were a result of vigilantism (Republic of South Africa, 2018). An average of 2 lives is claimed daily because of vigilantism in South Africa, this was revealed by a report where the Institute for Security (IIS) conducted an in-depth analysis of SAPS crime statistics reports (Lancaster, 2019).

2.0 RESEARCH METHODS/ METHODOLOGY

This study applied the qualitative approach to get the cyber criminological perspective of public vigilantism cases on social media concerning the right to life in South Africa. This methodology further enabled the researchers to gain more information and understand to establish the effects of social media and public vigilantism on Constitutional rights in South Africa. According to Neuman (2011), qualitative research refers to inductive, systematic, analytical, and process-oriented approaches for understanding, analyzing, explaining, and creating a phenomenon or setting theory. A qualitative approach seeks to achieve a thorough understanding of the views of the respondents (Eyisi Daniel 2016). An exploratory research design was used in this research. Research design is done to gain new insights, discover new ideas, and increase knowledge of the phenomenon (Inaam Ikhtar,2016). Research design is a plan that guides the researcher through the research process. To obtain data for this study, case studies and different articles based on vigilantism were utilized together with research that had been previously conducted by other researchers.

3.0 LITERATURE REVIEW

3.1 social media

According to Manning (2014), social media is what people use to interact with each other from different parts of the world about different phenomena and it goes beyond the sharing of information compared to how media was in the past. Social media is about communicating and updating each other through statuses, texts, videography, photos, and blogs on applications such as Facebook, Twitter, and websites like LinkedIn to name one, this was said by Alejandro (2010). Gilboa (2009) further added that socials have created a way for what is called “unprecedented interactivity” which allows people to have many different sources of what is trending and some of these sources are just simple sources such as the posting of texts and videos.

It is because of social media that the geographical barrier which was there for the longest time has been broken and people are able to network easily despite the location of a person. We now have “citizen journalists” that make use of advanced electronics and popular apps to report on events taking place (Alejandro 2010; Gilboa, 2009).

The new media does not only bring revolution to the reporting of news globally, but it is also the speed it has on circulating information and how fast that information gets to a very big audience (Aslam, 2014). Due to this, Alejandro (2010) describes the new media as the “web” that has brought change to the world and revolutionized how information is saved, published, looked for, and how it is used. According to her, the resourcing of news has grown and evolved from the pre-satellite era when it was still dependent on print media to the electronic media era.

Vigilantism and social media both employ activities, actions, and inactions of people from different aspects of life and that is what they have in common. While the former is defined by the wrongdoers, the latter is defined by those who make use of it. In both, the active roles of the people who make things happen cannot be overestimated. Social media can spread any type of information, including that of vigilantism. It is easy for people to take part and it is increasing because of the simplicity of journalistic activities involved (Alejandro, 2010).

The news which social media brings about vigilantism is always up to date, and it is things which are occurring or have recently occurred. This corresponds with the explanations of the cognitive process model's accessibility principle. According to the in-depth interview and focused group discussion (2017), the users of media platforms such as WhatsApp and Facebook say their major source of information on public vigilantism attacks is social media. The users of social media can comment on their minds and give their judgements at any given time because it is easy to do so even from far.

The realisticness of the construct, as described by the cognitive process model, explains why social media has contributed to the spread of vigilantism on a larger scale. Busching, Allen and Johnie (2016) are of the opinion that posting and circulating violent content is more of the same as prevalent as the media itself. The sharing of recordings, pictures and videos which are expressed openly without altering opinions that may bring shock based on vigilantism makes the event to be more memorable to the viewers and this contributes to them recognizing the existence of such doings and they may also resort to vigilantism if faced with a similar situation. This reflects as the reality of how things are happening and should be done to those who are sharing and their followers. Because of this, Mengu and Mengu (2015) argue that social media is essential for learning social practices and what is deemed as reality out there. There is a possibility of people starting to behave aggressively and violently with little empathy for the victims of vigilantism due to the content which they have observed on the socials. As for those who are not able to be physically there when vigilantism takes place, social media has given them the platform to participate online by giving aggressive opinions and violent comments. This was described as "cyber aggression" by Busching Allen and Anderson (2016) and they emphasized that aggressive behaviour is not necessarily limited to being physical.

Vigilantism is now a global concern as the media has exposed it to be beyond South Africa, but also an international problem. Concerns have now shifted from the perspective that failure of the justice system is the one giving rise to the increasing of public vigilantism, and social media is now one of the aspects giving rise to mob justice, despite its positive functions. People are now able to be a group of vigilantes online and say they are trying to bring justice.

3.2 Right to life

Section 11 of the Constitution of the Republic of South Africa stipulates the right to life to every person "and it is an unqualified right which cannot be limited even in an emergency state. Ubuntu is not only undermined by the occurrence of vigilantism in the black townships of South Africa, but it has been a major concern amongst Africans. In Limpopo Mashishimale outside Phalaborwa, reported by an article titled 'Suspects killed in front of cops' whereby the vigilantes hunted down, severely beaten, and stoned to death two males who used to disguise themselves by wearing female clothes to rob people. The police were not able to stop the mob due to the anger they had. Two people who robbed many belongings and were suspects on the killing of an old man aged 57 were also killed by the mob (AENS 2014). A revelation of a traumatized nation is shown through its uncontrollable anger in which people are still cruel even in the presence of the police.

In Khayelitsha another incident took place whereby the residents did not pity an alleged phone robber. The mob was not satisfied as the person managed to escape but they ran after him, caught him, and stabbed him till his demise (Lali 2014). This vigilantism is taking place in a country whose democratic constitution admires, views and endorse human life highly, which makes it shocking to believe that it is South Africa. Ncayiyana believes that until today, in South Africa, "termination of a person's life is unlawful, even if such is done to prevent the person from suffering and the person requests that their suffering should be put to an end where the suffering person has expressed a wish to die has even begged to be killed" (Ncayiyana 2012).

There is evidence which is sufficient e.g. (AENS 2014; Brodhead 2013; Golbaum 2014) to assist in proving the fact that mob justice system in this country resulted in the loss of many lives. People took the law into their own hands due to the poor justice system" of the country; "they've lost faith in the justice system. Crime rate in South Africa is increasing rapidly into a range in which victims fight for themselves because they think that they don't have any other choice. 'I am because we are' the element

of Ubuntu is being misused by some South Africans who plan or plot to commit crime and this is the bad side of Ubuntu's discourse and beliefs. In Port Elizabeth Angelina Maholwana felt that justice has been served after seeing the dead bodies of two young men who broke into her home, killed her son, and even tried to rape her (Jazzie 2014). 'I know that killing these boys will not bring back my son, but I sleep better knowing these boys will not hurt anyone again'. The lady was pleased with what the mob justice did as revenge for what they did to her son. All of this is not acceptable as it results in pitiful situations whereby innocent people may be killed, violating their Constitutional right to life. With that being said, the right to be presumed innocent until proven guilty is the next right to be discussed with is violated by vigilantism."

4.0 RESULTS AND DISCUSSIONS

4.1 Lack of trust in the justice system

The South African citizens are having insecurities that the justice system is not giving them justice against the criminals who steal, rape, rob, murder, and perpetrate other criminal activities. The justice system is responsible for the effectiveness of crime reduction and if it is failing, communities end up taking the law into their own hands (Mbiada & Sithuga, 2023). Some communities have taken the initiative of forming CPF'S (Community Policing Forums) which aim to deter crime by working hand in hand with the police. This is one of the best ways in which the community and the police can work together and build a good relationship which aims to fight crime. If every person is willing to assist and tell the police about any criminal activity, then it will be easier to fight crime.

4.2 Community beliefs on witchcraft

The practice of witchcraft is recognized as wicked, and it is against the Christian religion (Ally, 2015). In spite the fact that witchcraft has its roots in historical discussions, the practice still subsists, especially in rural communities globally (Gottschalk; Adnikrah, 2015). According to Ally (2015) the thought of zombies or "tokoloshe's" are trusted to have been created by witches and it is commonly a belief in South Africa. This is because witchcraft is assumed to portray tragedy. In this case the zombies are anticipated to be sent by witches to cause misery, such as sickness, collision, and loss of life (Ally, 2015). Grounded on substring literature, victims of witchcraft appear to have a gender element against women, mainly elderly who are constantly indicted based on their physical characteristics (Meel, 2009).

4.3 Rise in xenophobia

Masenya (2017), and Sebola (2017), and debated on occurrence of xenophobia. Due to the reason that attacks, and hatred are repeatedly directed to Africans than other racial groups, the researchers argued that the term Xenophobia must be changed to Afrophobia (Ndinda & Ndlovhu, 2016). However, Bangladeshis and Pakistanis were also being attacked as other Africans, this was argued by other researchers (Sebola, 2017). In South Africa there has been an outburst of violence against foreigners from countries such as Nigeria, Mozambique, and Zimbabwe. The killings of foreigners through vigilantism, harassment by the police and discrimination increased day by day (Wose Kinge, 2016). The misunderstanding about foreign nationals by the citizens in the townships and rural areas possess a recognition that foreigners are the main reason for the lack of job opportunities, the rise in crime, and the spread of AIDS (Hove, 2017). In this manner, xenophobia has brought a culture in which Africans recognize another black person as a threat Other South Africans have been attacked because of discrimination because of their dark skin color (Masenya, 2017). Corrective violence or hate crime can be referred to as attacks on foreigners by vigilantes, as it involves showing disapproval for other individuals' attributes by taking matters into their own hands (Munusamy, 2015).

5.0 CONCLUSION AND RECOMMENDATIONS

Based on the findings, it seems that public vigilantism is a pandemic in South Africa. The police and communities fail to build a working relationship, leading to more cases of people taking the law into

their own hands, violating the Constitutional rights stipulated in the Constitution of the Republic of South Africa. Public Vigilantism is one of the factors that result in the high crime rates of murder and attempted murder, therefore it needs to be addressed before it can be normalized by citizens.

The following recommendations are given based on the above findings of the study:

5.1 More resources for South African Police Services(SAPS)

The South African Police Service has a challenge of not having enough resources and in most cases when vigilantism occurs, the police arrive late at the scene because they did not have a police van that they could use to come and attend the matter. If the government could ensure that the SAPS has enough resources, then vigilantism can also be prevented in time and the lives of the victims could be saved.

5.2 Establishment of awareness campaigns

Establishing awareness campaigns is one of the measures that can be taken to educate communities about vigilantism and how it affects constitutional rights. The platform can also be used to make awareness of the rights that people have which are stipulated in the Constitution of the Republic of South Africa. These campaigns will give people a chance to voice out their views and new ways of preventing vigilantism can be developed.

5.3 Motivating the youth to participate in crime prevention

The youth are very important people in the community as they are the future. Involving them in crime prevention will give them interest and knowledge of fighting crime. If the youth get equipped with enough knowledge about vigilantism and its negative impacts, public vigilantism can be prevented even in the coming generations and we will be raising a generation that does not believe in taking the law into their own hands and upholds the Constitution.

5.4 Educate children about the law from the high school level

Another way to prevent public vigilantism is through inventing a subject that educates children in high school about the law and the Constitution precisely. The same way children are taught life orientation can be the same way they are taught about the law or the law can be added to the scope of life orientation so that children can have basic education about the supreme law of the country.

5.5 The government must invest in the measures put in place to prevent vigilantism

All the measures that are established to prevent public vigilantism will need funding to carry them out. The government must be willing to fund these measures to stop public vigilantism and to send a strong message that it is against the acts of vigilantism.

5.6 Educate people about the damage social media can cause

Many people use social media and although it has some good benefits of building people and growing their businesses, it can also be used to cause vigilantism as people post and share incidents of vigilantism while promoting it. In a nutshell, people need to be educated about the damage they are doing by promoting public vigilantism on social media.

REFERENCES

AENS, ‘Suspect killed in front of cops’, Daily Sun, p. 4, 2014.

Alejandro, J. Journalism in the Age of social media. Oxford, England: Reuters Institute for the Study of Journalism, University of Oxford, 2010.

Ally, Y. "Burn the witch": The impact of fear of witchcraft on social cohesion in South Africa. Port Elizabeth Pins 49. Nelson Mandela Metropolitan University, 2015. doi: http://dx.doi.org/10.17159/2309-8708/2015/n49a3

Busching, R., Allen, J. J. & Anderson, C. A. Violent Media Content and Effects, 2016. DOI: 10.1093/acrefore/9780190228613.013.1

Cupido, A.C., The development of vigilantism in South Africa (Doctoral dissertation, Stellenbosch: Stellenbosch University), 2021.

Eyisi Daniel,. The usefulness of qualitative approach and methods in research problem solving ability in science and education curriculum. Journal of education and practice, vol7, no15, pp92, 2016.

Geldenhuys, K., Mob justice serves no justice at all. ServiceCommunity-based Safety and Security Magazine, 113(11), pp.10-15, 2020.

Gilboa, E. Media and Conflict Resolution: A Framework for Analysis. Marquette Law Review, 93(1), 86-110, 2001.

Gottschalk, K. Vigilantism v. the State: a case study of the rise and fall of PAGAD 1996-2005. Pretoria: Institute for Security Studies, 2005.

Hove, M. When tears become a language: frictions in a xenophobic national 'imaginary'. Journal of Transient Migration, 1(1):112-117. DOI: 10.1386/tjtm.1.1.117_1, 2017

Hunter, M. Intimate crimes: heroin and the rise of amaphara in South Africa. The Journal of Modern African Studies, 59(1), pp.59-79, 2021. DOI: https://doi.org/10.1017/S0022278X20000658[Opens in a new window]

Inaam Ikhtar, Research Design September 2016 in book: Research in Social Science: Interdisciplinary Perspectives (pp.17) Edition: 1stChapter: Research DesignPublisher: Social research foundation, Kanpur, India, 2016.

Jazzie, Is necklacing returning in South Africa? viewed 16 October 2014, from http://www.whatishappeninginsouthafrica.blogspot.co.za

Jung, Danielle F, and Dara Kay Cohen. Lynching and Local Justice: Legitimacy andAccountability in Weak States. Cambridge: Cambridge University Press, 2020.

Kucera, M., & Mares, M. Vigilantism during demographic transition. Policing and Society, 25(2), 170-187. doi:10.1080/104394463.2013.8117997, 2015

Lali, V., 'No mercy for cellphone robber', Daily Sun, 14 July, p. 4. 2014.

Lancaster, L. At the heart of discontent: measuring public violence in South Africa.Retrieved April 20, 2017, 2016. from https://issafrica.s3.amazonaws.com/site/uploads/Paper292.pdf.

Manning, J. Social Media, Definition and Classes of. In K. Harvey, (Ed.) Encyclopedia of social media and Politics (pp. 1158-1162). Thousands Oak, CA: Sage, 2014.

Masenya, M. J. Afrophobia in South Africa: a general perspective of xenophobia. Bangladesh Sociological Society, 14(1):81-88, 2017. https://doi.org/10.1177/09750878221079803

Mbiada, C.J.T. and Sithuga, N.P., Does mob justice fit the conceptual theory of justice? International Journal of Research in Business and Social Science (2147-4478), 12(5), pp.395-401, 2023. DOI: https://doi.org/10.20525/ijrbs.v12i5.2424

Meel, B. M. Witchcraft in Transkei Region of South Africa: Case Report 9 (1):61-64. African Health Sciences, Kampala: University of Walter Sisulu, 2009.

Mengu, M. & Mengu, S. Violence and social media. Athens Journal of Mass Media and Communication, 1(3), 211-228. DOI: 10.30958/ajmmc.1-3-4, 2015.

Munusamy, R. South Africa: the place of shame, violence and disconnect. Retrieved June 31, 2018, from 2015 https://www.dailymaverick.co.za/article/2015-04-17-south-africa-the-place-of-shame-violence-and-disconnect/

Ncayiyana, D.J., 'Euthanasia – No dignity in death in the absence of ethos of respect for human life', The South African Medical Journal 102(6), 334. PMID: 22668890. doi: 10.7196/samj.6001, 2012.

Ndinda, E., & Ndlovhu, T. P. Attitudes towards foreigners in informal settlements targeted for upgrading in South Africa: a gendered perspective. Agenda, 30(2):131-146, 2016 DOI: 10.1080/10130950.2016.1212598

Neuman, W.L. Social Research Methods: Qualitative and Quantitative Approaches. 7th Edition, Pearson, Boston, 2011. DOI: 10.2307/3211488

Sebola, M. P. Xenophobic attitudes against immigrants and cheap political talks: sitting time bombs and explosives in South Africa. Bangladesh Journal of Sociology, 14(1): 89-103, 2017.

South African Police Services. Annual crime report. Retrieved October 22, 2019, from 2018, https://saps.gov.za

Wose Kinge, G. T. International dimensions of xenophobic attacks on foreign nationals in South Africa. Dissertation in Social Science, Potchefstroom: University of North-West, 2016.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(2): 8 – 18 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

BERT-BASED DETECTION OF CYBERBULLYING IN ONLINE TEXTS

Amrutha Muralidhar
B. M. S College of Engineering, Bangalore, India

ABSTRACT: Social media has experienced exponential growth in recent years, becoming integral to daily communication and interaction. However, along with this growth, cyberbullying has emerged as a significant issue, causing harm and distress to individuals online. This paper investigates the effectiveness of utilizing BERT-based models for identifying cyberbullying behavior in online text. A BERT classifier was trained on a labeled dataset containing instances of cyberbullying and assessed for its performance in accurately detecting such behavior. Results indicate that the BERT classifier achieves a strong accuracy rate of 94% on the test dataset. These findings suggest the potential of BERT-based models in bolstering online safety efforts and combating cyberbullying. The aim of this study is to contribute to the advancement of tools aimed at fostering digital well-being and cultivating safer online communities.

KEYWORDS*: Cyberbullying, Online Safety, Sentiment Analysis, Deep Learning, Text Classification*

1. INTRODUCTION

The social media landscape has undergone a seismic shift in recent years, witnessing unprecedented growth and becoming an indispensable aspect of daily life for millions worldwide. With over 62% of the world's population actively engaged in social media platforms (Petrosyan, 2024), these platforms have become integral to modern communication and social interaction.

Among its diverse user base, a significant contingent comprises children and adolescents, who leverage social media for communication, entertainment, and social interaction. Platforms like Instagram and Snapchat are particularly popular among young adults under 30 (Auxier & Anderson, 2021), revolutionizing interpersonal communication and providing novel avenues for connectivity and community engagement.

While the proliferation of social media offers myriad benefits in facilitating connections and fostering community, it also brings to light critical challenges, the most important of which is the occurrence of cyberbullying. Defined as the use of electronic communication to harass, intimidate, or demean others, cyberbullying poses a significant threat to the psychological well-being of young individuals navigating the digital landscape. Studies have underscored the alarming correlation between extensive social media use and increased vulnerability to cyberbullying victimization, emphasizing the urgent need for proactive intervention strategies (Craig et al., 2020; Horner et al., 2015). Research indicates that cyberbullying victimization rates vary widely, ranging from 5.3% to 66.2% for perpetration and 1.9% to 84.0% for victimization (Camerini et al., 2020).

On April 15th, 2020, United Nations Children's Fund (2020) issued a warning in response to the increased risk of cyberbullying during the COVID-19 pandemic due to widespread school closures, increased screen time, and decreased face-to-face social interaction. The statistics of cyberbullying are outright alarming: 36.5% of middle and high school students have felt cyberbullied and 87% have observed cyberbullying, with effects ranging from decreased academic performance to depression to suicidal thoughts.

In addition to cyberbullying, the spread of hate speech on social media platforms poses a serious threat, increasing the potential harm that can be done to vulnerable individuals. Though most platforms promote transparency and freedom of speech, the unrestrained spread of hate speech can worsen mental health conditions and prolong social divisions by creating a toxic online atmosphere (Calpbinici et al.,

2019). Ganson et al. (2024) analyzed data from 12,031 adolescents across six countries, finding that increased weekday screen time and use of various social media platforms were associated with higher prevalence of weight-related bullying victimization. Each additional hour of social media was linked to a 13% increase in bullying, with Twitter use showing a 69% increase. Their findings show the significance of addressing social media bullying among adolescents.

Various forms of online conduct, such as insults, threats, harassment, exclusion, and mockery, are indicative of the prevalence of cyberbullying. These forms of cyberbullying can manifest through text-based communication on social media platforms, messaging apps, and online forums. For instance, individuals may resort to insults and name-calling, such as calling someone derogatory names or belittling their character. Threats can take the form of intimidating messages, where individuals express intent to cause harm or distress. Harassment involves persistent and offensive communication aimed at causing emotional harm. Exclusion occurs when individuals purposefully exclude others from online interactions or communities, leading to feelings of isolation. Mockery involves ridiculing or mocking someone's appearance, intelligence, or behavior. Figure 1 illustrates the various forms of cyberbullying, which can have detrimental effects on the psychological well-being of individuals.

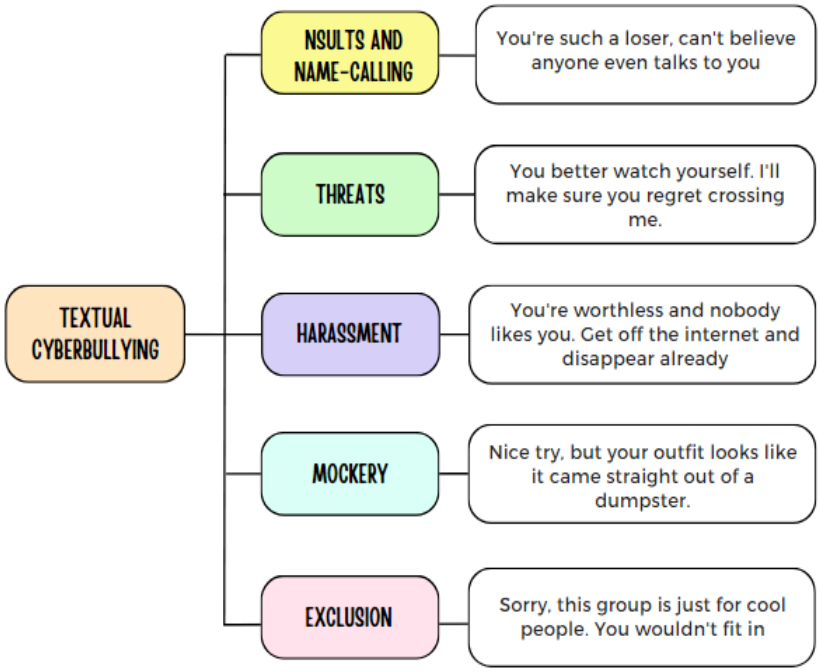

Fig 1. Forms of Cyberbullying

Unlike traditional bullying, which predominantly unfolds in physical spaces like schools, cyberbullying breaches geographical and temporal constraints, reaching victims at any time through their digital devices (Horner et al., 2015). The detrimental effects of cyberbullying on the emotional and psychological well-being of young individuals are well-documented, leading to anxiety, depression, low self-esteem, academic underperformance, and even suicidal ideation. To address this issue, we propose automating text analysis for cyberbullying detection on online platforms. Our research aims to answer the following questions:

R1: How to effectively identify patterns indicative of cyberbullying behavior?
R2: How accurate can we be in distinguishing between normal online interactions and cyberbullying instances?

In response to the escalating prevalence and impact of cyberbullying, we propose automating text analysis for cyberbullying detection on online platforms using a BERT based model. Through this research, we aim to cultivate safer online environments for youth and mitigate the adverse impacts of

digital harassment. By addressing these research questions, we strive to advance our understanding of cyberbullying detection and contribute to the development of effective preventive measures and interventions.

To address these questions comprehensively, this paper is structured as follows: Section 2 provides a review of existing literature and related work. Section 3 delineates the methodology employed in this study, encompassing the utilization of advanced classifiers such as LSTM with attention, Naive Bayes, and BERT. Section 4 offers a detailed exposition of our experimental results, evaluating the performance of each classifier against established benchmarks. Subsequently, in Section 5, we engage in a nuanced discussion of our findings, exploring their implications and potential avenues for future research. Finally, Section 6 encapsulates our conclusions, summarizing key insights and delineating the significance of our contributions to the broader discourse on cyberbullying prevention and mitigation strategies.

2. RELATED WORK

The proliferation of social networks and microblogging platforms has significantly increased instances of "cyber" conflicts and hate speech, posing considerable challenges for online moderation. Despite regulations prohibiting hate speech on most online platforms, the sheer volume of content makes manual moderation impractical, necessitating automated detection and filtering mechanisms. However, existing approaches to detecting cyberbullying and hate speech have shown varying levels of effectiveness, leaving room for improvement in terms of accuracy and efficiency.

One approach to addressing this gap is the Lexical Syntactic Feature (LSF) architecture proposed by Chen et al. (2012), which aims to identify potentially offensive individuals and content on social media. Their framework incorporates pejoratives, profanities, and syntactic rules to predict users' potential to send out offensive content based on writing style and specific cyberbullying content. While this approach offers insight into individual behaviors, it may not capture the full spectrum of offensive language and context present in online texts.

Özel et al. (2017) conducted a study aimed at detecting cyberbullying in Turkish social media messages. They employed information gain and chi-square feature selection methods to enhance classifier accuracy. Their findings indicated that considering both words and emoticons as features improved cyberbully detection accuracy, with Naïve Bayes Multinomial exhibiting the highest classification accuracy among the classifiers tested. Feature selection further improved classification accuracy up to 84%.

Martins et al. (2018) found that incorporating emotional information from text significantly improved the accuracy of hate speech detection. Their research demonstrated a precision rate increase from 41% in previous studies to 80.64% in their tests. However, their study did not address user characterization or the potential use of coding to circumvent anti-hate speech policies and detection systems. Watanabe et al. (2018) proposed an approach to detect hate expressions on Twitter, using unigrams and patterns collected from a training set. Their method achieved an accuracy of 87.4% in binary classification (offensive or not) and 78.4% in ternary classification (hateful, offensive, or clean).

Basak et al. (2019) categorized shaming tweets into six types and developed a classification system to identify shamers and nonshamers. Their findings revealed that most users participating in shaming events were likely to shame the victim, and shamers experienced faster growth in follower counts compared to nonshamers. Rodríguez, Argueta, and Chen (2019) proposed an approach to automatically detect hate speech on Facebook, employing graph analysis, sentiment analysis, and emotion analysis techniques to identify pages promoting hate speech and uncover associated topics.

Yadav et al. (2020) utilized contextual embeddings to generate task-specific embeddings for classification. They trained and evaluated their BERT model on two social media datasets. Roy et al. (2020) utilized tweet text with GloVe embedding vectors to capture semantic information, achieving precision, recall, and F1-score values of 0.97, 0.88, and 0.92, respectively.

Zhou et al. (2020) presented a study exploring fusion techniques of ELMo, BERT, and CNN text classification methods to enhance hate speech detection performance. Their results demonstrated improved classification accuracy.

Alam, Bhowmik, and Prosun (2021) developed ensemble-based model for classifying content into offensive and non-offensive categories. Akter et al. (2022) introduced machine-translated data to address data unavailability issues and evaluated various deep learning models' performance, like LSTM, BiLSTM, LSTM-Autoencoder, word2vec, BERT, and GPT-2. Their study showcased the effectiveness of the BERT model on both semi-noisy and fully machine-translated datasets.

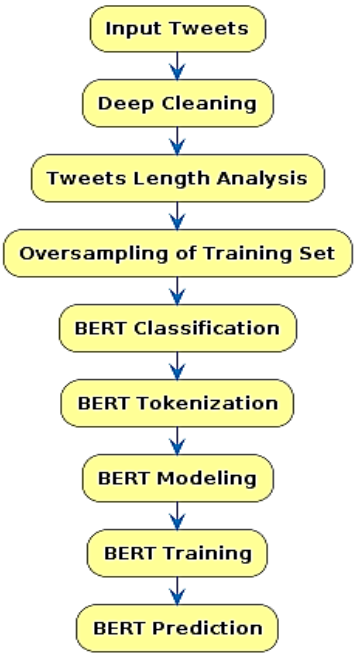

Fig.2 *Methodology Flowchart*

3. METHODOLOGY

This section outlines our methodology its flowchart is depicted in ***Fig.2***.

3.1. Data Preprocessing and Cleaning

The process is crucial for removing noise and irrelevant information, thus enhancing the effectiveness of subsequent classification algorithms, the flowchart is shown in ***Fig.3***. The following functions were applied for data preprocessing:

1. **Emoji Stripping:** Emojis were removed from the text using regular expressions to eliminate non-textual elements that may not contribute to the classification process.
2. **Contractions Expansion:** Contractions were expanded to their full forms to standardize the text and improve consistency in language usage.
3. **Language Filtering:** A language detection algorithm was applied to filter out non-English tweets, as the analysis focuses on English language text. This step ensures that only relevant data is considered for cyberbullying detection.
4. **Entity Stripping:** Various entities such as URLs, mentions, and non-ASCII characters were removed from the text to eliminate noise and irrelevant information.
5. **Hashtag Cleaning:** Hashtags were processed to remove redundant '#' symbols and hashtags occurring at the end of sentences, while retaining those occurring within the text.
6. **Character Filtering:** Special characters such as '$' and '&' present within words were filtered out to ensure uniformity in text representation.
7. **Whitespace Removal:** Extra whitespaces were removed from the text to improve readability and consistency.
8. **URL Shortener Removal:** Shortened URLs commonly used in tweets were removed to prevent misleading information.
9. **Numeric Removal:** Numeric characters were removed from the text to focus solely on textual content.
10. **Word Lemmatization:** Words were lemmatized to reduce inflectional forms and variants to their base or dictionary form, aiding in feature reduction and normalization.
11. **Short Word Removal:** Short words were filtered out from the text to eliminate noise and improve the relevance of the remaining words for classification.

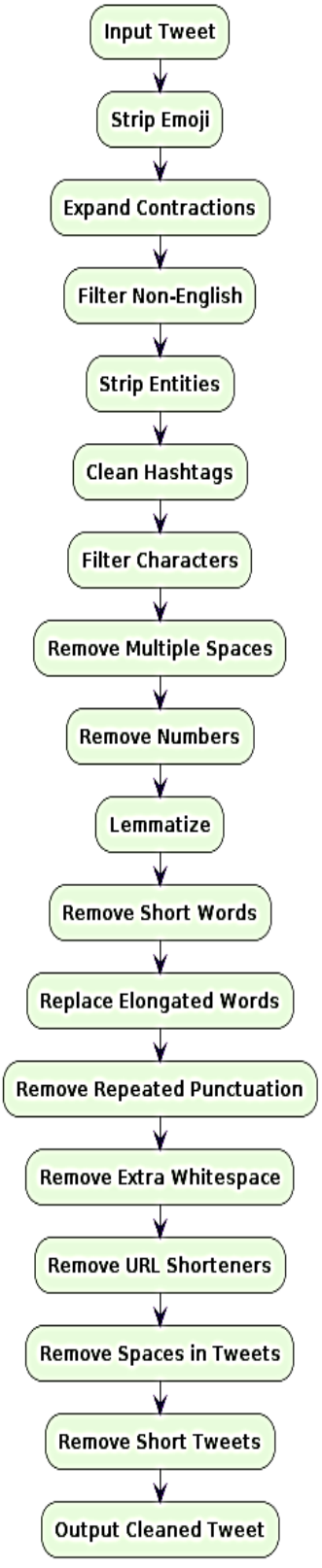

Fig.3 *Deep Cleaning Process*

12. Elongated Word Replacement: Elongated words, characterized by repeated letters, were replaced with their base form to standardize the text representation.

13. Repeated Punctuation Removal: Redundant punctuation marks were removed to enhance readability and simplify text representation.

14. Tweet Length Filtering: Short tweets containing fewer than a predefined number of words were removed to ensure an adequate amount of textual content for analysis.

This cleaning process can be summarized as follows:

$$\text{Cleaned Tweet} = f_{14}\left(f_{13}\left(\ldots f_2\left(f_1(\text{Raw Tweet})\right)\ldots\right)\right)$$

where □□ represents each cleaning function applied sequentially to the raw tweet.

3.2. Tweet Length Analysis and Oversampling

The examination of the class distribution showed that there was an imbalance among the classes as shown in ***Fig.4***, meaning that some have fewer occurrences than others. Oversampling approaches are used to rectify this imbalance and avoid bias towards the dominant class during model training. Oversampling involves randomly duplicating instances from the minority classes or generating synthetic instances to balance the class distribution. In this study, we opted to oversample the training set such that all classes have the same count as the most populated one.

The oversampling process can be represented mathematically as follows: Let □ be the desired count of instances for each class, and □ be the number of classes. For each class □, where □ = 1, 2,.., □, we calculate the oversampling factor □□ as:

$$F_i = \frac{N}{n_i}$$

Where □□ represents the current count of instances for class □. Then, for each class □, we randomly select instances from the original dataset to achieve the desired count □ using the calculated oversampling factor □□. This process is repeated until all classes have the same count of instances.

After oversampling, the class distribution is rebalanced as shown in ***Fig.5***, ensuring that each class contributes equally to the training process. This mitigates the risk of model bias towards the majority class and improves the overall performance of the classification model.

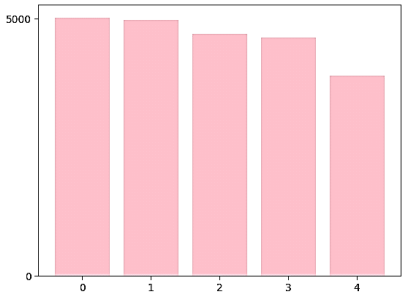

Fig.4 *Class Distribution before oversampling*

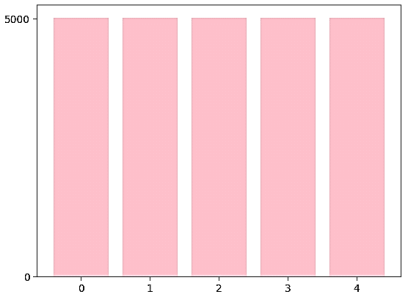

Fig.5 *Class Distribution after oversampling*

3.3. BERT Classification

We loaded a pre-trained BERT model and fine-tuned it on our sentiment classification task. This classification process is shown in ***Fig.6*** To enable reliable model assessment, the dataset was divided into training, validation, and test sets. Gradient descent optimization was then used to optimize the BERT model's parameters. This can be represented as the process of updating the parameters □ of the pre-trained BERT model using gradient descent optimization:

$$\theta_{fine-tuned} = \text{argmin}_{\theta} \sum_{i=1}^{N} \text{L}oss(\text{B}ERT(X_i), y_i)$$

where Loss represents the cross-entropy loss, □□ denotes the input data, □□ represents the corresponding true labels, and □ is the number of samples in the training set. Cross-entropy loss measures the dissimilarity between the predicted probability distribution (output of the model) and the true probability distribution (ground truth labels). This can be expressed as:

$$CrossEntropyLoss = -\frac{1}{N} \sum_{i=1}^{N} \sum_{c=1}^{C} log(p_{i,c}) (y_{i,c})$$

Where:

- □ is the number of samples in the dataset.
- □ is the number of classes.
- □□,□ is a binary indicator (0 or 1) of whether sample □ belongs to class □.
- □□,□ is the predicted probability that sample □ belongs to class *c* according to the model.

3.4. BERT Tokenization

In the tokenization process shown in ***Fig.7***, the dataset was initially split into training, validation, and test sets to facilitate subsequent model training and evaluation. A custom tokenizer function was utilized to tokenize the raw textual data into sequences of tokens. To ensure focused attention during model training and inference, attention masks were generated to differentiate between actual tokens and padding tokens. To ensure uniformity throughout the dataset, the longest tokenized tweet is used to determine the maximum token length.

3.5. BERT Modelling

In the BERT modeling phase, we construct a custom BERT classifier tailored to our sentiment classification task. This involves designing a model architecture that combines the power of BERT's transformer layers with additional dense layers for classification. The custom BERT classifier comprises a pre-trained BERT model, which serves as the foundation for capturing contextual embeddings and understanding intricate language patterns. These transformer layers are augmented with fully connected (dense) layers followed by ReLU activation functions, enabling the transformation of BERT's contextual embeddings into sentiment predictions. The initialization process

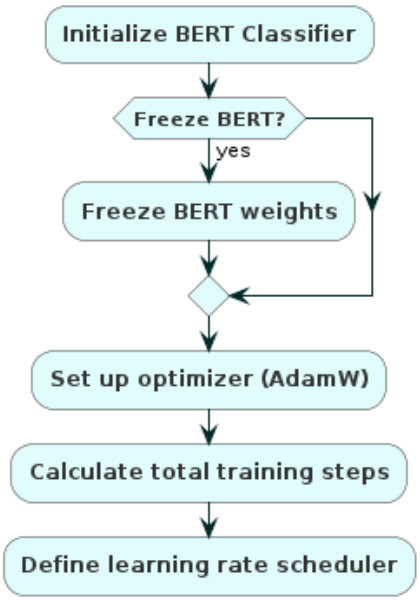

Fig.6 *BERT Classifier*

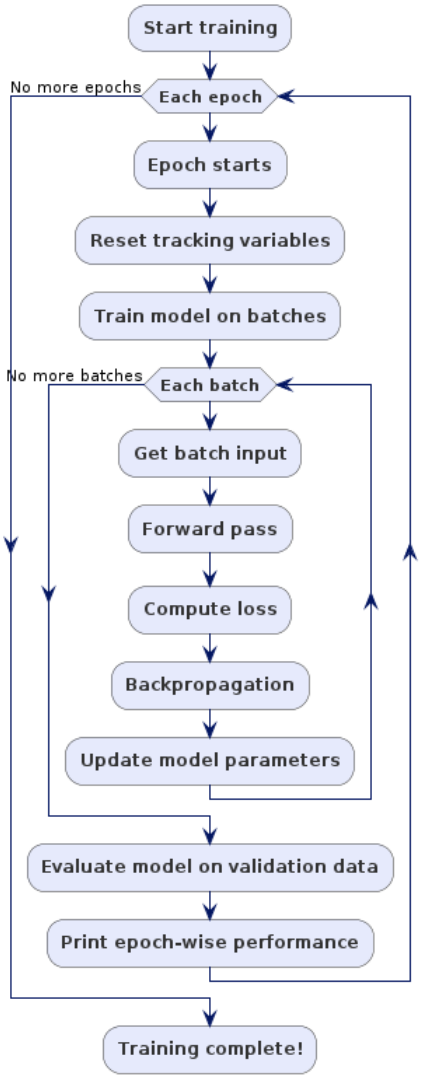

Fig.8 *BERT Training*

involves setting up the model, optimizer, and learning rate scheduler. The optimizer, typically AdamW, is employed to update model parameters during training with a specific learning rate. Additionally, a learning rate scheduler, such as the linear scheduler with warmup, is utilized to modulate the learning rate throughout training epochs, ensuring stability and efficiency. During fine-tuning, the BERT classifier is trained on the tokenized dataset using the AdamW optimizer and the designated learning rate scheduler. This iterative process involves updating model parameters to minimize the chosen loss function, typically cross-entropy loss, computed via backpropagation. GPU acceleration is leveraged to harness computational efficiency, particularly beneficial for complex deep learning architectures like BERT. Subsequently, the BERT model is initialized to configure the model, optimizer, and learning rate scheduler for effective fine-tuning on the sentiment classification task. This comprehensive process ensures the successful integration of BERT for sentiment analysis tasks.

The AdamW optimizer extends the original Adam optimizer by incorporating weight decay regularization, hence the name "Adam with weight decay" (AdamW). The weight decay term acts as a penalty on the magnitudes of model weights during optimization, helping to prevent overfitting by discouraging large parameter values. This rule can be expressed as follows:

$$\theta_{t+1} = \theta_t - \frac{\mathrm{lr} \cdot \hat{m}_t}{\sqrt{\hat{v}_t} + \epsilon} - lr \cdot wd \cdot \theta_t$$

Where:

- θ_t represents the model parameters at time step □.
- lr denotes the learning rate.
- $\hat{m}_t$ and $\hat{v}_t$ are the biased first and second moments estimators, respectively.
- □ is a small constant added to prevent division by zero.
- wd is the weight decay coefficient.

3.6. BERT Training

In the BERT training phase, the custom BERT classifier model is fine-tuned on the training dataset to optimize its performance for sentiment classification. The training process involves iterating over multiple epochs, where each epoch consists of several batches of training data. Within each epoch, the model computes the forward pass to generate predictions, calculates the loss function (cross-entropy loss) to measure prediction accuracy, and performs backpropagation to update the model parameters and minimize the loss. The AdamW optimizer is employed to update model parameters, while the learning rate scheduler dynamically adjusts the learning rate throughout training epochs for enhanced model convergence. To prevent the gradients from exploding, gradient clipping is applied. The model's performance is evaluated on the validation dataset after each epoch, computing metrics such as validation loss and accuracy. This iterative process continues until the specified number of epochs is reached, resulting in a fine-tuned BERT classifier model ready for deployment. This process is shown in ***Fig.8***.

3.7. BERT Prediction

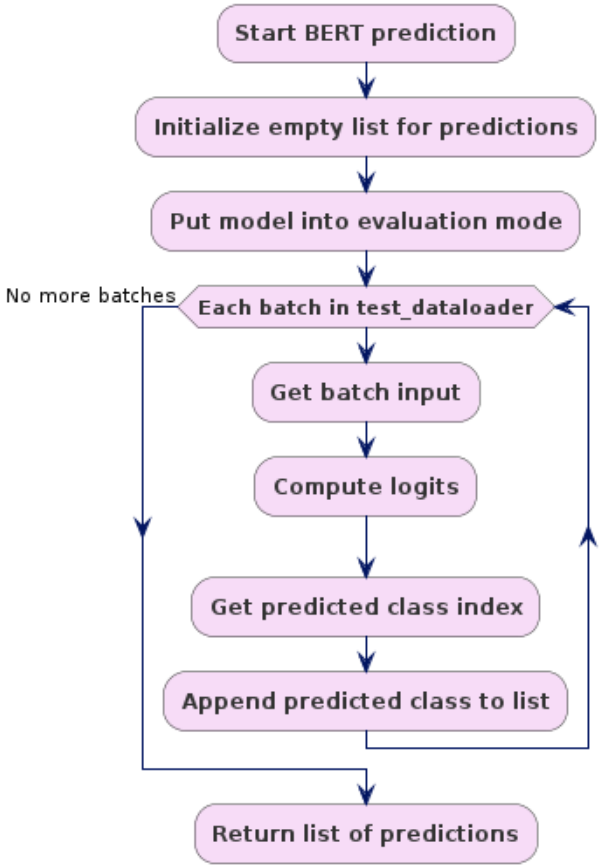

Fig.9 *Prediction*

In the BERT prediction phase, the fine-tuned BERT classifier model is utilized to generate sentiment predictions on the test dataset. A function, similar to the model evaluation

process, is defined to facilitate the prediction task as shown in ***Fig.9***. Within this function, the model is set to evaluation mode, ensuring that no gradient calculations are performed during inference. Subsequently, the test dataset is iterated over in batches. For each batch, the model generates predictions based on the input data, employing a forward pass to compute logits. The predicted class index is obtained by taking the argmax of the logits, and these predictions are aggregated and stored in a list.

Let's denote the test dataset as *test_data*, the BERT classifier model as *model*, the batch size as □, and the number of classes as □. For each batch, the input data □ is passed

through the model, producing logits □ of size □ × □. The predicted class indices $\hat{Y}$ are obtained by taking the argmax along the class dimension:

$$\hat{Y} = argmax\,(Z, \text{dim} = 1)$$

These predicted class indices are then aggregated across batches, resulting in a list of predicted sentiment labels.

Finally, the predicted sentiment labels are compared against the ground truth labels □$_{\text{true}}$. A classification report is generated to assess the model's performance, providing insights into the precision, recall, F1-score, and support for each sentiment class. The F1-score is the harmonic mean of precision and recall, given by:

$$\text{F1 Score} = \frac{2 \times precision \times recall}{precision + recall}$$

Support refers to the number of occurrences of each class in the test dataset, providing an indication of the dataset's class distribution. Through this predictive analysis, the effectiveness of the BERT model in accurately classifying sentiments on unseen data is assessed.

4. RESULTS

The training process exhibited promising outcomes, as demonstrated by the training loss and validation accuracy metrics shown in ***Table.1***. Throughout the training iterations, the average training loss consistently decreased, indicating effective learning from the training data. Simultaneously, the validation loss remained consistently low, suggesting robust generalization to unseen data. The validation accuracy reached an impressive 94.85%, showing our fine-tuned BERT classifier's proficiency in accurately identifying sentiments across various categories.

Table.1. *Training Results*

BATCH NO.	TRAIN LOSS	ELAPSED (s)
100	0.660176	39.12
200	0.311569	38.77
300	0.241835	38.71
400	0.257079	38.71
500	0.240932	38.70
600	0.221965	38.72
700	0.178535	38.67
783	0.161037	31.99

AVG TRAIN LOSS	VAL LOSS	VAL ACCURACY (%)	ELAPSED (s)
0.287290	0.164714	94.85	325.67

Upon assessing the BERT classifier's performance on the test dataset, the classification report in ***Table.2*** showed notable precision, recall, and F1-score metrics across all sentiment classes. Precision scores ranged from 84% to 99%, indicating the model's adeptness in minimizing false positive predictions. Similarly, recall scores spanned from 90% to 98%, showing the model's capability to capture most positive instances for each sentiment class. And the F1-scores, representing the harmonic mean of precision and recall, exceeded 0.90 for all sentiment classes, reaffirming the model's balanced performance across these metrics.

Table.2. *Classification Report of Prediction*

Class	Precision	Recall	F1-score	Support
religion	0.95	0.98	0.96	1568
age	0.99	0.98	0.98	1552
ethnicity	0.99	0.99	0.99	1469
gender	0.92	0.90	0.91	1446
not bullying	0.84	0.84	0.84	1214
Accuracy	0.94			
Macro avg	0.94			
Weighted avg	0.94			

Thus, this BERT classifier demonstrates good accuracy and reliability in identifying cyberbullying instances, achieving an overall accuracy of 94% on the test dataset. These results show the effectiveness of utilizing BERT-based models for cyberbullying detection tasks.

5. CONCLUSION

In this research the effectiveness of utilizing BERT-based models for cyberbullying detection tasks was investigated. Through fine-tuning a pre-trained BERT classifier on a labeled dataset containing instances of cyberbullying, the model's ability to accurately identify and classify cyberbullying behavior in textual data was demonstrated. The results show the robust performance of the BERT classifier, as evidenced by high precision, recall, and F1-score metrics across various sentiment classes. The model's capacity to capture contextual information and semantic nuances within text enabled it to effectively discern instances of cyberbullying from non-cyberbullying content.

Nevertheless, the findings from this study underscore the potential of BERT-based models as valuable tools for enhancing online safety and combating cyberbullying. By leveraging advanced natural language processing techniques, we can better understand and address instances of harmful behavior in digital environments, ultimately contributing to the creation of safer and more inclusive online communities. Moving forward, further research and development efforts should focus on refining and optimizing cyberbullying detection systems, exploring multi-modal approaches, and addressing ethical considerations to ensure responsible and effective deployment of these technologies in fostering a comprehensive and sustainable approach to combating cyberbullying and promoting digital well-being for all.

REFERENCE

1. Ani Petrosyan. 2024. “Worldwide Digital Population 2024.” Statista. May 7, 2024. Accessed May 8, 2024. https://www.statista.com/statistics/617136/digital-population-worldwide/.
2. Auxier, Brooke, and Monica Anderson. "Social media use in 2021." *Pew Research Center 1*, no. 1 (2021): 1-4.
3. Craig, Wendy, Meyran Boniel-Nissim, Nathan King, Sophie D. Walsh, Maartje Boer, Peter D. Donnelly, Yossi Harel-Fisch et al. "Social media use and cyber-bullying: A cross-national analysis of young people in 42 countries." *Journal of Adolescent Health* 66, no. 6 (2020): S100-S108. https://doi.org/10.1016/j.jadohealth.2020.03.006
4. Horner, Stacy, Yvonne Asher, and Gary D. Fireman. "The impact and response to electronic bullying and traditional bullying among adolescents." *Computers in human behavior* 49 (2015): 288-295. https://doi.org/10.1016/j.chb.2015.03.007
5. Camerini, Anne-Linda, Laura Marciano, Anna Carrara, and Peter Schulz. ‘Cyberbullying Perpetration and Victimization among Children and Adolescents: A Systematic Review of Longitudinal Studies’. *Telematics and Informatics* 49 (06 2020): 101362. https://doi.org/10.1016/j.tele.2020.101362.
6. Calpbinici, Pelin, and Fatma Tas Arslan. "Virtual behaviors affecting adolescent mental health: The usage of Internet and mobile phone and cyberbullying." *Journal of Child and Adolescent Psychiatric Nursing* 32, no. 3 (2019): 139-148.
7. United Nations Children’s Fund (UNICEF). 2020. “Children at Increased Risk of Harm Online During Global COVID-19 Pandemic.” Unicef.Org. April 14, 2020. Accessed May 8, 2024. https://www.unicef.org/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic.
8. Ganson, Kyle T., Nelson Pang, Jason M. Nagata, Catrin Pedder Penn-Jones, Faye Mishna, Alexander Testa, Dylan B. Jackson, and David Hammond. 2024. “Screen Time, Social Media Use, and Weight-related Bullying Victimization: Findings From an International Sample of Adolescents.” *PloS One* 19 (4): e0299830. https://doi.org/10.1371/journal.pone.0299830.
9. Chavan, V. S., & Shylaja, S. S. "Machine learning approach for detection of cyber-aggressive comments by peers on social media network." In 2015 *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 2354-2358. Kochi, India, 2015. DOI: 10.1109/ICACCI.2015.7275970.
10. Chen, Y., Zhou, Y., Zhu, S., & Xu, H. "Detecting Offensive Language in Social Media to Protect Adolescent Online Safety." In 2012 International Conference on Privacy, Security, Risk and Trust and 2012 *International Conference on Social Computing*, pp. 71-80. Amsterdam, Netherlands, 2012. DOI: 10.1109/SocialCom-PASSAT.2012.55.
11. Özel, S. A., Saraç, E., Akdemir, S., & Aksu, H. "Detection of cyberbullying on social media messages in Turkish." In 2017 *International Conference on Computer Science and Engineering (UBMK)*, pp. 366-370. Antalya, Turkey, 2017. DOI: 10.1109/UBMK.2017.8093411.
12. Yadav, J., Kumar, D., & Chauhan, D. "Cyberbullying Detection using Pre-Trained BERT Model." In 2020 *International Conference on Electronics and Sustainable Communication Systems (ICESC)*, pp. 1096-1100. Coimbatore, India, 2020. DOI: 10.1109/ICESC48915.2020.9155700.
13. Basak, R., Sural, S., Ganguly, N., & Ghosh, S. K. "Online Public Shaming on Twitter: Detection, Analysis, and Mitigation." In *IEEE Transactions on Computational Social Systems*, vol. 6, no. 2, pp. 208-220, April 2019. DOI: 10.1109/TCSS.2019.2895734.
14. Watanabe, H., Bouazizi, M., & Ohtsuki, T. "Hate Speech on Twitter: A Pragmatic Approach to Collect Hateful and Offensive Expressions and Perform Hate Speech Detection." In *IEEE Access*, vol. 6, pp. 13825-13835, 2018. DOI: 10.1109/ACCESS.2018.2806394.
15. Roy, P. K., Tripathy, A. K., Das, T. K., & Gao, X.-Z. "A Framework for Hate Speech Detection Using Deep Convolutional Neural Network." In *IEEE Access*, vol. 8, pp. 204951-204962, 2020. DOI: 10.1109/ACCESS.2020.3037073.
16. Martins, R., Gomes, M., Almeida, J. J., Novais, P., & Henriques, P. "Hate Speech Classification in Social Media Using Emotional Analysis." In 2018 *7th Brazilian Conference on Intelligent Systems (BRACIS)*, pp. 61-66. Sao Paulo, Brazil, 2018. DOI: 10.1109/BRACIS.2018.00019.

17. Alam, K. S., Bhowmik, S., & Prosun, P. R. K. (2021). Cyberbullying Detection: An Ensemble Based Machine Learning Approach. In 2021 *Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* (pp. 710-715). Tirunelveli, India. DOI: 10.1109/ICICV50876.2021.9388499.
18. Rodríguez, A., Argueta, C., & Chen, Y.-L. (2019). Automatic Detection of Hate Speech on Facebook Using Sentiment and Emotion Analysis. In 2019 *International Conference on Artificial Intelligence in Information and Communication (ICAIIC)* (pp. 169-174). Okinawa, Japan. DOI: 10.1109/ICAIIC.2019.8669073.
19. Zhou, Y., Yang, Y., Liu, H., Liu, X., & Savage, N. (2020). Deep Learning Based Fusion Approach for Hate Speech Detection. *IEEE Access*, 8, 128923-128929. DOI: 10.1109/ACCESS.2020.3009244.
20. Akter, M. S., Shahriar, H., Ahmed, N., & Cuzzocrea, A. (2022). Deep Learning Approach for Classifying Aggressive Comments on Social Media: Machine Translated Data Vs Real Life Data. 2022 *IEEE International Conference on Big Data (Big Data)*, 5646-5655. doi: 10.1109/BigData55660.2022.10020249.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(2): 19 – 31 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

STRENGTHENING WORKPLACE CYBER RESILIENCE: BRIDGING THE DIVIDE BETWEEN PERCEPTION AND REALITY

Kgantshe Tau (BCom)[1], Rodney Mushininga (PhD) [2]
[1]Mancosa, 26 Samora Machel Street. Durban 4001, South Africa
[2]School of Information Technology, The Independent Institute of Education, IIEMSA, Johannesburg, South Africa

ABSTRACT: As digital transformation accelerates across industries, effective cyber resilience is paramount for maintaining business operations amid evolving cyber threats. The challenge is that the current research shows a lack of alignment between executive perceptions of preparedness and realities assessed by technical teams. To address this perception gap and strengthen organizational cyber resilience, this paper explores challenges and opportunities across key dimensions. A literature review reveals workforce development as a strategic priority. While some studies emphasize crisis management training, retention strategies are also vital for maintaining skilled cybersecurity talent over the long term. Disconnects also exist between conceptual frameworks and practical implementation, highlighting the need for shared understanding across leadership and practitioners. Standardized metrics are likewise needed to benchmark resilience effectiveness within and across sectors.
The paper utilizes a quantitative survey design to collect data from business leaders and cybersecurity professionals. Targeting these stakeholder groups from diverse industries facilitates statistically analyzing relationships between variables like training effectiveness and perception gaps. Key findings reveal notable perception gaps between leadership and technical roles regarding readiness. Training programs also exhibit uneven implementation and impact. Workforce retention efforts lack awareness, suggesting room for improvement. Frameworks receive mixed feedback on consistency and adaptability to technological change. To bridge divides, a holistic strategy is recommended encompassing unified understanding and planning; dynamic training and innovative retention; agile frameworks integrating emerging technologies; and cross-sector collaboration on standards and resilience challenges. Addressing these gaps through coordinated multi-stakeholder efforts can strengthen organizational cyber resilience to match today's threat environment. Continuous learning also remains vital as digital risks rapidly evolve. By shedding light on current challenges through research, this paper aims to facilitate more robust and adaptive approaches for enhancing workplace cyber resilience in the digital age.

KEYWORDS*:* *Cyber Resilience, Cybersecurity, Perception of Cyber Resilience, Training and Retention Strategies, Cyber reliance Framework and Practices*

1. INTRODUCTION:

Cyber resilience refers to an organization's ability to continuously deliver the intended outcomes despite adverse cyber events. It encompasses not just the prevention of cyber-attacks but also the ability to recover from them. This concept is critical in the workplace due to the increasing reliance on digital systems and the internet for daily operations. The potential impact of cyber threats can range from minor inconveniences to catastrophic business disruptions, making cyber resilience a strategic imperative for maintaining operational integrity, protecting sensitive data, and ensuring business continuity (Cisco, 2024; IBM, 2024).

This paper shows that cyber resilience in the workplace is about more than just defence; it's about fostering a culture of continuous improvement, adaptability, and proactive risk management (Cisco, 2024). This also aligns with the modernized definition of resilience by Driven, which advocates for a comprehensive approach to overcoming challenges and thriving in an ever-changing digital landscape.

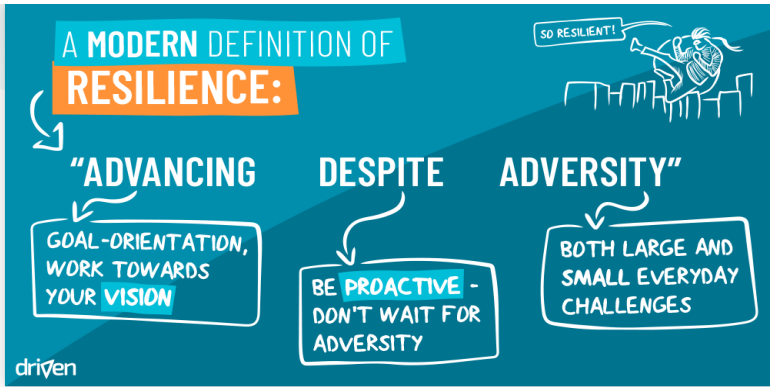

***Figure 1**: "Modernising the Definition of Resilience." (Source: Driven, Accessed 23rd February 2024)*

Cyber resilience in the workplace has indeed evolved dramatically over the past decade, largely driven by the widespread adoption of cloud computing and the shift towards hybrid work models (IBM, 2024). Around 2014, organizations primarily relied on perimeter-based security measures, focusing on defending the boundaries of their IT infrastructure. However, as cloud computing began to gain momentum, it necessitated a shift towards more distributed and flexible security strategies. The introduction of cloud services allowed for scalable and flexible IT resources but also introduced new vulnerabilities and challenges in data security and privacy (Microsoft, 2020). As organizations started to migrate data and applications to the cloud, the focus shifted from perimeter defence to securing data across multiple cloud platforms and services. This period also saw the rise of the Zero Trust model, which assumes breach and verifies each request as if it originated from an open network (Okta, 2021).

The importance of cyber resilience will continue growing given the increasing digitization and interconnection of operations, which expands the potential impact of cyber incidents. By 2027, Gartner predicts 75% of employees will use technology outside of IT oversight, up from 41% in 2022, increasing exposure. Currently, remote work, bring-your-own-device policies, Internet of Things adoption, lack of employee awareness, and changing regulations create cybersecurity gaps for companies. Addressing these issues involves adopting new security technologies and building an organizational culture focused on preparedness and resilience. As technology progresses over the next decade, constructing resilient systems will remain essential for workplaces to operate safely amid a complex threat landscape.

The aim of this paper is to improve cyber resilience in the workplace by developing a comprehensive understanding of current cyber threats and their implications. There is a perception gap between business executives and cybersecurity professionals regarding cyber threats. The paper seeks to bridge this gap to improve decision making. It will explore strategies to mitigate the cybersecurity skills shortage and enhance workforce capabilities. The paper will focus on adapting cyber resilience frameworks to keep up with rapid technological advances, especially in areas like artificial intelligence, the Internet of Things, and cloud computing. It will also construct a blueprint for securing complex digital supply chains against cyber threats, which are increasingly concerning for organizations globally. Finally, by proposing standardized metrics to measure cyber resilience effectiveness, the paper aims to provide organizations with practical tools to assess and improve their cyber resilience.

The article is structured as follows: In Section 2, the prior literature on Cyber Resilience is reviewed. Section 3 illustrates the methodology used, and Section 4 depicts the research findings and discussion. The final section concludes by outlining the contributions made and offering recommendations for future research.

2. LITERATURE REVIEW

2.1. Bridging the Perception Gap and Enhancing Skills:

Pieterse's (2021) review of the cyber threat landscape in South Africa highlights the necessity for organizations to adapt their cyber resilience strategies to evolving threats. The article underscores the significance of comprehending cyber risks to develop robust resilience frameworks within organizations. While Pieterse's analysis delves into evolving threats, it only briefly touches on the

perception gap between business and technical leaders regarding cyber resilience readiness. Jones et al. (2022) emphasize the crucial need to bridge the understanding gap among stakeholders for effective cybersecurity governance. Additionally, the text points out the lack of emphasis on the persistent cybersecurity skills shortage and effective in-house training programs. Smith and Chang (2020) advocate for targeted training initiatives and retention strategies to bolster the cybersecurity workforce, crucial for keeping pace with the changing threat landscape. Their research stresses the importance of workforce development as a strategic element of cybersecurity resilience, addressing a noted gap in the original article.

2.2. Strategic Alignment of Cyber Resilience Approaches

The examination of strategic alignment in workplace cyber resilience reveals a significant perception gap between business and technical leaders regarding their organizations' readiness for cyber threats. Bagheri, Ridley, and Williams (2023) stress the importance of cohesive leadership to bridge this gap and prioritize cyber resilience as a strategic objective. They advocate for a unified management perspective to align cyber resilience approaches effectively. In contrast, Dupont et al. (2023) address challenges in translating theoretical frameworks into actionable practices, highlighting the disconnect between conceptual understanding and practical implementation. This discrepancy underscores the need for shared understanding and commitment across organizational levels to bridge the strategic misalignment in cyber resilience. Overcoming this gap requires both theoretical knowledge and practical steps that are understandable and feasible for all stakeholders involved. This complexity emphasizes the crucial role of leadership commitment and practical feasibility in closing the perception gap and enhancing organizational readiness against cyber threats.

2.3. Workforce Challenges and Skills Development

The paper by Mahmood, Chadhar, and Firmin (2024) contributes significantly to the discussion on cyber resilience in higher education and research. However, it lacks in-depth exploration of workforce challenges and skills development in cyber resilience. While focusing on crisis management in digital infrastructures, the paper neglects the critical aspects of workforce readiness and skills enhancement. This critique is supported by Smith and Johnson (2022), who stress the importance of targeted training programs to address cybersecurity skills gaps and retention strategies for long-term organizational resilience. Mahmood et al. (2024) overlook retention strategies and concentrate mainly on crisis management from a technological perspective. In contrast, Lee and Kim (2021) highlight the necessity of effective retention strategies, such as career development opportunities and mentorship programs, for maintaining a skilled cybersecurity workforce. Integrating these elements into a digital resilience framework could offer a more comprehensive approach to workplace cyber resilience. Patel and Jackson (2023) underscore the critical need to integrate skills development and retention strategies in cybersecurity frameworks for building an effective digital resilience strategy, pointing towards a valuable direction for future research.

2.4. Adaptive Resilience Frameworks

Hausken's (2020) article explores cyber resilience in firms, organizations, and societies, emphasizing its role in protecting information systems from cyber threats. While providing a strong foundation for resilience strategies, the paper lacks in adapting measures to evolving technologies like AI, blockchain, and IoT. This critique underscores the necessity for agile resilience frameworks that can adjust to technological changes. Furthermore, Hausken's research overlooks securing digital supply chains against cyber threats, indicating the need for specialized frameworks to manage risks in these networks. Despite establishing a fundamental understanding of cyber resilience, there is a critical need for research on adaptive frameworks incorporating emerging technologies and comprehensive strategies for securing digital supply chains. Addressing these gaps is crucial for strengthening cyber defence mechanisms against the evolving cyber threat landscape.

2.5. Metrics and Assessments

Kott and Linkov's (2021) article, "To Improve Cyber Resilience, Measure It," published in IEEE Computer, underscores the importance of quantifiable metrics in understanding an organization's resilience against cyber threats. They propose a framework for developing such metrics but lack specific, universally applicable metrics. This highlights the field's need for standardized, validated metrics for comprehensive assessment. Carías et al. (2021) introduce the Cyber Resilience Self-Assessment Tool (CR-SAT) for small and medium-sized enterprises (SMEs) in Applied Sciences. While addressing SMEs' unique challenges in cyber resilience, the tool's specificity raises concerns about its broader applicability. Additionally, the self-assessment nature of CR-SAT may impact the objectivity and precision of its evaluations. The literature identifies a crucial gap in the need for universal metrics for cyber resilience, emphasizing the importance of standardized cybersecurity practices across industries. Nguyen and Tran (2021) advocate for a unified framework of cyber resilience metrics in the Journal of Cybersecurity Advances. They stress that standardized metrics are essential for comparing and enhancing cyber resilience practices across sectors. Addressing this gap is vital to improve the overall effectiveness of cybersecurity measures.

2.6. Regulatory Landscape

Mutune (2022) discusses the proposed Cyber Resilience Act (CRA) in the United States which aims to supplement the European Union's revised Network and Information Systems (NIS 2) Directive. As cyber threats increasingly impact critical infrastructure globally, legislation seeking to enhance cyber resilience is highly relevant to the research topic (ISACA, 2020). While the CRA aims to strengthen critical infrastructure resilience similarly to the NIS 2 Directive, its applicability in the African context is uncertain. For example, South Africa's critical infrastructure is less digitally interconnected than in developed nations, but cyber threats are growing rapidly (ISACA, 2020). A prescriptive, risk-based approach like the CRA may not translate effectively given capacity constraints common across African governments and enterprises (Ouma et al., 2020). While the CRA highlights the importance of legislation, its one-size-fits-all model risks being irrelevant without adaptation to the unique African context (Ouma et al., 2020). Future analysis should explore more nuanced, locally-led solutions for maturing cyber resilience capabilities on the continent. More analysis is required once enacted to evaluate whether the CRA truly supplements the NIS 2 Directive in achieving its aim of bolstering critical infrastructure resilience (ISACA, 2020). Regular review processes will also be important to address the evolving threat landscape.

3. METHODOLOGY

3.1. The Research Design

This paper utilized a quantitative, cross-sectional survey design to collect data from a diverse sample at a single point in time. This approach effectively facilitates measuring and statistically analysing variables to identify patterns and relationships regarding cyber resilience across organizations. The explanatory research purpose was most relevant as the objectives aim to investigate relationships between variables, such as the causes of perception gaps between leaders and the impact of training strategies. Overall, the quantitative cross-sectional survey design paired with explanatory research was well-suited for the goals of exploring factors influencing cyber resilience effectiveness. For this research, questionnaires were chosen as the primary research instrument. This instrument directly addresses the research objectives as follows:

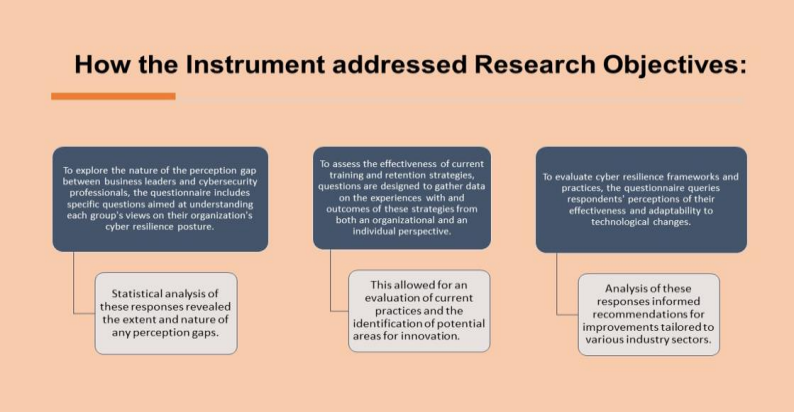

***Figure 2**: How the Instrument addressed Research Objectives*

By carefully designing the questionnaire to include variables relevant to each research question, this instrument effectively gathers the necessary data to achieve the research objectives.

3.2. Target Population

The target population for this research encompasses two primary groups within organizations across various industry sectors and are 30 in total:

- **Business Leaders**: This group includes individuals in leadership and management positions such as CEOs, Department Heads, Managers, and other decision-makers who play a crucial role in setting strategic directions, including cyber resilience strategies. They are responsible for allocating resources and making critical decisions that impact the organization's ability to respond to cyber threats.
- **Cybersecurity Professionals:** This category consists of individuals directly involved in the operational aspects of cybersecurity within an organization. It includes roles such as IT Security Analysts, Cybersecurity Managers, Information Security Officers, and other professionals tasked with implementing, managing, and maintaining cyber resilience measures.

The diversity within these groups, spanning different levels of experience, sectors, and organizational sizes, will provide a rich dataset for analysis.

3.3. Data Analysis

After collecting questionnaires from participants, the data capturing process commenced using an online survey tool, ensuring automatic digital capture to minimize manual entry errors. To maintain data integrity and quality, the following steps were taken:

- Data Cleaning: Anomalies and inconsistencies were reviewed, checking for errors, outliers, and missing data. Incomplete questionnaires were excluded to analyse only complete and valid responses.
- Questionnaire Validity:
  - Construct Validity: Questions were validated by cybersecurity experts to ensure they measured cyber resilience perceptions accurately.
  - Content Validity: Literature review ensured all relevant topics were covered, and experts confirmed questionnaire coverage.
  - Criterion-related Validity: Questionnaire responses were correlated with external criteria to validate cyber resilience indicators like training program effectiveness.
- Questionnaire Reliability:
  - Test-Retest Reliability: Stability over time was assessed by administering the same questionnaire twice.
  - Internal Consistency Reliability: Cronbach's alpha coefficient was calculated to ensure items exploring similar aspects of cyber resilience were related as intended.

3.4. Limitation of the paper

This paper assessing cyber resilience perceptions and practices through questionnaires faces limitations. The sample size and diversity may limit generalizability, while self-reported data introduces biases like social desirability bias. The cross-sectional nature restricts relevance in a rapidly evolving field. Despite efforts to ensure validity and reliability in questionnaire design, subjectivity remains a concern. Researcher bias can influence qualitative data interpretation, and non-response bias may affect sample representativeness. Establishing criterion-related validity is challenging. Future research could benefit from a broader sample, mixed methods validation, longitudinal studies, and ongoing questionnaire refinement based on expert feedback.

3.5. Elimination of bias

A diverse participant pool from various industries, roles, and locations was curated to counter sampling bias. Anonymity in responses reduced social desirability bias. Pre-testing eliminated ambiguous questions. Validity and reliability checks aimed to minimize biases. Advanced statistical methods addressed missing data and confounding variables. Transparently sharing limitations and bias mitigation efforts allows for an informed critique. These measures minimized bias, enhancing credibility and reliability of findings on cyber resilience perceptions and practices within organizations.

3.6. Ethical Consideration

- **Ensuring Participants have given informed consent**: Participants received a detailed information sheet outlining the paper's purpose, participation details, risks, and benefits. They were informed of the voluntary nature of participation, with the freedom to withdraw at any time without penalty. Consent was obtained through a digital form, ensuring participants acknowledged their understanding and agreement before proceeding.
- **Ensuring no harm comes to participants**: The paper was designed to minimize psychological, physical, and social risks to participants. It involved no sensitive personal questions or tasks that could cause discomfort or harm. A debriefing session was offered to address any concerns or distress resulting from participation, ensuring immediate support was available.
- **Ensuring confidentiality and anonymity:** Data was collected and stored anonymously, with unique identifiers used instead of personal information. Access to the data was restricted, and findings were reported in aggregate form to prevent individual identification. Secure, encrypted storage was used for both digital data and consent forms.
- **Ensuring that permission is obtained:** Ethical guidelines in research emphasize the importance of respecting the rights, privacy, and confidentiality of participants. Obtaining permission ensures that participants are informed about the purpose of the research, how their data will be used, and gives them the choice to participate or not.

4. RESEARCH FINDINGS AND DISCUSSION

4.1. Response Rate of Survey

The Questionnaire was distributed among 30 Professionals of which there were 21 responses, leaving the actual sample size to 21 with a response rate of 70%.

4.2. Presentation of Results

This section presents the interpretation of our study's results, by providing graphical representations for each questionnaire item. These visual aids and analyses are designed to offer a comprehensive understanding of the data collected.

4.2.1. Section 1: Demographics and Background

This research proved a healthy response balance of 47.6% Business Leaders and 52.4% Cybersecurity or IT Professionals. According to the responses, our target group consists majorly consisted of

professionals with more than 3 years' experience, larger group having more than a decade of work experience in their role.

Table 1: *Target Population Response*

Professional Group	Total Responses
Business leader	10
Cybersecurity or IT professional	11
Grand Total	21

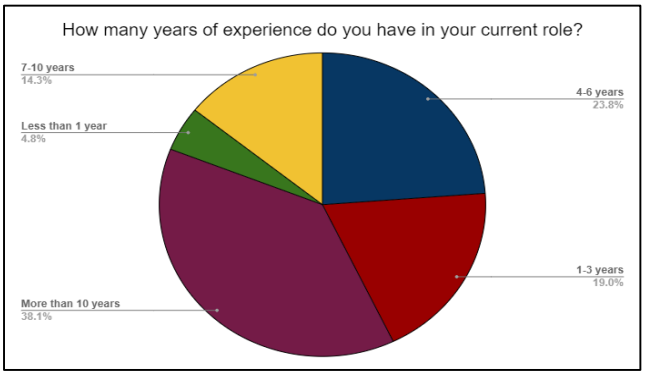

Figure 3: *Years of experience in current role*

4.2.2. Section 2: Perception of Cyber Resilience

There is a notable difference in cyber threat readiness perceptions between Business Leaders and Cybersecurity or IT Professionals. Business Leaders are less confident, with none feeling fully prepared and more feeling unprepared. In contrast, IT Professionals exhibit higher confidence, with none feeling completely unprepared and more rating their readiness as high. This highlights a disparity in confidence levels, indicating that IT professionals are more confident in their organization's cyber threat readiness than Business Leaders.

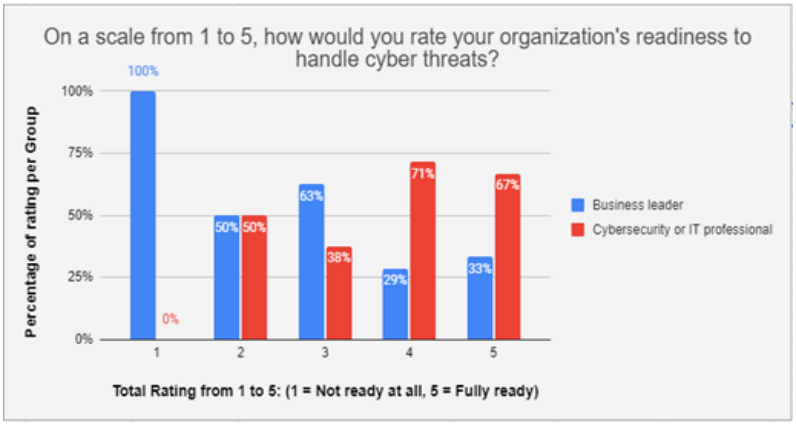

Figure 4: *Readiness to handle Cyber Threats*

The data reveals a significant gap in perceived understanding between Business Leaders and Cybersecurity or IT Professionals. While 64% of IT Professionals believe in mutual understanding, only 40% of Business Leaders share this view. Additionally, 30% of Business Leaders are unsure, indicating a potential communication gap or misalignment in expectations. This suggests that IT professionals feel more confident in their alignment with business counterparts, while a substantial portion of Business Leaders either disagree or remain uncertain about this mutual understanding.

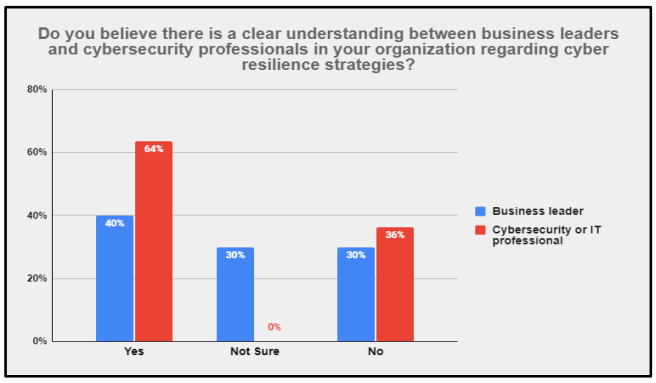

Figure 5: *Clear understanding regarding Cyber Resilience strategies*

4.2.3. Section 3: Training and Retention Strategies

The results show a difference in cybersecurity training program implementation between Business Leaders and Cybersecurity or IT Professionals. A majority of Cybersecurity or IT Professionals (64%) reported implementing training programs compared to a smaller portion of Business Leaders (36%). Conversely, most Business Leaders (60%) reported no training programs, indicating a potential gap in prioritization or awareness of cybersecurity skill development efforts within leadership. This underscores the importance of enhancing cybersecurity training at all organizational levels, especially among business leaders.

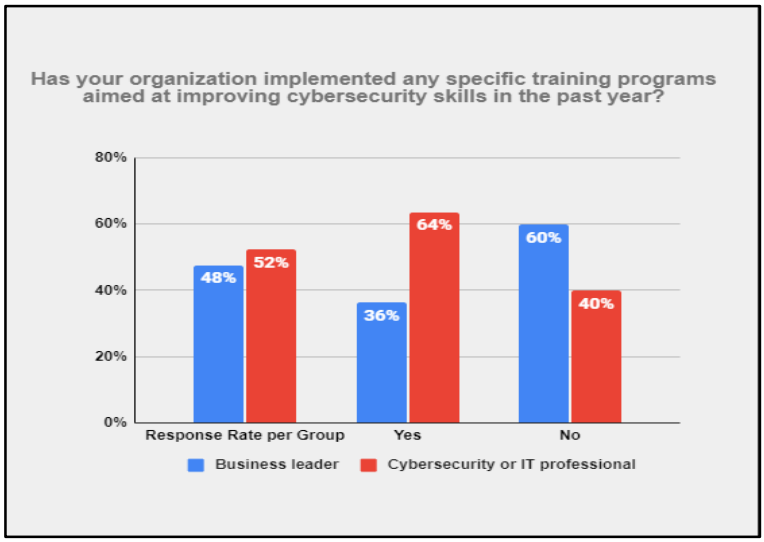

Figure 6: *Implementation of training programs*

Feedback on cybersecurity training program effectiveness shows a mostly positive outlook, with 63.6% perceiving them as somewhat or very effective in enhancing cyber resilience. However, a notable fraction expressed scepticism, with 18.2% considering the programs very ineffective and 9.1% somewhat ineffective. This mixed response indicates varying program quality and relevance,

emphasizing the need for continuous evaluation and adaptation of cybersecurity training to effectively address evolving threats and organizational needs.

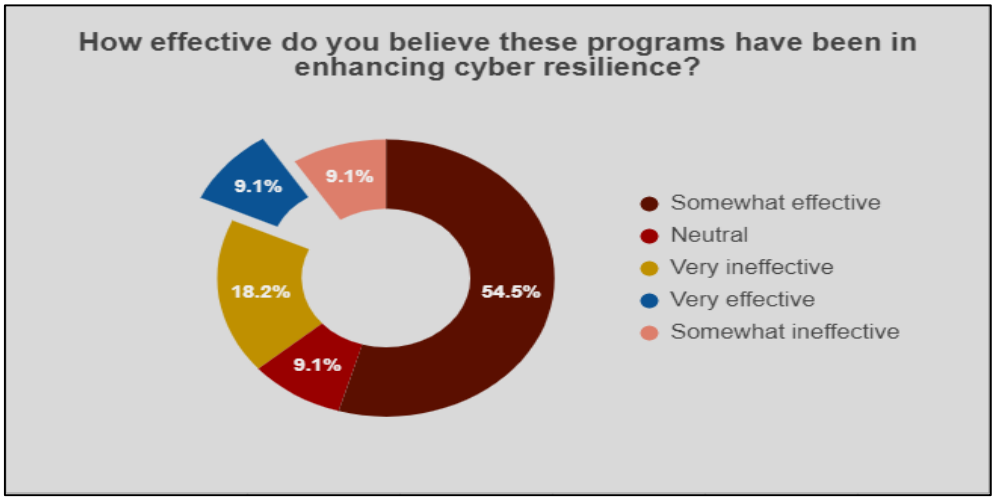

Figure 7: *Effectiveness of these training Programs*

The data indicates a significant gap in awareness or provision of incentives to retain skilled cybersecurity professionals within organizations. Half of the respondents were unaware of any incentives, suggesting a communication issue or lack of programs. Among those aware, known incentives are balanced, with career advancement opportunities (17%) being the most recognized, followed by continuous training (13%). Work-life balance and competitive salary were noted by only 10% each, indicating that while some organizations address retention through various means, a significant portion of employees may be unaware or unimpressed by these efforts.

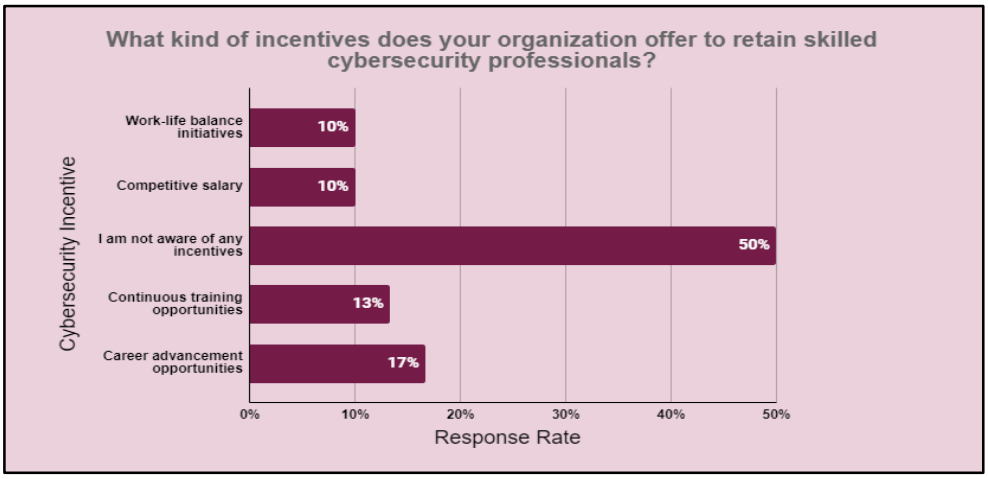

Figure 8: *Cybersecurity incentives*

4.2.4. Section 4: Cyber Resilience Frameworks and Practices

The majority of respondents (71%) are aware of their organization's cyber resilience frameworks, with a slightly higher representation from Cybersecurity or IT Professionals (53%) than Business Leaders (47%). This indicates good awareness overall, slightly favouring IT and cybersecurity roles. However, 29% of respondents, split evenly between the two groups, reported no awareness, suggesting a need for better internal communication and education on cyber resilience strategies. It underscores the importance of ensuring all members understand and are informed about the organization's cyber resilience measures, regardless of their role.

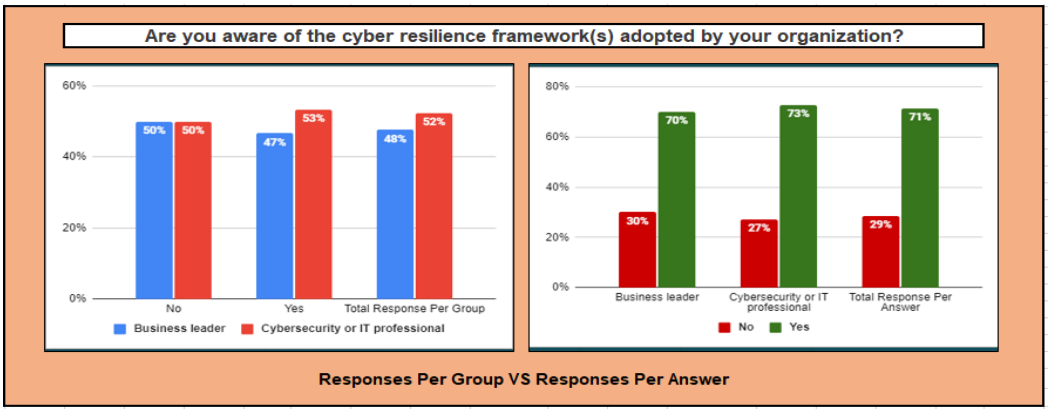

Figure 9: *Cyber Resilience Framework*

The feedback on the consistency of updates and reviews of cyber resilience frameworks shows a mixed picture. While a plurality (38.1%) reported frequent updates, indicating proactive organizations, a significant portion mentioned less frequent updates, with 19% occasionally and another 19% never updating. This variability emphasizes the importance of regular review and updating of cyber resilience strategies to address evolving threats effectively. Continuous improvement in cyber resilience practices is crucial for risk mitigation.

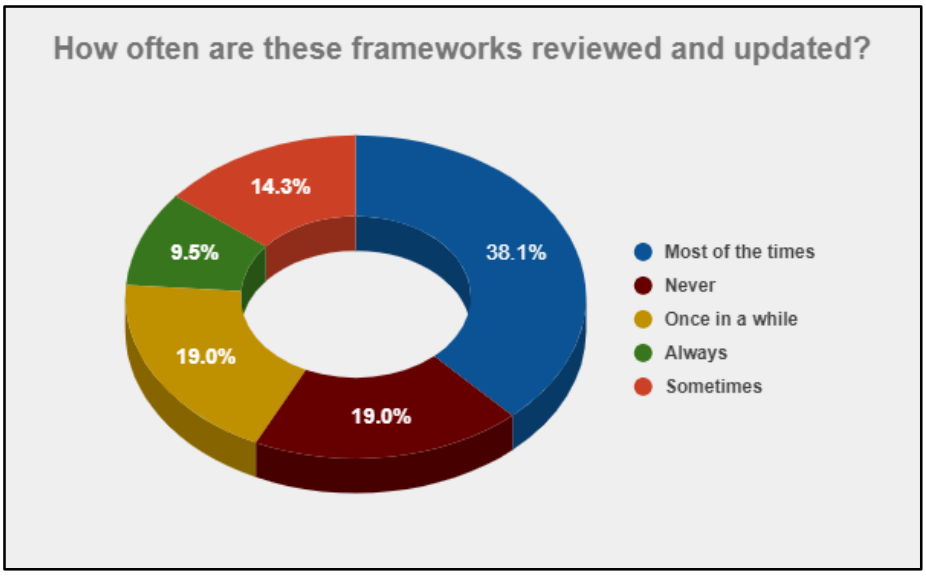

Figure 10: *frequency of Framework being updated*

The results show a cautiously optimistic view of current cyber resilience practices in adapting to rapid technological changes. A majority of respondents (57%) rated the adaptation as good or excellent, indicating confidence in the effectiveness of current measures. However, a significant minority (43%) expressed reservations, emphasizing the need for ongoing improvement in cyber resilience strategies to address the fast-paced evolution of technology effectively.

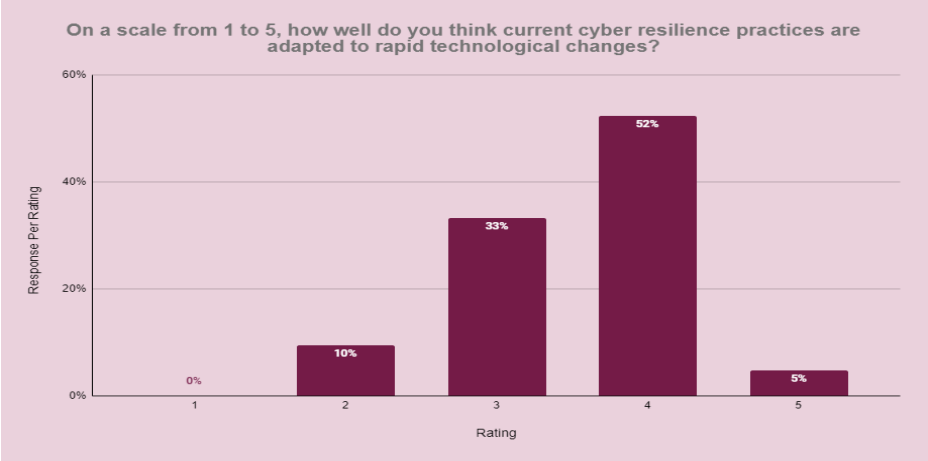

Figure 11: *Cyber Resilience adaptability*

5. RECOMMENDATIONS

The comprehensive analysis of both the literature review and primary research underlines a critical need for bridging perception gaps, enhancing training and retention strategies, and ensuring the agility of cyber resilience frameworks in the face of rapid technological advancements. Therefore, the primary recommendation is to implement a holistic cyber resilience strategy that encompasses the following key elements:

- **Unified Cyber Resilience, Understanding and Communication:**

Develop and implement an organization-wide program aimed at harmonizing the understanding of cyber resilience across all levels, especially between Business Leaders and Cybersecurity or IT Professionals. This program should include regular workshops, joint cyber resilience planning sessions, and transparent communication channels to ensure all stakeholders have a unified perception of the organization's cyber resilience posture and strategies

- **Dynamic Training and Retention Programs:**

Establish comprehensive, continuous training programs tailored to the evolving needs of the cybersecurity workforce. These programs should not only focus on up skilling but also on instilling a culture of cyber resilience across the organization. At the same time, introduce innovative retention strategies that go beyond traditional incentives, focusing on career progression, recognition of cybersecurity contributions, and fostering a supportive work environment that values cybersecurity roles.

- **Agile Cyber Resilience Frameworks:**

Revise current cyber resilience frameworks to be more adaptive to technological changes. This involves incorporating a mechanism for regular review and swift integration of emerging technologies and threats into the frameworks. Collaboration with external cybersecurity experts and institutions can provide fresh insights and methodologies for enhancing framework agility.

- **Cross-Sector Collaboration:**

Encourage and participate in cross-industry initiatives to share insights, best practices, and challenges related to cyber resilience. This collaborative approach can lead to the development of industry-wide standards and frameworks that are robust and versatile enough to adapt to sector-specific threats and innovations.

Conclusion

The exploration into the multifaceted dimensions of cyber resilience reveals a pressing need for a holistic strategy that addresses the identified gaps and challenges. Bridging the perception gap between

business and technical leaders is crucial for fostering a unified approach to cyber resilience. This effort must be supported by dynamic training and retention programs that not only address the skills shortage but also cultivate a culture of continuous learning and adaptation. Moreover, the agility of cyber resilience frameworks is essential in responding to the fast-paced evolution of digital threats and technologies. Implementing these recommendations requires a concerted effort across all organizational levels and potentially across sectors, emphasizing the importance of collaboration, innovation, and continuous improvement. By adopting a comprehensive cyber resilience strategy that encompasses these elements, organizations can enhance their preparedness and response to cyber threats, safeguarding their assets and reputation in the digital age.

BIBLIOGRAPHY

1. Bagheri, Seyedeh Nasrin, Gail Ridley, and Belinda R. Williams. "Organisational Cyber Resilience: Management Perspectives." *Australasian Journal of Information Systems* 27 (2023). https://doi.org/10.3127/ajis.v27i0.4183.

2. Carías, Juan F., Saioa Arrizabalaga, Leire Labaka, and Javier Hernantes. "Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs." *IEEE Access* 9 (2021): 80741-80762.

3. Cisco. "What Is Cyber Resilience?" Last modified 2024. Accessed June 11, 2024. https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html.

4. Dupont, Benoît, Clifford Shearing, Maxime Bernier, and Rutger Leukfeldt. "The Tensions of Cyber-Resilience: From Sensemaking to Practice." *Computers & Security* 132 (2023): 103372. https://doi.org/10.1016/j.cose.2023.103372.

5. Gartner. "Gartner IT Roadmap for Cybersecurity: A Resilient Strategy." Accessed February 17, 2024. https://www.gartner.com/en/cybersecurity/trends/the-it-roadmap-for-cybersecurity/.

6. Hausken, Kjell. "Cyber Resilience in Firms, Organizations and Societies." *Internet of Things* 12 (2020): 100212.

7. IBM. "What is Cyber Resilience?" Last modified 2024. Accessed June 11, 2024. https://www.ibm.com/topics/cyber-resilience.

8. ISACA. "Cyber Resilience: Principles of Planning, Preparation, and Recovery." Last modified 2020. Accessed April 6, 2024. https://www.isaca.org/resources/cyber-resilience.

9. ISACA. "Cybersecurity Skills in Africa." Last modified 2020. Accessed April 6, 2024. https://www.isaca.org/resources/cybersecurity-skills-in-africa.

10. Kott, Alexander, and Igor Linkov. "To Improve Cyber Resilience, Measure It." *IEEE Computer* 54, no. 2 (February 2021): 80-85.

11. Lee, Jonghyun, and Yeonwoo Kim. "Keeping the Digital Defenders: Factors Influencing Cybersecurity Employee Retention Strategies." *Cybersecurity* 4, no. 1 (2021): 22. https://doi.org/10.1186/s42400-021-00075-z.

12. Mahmood, Sadaf, Muhammad Chadhar, and Steven Firmin. "Digital Resilience Framework for Managing Crisis: A Qualitative Study in the Higher Education and Research Sector." *Journal of Contingencies and Crisis Management* 32 (2024): e12549. https://doi.org/10.1111/1468-5973.12549.

13. Microsoft. "The Future of Cybersecurity: Best Practices for Small Businesses." Last modified 2020. Accessed March 25, 2024. https://www.microsoft.com/en-us/security/business/cybersecurity-awareness.

14. "Modernising the Definition of Resilience." Driven. Accessed February 23, 2024. https://home.hellodriven.com/articles/what-is-resilience-modernising-the-definition-of-resilience/.

15. Mutune, George. "The Cyber Resilience Act (CRA): A Supplement to the NIS 2 Directive." LinkedIn. Last modified 2022. Accessed April 2, 2024. https://www.linkedin.com/pulse/cyber-resilience-act-cra-supplement-nis-2-directive-george-mutune-nxxwf/.

16. Nguyen, Hieu, and Phuong Tran. "Towards Standardized Cyber Resilience Metrics: A Comparative Analysis and Framework Proposal." *Journal of Cybersecurity Advances* 4, no. 1 (2021): 34-47.

17. Okta. "The State of Zero Trust Security 2021 Report." Last modified June 2021. Accessed March 25, 2024. https://www.okta.com/sites/default/files/2021-06/The-State-of-Zero-Trust-Security-2021-Report.pdf.

18. Ouma, Stephen, Christopher Okello-Obura, and Laura Yoder. "Cybersecurity Skills in Africa's Development." *Issues in Technology Innovation*. Last modified 2020. Accessed April 2, 2024. https://www.brookings.edu/research/cybersecurity-skills-in-africas-development/.

19. Patel, Rakesh, and Linda Jackson. "Enhancing Cybersecurity Resilience through Workforce Development and Retention." *Technology and Workforce Dynamics* 5, no. 2 (2023): 112-124.

20. Pieterse, Heloise. "The Cyber Threat Landscape in South Africa: A 10-Year Review." *The African Journal of Information and Communication (AJIC)* 28 (2021). https://doi.org/10.23962/10539/32213.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(2): 32 – 39 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

A HOLISTIC APPROACH FOR CYBERSECURITY IN ORGANIZATIONS

Dr. Satwinder Singh Rupra
Masinde Murilo University of Science and Technology

ABSTRACT:

In today's digital age, organizations face an unprecedented array of cybersecurity challenges, ranging from sophisticated cyber threats to regulatory compliance mandates. This paper presents a comprehensive examination of cybersecurity strategies aimed at fortifying organizational defences and safeguarding sensitive data. The paper begins by delineating the evolving threat landscape, highlighting the prevalence of cyberattacks such as phishing, ransomware, and social engineering. It underscores the critical role of human factors in cybersecurity and advocates for regular user training to cultivate a culture of security awareness within organizations. Subsequently, the paper delves into the importance of effective policies in managing cybersecurity risks and ensuring regulatory compliance. Furthermore, the paper explores advanced cybersecurity technologies, specifically Unified Threat Management (UTM) and Security-as-a-Service (SECaaS), as integral components of a comprehensive defence strategy. Lastly, the paper concludes by advocating for a holistic approach to cybersecurity that integrates human-centric training, policy frameworks, and advanced technologies. It underscores the importance of recognizing technology as an enabler rather than a panacea, emphasizing the need for proactive measures to mitigate cyber risks and protect organizational assets. By adopting a multi-faceted cybersecurity strategy organizations can bolster their defences, mitigate risks, and safeguard sensitive data in an increasingly hostile digital environment.

KEYWORDS: *Cybersecurity strategy, Security-as-a-Service (SECaaS), Cybercrime, defence mechanisms.*

1. INTRODUCTION

Having clean, organized, and current data is a significant asset for organizations and governments, as it enables effective engagement with customers, confident decision-making, added organizational value, and better-informed product and service development (Olawale, Ajayi, Udeh and Odejide, 2024). However, the digital landscape is rife with hackers seeking unauthorized access to information. Cybercriminals are becoming increasingly sophisticated, with approximately 450,000 new malware types emerging daily, posing a threat to the data of both individuals and businesses (Aboaoja, Zainal, Ghaleb, Al-Rimy, Eisa and Elnour 2022). Consequently, it is crucial to protect this data from such cyber threats.

The financial impact of cybercrime surpasses that of natural disasters annually and is projected to be more profitable for cybercriminals than the combined global trade of all major illegal drugs (Kshetri 2021). The costs associated with cybercrime include data damage and destruction, stolen money, lost productivity, intellectual property theft, personal and financial data theft, embezzlement, fraud, post-attack disruption, deletion of compromised data and systems, and reputational damage. Cybercriminals can effectively hold businesses and the economy hostage through various tactics, including breaches, ransomware, and denial-of-service attacks (Kshetri 2021).

Data protection involves safeguarding vital information from corruption, compromise, or loss. Its importance has increased as the volume of data generated and stored grows at an unprecedented rate. The COVID-19 pandemic forced millions of employees to work from home, necessitating secure remote data transfer and access. Therefore, businesses must adapt to protect data whether it is in a central office data center or on employees' home laptops (Olawale, Ajayi, Udeh and Odejide 2024).

2. PROBLEM STATEMENT

As more organizations today continue to use internet and data as vital business tools to conduct their routine and daily processes, the need for security of information assets of an organisation cannot be over-emphasised. Organizations are utilising the opportunities offered by computers and online systems to adopt innovative business operations, to increase business efficiency, to develop customer-centric strategies, and to stay competitive with the use of technology. It is therefore imperative to ensure that their data is protected against any kind of failures or attacks. Although, computers and online systems offers several benefits for achieving business success, if these services used are not sufficiently available, reliable, and secure, cybercriminals will hold businesses and the economy hostage through breaches, ransomware, denial of service attacks and more. For organizations the consequences include reputational damage, financial loss, ransomware costs, operational standstill among others. For individuals, the consequences may further include identity theft, blackmail campaigns, social engineering attacks and many others. Therefore, it is essential to have a comprehensive, a holistic cybersecurity strategy for data protection in organizations that would aid businesses and the governments alike to protect their information assets.

3. LITERATURE REVIEW

In the third quarter of 2023, internet users globally experienced about 15 million data breaches, marking a 167 percent increase from the previous quarter (Umbach, Singh and Walker 2023). It is almost certain that a cyberattack will affect anyone connected to the internet; however, predicting the exact timing is impossible. Hence, it is essential for everyone to prepare and plan for the prevention of such crises (Pureti 2024).

As more data is generated and networks become more accessible, cybercriminals are finding new vulnerabilities to exploit. In our increasingly digital and connected world, cybercrime pervades all industries. The following facts and statistics highlight the current cybercrime landscape:

- The cost of cybercrime is expected to reach $10.5 trillion by 2025, as reported in the latest edition of the Cisco/Cybersecurity Ventures "2022 Cybersecurity Almanac" (Cisco/Cybersecurity Ventures 2022).
- In October 2022, hackers attacked an Australian communications platform managing Department of Defence data, executing a ransomware attack that likely compromised sensitive government information (Sarre and Prenzler 2023).
- Also in October 2022, a newly identified hacking group targeted telecommunications, internet service providers, and universities in the Middle East and Africa. This group deploys malware directly into system memory, effectively bypassing native security solutions (Horak 2023).
- In September 2022, hackers infiltrated the Mexican Defence Ministry, accessing six terabytes of data that included internal communications, criminal records, and surveillance data on Ken Salazar, the U.S. Ambassador to Mexico. Mexican President Andres Manuel Lopez Obrador confirmed the authenticity of the leaked information, which included his personal health data (Havler-Barrett 2022).
- Kenya has been the most affected by cybercrime in East Africa, with banks being the primary targets as financial technology adoption increases. Kenya ranks second in Africa for the number of cybercrimes, following Nigeria (Rotich 2020).

Cybersecurity is, therefore, crucial as it protects various types of data from theft and loss, including sensitive data, protected health information (PHI), personally identifiable information (PII), intellectual property, personal information, and information systems of governments and businesses (Pureti 2024).

Top Cyber-Attacks Faced by Organizations

Phishing attacks currently represent the most widespread security threat to the IT sector, with many individuals still falling victim to phishing emails. Cybercriminals have adopted more sophisticated techniques to execute business email compromise (BEC) attacks effectively, resulting in phishing

emails and malicious URLs remaining prevalent on the web. These attacks are now highly localized, more personalized, and geo-targeted (NIST 2019).

The 2019 Data Breach Investigations Report by Verizon indicates that 32% of data breaches that year involved phishing activities (NIST 2019). Consequently, experts predict that targeted phishing will become increasingly common in the coming years. Additionally, 2020 witnessed the creation of over 60,000 phishing websites, with 1 in every 8 employees inadvertently sharing information on these sites (Rotich 2020). In response, businesses are increasingly adopting and investing in comprehensive security awareness programs. Organizations are also implementing simulators to identify and understand emerging phishing patterns and the tactics of cyber attackers (Ochmann 2020).

Crime as a Service (CSaaS)

Crime As a Service (CSaaS) is a relatively new concept in the cybercrime realm, where seasoned cybercriminals create advanced tools or services that they sell or rent to less experienced criminals. This allows even those with limited knowledge and expertise to execute attacks with relative ease. This evolution in the cybercrime industry mirrors trends seen in legitimate software and digital services (Huang, Siegel and Madnick 2017).

Ransomware operators are prominent adopters of the CSaaS model. Underground digital marketplaces now provide virtually all components of a cybercrime toolkit to those willing to pay, ranging from victim targeting and initial compromise to evasion, operational security, and malware delivery (Hyslip 2020).

Professional attack tools, often with bypassed licensing, are also widely available. For instance, Cobalt Strike, initially intended for use by security professionals to emulate advanced attackers, is now prevalent in most ransomware incidents. Brute Ratel, another advanced exploitation tool marketed as a Cobalt Strike replacement, has also been observed in numerous ransomware incidents (Hyslip 2020).

The misuse of legitimate software and Windows operating system components continues to challenge defenders. Criminal actors increasingly exploit legitimate executables, such as trial versions of commercial software products and remote access tools, along with “living off the land binaries” (LOLBins), to evade detection and deploy malware (Kshetri 2021).

The resurgence of “bring your own driver” attacks, where malicious actors use vulnerable drivers from legitimate software to elevate privileges and attempt to disable endpoint detection and response products to avoid detection is also being seen (Hyslip 2020).

On the mobile front, there has been a continued presence of malicious or fraudulent fake applications evading detection by major mobile app marketplaces. Some of these apps are part of a rapidly growing cybercrime category: financial trading fraud. Sophos has tracked the rapid expansion of cryptocurrency and other trading scams, such as “pig butchering” schemes, which use fake applications to trick victims into exposing their mobile crypto wallets or transferring funds directly. This includes the abuse of Apple’s iOS ad-hoc application deployment schemes (Sophos 2023).

Insider vs Outsider Threats

Historically, data breaches reported in the news are typically executed by outsiders. While these breaches can cause significant damage, they are generally addressed with traditional security measures. Insider threats, however, are more challenging to prevent and detect using standard security solutions (Hunker and Probst 2011).

One reason insider threats are difficult to mitigate is that insiders do not always compromise data security intentionally. Many data breaches caused by insiders are completely accidental. To combat these risks, as well as intentional threats from malicious insiders, a holistic security approach is essential. This approach must effectively address both insider and outsider threats, managing both unintentional and intentional risks posed by those within the organization (Chirayath 2023).

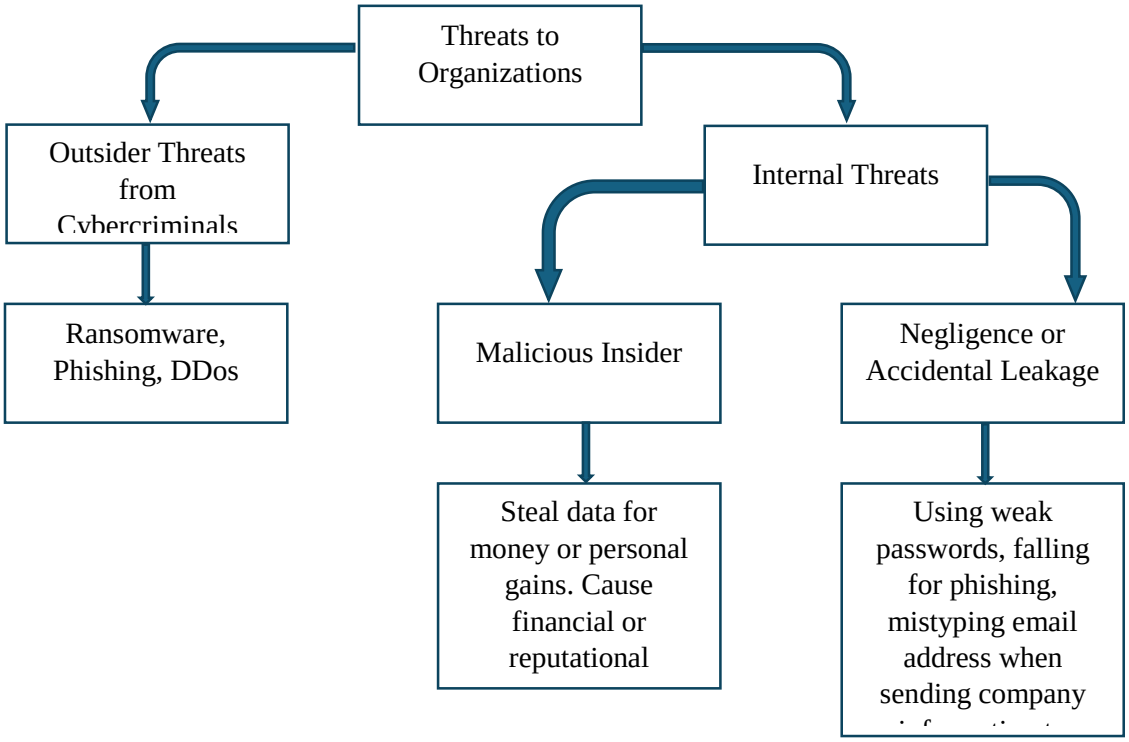

Fig.1. *Threats in Organizations*

4. SUGGESTED CYBERSECURITY STRATEGY

The Human Factor: Regular User Training

The term "people" refers to the human resources available within the organization. People are responsible for executing tasks outlined in processes, often utilizing technology. Many businesses tend to focus heavily on technology and processes while neglecting the human element. Therefore, ensuring that the team comprises individuals with appropriate skills and effective communication is crucial.

Mere implementation of security measures and selective information dissemination is insufficient. Organizations need their employees to be fully aware of security measures and equipped to respond effectively to suspicious activities. Human error constitutes the primary cause of security incidents, and addressing this issue is essential in mitigating attacks within the organization. Security Awareness Training is pivotal in this regard. Training employees to recognize and respond to cyber threats effectively can prevent the development of cyber attacks (Ghafir, Saleem, Hammoudeh, Faour, Prenosil, Jaf and Baker 2018).

Key aspects of the training include: (Hatzivasilis, Ioannidis, Smyrlis, Spanoudakis, Frati, Goeke and Koshutanski 2020)

- Comprehensive Training: Initial training should encompass a wide range of topics. Effective campaigns tailor training to individual needs, offering various options to suit organizational requirements.
- Simulated Scenarios: Testing users with simulated phishing emails and scams is crucial. Studies have shown that simulated scenarios, coupled with awareness training, yield better results than standalone training. These scenarios involve sending fake phishing emails to users to assess their response to potential threats.
- Cultural Shift: Awareness campaigns require collective participation. While decision-makers acknowledge the importance of IT security and awareness training, it is essential to ensure that every individual within the organization values cybersecurity. Leadership must communicate the significance of training to all employees to foster a culture of cybersecurity awareness.

- Results Orientation: Like any organizational initiative, awareness campaigns should be results-driven. Clear goals must be established, and progress updates should be provided regularly to assess the effectiveness of the program.

Effective Policies

A cybersecurity policy consists of formal documented guidelines provided by an organization to its employees, outlining approaches to safeguard the organization's data. It delineates rules, principles, and approaches that individuals should adhere to in order to protect sensitive information, data, and digital assets, thereby ensuring optimal management of cybersecurity risks (Kshetri 2021).

Cybersecurity policies and procedures serve as a roadmap for organizations, outlining responsibilities and best security practices necessary to protect digital resources. A comprehensive cybersecurity policy should address the following areas: (Ochmann 2020; Ghafir, Saleem, Hammoudeh, Faour, Prenosil, Jaf, and Baker 2018)

- Risk Management: A well-defined policy identifies and addresses risks and vulnerabilities within the infrastructure, implementing appropriate security protocols and measures to mitigate these risks effectively.
- Compliance Requirement Adherence: A robust policy ensures organizational compliance with all regulations and laws pertaining to data protection, thereby mitigating legal risks associated with cybersecurity breaches.
- Incident Response: The policy should outline reporting procedures, quarantine methodologies, and recovery processes to facilitate effective incident response and minimize the impact of security breaches.
- Employee Awareness: Enforcing cybersecurity policies enables organizations to define employee roles and responsibilities, ensuring the security of all digital assets. A cybersecurity awareness policy is crucial as it educates employees about various cyber threats and equips them with procedures to prevent common attacks.

The UTM Technology and Security-as-a-Service

Cybercriminals are continuously advancing their tactics, leading to a rise in data breaches. Recent studies identify phishing attacks, ransomware, social engineering, and IoT attacks as top cybersecurity threats. These malicious activities can result in substantial financial losses, reputational damage, and legal liabilities (Padmaraju 2024).

Maintaining a proactive stance in cybersecurity is imperative to thwart cyberattacks and safeguard sensitive data. Embracing the latest cybersecurity technologies empowers organizations to fortify their security posture and mitigate potential risks. By doing so, organizations can protect their information assets and shield themselves from looming threats. Consequently, keeping abreast of the latest cybersecurity technologies is no longer a choice but a necessity to ensure data safety and business continuity.

At a minimum, organizations prioritizing data security should deploy a next-generation firewall (NGFW) and endpoint security solutions. NGFWs offer enhanced features compared to traditional firewalls, providing comprehensive threat protection (Singh and Singh 2024).

For larger enterprises, Unified Threat Management (UTM) software or security appliances are recommended. UTMs, available as cloud-based services or virtual appliances, offer integrated threat protection alongside fundamental networking and security services. These include network address translation (NAT), remote routing, next-generation firewalls (NGFW), secure email and web gateways, intrusion prevention systems (IPS), WAN connectivity, and virtual private networks (VPN), among others. UTMs deliver critical security capabilities, including asset discovery, vulnerability assessment, behavioural monitoring, threat detection, and security intelligence and correlation. Moreover, UTMs facilitate compliance management with standards like PCI, HIPAA, and ISO (Padmaraju 2024).

Security-as-a-Service (SECaaS) presents a cloud-based approach to outsourcing cybersecurity needs. Outsourced security services encompass data protection, VoIP security, database security, and general network security. These solutions aid organizations in combating network threats such as malware and botnets. SECaaS is pivotal for corporate data security as it offers scalability as businesses expand and eliminates the need for costly on-premises security infrastructure (Singh and Singh 2024).

In essence, whether implementing UTM or SECaaS, organizations must prioritize technologies offering early detection and prevention capabilities, alongside centralized analytics and automated response mechanisms, to bolster their defence against cyber threats.

5. SUMMARY

In today's interconnected digital landscape, where cyber threats are evolving at an alarming rate, organizations must implement a comprehensive data protection mechanism to safeguard their sensitive information. The synergy between the three proposed cybersecurity strategies: Regular User Training, Effective Policies, and UTM Technology and Security-as-a-Service forms the cornerstone of such a mechanism.

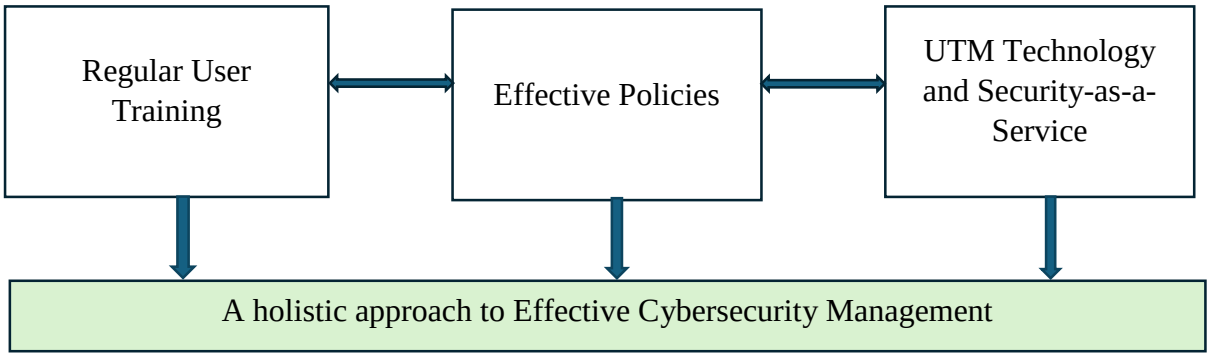

***Fig.2**. Holistic Cybersecurity Management*

By integrating Regular User Training, Effective Policies, and UTM Technology and Security-as-a-Service, organizations can establish a multi-layered defence strategy that addresses both human and technical aspects of cybersecurity. This holistic approach not only enhances the organization's resilience to cyber threats but also instils confidence among stakeholders regarding the protection of sensitive data and the continuity of business operations.

6. CONCLUSION

This paper describes some specific areas where our Information System is weak and should be beefed up. Our Information Systems are confronted with not only infinitely varying possible threats, but several specific known threats including staff who operate these information systems.

In order to thwart potential attacks, a fundamental shift in mindset is imperative among all employees is imperative. This will involve education, institutionalization of sane practices, heightened awareness of security threats, increased concern and importance placed on the security of our data, and willingness to use secure access tools.

Most importantly, however, is to abolish reliance on technology as the sole provider of all security provisions. While technology plays a vital role in fortifying our systems, it cannot offer a foolproof solution by itself. Because there are so many ways to get through even the most wonderful firewall, the security and vulnerability of internal data systems needs to be taken just as seriously as those that are external.

While achieving impenetrable barriers to data stores and information systems is unrealistic, our focus should be on minimizing the impact of inevitable breaches. This includes preventing information

leakage that could compromise system integrity, safeguarding against unauthorized access, and mitigating insider threats through stringent access controls and monitoring mechanisms.

REFERENCES

Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-Rimy, B. A. S., Eisa, T. A. E., and Elnour, A. A. H. "Malware Detection Issues, Challenges, and Future Directions: A Survey." *Applied Sciences* 12, no. 17 (2022): 8482.

Chirayath, S. S. "Insider Threats and Strategies to Manage Insider Risk." In *Human Reliability Programs in Industries of National Importance for Safety and Security*, 51-59. Singapore: Springer Nature Singapore, 2023.

Cisco/Cybersecurity Ventures. *2022 Cybersecurity Almanac*. Cisco/Cybersecurity Ventures, 2022.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., and Baker, T. "Security Threats to Critical Infrastructure: The Human Factor." *The Journal of Supercomputing* 74 (2018): 4986-5002.

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., and Koshutanski, H. "Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees." *Applied Sciences* 10, no. 16 (2020): 5702.

Havler-Barrett, C. "Mexico's Truth Stares Down Barrel of a Gun." *Index on Censorship* 51, no. 4 (2022): 16-20.

Horak, G. "Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa." PhD diss., Harvard University, 2023.

Huang, K., Siegel, M., and Madnick, S. "Cybercrime-as-a-Service: Identifying Control Points to Disrupt." Tech. Rep., Massachusetts Institute of Technology (MIT), 2017.

Hunker, J., and Probst, C. W. "Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques." *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.* 2, no. 1 (2011): 4-27.

Hyslip, T. S. "Cybercrime-as-a-Service Operations." In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 815-846, 2020.

Kshetri, N. *Cybersecurity Management: An Organizational and Strategic Approach*. University of Toronto Press, 2021.

NIST. *Data Breach Investigations Report*. Verizon, 2019.

Ochmann, J. "The Logic of Security." *Security Dimensions. International and National Studies* 33 (2020): 189-216.

Olawale, O., Ajayi, F. A., Udeh, C. A., and Odejide, O. A. "Remote Work Policies for IT Professionals: Review of Current Practices and Future Trends." *International Journal of Management & Entrepreneurship Research* 6, no. 4 (2024): 1236-1258.

Padmaraju, A. K. *Future-Proofing Security: AWS Security Hub and Service Now Integration*, 2024.

Pureti, N. "The Rising Tide of Malware: Protecting Your Organization in 2024." *International Journal of Advanced Engineering Technologies and Innovations* 1, no. 3 (2024): 420-448.

Rotich, E. K. "Cyber Terrorism and National Security in Africa: A Case Study of Kenya." PhD diss., University of Nairobi, 2020.

Sarre, R., and Prenzler, T. "Australian Public and Private Crime Prevention Partnerships in Cyberspace." In *Handbook on Public and Private Security*, 85-102. Cham: Springer International Publishing, 2023.

Singh, L., and Singh, R. "Comparative Analysis of Traditional Firewalls and Next-Generation Firewalls: A Review." In *Latest Trends in Engineering and Technology: Proceedings of the 2nd International Conference on Latest Trends in Engineering and Technology (ICLTET 2023), July 13-14, 2023, Mohali, India*. CRC Press, 2024.

Sophos. *The Rise of Financial Trading Fraud*. Sophos Security Report, 2023.

Umbach, R., Singh, A., and Walker, A. "“Your Protection Is in Your Hands Only”: User Awareness and Adoption of Privacy and Security Practices in Five Majority World Countries." *Journal of Online Trust and Safety* 2, no. 1 (2023).

Scientific and Practical Cyber Security Journal (SPCSJ) 8(2): 40 – 50 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

MATHEMATICAL MODELING: ALGORITHMIC STRUCTURES OF DOD COMMON ACCESS CARDS

Charde'Lyce Edwards BSCS
Full Sail University, Computer Science

ABSTRACT: This study presents a comprehensive examination of the mathematical complexities inherent in the department of defense (dod) common access cards (cac). It delves into the historical progression of the program, tracing its evolution alongside advancements in mathematical modeling. With a specific focus on the algorithmic generation of the bar-code, this paper unveils the equation orchestrating this crucial security feature, vital for maintaining the integrity and security of dod cac cards. Through the unraveling of this mathematical tapestry, the research offers compelling insights into the intricate interplay between mathematics and modern security technology. By seamlessly blending historical context with a detailed exploration of algorithmic intricacies, this study provides a thorough and captivating analysis of this pivotal aspect of security technology. Moreover, it sets the stage for understanding the profound implications of mathematical modeling on security measures, underscoring the critical role of mathematics in shaping modern security practices.

KEYWORDS*:* *Department of Defense (DOD), Common Access Cards (CAC), Mathematical Modeling, Algorithmic Structures, Security Technology*

1. INTRODUCTION

Bar-codes stand as the quintessential symbol of technology's seamless integration into our daily routines, offering efficiency and convenience in various domains, from retail transactions to inventory management. As succinctly noted, "Bar-codes are the most common type of encoding, a feature available in almost all ID card software. They are quick and affordable to print because they do not require special ribbons, cards, encoding modules, or advanced software." (Barcode Encoding - Introduction to ID Card Software - Learning Center — AlphaCard, n.d.).

However, in the realm of bar-code technology, it becomes evident that its sig- significance transcends beyond commercial applications, particularly within secure environments such as the Department of Defense (DOD), where Common Access Cards (CAC) serve as essential tools for authentication and access control. The use of bar-codes in security applications underscores the adaptability and versatility of this technology in safeguarding sensitive information and controlling access to restricted areas.

This research embarks on a comprehensive exploration of the mathematical foundations that support the algorithmic structures of DOD Common Access Cards. Unlike previous approaches, this study introduces an updated method for defining the math- mathematical equation that governs the generation of PDF417 bar-codes. By tracing the historical evolution of bar-code technology and advancements in mathematical modeling, the symbiotic relationship between mathematics and modern security technology is emphasized, highlighting the significance of these insights for ensuring the integrity and security of access credentials. Moreover, it sets the stage for understanding the profound implications of mathematical modeling on security measures, underscoring the critical role of mathematics in shaping modern security practices.

1.1 BACKGROUND

1.1.1 HISTORY AND DEVELOPMENT OF PDF417 BAR-CODES

The emergence of the bar-code dates back to the 1940s when Bernard Silver and Norman Joseph Woodland envisioned a system to streamline supermarket checkout processes. Their vision culminated in 1974 with the development of the Universal Product Code (UPC) by a team led by George Laurer, marking a pivotal moment in bar-code history. Initially conceived as a one-dimensional encoding system, the UPC revolutionized retail operations, ushering in an era of faster and more accurate product scanning. As bar-codes permeated every facet of modern life, their significance transcended beyond commercial transactions to encompass security and identification. However, the limitations inherent in one-dimensional bar-codes soon prompted the exploration of more advanced encoding technologies. This pursuit led to the inception of two-dimensional (2D) bar-codes, which, grounded in mathematical principles, naturally evolved to tackle the intricacies of ensuring seamless data retrieval across diverse applications.
Among the most notable formats is PDF417, introduced in the 1990s by Dr. Ynjiun P. Wang, boasting enhanced data storage capabilities within a compact footprint. PDF417 bar-codes revolutionized bar-code applications by incorporating mathematical algorithms to generate spacing and output, facilitating secure identification and com- comprehensive data storage across various sectors. The discovery of this secure method prompted institutions such as the Department of Defense (DOD) to leverage the versatility of bar-codes, particularly PDF417, by implementing Common Access Cards (CAC), thereby enhancing authentication and access control measures within secure environments.

Having explored the historical and developmental journey of PDF417 bar-codes, it's essential to delve deeper into their structural components and encoding principles. From its humble beginnings in supermarket checkout lines to the applications in security technology, the bar-code has emerged as an indispensable tool in the digital landscape of the modern era. (The Science Behind Barcode Decoding Algorithms - FasterCapital, n.d.)

1.1.2 DESCRIPTION OF PDF417 BAR-CODE STRUCTURE AND COMPONENTS

The PDF417 bar-code consists of multiple rows of linear bar-code symbols stacked on top of each other. Each symbol represents a codeword that encodes a specific set of data and is structured into three main components:

1. **Start and Stop Patterns**: The PDF417 bar-code begins with a start pattern and ends with a stop pattern, which provide the boundaries of the bar-code. These patterns help scanners identify the beginning and end of the bar-code.
2. **Codewords**: The data encoded in the PDF417 bar-code is divided into codewords. Each codeword represents a character or a set of characters, depending on the encoding mode used. PDF417 supports multiple encoding modes, including text, numeric, byte, and byte compaction.
3. Error Correction Codewords: PDF417 includes built-in error correction capabilities to ensure data integrity even if the bar-code is partially damaged or obscured. Error correction codewords are added to the bar-code to detect and correct errors during scanning. The level of error correction can be adjusted to balance data capacity and redundancy.(CHIPS Articles: Safeguarding Your Common Access Cards and Military Identification Cards, n.d.)

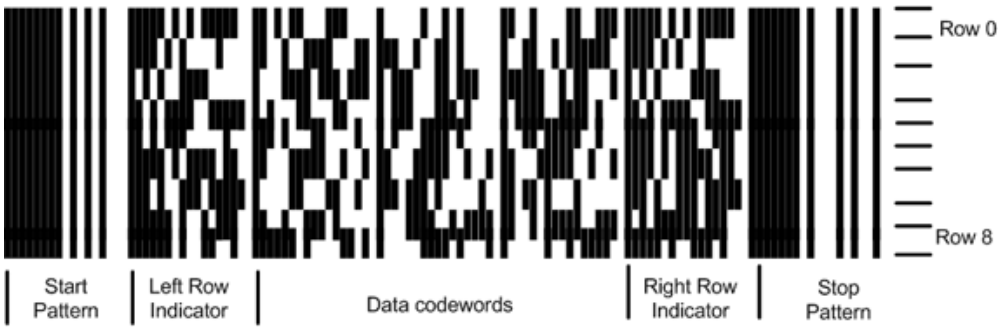

Fig.1. *Anatomy of PDF417 bar-code*

Additionally, the PDF417 bar-code structure is flexible and can accommodate various data formats and sizes. It supports up to 90 different symbols, each consisting of 17 modules (black and white bars) in width and up to 30 rows in height.

1. **Quiet Zones**: PDF417 bar-codes require quiet zones, also known as margins, on all sides to ensure accurate scanning. These quiet zones are empty spaces that provide separation between the bar-code and any surrounding text or graphics.
2. **Data Columns**: PDF417 bar-codes are divided into data columns, each containing a set number of codewords. The number of data columns determines the bar-code's width and affects its overall data capacity.
3. **Rows**: PDF417 bar-codes consist of multiple rows of codewords stacked vertically. The number of rows depends on factors such as the amount of data encoded and the desired bar-code size.
4. **Structured Append**: PDF417 supports structured append, allowing multiple PDF417 symbols to be linked together to encode larger datasets. This feature enables efficient data management and retrieval.(2 Overview - PDF417 Fonts Encoder 5 User Manual, n.d.)

1.1.3 ENCODING PRINCIPLES AND SPECIFICATIONS

Encoding principles are fundamental to PDF417's versatility, enabling the representation of vast amounts of data within a limited space. Unlike traditional linear bar-codes, PDF417 transcends the confines of a single dimension, harnessing the power of two- dimensional encoding. As explored by DENSO WAVE, "..information can be encoded in both the transverse and the longitudinal directions (two dimensions).' This bidirectional encoding capability not only enhances data capacity but also facilitates robust error correction, ensuring the integrity and reliability of information retrieval." (What Is a 2D Code? Technical Information of Automatic Identification DENSO WAVE, n.d.) The integration of both transverse and longitudinal encoding epitomizes the sophistication underlying PDF417's encoding principles, emphasizing its indispensable role in modern security and data management contexts

2 MATHEMATICAL FOUNDATIONS

2.1 MATHEMATICAL MODELING OF PDF417 BAR-CODE GENERATION

Mathematical modeling of PDF417 bar-code generation entails a meticulous endeavor to ensure precise data encoding within the symbol's complex framework. The PDF417 symbol can encompass varying numbers of rows, ranging from as few as 3 to as many as 90. Each row adopts characters from a designated cluster for data encoding, with cluster assignment repeating systematically every third row. This organized allocation of clusters to rows is governed by a formula, ensuring efficient decoding strategies and enabling scanners to decipher PDF417 symbols seamlessly, even across multiple rows:

Cluster number = ((row number − 1) mod 3) × 3

facilitates efficient decoding strategies, enabling scanners to decipher PDF417 symbols seamlessly, even across multiple rows.

The structural composition of rows adheres to a distinct pattern, commencing with a left-row indicator (L) followed by a sequence of data region characters, with the most significant characters positioned adjacent to the left-row indicator. Subsequently, each row concludes with a right-row indicator (R). These row indicators, symbolized characters located near the start and stop patterns, encode critical information such as the row number, total row count (ranging from 3 to 90), data region column count (ranging from 1 to 30), and error correction level (ranging from 0 to 8). This meticulous structuring of rows and clusters within the PDF417 symbol ensures efficient data encoding and robust bar-code integrity, facilitating accurate and reliable data retrieval across various applications. (PDF417 Specification for Barcode Symbology, n.d.).

After establishing the fundamental principles of PDF417 bar-code generation, the mathematical foundations provide a comprehensive framework for understanding the intricate algorithms and equations governing their structure and encoding. From calculating row height to implementing error correction mechanisms, each aspect con- tributes to the robustness and reliability of PDF417 bar-codes across various security and data management applications.

2.1.1 EQUATIONS FOR CALCULATING ROW HEIGHT

The fundamental unit governing the bar-code's structure is the module, dictating crucial aspects of its design. Central to this is the individual row height, intricately tied to the module height, ensuring uniformity and precision within the symbol. Complementing this, the width of a module, commonly denoted as the X dimension, further defines the symbol's spatial dimensions. However, it is the ratio of module height to width, known as the y-height, that holds particular significance.

$$W = (17C + 69)X + 2Q$$

$$H = RY + 2Q$$

where:

H = Height of symbol
W = Width of symbol
C = Number of columns in the data region
R = Number of rows
X = X-dimension of the symbol
Y = Row height
Q = Size of Quiet Zone (minimum 2X)

Fig.2. *Width and Height Equations (PDF417 Specification for Barcode Symbology, n.d.)*

With industry standards advocating for a minimum y-height of 3.0, emphasis is placed on maintaining adequate proportions for enhanced decodability. This meticulous attention to detail underscores the commitment of the symbology to optimal readability and reliability, ensuring that PDF417 symbols fulfill their role effectively across various applications. (2 Overview - PDF417 Fonts Encoder 5 User Manual, n.d.)

2.1.2 OVERVIEW OF BASE 929 ENCODING SCHEME

The BASE 929 encoding scheme, integral to PDF417 bar-code generation, employs a meticulous process to compute error correction codewords, ensuring data integrity and reliability. These codewords are derived as the complement of coefficients obtained by dividing the symbol data polynomial $d(x)$ by the generator polynomial $g(x)$, multiplied by x^k, within the Galois Field GF(929). Negative values within this field are treated with the complement of their absolute values, ensuring consistency in encoding. The generator polynomial for k error correction codewords is defined as

$$g(x) = (x - 3)(x - 3^2) \cdots (x - 3^k)$$

serving as the cornerstone of the encoding process. (PDF417 Specification for Barcode Symbology, n.d.)

Among all physical parts of a PDF-417, the data codewords are used for encoding the message data, which could be numbers, letters, or other symbols. PDF417 uses Reed–Solomon error correction. PDF417 bar-code symbology adopts a base 929 mode, where each codeword represents a numeric digit ranging from 0 to 928. Among these codewords, 900 are designated for information data encoding, while the remaining 29 serve specific functions within the bar-code. PDF417 supports three distinct encoding modes—text, byte, and numeric—which can be combined as needed. In the text mode, each codeword signifies 1 or 2 characters, while in the byte mode, groups of 5 codewords represent 6 bytes. Numeric encoding mode utilizes groups of 15 codewords to represent 44 decimal digits, ensuring flexibility and efficiency in data representation within PDF417 bar-codes. (VB.NET PDF417 Generator — Generate, Draw PDF417 Barcode Image In VB.NET Applications With Valid Data Input, n.d.)

2.2 ALGORITHM DESIGN

The evolution of the PDF417 bar-code generation algorithm reflects a journey marked by refinement and abstraction, drawing inspiration from the principles of Set Theory. Originally, the algorithm involved intricate calculations to determine row height (Y) and cluster number (K) for each codeword, encapsulated in separate equations:

1. **Calculate Row Height (Y) in terms of X (minimum width of a vertical bar):**

$$Y \geq 3X$$

This ensures that the height of each row (Y) is at least three times the width of a vertical bar (X), providing sufficient space for encoding data.

2. **Calculate Cluster Number (K) for Each Codeword: Equation 1:**

$$K = b_1 - b_2 + b_3 - b_4 + 9 \mod 9$$

Equation 2:

$$K = E_1 - E_2 + E_5 - E_6 + 9 \mod 9$$

By following these steps, the algorithm generates each row of the PDF417 bar- code, incorporating the necessary components such as quiet zones, start and stop patterns, and data codewords, resulting in the complete bar-code symbol.

However, guided by the pursuit of elegance and clarity, these calculations under- went a transformation. Through a process of consolidation, they were unified into a single expression, symbolized by the union operator, reflecting the essence of Set Theory.

$$\text{PDF417\_Barcode} = \bigcup_{i=1}^{N_{\text{rows}}} \text{Row}_i$$

Fig.3. *Proposed Equation*

This abstraction not only streamlined the algorithms for row height and the cluster but also imbued it with a sense of cohesion and clarity, echoing the rigorous standards of mathematical modeling.

2.2.1 STEP-BY-STEP EXPLANATION OF THE ALGORITHM

The process of generating a PDF417 bar-code can be summarized into several key steps. At its core, the PDF417 bar-code comprises multiple rows, each containing essential components for encoding data. The total number of rows, denoted as N_{rows}, encapsulates the entire bar-code symbol. Within each row, represented as Row_i, various components are arranged to ensure accurate encoding and decoding. These components include the quiet zone, start and stop patterns, row left and right codewords, and the data codewords themselves. By structuring the bar-code in this manner, the algorithm orchestrates the generation of a complete PDF417 bar-code symbol, ready for scanning and interpretation.

2.2.2 CONSIDERATIONS FOR PARAMETER SELECTION AND OPTIMIZATION

However, there are several considerations that should be noted when utilizing this formula:

1. **Union of Rows**: The formulation of the PDF417 bar-code algorithm involves the union of multiple rows, each containing essential components such as quiet zones, start and stop patterns, data codewords, and row left and right code- words. The selection of parameters for each row, including the size of quiet zones and the placement of codewords, directly impacts the overall bar-code quality and readability.

[2]These equations determine the cluster number (K) for each codeword in the PDF417 bar-code. The values b_1, b_2, b_3, b_4 and E_1, E_2, E_5, E_6 are derived from the encoded data, and the modulo operation ensures that the result remains within a valid range.

2. **Row Height**: Optimizing the height of each row ensures sufficient space for encoding data and maintaining bar-code readability. The row height should be carefully chosen to accommodate the required number of data codewords while adhering to industry standards and best practices.
3. **Start and Stop Patterns**: The design and placement of start and stop patterns play a crucial role in bar-code scanning and decoding. Parameters such as pat- tern size, spacing, and alignment should be optimized to facilitate reliable bar-code recognition and decoding.
4. **Quiet Zones**: Adequate quiet zones between rows and around the bar-code symbol are essential to minimize interference and ensure accurate scanning. The size of quiet zones should be carefully determined based on scanning device requirements and environmental conditions.
5. **Data Codewords**: The selection of parameters for data codewords, including encoding mode, error correction level, and data compression, influences bar-code capacity and reliability. Optimizing these parameters ensures efficient data encoding and robust error detection and correction capabilities.
6. **Checksums**: Incorporating check-sums into the bar-code data enhances error detection and correction during scanning. The choice of checksum algorithm and implementation should be optimized to balance data redundancy and bar-code efficiency.
7. **Testing and Validation:** Thorough testing and validation of the bar-code generation algorithm are essential to ensure that selected parameters and optimizations meet the requirements of specific applications. Testing should encompass a variety of scanning devices and environments to assess bar-code readability and reliability comprehensively.

3 IMPLEMENTATION WALK-THROUGH

3.1 PROGRAMMING ENVIRONMENT AND TOOLS USED

In the programming environment, Visual Studio Code (VSCode) served as the primary tool for developing the PDF417 bar-code generation code. Leveraging the capabilities of VSCode, I seamlessly integrated the ZXing.PDF417 package into the C project. However, the essence of the implementation lay in ensuring the incorporation of my equation, into the code base. This involved several adjustments and customization within the provided framework, aligning the generated bar-codes with the theoretical union equation.

3.2 DETAILED CODE WALK-THROUGH

The proceeding is a detailed explanation of the C# code that is used to generate PDF417 bar-codes.

3.2.1 Input Data

In order to pragmatically use the prior defined equation method this research is proving, first the input data must be defined an example will be used in this instance It begins by defining the input data, including the name, social security number (SSN), and Department of Defense (DOD) ID number. These data elements are encoded into the PDF417 bar-code.

```
string name = " John Doe"; string ssn = " 123
-45 -6789 "; string dod Id = " 1234567890 ";
```

3.2.2 Conversion to Binary

Next, convert the input data to binary format. This is achieved by iterating over each character in the input strings and converting them to their binary representations.

```
string binary Name = String To Binary ( name ); string binary Ssn
= String To Binary ( ssn );
string binary Dod Id = Convert. To String ( Convert. To Int32 ( dod Id ), 2).
            Pad Left (40 , '0 ');
```

3.2.3 Compression

After converting the data to binary, it is compressed to reduce the size before encoding it into the bar-code.

```
byte [] compressed Data = CompressString ( combined Data );
```

3.2.4 PDF417 Barcode Generation

Finally, the PDF417 is generated using the compressed binary data. The data is divided into rows, and each row is encoded separately to form the complete bar-code.

```
Bitmap bar-code = Generate PDF 417 Barcode ( compressed Data );
```

3.2.5 Concatenation of Row Images

In this step, the images of each row are concatenated form the complete bar-code image.

```
static Bitmap Concatenate Images ( Bitmap image1 , Bitmap image2 )
{
        Bitmap combined Image = new Bitmap ( image1 . Width , image1 . Height
                + image2 . Height);
        using ( Graphics g = Graphics. From Image ( combined Image ))
        {
                g. Draw Image ( image1 , 0 , 0);
                g. Draw Image ( image2 , 0 , image1 . Height);
```

```
        }
        return combined Image ;
}
```

3.3 TESTING AND VALIDATION PROCEDURES

In the testing and validation phase, the code was executed, debugged, and the resulting PDF417 bar-codes were generated and printed out for examination. This process ensured that the code executed as intended and produced the expected output.

3.3.1 Presentation of Generated PDF417 Bar-codes

Here is the generated PDF417 bar-code:

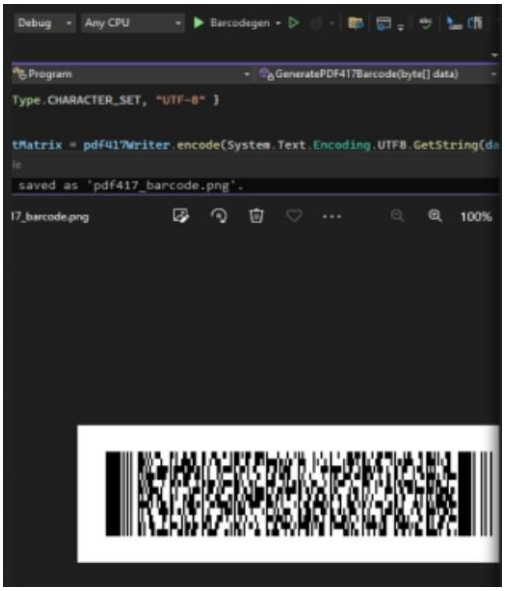

Fig.4. *PDF417 Bar-code*

4 RESULTS AND ANALYSIS

4.1 COMPARISON WITH EXISTING BARCODE GENERATION METHODS

The equation presented in this study for generating PDF417 bar-codes offers a novel approach that distinguishes itself from existing bar-code generative methods. While traditional methods often rely on predefined algorithms and mathematical mod- els, the equation proposed here offers a more flexible and adaptable framework. By emphasizing the dynamic composition of the bar-code through the union of rows, this enables greater customization and scalability in bar-code generation. Moreover, the equation's incorporation of mathematical principles tailored to the specific requirements of Department of Defense (DOD) Common Access Cards (CAC) underscores its relevance and effectiveness in the realm of security technology. This comparative analysis highlights the innovative potential of the proposed equation in advancing the field of bar-code generation and enhancing security measures for sensitive applications.

4.1.1 Limitations and Challenges of the Proposed Algorithm

While the proposed algorithm for generating PDF417 bar-codes offers significant advantages in terms of flexibility and adaptability, it is not without its limitations and challenges. One notable limitation is the requirement to follow virtually the same steps for each cluster, albeit with a streamlined approach to enhance readability. While this simplification improves the algorithm's usability, it may also introduce constraints in certain scenarios where intricate customization is necessary. Additionally, great lengths were taken during the algorithm's development to ensure that it consistently outputs a valid bar-code. However, despite these efforts, the complexity of bar-code generation poses inherent challenges, including the need to balance readability, data capacity, and error correction. Addressing these challenges necessitates a delicate balance between algorithmic efficiency and bar-code quality, highlighting the ongoing need for refinement and optimization in bar-code generation techniques.

4.2 Suggestions for Future Research and Improvements

As the field of bar-code generation continues to evolve, there are several promising directions for future research and improvements:

1. One avenue for exploration is the enhancement of error correction mechanisms within the algorithm to improve bar-code reliability, particularly in environments prone to data corruption or interference.
2. Additionally, further investigation into optimizing the algorithm's performance could lead to advancements in bar-code generation efficiency, enabling rapid production of complex bar-codes with minimal computational resources.
3. Moreover, exploring alternative encoding schemes or incorporating emerging technologies, such as machine learning algorithms, could offer novel approaches to bar-code generation with improved data density and security features.

Collaborative efforts between researchers and industry stakeholders could facilitate the development of standardized benchmarks and evaluation metrics for assessing the effectiveness and robustness of bar-code generation algorithms, fostering innovation within the field.

DECLARATIONS

The following are the declarations presented by the author on the availability of the material as well as the funding"

5 CONCLUSION

5.1 IMPLICATIONS FOR BAR-CODE SECURITY AND TECHNOLOGY

The development of the proposed algorithm carries significant implications for bar-code security and technology. By providing a more dynamic and adaptable framework for generating PDF417 bar-codes, the algorithm enhances the resilience of bar-code-based security measures, particularly in applications requiring stringent data protection and authentication protocols, such as government-issued identification cards and product authentication labels. Furthermore, this emphasis on error correction and readability optimization contributes to the overall robustness and reliability of bar-code systems, reducing the risk of unauthorized access or data tampering. As bar-code technology continues to play an increasingly integral role in various industries, including logistics, retail, and healthcare, the adoption of advanced bar-code generation techniques offers opportunities for enhancing operational efficiency, supply chain visibility, and consumer trust. By leveraging the capabilities of the proposed algorithm,

organizations can increase their security posture and unlock new possibilities for leveraging bar-code technology in a rapidly evolving digital landscape.

5.2 CLOSING REMARKS

Through the unveiling of the mathematical intricacies behind PDF417 bar-code generation, this study illuminates the symbiotic fusion of mathematics and modern security technology. As we navigate the evolving landscape of digital security, the insights gleaned from this research serve as a catalyst for future advancements in bar-code technology. With an unwavering commitment to exploration and collaborative endeavor, we stand poised to unlock new possibilities and address emerging challenges in the realms of digital security and information management, and journey towards a safer and more resilient digital landscape.

REFERENCES

1. Barcode Encoding - Introduction to ID card software - Learning Center — AlphaCard. Retrieved from https://www.alphacard.com/learning-center/intro-to-id-card-software/encoding-options/barcode-encoding/

2. CHIPS articles: Safeguarding your common access cards and military identification cards. Retrieved from https://www.doncio.navy.mil/Chips/ArticleDetails.aspx?ID=8042

3. DENSO WAVE. (n.d.). What is a 2D code? Retrieved from https://www.denso-wave.com/en/adcd/fundamental/2dcode/2dcode/index.html

4. Department of the Navy Chief Information Officer. (n.d.). CHIPS articles: Safeguarding your common access cards and military identification cards. Retrieved from https://www.doncio.navy.mil/Chips/ArticleDetails.aspx?ID=8042

5. FasterCapital. (n.d.). The science behind bar-code decoding algorithms. Retrieved from https://fastercapital.com/topics/the-science-behind-barcode-decoding-algorithms.html

6. Morovia Corporation. Overview - PDF417 Fonts & Encoder 5 User Manual. Retrieved from https://www.morovia.com/manuals/pdf417-font-encoder/chapter.overview.php

7. Updated plan for the removal of Social Security Numbers (SSNs) from Department of Defense (DOD) identification (ID) cards. Privacy, Civil Liberties, and Freedom of Information Directorate U.S. Department of Defense. Retrieved from https://dpcld.defense.gov/Portals/

8. VB.NET PDF417 Generator — generate, draw PDF417 bar-code Image in VB.NET applications with valid data input. (n.d.). Retrieved from https://www.onbarcode.com/vbnet/data-encoding/pdf417.html

Scientific and Practical Cyber Security Journal (SPCSJ) 8(2): 51 – 58 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

STRENGTHENING CYBERSECURITY IN NIGERIA: A HOLISTIC APPROACH

Adekunle Emmanuel Makanjuola[1], Mary Mojirade Ayantunji[2]
[1]Department of Social Studies, Federal College of Education
[2]Department of Arts & Social sciences Education, Lead City University

ABSTRACT: Given Nigeria's growing reliance on technology, it is imperative that the country take a comprehensive approach in order to strengthen its cybersecurity posture. This article provides an analysis of the current vulnerabilities, focusing on the limitations of the regulatory frameworks that are now in place, the degrees of public awareness, and the protection from vital infrastructure. As a result, it is recommended that a multi-pronged plan be proposed in order to solve these difficulties. The establishment of a comprehensive cybersecurity law, the implementation of national awareness campaigns and the incorporation of cybersecurity education into curriculums, the execution of vulnerability assessments and the enforcement of stricter protocols for critical infrastructure sectors, the investment in capacity building programmes to develop a skilled cybersecurity workforce, and the promotion of international cooperation to share best practices and threat intelligence are all included. Through the implementation of these interrelated measures, Nigeria is able to considerably boost its cybersecurity defences and develop a digital environment that is safer for its residents and enterprises.

KEYWORDS: *Cybersecurity, Holistic Approach, Nigeria, Digital Security, Capacity Building*

1. INTRODUCTION

Nigeria is currently experiencing a widespread and significant transformation in the digital realm. The 2024 Global System for Mobile Communications report reveals that mobile phone usage has reached remarkable levels, with more and more people using their handsets to browse the internet and carry out financial transactions [1]. Jumia's financial statement is evident that this spike has contributed to the growth of e-commerce, with online marketplaces making purchasing and commercial transactions easier [2]. The fintech innovation study revealed the incorporation of technology into everyday life, as seen by the emergence of start-ups providing mobile banking and digital payment services [3]. Nevertheless, this increasing reliance on technology is accompanied with negative consequences. The Nigerian Data Protection Commission (NDPC) report showed that Nigeria is confronted with a substantial predicament posed by cybercriminals that employ phishing, scams, identity theft, and financial fraud [4]. Ransomware attacks present an escalating danger to vital infrastructure and enterprises, with the potential to result in substantial financial damages [5]. Insufficient data security measures worsen the problem, making personal information susceptible to breaches and misuse [6]. The cyber dangers provide a genuine peril to Nigeria's economic progress, national security, and the confidence that residents place in digital platforms.

Nigeria's digital ecosystem is thriving, since there has been a significant increase in the adoption of mobile phones [1]. However, this reliance on digital technology exposes individuals, organisations, and essential infrastructure to a perilous network of cyber assaults. Cyber assaults can have severe repercussions. Individuals are highly vulnerable to cybercriminals who engage in phishing scams, identity theft, and financial fraud [4]. Envision a scenario where a teacher is deceived by a cunningly camouflaged email that seems to originate from their financial institution, leading them to unwittingly provide their login credentials. Subsequently, these pilfered login details can be employed to deplete their diligently accumulated funds, resulting in significant economic distress. Businesses are also susceptible.

Ransomware assaults, in which malevolent individuals encrypt a company's data and want a payment in exchange for its decryption, are become more prevalent [5]. An act of cyber intrusion targeting a prominent retailer has the potential to severely impair its functioning, resulting in financial losses, harm to its reputation, and potentially even workforce reductions. The most concerning dangers are associated with essential infrastructure. Power grids, transportation systems, and communication networks are susceptible to cyber attacks. A case study conducted in 2022, revealed that a power grid can be effectively targeted, resulting in the complete loss of electricity in entire cities [7]. This would lead to the disruption of crucial services and trigger widespread fear. The repercussions of these cascading impacts can severely undermine a nation's security and stability. The potential ramifications of cyber strikes in Nigeria are severe. To ensure the security of its inhabitants, enterprises, and key infrastructure, the nation must comprehend these risks and adopt strong cybersecurity measures, thereby promoting a safer digital future.
The digital ecosystem in Nigeria is experiencing significant growth, but it is also plagued by numerous cyber risks. In order to properly address these hazards, a disjointed strategy will not be adequate. The adoption of a comprehensive approach to cybersecurity is thereby advocated [8]. This method surpasses mere technical solutions, incorporating a network of procedures that tackle weaknesses at several levels. Envision a meticulously maintained residence. A solid base guard against structural problems, while a robust roof provides protection from the weather. However, a house lacking locks renders it susceptible to trespassers. Adopting a holistic approach to cybersecurity is similar to strengthening the overall system. The statement recognises the interdependence of vulnerabilities: inadequate legal structures empower cybercriminals, while insufficient public information renders individuals susceptible to phishing assaults [9]. Simultaneously tackling these vulnerabilities, a holistic strategy enhances the entire cybersecurity posture. Moreover, cybersecurity does not rely solely on one individual. Collaboration among legislators, corporations, law enforcement agencies, and ordinary individuals is essential [10]. An all-encompassing approach promotes this collaboration, guaranteeing that each individual plays a crucial part in establishing a secure digital environment. Essentially, a holistic approach surpasses temporary solutions and constructs a resilient cybersecurity defence system, protecting Nigeria's digital realm for individuals, businesses, and the nation as a whole.

2. CURRENT STATE OF CYBERSECURITY IN NIGERIA

The digital revolution in Nigeria has both positive and negative consequences. As mobile phone usage increases rapidly [1], it creates opportunities for e-commerce and financial inclusion. However, it also exposes the country to an expanding network of cyber dangers. Regrettably, the present condition of cybersecurity in Nigeria exposes notable weaknesses. A significant issue arises from the legal structure. Although there are existing cybersecurity laws, scholars therefore, contend that these laws are fragmented and lack the necessary strength to effectively discourage cybercrime [11, 12]. This provides a secure refuge for malevolent individuals who take advantage of vulnerabilities to initiate phishing schemes, pilfer identities, and perpetrate financial deception [6]. Public awareness is also a challenging aspect. Research indicated a worrisome deficiency in cybersecurity literacy among a significant portion of the Nigerian population [13]. Their lack of awareness renders them more vulnerable to becoming targets of online scams and social engineering strategies. Envision receiving an email that appears to be authentic, requesting your banking information - lacking sufficient knowledge, it is simple to become a victim of such deceit.

Ultimately, Nigeria's crucial infrastructure, which serves as the foundation of the digital economy, is exposed to substantial weaknesses. The presence of outdated systems and inadequate security processes renders them very vulnerable to ransomware assaults, as emphasised in a recent case study [7]. An effective assault on a power grid, for instance, has the potential to incapacitate whole urban areas, resulting in significant economic turmoil and social upheaval. These vulnerabilities reveal a worrisome depiction of Nigeria's present state of cybersecurity. Nevertheless, by recognising these vulnerabilities

and embracing a comprehensive strategy, Nigeria may construct a more robust digital future for its populace and enterprises [11, 12].

3. CHALLENGES IN NIGERIAN CYBERSECURITY

The digital growth in Nigeria has both positive and negative consequences. Although it promotes economic expansion and involvement in the financial system, it also makes the country vulnerable to an increasing network of cyber risks. Regrettably, Nigeria has numerous significant obstacles that impede its capacity to adequately protect itself in the realm of cyberspace.

1. A Patchwork of Laws, Not a Cybersecurity Shield

The legislative framework for cybersecurity in Nigeria is currently fragmented and contains numerous vulnerabilities. Scholars have stated that, the existing sectoral regulations lack consistency and fail to effectively handle emerging and growing cyber dangers [9]. These weaknesses provide a secure environment for cybercriminals to exploit and carry out activities such as launching phishing scams, stealing identities, and committing financial fraud [6]. Implementing comprehensive cybersecurity legislation with explicit directives and more severe punishments will discourage cybercriminal activities and provide law enforcement with enhanced capabilities to investigate and bring legal action against cyber attacks with more efficiency [14].

2. When Knowledge is Power, Lack of Awareness Makes Nigerians Vulnerable

Studies indicate a worrisome deficiency in cybersecurity knowledge among a significant number of individuals in Nigeria [13]. The presence of this digital literacy gap increases their vulnerability to online scams and social engineering approaches. Envision receiving an email that appears to be authentic, requesting your banking information - lacking sufficient knowledge, it is simple to become a victim of such deceit. The poor awareness, as emphasised by scholars is worsened by the restricted availability of education and digital resources in rural populations [15]. Implementing public awareness programmes that specifically target different groups is essential in order to close the knowledge gap and enable Nigerians to securely traverse the digital world.

3. A Skill Gap Threatens Nigeria's Cybersecurity Defences

Nigeria is experiencing a severe scarcity of cybersecurity personnel that possess the requisite expertise to effectively counter advanced cyber attacks. Therefore, it is evident, that this deficiency in skills obstructs the country's capacity to enforce strong cybersecurity measures and adequately counter cyber threats [16]. Tertiary institutions and training institutes frequently do not have the capability to provide extensive cybersecurity programmes. This is imperative to enhance investment in this domain [16]. Developing a proficient workforce is crucial in order to acquire the necessary competence to meet the cybersecurity requirements of the nation.

4. Critical Infrastructure: A Fragile Lifeline in Need of Protection

Nigeria's crucial infrastructure, which serves as the foundation of the digital economy, is exposed to substantial vulnerabilities. For instance, electrical grids and financial institutions frequently depend on outdated technologies that have inherent vulnerabilities [17]. Obsolete technologies are highly vulnerable to cyber attacks, which greatly jeopardise both national security and economic stability. Moreover, the problem is worsened by the absence of strong security standards and regular updates to these systems. Failure to perform adequate maintenance and keep software up to date leaves critical infrastructure susceptible to exploitation [17].

4. HOLISTIC APPROACH TO STRENGTHENING CYBERSECURITY

The digital environment in Nigeria is experiencing significant expansion, however, this progress is accompanied by an increase in cyber risks. Conventional, incremental solutions are no longer sufficient.

To establish a strong cybersecurity defensive system, it is necessary to adopt a comprehensive approach, as suggested by experts such as [8]. This method extends beyond technology alone and includes a network of safeguards that target weaknesses at various levels.

1. Legal & Regulatory Framework: Building a Strong Foundation

A comprehensive legal framework is the foundation of a holistic strategy. Studies have emphasised that the existing fragmented legislation creates opportunities for cybercriminals to exploit [9]. An all-encompassing legislation on cybersecurity, as advocated would create explicit directives; discourage cybercrime by imposing more severe punishments, and enable law enforcement to efficiently counter cyber threats [18]. This legislative framework serves as the basis upon which other measures can be constructed.

2. Public Awareness & Education: Empowering Citizens

Cybersecurity is not solely a technological obstacle; it necessitates a collaborative endeavour that indicates a notable deficiency in cybersecurity knowledge among a substantial number of individuals in Nigeria [13]. The presence of this digital literacy gap renders people vulnerable to online scams and social engineering approaches. Envision receiving an email that appears to be authentic - lacking sufficient knowledge, it is simple to become a target of such deceit. Public awareness efforts play a vital role in closing this gap in knowledge [15]. Through the dissemination of knowledge on secure online habits and potential dangers, we enable individuals to actively contribute to the establishment of a protected digital environment.

3. Critical Infrastructure Protection: Shielding the Backbone

Nigeria's crucial infrastructure, which is the essential foundation of the digital economy, is exposed to substantial vulnerabilities. Obsolete systems and inadequate security measures make them vulnerable to cyber attacks, posing a threat to national security and economic stability [17]. A comprehensive approach gives top priority to the safeguarding of essential infrastructure. This entails doing vulnerability assessments, adopting strong security measures, and ensuring frequent system updates are enforced.

4. Capacity Building & Skills Development: Investing in the Workforce

The field of cybersecurity is a continuous struggle, and proficient experts are important in safeguarding against constantly changing dangers. The severe scarcity of cybersecurity experts in Nigeria is a pointer that lack of these talents impedes the country's capacity to enforce comprehensive security measures and successfully counter cyber threats [16]. It is therefore, essential to invest in capacity building programmes, for efficiency. Enhancing cybersecurity education at colleges and providing specialised training programmes are crucial measures to cultivate a proficient workforce capable of protecting the nation's digital future.

5. Technological Solutions: Equipping the Defenders

Technology is essential in every cybersecurity plan. Nevertheless, technology by itself is not a panacea. Efficient remedies must be executed inside the structure formed by the remaining foundations. This involves implementing firewalls, intrusion detection systems, and other security measures to actively monitor and safeguard against cyber threats.

6. International Cooperation: Sharing Intelligence, Building Alliances

The frontiers of cyber risks surpass geographical bounds and therefore necessitated the importance of international cooperation in sharing optimal methods, threat intelligence, and synchronised reactions to cyber threats [19]. Nigeria's cybersecurity posture is enhanced by collaboration with international organisations and other governments, contributing to a worldwide endeavour to address this persistent concern.

5. STRATEGIES AND INITIATIVES TO STRENGTHENING NIGERIA'S CYBERSECURITY

Nigeria's digital environment requires a strong and effective cybersecurity protection. An all-encompassing approach, incorporating multiple pillars, is essential for ensuring effective protection. Let us examine these fundamental principles and particular tactics and programmes that can be put into practice:

1. Legal & Regulatory Framework: Building a Strong Foundation

Create an all-encompassing legislation on cybersecurity that will precisely delineate cybercrimes, delineate investigation protocols, and institute more stringent sanctions for cyber offences [9]. Create a specialised cybercrime investigation division within law enforcement organisations to handle cybercrimes and enhance expertise in digital forensics. Adopt and approve pertinent global agreements on cybercrime and cooperate with international law enforcement organisations to locate and apprehend cybercriminals who operate in several countries.

2. Public Awareness & Education: Empowering Citizens

Implement a focused nationwide cybersecurity awareness initiative using diverse media channels to instruct individuals on best practices for online safety, methods to identify phishing frauds, and strategies to counter social engineering tactics. Integrate a cybersecurity component into the national curriculum across various educational levels, providing younger generations with essential digital literacy skills. Collaborate with non-governmental organisations (NGOs) and community leaders to coordinate workshops and seminars focused on promoting cybersecurity awareness in rural regions.

3. Critical Infrastructure Protection: Shielding the Backbone

Perform an extensive evaluation of the susceptibility of crucial infrastructure sectors such as power grids and banking institutions at a national level. Establish and implement rules tailored to critical infrastructure sectors, requiring strong security mechanisms and frequent system updates. Promote cooperation between governmental entities and commercial enterprises that possess and manage essential infrastructure to exchange optimal methods and allocate resources towards collaborative cybersecurity endeavours.

4. Capacity Building & Skills Development: Investing in the Workforce

Enhance cybersecurity education at higher education institutions by providing dedicated undergraduate and graduate programmes focused on cybersecurity. Deliver focused training programmes for IT personnel regarding evolving cyber risks, incident response, and security best practices. Facilitate collaborations between educational institutions and industry leaders to provide training programmes that are in line with the latest industry requirements.

5. Technological Solutions: Equipping the Defenders

Deploy firewalls, intrusion detection and prevention systems (IDS/IPS), and data encryption solutions to actively monitor and safeguard networks against cyber threats. Deploy vulnerability management systems to detect and rectify security vulnerabilities in systems and applications. Conduct thorough investigation and examination of the capabilities of technologies such as blockchain for safeguarding data storage and artificial intelligence for identifying and reducing risks.

6. International Cooperation: Sharing Intelligence, Building Alliances

Collaborate with regional cybersecurity organisations such as the African Union's African Cybersecurity and Information Assurance Agency (CAIAA) to exchange optimal methods and information regarding potential risks. Formulate bilateral or multilateral agreements with foreign nations to streamline the exchange of information regarding cyber risks and enable prompt communication and coordinated actions in response. Enhance the expertise of cybersecurity professionals by participating in international training programmes provided by organisations such as the International Telecommunication Union (ITU).

6. BENEFITS OF A HOLISTIC APPROACH

The digital landscape in Nigeria is both advantageous and disadvantageous. Although it facilitates economic expansion and promotes financial access, it also exposes the country to an increasing network of cyber risks. Conventional, incremental solutions are no longer sufficient. An all-encompassing cybersecurity strategy, akin to a heavily walled castle, necessitates robust defences on various fronts. By targeting weaknesses at several levels, this method has the potential to greatly enhance Nigeria's digital security position.

An effective defence against cybercrime begins with a robust legal framework. Stringent cybersecurity legislation with severe sanctions discourages offenders and enables law enforcement to efficiently investigate and punish cyber assaults. This fosters confidence in the digital realm, instilling a sense of security among individuals when engaging in online transactions. Public awareness campaigns hold equal significance. By providing citizens with knowledge and skills to recognise and prevent online dangers, they are empowered to actively protect the digital realm. Citizens, no longer susceptible to phishing scams, have formed a formidable barrier against cybercrime. Firewalls and intrusion detection systems are essential components of advanced security measures. These solutions actively oversee and safeguard networks, promoting a more secure environment for businesses to function and carry out online transactions. This resilient defence mechanism establishes the basis for a flourishing digital economy.

Investing in cybersecurity education and training programmes enhances the internal resilience of the system. An adept labour force can actively detect and resolve weaknesses in vital infrastructure, such as electricity networks and financial establishments. These specialists serve as the protectors of the fundamental infrastructure of the digital economy, ensuring that vital services continue to function and defending the security and stability of the nation's economy. Ultimately, international collaboration is crucial. Nigeria can enhance its defences and provide a more secure digital environment for everyone by collaborating with other nations and organisations to exchange best practices and threat intelligence. This worldwide endeavour guarantees a more secure and affluent future for all individuals.

7. CONCLUSION

Nigeria's digital revolution is a double-edged sword. While it unlocks doors to economic growth and financial inclusion, it also exposes the nation to a growing web of cyber threats. Imagine trying to defend a grand castle with just a single, rickety gate – that's the vulnerability of a piecemeal approach to cybersecurity. A holistic approach, however, is like fortifying the entire castle. This comprehensive strategy strengthens Nigeria's defences on multiple fronts, building a secure digital environment for all. These include: strong legal walls, public awareness Ramparts, technological bulwarks, skilled workforce watchtowers and an international alliances.

Therefore, the benefits of this holistic approach are far-reaching. Clear laws and an empowered citizenry breed trust in online transactions, fostering a thriving digital economy. Secured critical infrastructure ensures a stable national security and economic climate. With increased confidence in the digital space, businesses and citizens can operate and flourish. Building this secure digital castle requires a collective effort from policymakers, businesses, individuals, and educational institutions. By working together, we can transform Nigeria's digital landscape into a secure and prosperous space for all.

RECOMMENDATIONS

1. Assume a leadership role by implementing comprehensive cybersecurity legislation, allocating resources towards public awareness initiatives to educate the population, and promoting international cooperation to address cyber threats at a worldwide level.

2. Employ strong security policies to safeguard their digital assets, educate staff on optimal cybersecurity practices, and collaborate with necessary authorities to exchange threat intelligence and enhance the defensive network.
3. Employ appropriate online hygiene practices such as utilising robust passwords, regularly updating software, and exercising caution when encountering dubious emails and links. Notify the authorities of any suspected cybercrime in order to aid them in tracing and capturing the culprits.
4. Incorporate cybersecurity modules into the curriculum at every educational level, providing future generations with the necessary information and abilities to properly navigate the digital realm.
5. Conduct workshops and seminars in rural regions to address the digital knowledge gap and empower communities to enhance their online security.
6. Facilitate cooperation among educational institutions, corporations, and government organisations. This collaboration has the potential to facilitate the creation of specialised training programmes and the sharing of optimal methods, ultimately enhancing cybersecurity for all.

REFERENCES

[1]. GSMA (2024). *The Mobile Economy Sub-Saharan Africa 2024.* https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf

[2]. Jumia 2023. *Jumia Group Financial Statements 2023*. https://www.google.com/search?q=Jumia+(2023)+Jumia+Group+Financial+Statements+2023+%5BFinancial+Statement%5D&oq=Jumia+(2023)+Jumia+Group+Financial+Statements+2023+%5BFinancial+Statement%5D&aqs=chrome..69i57.6692870j0j15&sourceid=chrome&ie=UTF-8

[3]. Pricewaterhouse Coopers Nigeria (PwC Nigeria) 2023. *Nigeria Fintech Report 2023*. https://www.pwc.com/ng/en/assets/pdf/fintech-banking-sector-nigeria.pdf

[4]. Nigerian Data Protection Commission (NDPC) (2023) *Nigerian Cybersecurity Report 2023*. https://ndpc.gov.ng/Files/AnnualReport2023.pdf

[5]. Cyber Security Experts of Nigeria (CSEAN) 2024. *National Cyber Threat Forecast 2024*. https://csean.org.ng/national-cyber-threat-forecast-2024/

[6]. Nigeria Data Protection Bureau (NDPB) 2022. *Annual Report 2022*. https://csean.org.ng/national-cyber-threat-forecast-2024/

[7]. Atlantic Council 2022. Securing the Energy Transition against Cyber Threats: Report of the Atlantic Council Task Force on Cybersecurity and the Energy Transition. https://www.atlanticcouncil.org/wp-content/uploads/2022/08/Securing-the-Energy-Transition-against-Cyber-Threats.pdf

[8]. Chernov, D., & Sornette, D. 2020. *Critical risks of different economic sectors. Based on the Analysis of More Than, 500.* Switzerland: Springer Cham

[9]. Sibe, R. T., & Kaunert, C. 2024. Cyber Crime in Nigeria - Reviewing the Problems. In *Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria* (pp. 19-55). Cham: Springer Nature Switzerland.

[10]. Hu, M. 2024. National Security and Federalizing Data Privacy Infrastructure for AI Governance. *William & Mary Law School Research Paper*, (09-488).

[11]. Akongburo, R. A., Boshe, P., Dei-Tutu, S. A., & Hennemann, M. (Eds.). 2024. *African Data Protection Laws: Regulation, Policy, and Practice* (Vol. 3). Walter de Gruyter GmbH & Co KG.

[12]. Katagiri, N. 2024. Why Soft Measures Are Too Soft: International Law and Norms. In *How Liberal Democracies Defend Their Cyber Networks from Hackers: Strategies of Deterrence* (pp. 77-94). Cham: Springer Nature Switzerland.

[13]. Essien, E. S., & Edun, E. E. 2024. Digitalizing cyber security for data management in higher education: Implication for Educational Management in Nigeria. *International Journal of Education and National Development*, *2*(1), 70-78.

[14]. Adewopo, V., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M., & Elsayed, N. 2024. A Comprehensive Analytical Review on Cybercrime in West Africa. *arXiv preprint arXiv:2402.01649*. https://www.arxiv.org/pdf/2402.01649

[15]. Kuteesa, K. N., Akpuokwe, C. U., & Udeh, C. A. 2024. Theoretical perspectives on digital divide and ICT access: comparative study of rural communities in Africa and the United States. *Computer Science & IT Research Journal*, *5*(4), 839-849.

[16]. Aliyu, A. A. 2024. A Multi-Pronged Framework for a Cyber-Secure Nigeria. *Scientific and Practical Cyber Security Journal* (SPCSJ) 8(1): 69 – 75 ISSN 2587-4667

[17]. Usama, M., Ullah, U., & Sajid, A. 2024. Cyber Attacks against Intelligent Transportation Systems. In *Cyber Security for Next-Generation Computing Technologies* (pp. 190-230). CRC Press.

[18]. Hiller, J., Kisska-Schulze, K., & Shackelford, S. 2024. Cybersecurity carrots and sticks. *American Business Law Journal*, *61*(1), 5-29.

[19]. Rasel, M. 2024. Synergizing Cyber Threat Intelligence Sharing and Risk Assessment for Enhanced Government Cybersecurity: A Holistic Approach. *Journal Environmental Sciences and Technology*, *3*(1), 649-673.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(2): 59 – 67 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

SYSTEMIC SECURITY FRAMEWORK FOR HEI'S

Alexei Arina
Department of Software and Automation Engineering,
Technical University of Moldova

ABSTRACT: Ensuring cyber security is increasingly important for Higher Education Institutions (HEI's), the development of security frameworks based on international standards in the field, developed according to a systemic and holistic approach, has become mandatory with the digitization of the academic field and the growing number of ICT security threats. The applications used for the management of cyber security automate the entire process and enable the joint use of security requirements and the overview of the process of securing university ICT, to achieve an optimal level of cyber security of academic electronic services. In this sense, the use of European directives, security standards, and scientific methods used for the development of security frameworks, but also of formal models for the development of security systems has an important and defining role, so that the solutions developed are applicable and based on evidence scientific.

KEYWORDS*: cyber security, HEIs, management, framework, application.*

1. INTRODUCTION

The transition to the digital economy, modern health and education systems, the automation of industrial processes has favoured the development of cyber do-mains and influenced the global role they have today, to interconnect businesses and people within the global Internet communication network (Luo 2016; Huang et al. 2016).
In the new realities, where modern information technologies, IoT devices and extended Cloud services are increasingly used, ensuring cyber security is mandatory to ensure public security, business continuity and people's right to privacy in general (Asosheh, Hajinazari, and Khodkari 2013). Cyber assets have become so important that the World Economic Forum has emphasized the need to create a new class of assets, with the same importance as financial and economic assets (Merchan-Lima et al. 2020).
The purpose of scientific studies on cyber security is to provide a holistic (comprehensive) perspective, which addresses information assets through the multitude of dependencies on the technologies used, which makes the cyber security assessment process very important (Alexei 2021). The Cambridge dictionary defines the term holistic as: "that which refers to something whole or the total system, not just to its parts" (Cambridge University Press 2022).

2. THE PROBLEM OF CYBER SECURITY IN ACADEMIA

University information systems are open by design (Alexei 2021; Jang-Jaccard and Nepal 2014), decentralized, multi-user and present important platforms for study, research and university management. With the development of information and communication technologies, academic data and the communication networks used to transport them, have become important part of the university cyber domain. Thus, the digitization of universities, at the national and international levels, is required at a fast pace. The technological development of academic institutions is continuous, a strong impetus was the Covid-19 pandemic, as a result of which the entire academic activity was carried out remotely, thus increasingly using the cyber environment for online classes, access to digital courses, examination sessions, etc., which generated new conditions of activity. University campuses are becoming some of the most technologically advanced spaces.
Implementing technologies in HEIs is valuable for developing modern learning environments, but it increases the vulnerability of communication networks and the number of security threats. The multitude of technologies used creates many vulnerabilities due to the MAN (Metropolitan Area

Network) and CAN (Campus Area Network) communication networks, unlike other organizations (Joshi and Singh 2017), for example, in the banking sector.

The digitization of academic institutions highlighted the insufficiency of comprehensive studies and analyses of cyber security, becoming over time an important problem for the educational field (Fouad 2021), requiring multiple scientific studies on this dimension. The interest of cyber attackers is diverse: the theft of intellectual property, which refers to the results of research carried out by HEIs, often for organizations that are part of the Critical State Infrastructure, which have much more secure systems, and to university systems attackers can gain access much easier; significant financial losses or interruption of electronic academic services, unavailability of electronic communication networks.

In the annual reports published by Microsoft and Check Point Software (Check Point Research 2022), the multinational provider of solutions for securing organizations, the most targeted industries in 2022 were the education and research sector, the ICT (Information and Communication Technology) sector and non-governmental organizations (Figure 1).

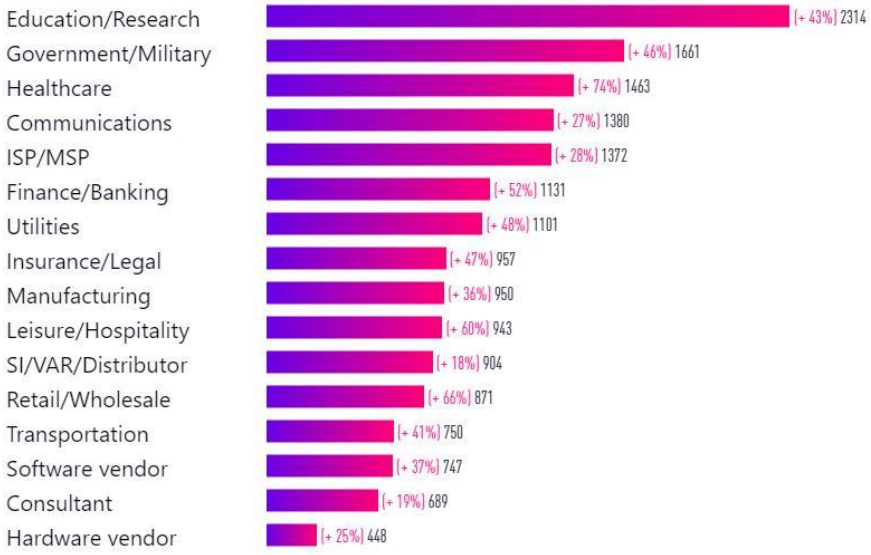

Fig.1. *The number of weekly security attacks reported in 2022, compared to 2021 (Check Point Research 2022)*

Also, as can be seen in Figure 2, according to the Microsoft Digital Defense Report (Microsoft 2023) published in October 2023, the education sector remains the most targeted by cyber attackers.

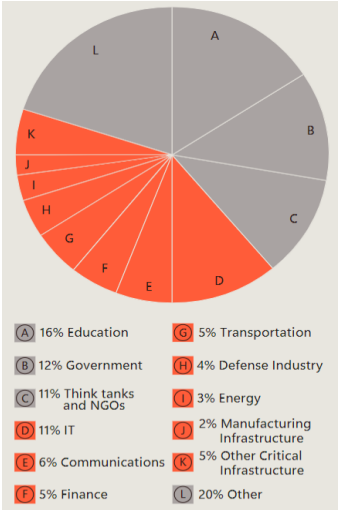

Fig.2. *Most targeted sectors globally (Microsoft 2023)*

Although the educational field witnesses a continuous annual increase in the number of cyber-attacks, few studies focused on the implementation of holistic security frameworks in HEIs have been identified in the specialized literature (Fouad 2021), (Rehman, Masood, and Cheema 2013), compared to other banking (Panja et al. 2013), medical (Coventry and Branley 2018) or industrial fields (Ani, He, and Tiwari 2019). None of the three dimensions with major social impact, described previously, affect any criterion of existentialism (Fouad 2021).

The need for a holistic approach to cyber security in HEIs is increasingly highlighted, in order to ensure the achievement of educational processes, the security of university data and financial resources, to add value to the development of the theoretical and practical bases of the cyber security field. The development of an application that allows the implementation of common security requirements for HEIs would respond to the European normative frameworks, which through the NIS_2 Directive (European Parliament 2022), require the implementation of common security requirements for the same fields. Thus, in the following sections, the security framework developed for HEIs and the prototype of an application will be presented that will allow to joint use of the security requirements for HEIs from the Republic of Moldova.

3. CYBERSECURITY FRAMEWORK

The security framework was developed using the Security Requirements Engineering SRE scientific method (Mellado, Fernández-Medina, and Piattini 2006). The development of the security framework was presented in a previously published paper (Alexei Ar., Nistiriuc P., and Alexei An., 2022) and includes:" development of security policies, identification of important informational assets, identification of security objectives and system dependency, identification of security threats, cyber risk assessment, identification of security requirements, completing the repository with relevant security controls" (Alexei Ar., Nistiriuc P., and Alexei An., 2022).

The graphical representation in Figure 3 of the operational security framework enables the analysis of the entire research rationale and the essential elements of the proposed security framework.

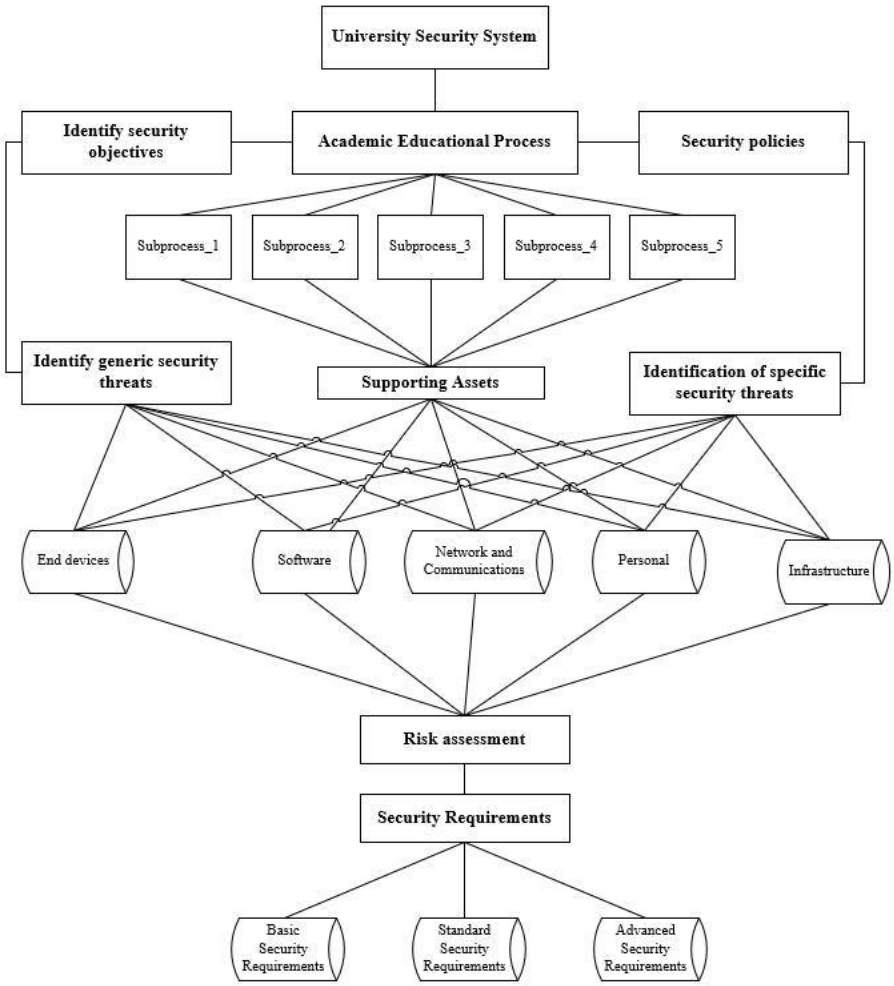

Fig.3. *University Operational Security Framework*
(Alexei Ar., Nistiriuc P., and Alexei An., 2022)

The operational security framework will be able to be evaluated in terms of the identified Key Performance Indicators (KPIs), for each of the 7 stages. Performance indicators are used to measure the level of security within organizations (Bolun 2021), concerning a specific control point, to provide evidence for effective administration: technical and managerial (Alexei Ar., Nistiriuc P., and Alexei An., 2022).

Performance indicators can serve as tools used for decision-making (Wang 2005) and for setting measurable objectives (Bolun 2021). The key indicators of the proposed security framework have been identified according to the operationalization stages and represent the finality of each stage, as reflected in Figure 4.

The performance indicators were selected according to the provisions of inter-national standards, such as ISO 27001 (ISO/IEC 2023) and ISO 27005 (ISO/IEC 27005 2018), of the European regulatory framework the NIS_2 directive (European Parliament 2022), based on the Clements-Hoffman security model (Lance J. Hoffman and Don Clements 1977).

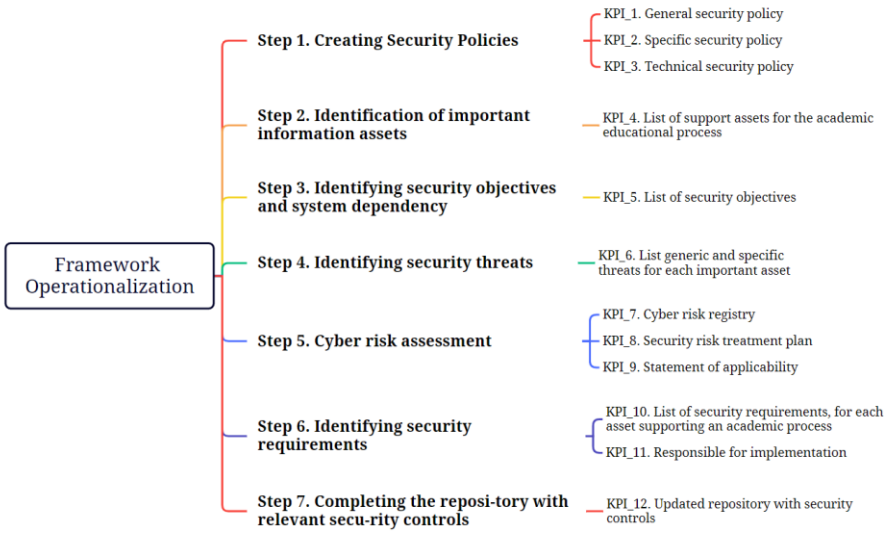

Fig. 4. *Framework implementation stages and KPIs (Alexei Ar., Nistiriuc P., and Alexei An., 2022)*

The goal of security is subjective, while performance indicators are objective and allow the evaluation of a certain security framework by experts or audit teams. Thus, indicators related to security policies are important to ensure that users comply with the provisions of the security framework, so the intention to implement a security framework must be supported by specific documents, administrative security policies and system-based policies (technical). In the case of administrative security policies, information through periodically revised documents, depending on the changes made in the university ICT systems, can ensure the compliance of the user's actions of the ICT system with the security requirements of the framework. System-based security policies are the configurations of ICT technologies through which access to university ICT can be controlled.

According to the Clements-Hoffman model, assets represent the reference point of security systems, so generating the list of supporting assets will allow an overview of the components of university ICT systems that require security.

Security objectives represent the fundamental principles of cyber security, determining the relationship between the security objective and the primary university asset, contributes to the correct and reasoned determination of security requirements. Therefore, if availability is critical for a particular asset, then the security requirements implemented must prioritize preventing/correcting problems related to the availability of university academic services.

Security threats are fuzzy sets of data, but to achieve an optimal security scenario, it is necessary to determine a defined set of generic and specific threats, as an essential part of the security system, to know the spectrum of existing threats, and along the way this the list must be updated periodically as new threats risk exploiting university ICT assets, which will enable the implementation of security control 5.7. Threat intelligence, of the ISO 27001 standard (ISO/IEC 2023).

According to the ISO 27005 standard (ISO/IEC 27005: 2018), any organization that implements security systems must perform a cyber risk assessment to identify the risks associated with the use of ICT technologies, thus increasing the effectiveness of these systems. In this sense, the risk register will allow centralized management for the analysis of existing risks in ICT systems. Based on the risk management plan, the managers will make decisions regarding the risks that can be ignored or treated.

Security requirements are the building blocks of a security system, according to the Clements-Hoffman model (Lance J. Hoffman and Don Clements 1977). Their identification will allow them to secure the vulnerable access paths to the ICT systems and the implementation of the common requirements for academia. To control the process of implementing the security requirements, responsible persons must be appointed. The Statement of applicability is a mandatory document, which must be completed by any university that intends to be certified with the ISO 27001 standard. In the declaration, the implemented security requirements are argued and objective justifications are provided in the case of certain ISO 27001 (ISO/IEC 2023) requirements that are not relevant to the HEIs.

The indicator that refers to the updated repository with security controls will be able to be used to implement the common security requirements, according to the provisions of the NIS2 directive (European Parliament 2022). Moreover, it will allow mandatory security checks to be performed, such as 5.27. Learning from security incidents and 5.28. Collection of evidence, of the ISO 27001 standard (ISO/IEC 2023).

4. DEVELOP A SECURITY FRAMEWORK APPLICATION PROTOTYPE

The previous section presented the implementation steps and key activities of the security framework. To ensure the unification of efforts in the implementation of the security framework, an application prototype (i-CSSCE) was developed that will allow the selection of the performance indicators for each stage. Finally, a report is generated that can be used to evaluate the level of implementation of the security framework and to observe the indicators that have not yet been satisfied, for decision-making. The tool could be used simultaneously by several users and HEIs, allows the creation of several projects, presents itself as a management platform for academic electronic services, which allows the management of organizational and operational aspects of the security framework, by identifying important information assets, identifying security threats, security requirements and controls that have been or are needed to be implemented to make informed decisions.

The i-CSSCE tool can support the implementation process of the activities proposed by the security framework, to minimize the effort required for information security management activities. It was designed as a web application written in PHP, HTML5, and JavaScript and uses MySQL databases. Client-side viewing takes place in the browser and will be able to run on any system that supports PHP, JavaScript, and MySQL. The tool consists of several separate modules, which will be usable depending on the user's access rights. The user interface of the application consists of several related web pages, which can be accessed from the menu, each page is associated with certain specific activities and interacts with each other through a MySQL-based database.

According to the Clements-Hoffman formal model, which describes the primary components of a security system, functions were created that will later allow management the relationships between them, the EER diagram reflecting the relationships between the elements of the security framework can be analysed in the figure 5.

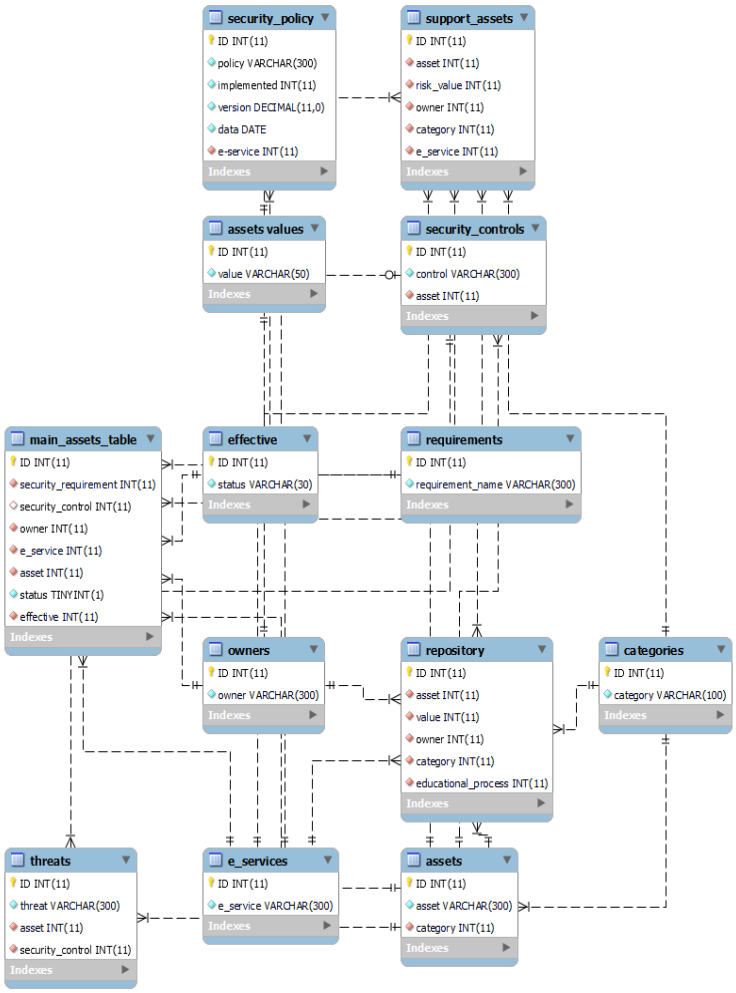

Fig.5. *The relationships between the elements of i-CSSCE*

The i-CSSCE tool allows management and assess the level of implementation of the operational security framework.

5. CONCLUSION

The basic objective of i-CSSCE consists of determining the necessary actions for the implementation of a complete security system framework and the implementation of common security requirements for the educational field, which is one of the European priorities, according to the provisions of the European NIS_2 Directive. The i-CSSCE prototype could be used as a guide in the process of implementing the security framework and to have an overview of the status of ICT security in HEIs.

The holistic approach to cyber security in HEIs is increasingly important, because as described in the introduction of this article, the educational field, especially HEIs is one of the most targeted fields in 2023, so the systemic and comprehensive approach becomes mandatory for the academia.

The development of the security framework and application prototype according to the Clements-Hoffman model, which establishes the relationships between the elements of the security systems, will allow us to systematically and holistically approach cyber security in HEIs.

REFERENCES

1. Alexei, Arina. 2021. “Network Security Threats to Higher Education Institutions.” In *CEE E|Dem and E|Gov Days*, 32333. Budapest. https://doi.org/10.24989/ocg.v341.24.
2. Alexei Ar., Nistiriuc P., and Alexei An. 2022. “The Holistic Approach to Cybersecurity in Academia.” In *CEEeGov '22: Proceedings of the Central and Eastern European eDem and eGov Days*, edited by NY, USA ACM. New York. DOI: https://doi.org/10.1145/3551504.3551516.
3. Ani, Uchenna Daniel, Hongmei He, and Ashutosh Tiwari. 2019. “Human Factor Security: Evaluating the Cybersecurity Capacity of the Industrial Workforce.” *Journal of Systems and Information Technology* 21 (1): 2–35. https://doi.org/10.1108/JSIT-02-2018-0028.
4. Asosheh, Abbass, Parvaneh Hajinazari, and Hourieh Khodkari. 2013. “A Practical Implementation of ISMS.” In *7th International Conference on E-Commerce in Developing Countries:With Focus on e-Security*. IEEE. https://doi.org/10.1109/ECDC.2013.6556730.
5. Bolun, I. 2021. “Prioritization of Cybersecurity Measures.” In *The 11th International Conference OnElectronics, Communications and Computing*, 194–99. Chișinău.
6. Cambridge University Press. 2022. “Cambridge Academic Content Dictionary.” 2022. https://dictionary.cambridge.org.
7. Check Point Research. 2022. “Cyber Security Report.” https://www.checkpoint.com.
8. Coventry, Lynne, and Dawn Branley. 2018. “Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward.” *Maturitas* 113 (July):48–52. https://doi.org/10.1016/j.maturitas.2018.04.008.
9. European Parliament, Council of the European Union. 2022. “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive).”
10. Fouad, Noran Shafik. 2021. “Securing Higher Education against Cyberthreats: From an Institutional Risk to a National Policy Challenge.” *Journal of Cyber Policy* 6 (2): 137–54. https://doi.org/10.1080/23738871.2021.1973526.
11. Huang, X., P. Craig, H. Lin, and Z Yan. 2016. “SecIoT: A Security Framework for the Internet of Things.” *Security and Communication Networks* 9 (16): 3083–94.
12. ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT. International Organization for Standardization. Geneva, Switzerland, 2022.
13. ISO/IEC 27005: Information technology – Security techniques – Information security risk management. International Organization for Standardization. Geneva, Switzerland, 2018.
14. Jang-Jaccard, Julian, and Surya Nepal. 2014. “A Survey of Emerging Threats in Cybersecurity.” In *Journal of Computer and System Sciences*, 80:973–93. Academic Press Inc. https://doi.org/10.1016/j.jcss.2014.02.005.
15. Joshi, Chanchala, and Umesh Kumar Singh. 2017. “Information Security Risks Management Framework – A Step towards Mitigating Security Risks in University Network.” *Journal of Information Security and Applications* 35 (August). https://doi.org/10.1016/j.jisa.2017.06.006.
16. Lance J. Hoffman, and Don Clements. 1977. “FUZZY COMPUTER SECURITY METRICS: A PRELIMINARY REPORT.” Berkeley.
17. Luo, X. 2016. “Security Protection to Industrial Control System Based on Defense-in- Depth Strategy.” *WIT Transactions on Engineering Sciences* 113:19–27.
18. Mellado, Daniel, Eduardo Fernández-Medina, and Mario Piattini. 2006. “Applying a Security Requirements Engineering Process.” In , 192–206. https://doi.org/10.1007/11863908_13.
19. Merchan-Lima, Jorge, Fabian Astudillo-Salinas, Luis Tello-Oquendo, Franklin Sanchez, Gabriel Lopez-Fonseca, and Dorys Quiroz. 2020. “Information Security Management Frameworks and Strategies in Higher Education Institutions: A Systematic Review.” *Annals of Telecommunications*, July. https://doi.org/10.1007/s12243-020-00783-2.
20. Microsoft. 2023. “Microsoft Digital Defense Report.”
21. Panja, Biswajit, Dennis Fattaleh, Mark Mercado, Adam Robinson, and Priyanka Meharia. 2013. “Cybersecurity in Banking and Financial Sector: Security Analysis of a Mobile Banking

Application." In *2013 International Conference on Collaboration Technologies and Systems (CTS)*, 397–403. IEEE. https://doi.org/10.1109/CTS.2013.6567261.

22. Rehman, Huma, Ashraf Masood, and Ahmad Raza Cheema. 2013. "Information Security Management in Academic Institutes of Pakistan." In *2013 2nd National Conference on Information Assurance (NCIA)*. IEEE. https://doi.org/10.1109/NCIA.2013.6725323.
23. Wang, Andy Ju An. 2005. "Information Security Models and Metrics." In *Proceedings of the 43rd Annual Southeast Regional Conference on - ACM-SE 43*, 178. New York, New York, USA: ACM Press. https://doi.org/10.1145/1167253.1167295.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(2): 68 – 75 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

SYSTEM SURVIVABILITY THREATS AND FACTORS INFLUENCING ATTACKS IN HEALTH FACILITIES

Joseph SIMIYU[1] Dorothy RAMBIM[1], Jasper ONDULO [1]
[1]Masinde Muliro University of Science and Technology, 190, Kakamega, 50100, Kenya

ABSTRACT: The adoption of e-health offers affluence medical benefits, unfortunately source of effective data is poorly protected, it is also susceptible to dangerous threats and attacks. While the volume of medical data dictates the use of technology, a failure of e-health systems to include security survivability as apriority in making e-health systems compromise easier. With this numerous security issues, the system can suffer more and never recover to assure users on their mission mandate. Despite efforts to secure Kenya's cyber space by assuring Kenya electronic transactions and online services such as e Government and health, system survivability and security attacks continues to jeopardize e-health confidentiality, credibility, reliability and availability for both providers and users. Therefore, it is important to understand issues around system survivability after attack rather than just security. Overall, this paper will try to come up with a system survivability issues for fighting information systems crime in the health sector in Kenya. Specifically, this research study will seek to outline the major system survivability threats and vulnerabilities within health sector in Kenya.

KEYWORDS: *e-health, Survivability, System Vulnerabilities, Security Risks*

1. INTRODUCTION

Survivability is defined as the ability of a system to provide essential services in the presence of attacks and failures, and to recover full services in a timely Manner. According to M. Farrukh Khan, Raymond A. Paul, in Advances in Computers, 2012) [i]. Survivability has been considered as a key inherent property of a reliable system. A survivable system continues to function, despite the presence of malicious attacks or arbitrary faults. The fact that a system has well-defined functions and correct implementations does not guarantee that the system is survivable. Some damages, which are resulted from novel, well-orchestrated malicious attacks, are simply beyond the abilities of most system developers to predict. In those situations, even a strong system with well-established security could possibly be compromised.

Globally Information technology is a very important tool in any current organization. Today organizations are driven by emerging technologies of which when implemented improve the welfare of clients and changes how people interact and promote social participation. These new technologies improve the productivity and competitiveness of organizations while opening up new areas to be explored and creating business and job opportunities as hold forth by Shenoy, A., & Appel, J. M. (2017).[ii].

In Africa, many countries have reported the upsurge of digital threats and malicious activities. The threats has been as a results of sabotaged public infrastructure, losses from digital fraud and illicit financial flows, and national security breaches involving espionage and intelligence theft by militant groups. While the individual governments on the continent seem to be very slow to appreciate the importance of the concept of information systems safety, the regional political body, the African Union (AU) seems to be making some gains in raising awareness and advocating for better cyber safety, to the continent's ministers of Information and Communications Technology. The African Union Commission (AUC) put out a call for experts to join its African Union Cyber Security Expert Group (AUCSEG) based on a resolution by its executive council and also created Africa Cyber Security collaboration and coordination committee to advise the AUC and policy makers on Cyber strategies, with many other specific tasks. Call for experts, AU, (2018)[iii]

This study determines the nature and characteristics of threats, assess the emerging threats and vulnerabilities that influence the health sector in Kenya and more specifically Referral Hospital

hospitals. A qualitative review was undertaken by a literature search of the survivability and vulnerabilities to identify threats and the factors influencing system survivability attacks in healthcare. In this paper, we examine the major system survivability threats and factors influencing them in healthcare facilities. The rest of the paper is organized as follows, II. provides emerging survivability threats and vulnerabilities in the health facilities, Factors Influencing system survivability attacks in healthcare is provided in section III, section IV discussion and conclusion.

2. EMERGING SYSTEM SURVIVABILITY THREATS AND VULNERABILITIES IN THE HEALTH FACILITIES

There are several issues that make health care security more complicated and have increased vulnerability over time (Burns, 2016)[iv]. In addition to this proliferation in emerging technology, many healthcare companies tend to use obsolete systems in many fields, such as Window XP, which has not been supported since 2014. (Milliman, 2016)[v], enabling hackers and malware to easily avoid detection, for example, the recent WannaCry attack. The propriety nature of medical device software means that healthcare IT teams may not be able to access the internal software in medical devices, so they rely on manufacturers to build and maintain security in those devices which were lacking. There is also a problem with lack of funding for security and system survivability, while hospitals and other organizations spend funding to become more integrated; they do not spend enough time and money to keep software updated and systems safe (Kotz *et al*., 2016)[vi]. This is exacerbated by a lack of industry expertise on system survivability security resulting from a general lack of technology and the prohibitive expense of security personnel. In summary, a rapid shift to electronic health records and interconnected devices, along with historical and ongoing lack of investment in survivability of systems and a lack of understanding of health personnel ’s safety work behaviors have made the health sector vulnerable to attacks.

Although healthcare has vulnerabilities to exploit, attackers need to be motivated to commit attacks. Motivation includes the potential for financial and political benefit and possibly taking life in a cyberwarfare process. Economic benefit is the highest of those motivations. Data on health care is far more valuable than any other data. The value can exceed €888.05 for a complete set of medical credentials (Sulleyman, 2017). Stolen medical identification may be used by claiming somebody ’s identity or insurance records to access health care and prescription drugs. Uses extend to organized crime perpetrating sophisticated fraud. Fraudsters have earned billions in the last few years by filing fraudulent claims and dispensing drugs to sell on the dark web (McCarthy, 2016). Sometimes there is even sufficient information in medical records to open bank accounts, secure loans or obtain passports.

Effects of Cybercrime on Healthcare: The health sector has seen a drastic increase in the amount and scale of data breaches in the last few years. Breaches lead to financial loss, reputational loss and reduced patient safety. Report indicates the average cost of missing or stolen medical records containing confidential and sensitive information is massive (Seh AH, 2020)[vii], and continued advertisement associated with large breaches may jeopardize patient trust which may result in less willingness to share data (Whitler, 2017**)**[viii]. This is especially problematic for patients with conditions such as sexual or mental health conditions being stigmatized.

Despite warnings issued and the availability of security patches, the scale of the WannaCry attack was exceptional, with over 300,000 computers worldwide demanding that users pay ransoms on bitcoin (Scott & Wingfield, 2017)[ix]. A number of hospitals have experienced system wide lockouts, patient care delays, and loss of function in connected devices such as MRI scanners, and refrigerators for blood storage. This attack was not directed specifically at healthcare organizations, yet the damage was widespread. Other ransomware targeted specifically the healthcare sector.

Many malware attacks have led to major incidents, such as healthcare trust suffering an unspecified cyber-attack which results in the shutdown of IT systems and scheduled operations and outpatient appointments being cancelled for days (Evenstad, 2016)[x]. Medjack (Medical Device Hijack) is attack that was detected to inject malware into unprotected medical devices for lateral movement through the hospital network (Storm, 2015)[xi]. The infected medical devices creates poor ties in hospital safety

defenses, including diagnostic equipment (including MRI machines), therapeutic equipment (e.g., infusion pumps), and life-supply equipment (including ventilators).
Simulated attacks by 'White Hacker' have highlighted that there are other vulnerabilities which mean "Medical devices are the next security nightmare". There is potential for attacks similar to what used to be considered science fiction. For example, brain jacking where a suitable device could be inserted (Pycroft *et al*., 2016)[xii]. Simulated attacks on devices such as pacemakers and defibrillators, insulin pumps and pumps for drug infusion have been carried out. These attacks have remotely controlled machines to modify surgery or send lethal doses of drugs. Though currently only simulated such attacks may occur (Klonoff, 2015)[xiii]. Risks will continue to increase if cybersecurity has not been designed from the start of the product or project lifecycle.

Ransomware and other Malware: Malware is a serious problem across all industries, however, in healthcare, a malware infection can mean life or death. Healthcare operates an intricate series of interconnected reporting and services. The interlocking network that communicates information on our behalf to better our health is especially vulnerable to ransomware and other malware attacks. In the aforementioned NHS WannaCry attack, hospitals are forced to close their doors to new patients, and existing patients' treatment are interrupted because of an inability to access records. The HHS 'Wall of Shame', which lists healthcare data breaches data breaches affecting almost millions of individuals. Healthcare is among the leading cyber-criminal-targeted industries (Kruse et al., 2017)[xiv]. Breaches may be caused by hacking, malware and threats to insiders. While insider threats are issues created by employee errors or deliberate actions (e.g., responding to phishing emails, a social engineering attack to extract login credentials or launch a malware attack, erroneous security settings, password misuse, loss of laptops and sending unencrypted emails). This thus becomes a moderating factor together with DDOS and ransomware attacks.

Ransomware exploits vulnerabilities to hijack monetary benefit infrastructures for target information technology (IT). Because of the nature and value of information, access to medical information allows cyber criminals to commit identity theft, medical fraud, and extortion, and to illegally get controlled substances. Medical information's utility and versatility, extensive centralized storage of medical information, relatively weak IT security systems, and the expanding use of healthcare IT infrastructure all contribute to an increase in cyber-attacks on healthcare institutions. Research suggests that an individual's medical information is 20–50 times more valuable to cyber-criminals than personal financial information (Kruse *et al*., 2017). As such, cyber-attacks targeting medical information are increasing 22% per year (Kruse *et al*., 2017). Ransomware uses a hybrid encryption system that combines the two cryptographies to create an asymmetric cryptosystem in which data is encrypted using a randomly generated symmetric key, which is then encrypted using a public key where one party has the appropriate private key (Krisby, 2018)[xv]. The cyber-criminal uses the private key to decrypt the symmetric key to decrypt the data back "into "plaintext" and give the key back to the victim, who can then use it to access their device again (Krisby, 2018). When encrypted, the code is unavailable and indecipherable. The user receives a pop-up notification that requires a ransom payment (usually in untraceable digital currency such as bitcoin) in exchange for the decryption key (Pope, 2016)[xvi].
Often, Ransomware does not destroy data but will lock up data before a ransom is paid (Richardson & North, 2017)[xvii]. Even if the infection with ransomware is removed the data can remain encrypted. But it is necessary to remember that the mere infection of a ransomware computer does not suffice. To get an encryption key and report its results, the ransomware has to communicate with a server (Richardson & North, 2017). This includes a server hosted by a corporation that avoids criminal activity and ensures anonymity for the attackers (called Bulletproof Hosting). These businesses are often located in China or in Russia (Richardson & North, 2017).
During a ransomware attack, malware is injected into a network to infect and encrypt sensitive data until a ransom amount is paid.
Ransomware attacks are a growing threat amongst healthcare providers according to an analysis last year. More than 1 in 3 healthcare organizations globally fell victim to a ransomware attack in 2020.
The reason for its prevalence is that hackers understand how critical it is for the healthcare sector to minimize operation disturbances. During a ransomware attack, healthcare victims panic, fearing the

regulatory consequences that follow the theft of patient data. Data Breach Investigations Report (DBIR).

Phishing: Like all industries, healthcare is at risk from phishing. According to Data Breach Investigations report (Verizon, 2023)[xviii] around 66% of malware was initiated as an email attachment. Although the WannaCry ransomware was unlikely to have begun its life in an email, much malware continues to be executed via phishing. However, phishing emails and texts are also a threat to personal data, including login credentials.

The National Health Information Sharing and Analysis Center have recently reported that the healthcare industry is at the most risk of fraudulent emails. However, little is being done to combat this, with 98% of healthcare organizations not taking the first steps in helping to prevent phishing by setting in place Domain-based Message Authentication, Reporting & Conformance (DMARC).

Insider threats: Insider threats to hospital resources are a concern across the board and can be carried out by patients as well as staff and can be both malicious and accidental. The HIMSS Cybersecurity Survey (2017), found that Insider threats were deemed to be worrying enough to set up specific programs of protection by 75% of respondents.
Spoofing: Spoofing is when someone hides their identity to evade detection for their wrong acts and pretends to be someone else in an attempt to gain trust and get sensitive system information. The common spoofing done by changing the hardware or MAC address is called MAC cloning, changing the IP address or the unique identity on the network is called IP spoofing, and impersonating as someone else in their digital communication is called email spoofing.

Information-gathering attacks: Information gathering is the practice of attacker gaining priceless details about probable targets. This is not an attack but only a pre-phase of an attack and is totally passive as there is no explicit attack. Systems including computers, servers, and net-work infrastructure, including communication links and inter networking devices, are sniffed, scanned, and probed for information like whether the target system is up and running, what all ports are open, details regarding the operating system and its version, etc. Some of the information-gathering attacks are sniffing, mapping, vulnerability scanning, phishing, etc.

Password attacks: The simplest way to achieve control of a system, or any user account, is through a password attack. If the personal and behavioral details of the victim are known, the attacker starts with guessing password. Frequently, the attacker uses some form of social engineering to trace and find the password. Dictionary attack is the next step in password attacks and is automated.

Virus: Computer viruses are the most communal threat to the computer users. Computer viruses are malicious software designed to blow out from one computer to another through file transfer, piggybacks on genuine programs and OS, or e-mails. The email attachments or downloads from particular websites contaminate the computer and also other computers on its list of contacts by using the communication network. Viruses influence the system security by changing the settings, accessing confidential data, displaying unwanted advertisements, sending spam to contacts, and taking control of the web browser According to Thomas C. (2009), the viruses are identified as executable viruses, boot sector viruses, or e-mail viruses.

Worms: Computer worms are fragments of malicious software that reproduce swiftly and blow out from one computer to another through its contacts, again spreading to the contacts of these other computers and so on and reaching out to a large number of systems in no time. Captivatingly, worms are prepared for spreading by exploiting software vulnerabilities. Worms display unwanted advertisements. It uses up tremendous CPU time and network bandwidth in this process thereby denying access to the systems or network of the victim, creating chaos and trust issues on a communication network.

Trojans: Trojans are programs that appear as perfectly genuine but, in reality, have a malicious part embedded in it. Trojans are spread usually through email attachment from the trustworthy contacts and also on clicking on fake advertisements. The payload of Trojans is an executable file that will install a server program on the victim's system by opening a port and always listening to that port whereas the server is run on the attacker's system. Hence, whenever the attacker wants to login to the victim machine, they can do so by means of the backdoor entry making it hidden from the user.

Spyware and adware: Spyware and adware are software with a common property of collecting personal information of users without their knowledge. Adware is intended to track data of the user's surfing behaviors, and, based on that, pop-ups and advertisements are displayed. Spyware on the other hand gets installed on a computer and gathers information about the user's online activities without their knowledge. Spyware contains key loggers that record every-thing typed on the keyboard, making it unsafe due to the high threat of identity mugging.

Botnets: A collection of compromised systems or bots acts as a team of infected computers under the control of a bot master to remotely control and send synchronized attacks on a victim host. This army of bots, agents, and bot master constitute a botnet. Botnets are used for sending spams and also for distributed denial of service attacks.

Denial-of-service attacks: Denial-of-service (DoS) attacks as the name suggests denying users from accessing or using the service or system. This is mainly done by overwhelming the bandwidth, CPU, or memory wherein the access to the network of the victim machine or server offering the service gets

denied. DoS attacks thus interrupt the service of a computer or network systems, making it inaccessible or too inferior in performance.4.16 Distributed DoS In distributed DoS (DDoS) attacks, the victim is targeted from a large number of individual compromised systems simultaneously. The DDoS attacks are normally done with the help of botnets. The botmaster is the attacker who indirectly attacks the victim machine using the army of bots or zombies. DDoS attacks occur when a large number of compromised systems act synchronously and are being coordinated under the control of an attacker in order to totally exhaust its resources and force it to deny service to its genuine users. It is the upsurge in the traffic volume that loads the website or server causing it to appear sluggish (Thomas C. 2009)

3. FACTORS INFLUENCING SYSTEM SURVIVABILITY ATTACKS IN HEALTHCARE

Top Management should be responsible for informing their employees of the importance of systems survivability, make it efficient for people to participate, take ownership and manage their responsibilities (Abbas *et al*., 2015)[xix]. They also ought to invest in a solution that benefits everyone and finally monitor performance. Further, organizational resources come in whereby organizations lack industry expertise on survivability attacks resulting from a general lack of technology and the prohibitive expense of security personnel.

Game theory models the attacker and system administrator's fundamentally selfish and aggressive actions and analyzes the potential strategies bringing in the human aspect of cyber security (Shiva & Sankardas, 2010). Securitization theory suggests there is currently a general perception that there is a lack of awareness and information in Kenya on systems security matters, leading to IT literacy as an individual factor. For systems survivability, intersectionality can help us better understand how system attacks issues are not just technical but are both legal and governmental, and cultural and economic, and so on which leads to policy formulation of IT policies for cyber security.

Based on the above from the literature review, the researcher aimed at reviewing organizational and individual factors, coupled up with mediating factors to come up with a framework for system survivability. From this, the researcher aimed to develop and validate a framework that addresses the human factors, organizational culture, and IT policies side of system survivability in the health sector.

Increased use of Cloud computing and online security

Cloud computing is being taken up by healthcare as it offers benefits such as improved access to data and cost efficiency. The use of Cloud computing within healthcare is set to soar, however, cloud computing brings its own risks (I Kravchenko, 2021). Data within cloud repositories need to be correctly protected, according to Open Web Application Security Project (OWASP) guidelines. Protecting data at rest and during transit across web services requires not only robust encryption measures but also appropriate and effective authentication, such as second factor and risk based.

Internet-enabled healthcare attacks (Internet of Things - IoT devices)

Healthcare has embraced Internet-connected devices in a bid to use health data to improve patient outcomes. Apps like OpenAPS which are an optimized data-driven insulin delivery system and internet enabled activity trackers which help in cancer treatment are paving the way for the IoT to improve healthcare. However, the IoT has known security and privacy issues. Many healthcare based IoT devices aggregate personal data which is then stored in a cloud repository and used to analyze conditions, treatments, among others. Security issues such as DDoS attacks like the massive Mirai Bot (NJCCIC, 2016), which are based on IoT devices, are a potential threat that could disrupt treatment. The protection of personal data to prevent exposure is another. Redundancy issues are also another area of concern, as more hospitals become dependent on Internet-enablement of systems.

Lack of Data Encryption

Protecting sensitive business data in transit and at rest is a measure few industries have yet to embrace, despite its effectiveness. The health care industry handles extremely sensitive data and

understands the gravity of losing it which is why HIPAA compliance requires every computer to be encrypted (Thakur, K., Hayajneh, T., & Tseng, J. 2019)[xx]

4. CONCLUSION

Some of the survivability crimes and threats are wrongdoing that are executed utilizing PCs or are in any case identified with them. Access to boundless information over the world is great yet it accompanies its reasonable portion of issues. In this paper, we have explored the principal vulnerabilities and risks that target health systems survivability and proposed a comprehensive system survivability model to address these challenges. Through the analysis of a case study and a review of relevant literature, we have developed a model that can be adopted for use as a strategy to overcome. By adopting this model, organizations can enhance their ability to identify and mitigate vulnerabilities in their environment, thereby improving their overall security posture.

REFERENCES

1. [i]. Farrukh Khan, Raymond A. Paul, 2012. In Advances in Computers, M
2. [ii] Shenoy, A., & Appel, J. M. (2017). Safeguarding Confidentiality in Electronic Health Records. *Cambridge quarterly of healthcare ethics : CQ : the international journal of healthcare ethics committees*, *26*(2), 337–341. https://doi.org/10.1017/S0963180116000931
3. [iii] Experts, A. U. (2018). *Call for Experts.*
4. [iv] Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A brief chronology of medical device security. *Communications of the ACM*, *59*(10), 66–72.
5. [v] Index, M. M. (2016).
6. [vi] Kotz, D., Gunter, C. A., Kumar, S., & Weiner, J. P. (2016). Privacy and Security in Mobile Health: A Research Agenda. *Computer*, *49*(6), 22–30. https://doi.org/10.1109/MC.2016.185
7. [vii] Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Khan RA. Healthcare Data Breaches: Insights and Implications. Healthcare (Basel). 2020 May 13;8(2):133. doi: 10.3390/healthcare8020133. PMID: 32414183; PMCID: PMC7349636.
8. [viii] Whitler, Kimberly & Farris, Paul. (2017). The Impact of Cyber Attacks on Brand Image: Why Proactive Marketing Expertise Is Needed for Managing Data Breaches. Journal of Advertising Research. 57. 3-9. 10.2501/JAR-2017-005.
9. [ix] Scott, M., & Wingfield, N. (2017). *Hacking attack has security experts scrambling to contain fallout*. New York, USA: New York Times.
10. [x] Coventry, Lynne & Branley-Bell, Dawn. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 113. 10.1016/j.maturitas.2018.04.008.
11. [xi] Storm, D. (2015). *MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks*. London, UK: Computerworld.
12. [xii] Pycroft, L., Boccard, S. G., Owen, S. L. F., Stein, J. F., Fitzgerald, J. J., Green, A. L., & Aziz, T. Z. (2016). Brainjacking: implant security issues in invasive neuromodulation. *World Neurosurgery*, *92*(1), 454–462.
13. [xiii] Klonoff, D. C. (2015). Cybersecurity for connected diabetes devices. *Journal of Diabetes Science and Technology*, *9*(5), 1143–1147.
14. [xiv] Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10.
15. [xv] Krisby, R. M. (2018). Health care held ransom: modifications to data breach security & the future of health care privacy protection. *Health Matrix*, *28*(1), 365.
16. [xvi] Pope, J. (2016). Ransomware: minimizing the risks. *Innovations in Clinical Neuroscience*, *13*(11–12), 37-41.
17. [xvii] Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10-12.
18. [xviii] Data Breach Investigations report (Verizon, 2023

19. [xix] Abbas, A., Bilal, K., Zhang, L., & Khan, S. U. (2015). A cloud-based health insurance plan recommendation system: A user centered approach. *Future Generation Computer Systems*, *43*(1), 99–109.