Detection of Cybercrime Victimization Factor and Prevention Measures in the USA.

From 2010 to 2019.

By

Chibuzo Anokam

Masters In Forensic Computing

St. Joseph's University, New York

Table of contents

ABSTRACT

Technology has evolved into a powerful and wonderful tool that has aided in propelling business and many other industries to the forefront of their respective fields. It has resulted in new and inventive ways to get things done faster and better. Despite the numerous advantages, it is a tool used by criminals to engage in illegal international activities. Cybercriminals have recognized the opportunities presented by the cyber landscape and have exceeded expectations, resulting in a high number of dangers arising from the use of digital technology to promote fraudulent goals. As a result, it is critical to investigate these fraudulent operations in order to determine the most common cybercrime victimization factors. Data on crimes reports were evaluated and descriptive analyses and reports were produced as a result of the research. The large sample of respondents was discovered to be victims of at least three main types of cybercrime victimization factors. These criteria were categorized as dichotomous variables, with 1 indicating that the respondent

had experienced each of the ten forms of cybercrime at least once in the previous year and 0 indicating that the respondent had not.

INTRODUCTION

Background

Nowadays, the Internet is becoming part and parcel of the modern lifestyle of people throughout the world. However, online criminality has also risen with the developments in cyberspace. At present, the risk of cybercrime can be visualized in the form of offenses analogous to the physical world, such as cyberbullying and online theft which are termed *cyber-enabled* crimes. Security risks that affect the computer itself, such as malware infections, ransomware infections, theft, and misuse of personal data which is known as *cyber*crime (Bergmann *et al*, 2018).

With the development of information technology and the expansion of the internet, cybercrime has become technologically

advanced, aggressive and one of the fastest-growing types of crime (Mesko, 2018). The persistent abuse of computers and the Internet put together, enables some people to commit crimes and victimize others. Cyberspace users have excessive confidence in the use of cyberspace, which unfortunately makes them exposed to risks in cyberspace. Oftentimes, their perception is that the likelihood of their victimization is lower than other potential victims of traditional crimes in the real world.

Adequate knowledge of crime patterns, commission, and victim responses are crucial for developing prevention strategies through user awareness programs (Mesko, 2018). To a large extent, cybercrime control is more difficult than offline crime control. This has indicated the need for more studies on the factors of cybercrime victimization, to help fight the growing threats from cyberspace (Catherine *et al*). This research explicitly examines the prevalent cybercrime victimization factors through a detailed analysis of existing literature and report data to have insights into

routine activity theory.

LITERATURE REVIEW

Cybercrime – emergence and structure:

Technologies and communications are continuously evolving, requiring ever-changing notions of crime and criminality to adapt to an online environment. The prevalence of technology and the internet has fundamentally altered how we live, communicate, travel, share information, and transfer funds.

There have been cybercrime with a massive impact in recent years on the Internet. A computer virus dubbed 'Love Bug' in May 2000 was the first major record, causing estimated damages of $7-10 billion worldwide to computer operators, including government entities even in the USA (Sumanjit & Tapaswini, 2013). The main suspect was a college dropout from the

Philippines, but all accusations were dismissed and Onel de Guzman, suspect at that time, was not punished since the Philippines did not have any computer hacking legislation under which he could be charged (Philippsohn, 2001).

Griffin (2012) believes that cybercrime is quite an unknown topic with several challenges and concerns which must be resolved. He examined online concerns including privacy, anonymity, and rights, and suggests how laws may be built around these ideas to better apply to criminal scenarios. He discussed how things can be handled from a legal viewpoint. For example, the case of the United States v. Jones from the perspective of online privacy. The Fourth Amendment to the United States Constitution indicates that an individual has the right to privacy, and thus the United States lost the trial since the government would be invading the offender's privacy throughout the inquiry to obtain evidence against him.

Cybercrime is becoming more serious. Cybercrimes are difficult to identify and prosecute due to how the crime is carried out through the internet anonymously. A survey from computer and security experts as far back as 2002 shows an upward trend that demonstrates a requirement for a timely review of existing approaches to fighting this new phenomenon within the modern era. (chang et al., 2003). The main goal of this literature review is to discuss the detection of cybercrime victimization factors and prevention measures within the U.S.A from 2010-2020.

Personal Electronic Devices – use over time:

Smartphones have a unique mix of technology such as digital cameras, internet messaging, music, and multimedia material and it is recognized that their presence and use have changed human relationships in society, therefore enabling more complicated cybercrimes. In 2012, for example, 70% of all mobile devices in the United States were smartphones (Hardawar, 2012). The study revealed that more than 95% of young individuals in the US

already use smartphones, and 30% also say that they 'cannot live without a smartphone (Gibson, 2014).

The use of personal electronic devices (PEDs) and the Web has risen over time, affecting the human quality of life, but also causing controversy and numerous probable health and safety problems. The objective of this literature is that new chances for cybercrime have been available through PEDs, and users have become increasingly exposed.

Exposure to cybercrime:

The usage of the Internet and cellphones is growing more common. People are becoming increasingly anxious about the protection of their privacy in cyberspace as they are forced to trust electronic devices with personal information due to employment or social obligations. According to a poll of internet users in the US, 86% feel their risk of cybercrime victimization has grown (Baker, 2019). Despite this, only 46% of respondents had updated any of

their passwords in the previous year, and just 12% had been victims of online banking fraud or had their email or social media accounts stolen.

Cybercrime prevention methods:

Reyns, Randa, and Henson (2016) investigated this topic and conducted research to identify factors that may prevent cybercrime victimization on a technological level; they accomplished this by examining relationships between exposure to cyberspace, cybercrime victimization, and online communication within an opportunity framework. They concluded that exposure to cyberspace and habitual online communication activities were predictors of cybercrime victimization. Furthermore, it was ascertained that adopting cautious steps online undermines the premise, which is that, interaction in technologies might be effective in cybercrime prevention strategies.

Organized Cyber Crime

According to research, there is some disagreement over the types of cybercrime that occur. According to McCusker (2006), the synergy between the Internet and organized crime is a natural trend that will likely continue to expand in the future. The prior focus was on traditional organized crime groups that use the Internet as a conduit to carry out their criminal activities. The Internet has been utilized as a main facilitator for crimes for some years, but that does not mean it is an integral element of the crime (Lavorgna, 2015).

Cybercrime in its many manifestations necessitates a high degree of cooperation and organization. There are few studies concentrating on the existence of both traditional organized crime and newly formed criminal groups in the cyber landscape (Leukfeldt *et al*, 2016), and the existing criminology literature has not adequately addressed the nature and rate of criminal adaptability (Lavorgna & Song *et al*, 2016).

McGuire (2012) identified three major categories (type I, II, and III) and six subtypes (swarm, hubs, extended hybrids, clustered hybrids, aggregates, and hierarchies) of cyber-organized crime organizations and estimated that up to 80 percent of cybercrime involves organized crime. Certain fundamental features of conventional organized crime organizations need to be reassessed when gangs operate online, according to McGuire's research. In cyberspace, for example, the size of a group has little to do with the impact and extent of their crimes.

Conclusion

Cybercrime is predominantly a crime based on cyberspace where any person may be victimized in any part of the world. Policymakers may be able to determine whether federal law enforcement has the tools and resources, including funds and people, to tackle these threats if they have a comprehensive understanding of the scope of the cybercrime problem. The United

States has frequently investigated cybercrime and related federal resources in the context of maintaining cybersecurity. Furthermore, officials have shown an interest in maintaining the government cyber workforce's strength and efficacy. As a result, recognizing the real nature and scale of the cyber threat may aid the United States in conducting oversight in these areas and ensuring that the proper resources are in place.

Research Method

The aim of the research is to explore the victimization factors and detect the most frequent factors over time. Also, it aims to suggest preventive measures to cybercrime as a use of security measures. Hence, the use of quantitative methodology a preferred choice for this research. Quantitative research methods is used when research questions are focused on a large group of people. This makes it possible to apply research findings to a general population.

The objectives to possibly achieve these aims will be to; Research the new trends of cybercrime victimization and analyze the most common factors and Map the analyzed factors to preventive measures.

Research Questions

Following the section above, the research questions are to figure out what the most frequent trend of cybercrime victimization factors are, and also, what are the active preventive measures to counter these factors since 2010. This will assist in the understanding of factors that shape victimization and the subsequent use of prevention measures online.

The variables to be considered for this research are the dependent and the independent variables. The dependent variable is represented by the Cybercrime Victimization Factors i.e phishing, non-payment/non-delivery, extortion, personal data breach, identity theft, spoofing, misrepresentation, confidence

fraud/romance, harassment/threats of violence, and BEC/EAC while the independent variable will be represented by the various preventive measures i.e self-control and routine activity.

The variable to be measured is the dependent variable and this will be done using the ordinal measuring scale. Ordinal scales build upon nominal scales by assigning numbers to objects to reflect a rank ordering on an attribute. This is to ensure that the factors affecting cybercrime victimization are explicitly ranked according to frequency (most occurring).

Type of Study

The type of study to be employed in this research is the evaluation method. This is because there will be research consisting of data analysis and reporting. This systematic process will involve collecting data about the topic to enhance knowledge and decision-making for practical applications.

Data Source and Analysis

The data for this research was obtained from a secondary source, i.e Statistia. This is a reliable data repository for qualitative and quantitative research. Data obtained from this source was analyzed from respondents' experience following the top ten forms of cybercrime victimization factors. These factors were coded as dichotomous variables with 1= “the respondent reported that he/she experienced each of the above five forms of cybercrime at least once in the past year” and 0 = “the respondent indicated that he/she did not experience it”.

The data was analyzed. For each form of cybercrime victimization factors, there was a descriptive analysis on levels of self-control while holding sex, age, race, marital status, and employment status constant. This was done using data analyzing software like the Microsoft excel better visualization.

	N	Mean (%)	SD	Min	Max
Age	241,342	40	19.12	18	87
Sex Male	82,056	34.0%			
Female	159,286	66.0%			
Race	203,451	84.3%			
White	37,891	15.7%			

Non white					
Marital Status					
Married	88,331	36.6%			
Single	153,011	63.4%			
Employment					
Employed	149,219	61%			
Unemployed	94,123	39%			

Table 1. Total data sample

Results

Demography of all respondents who were victims of cybercrime from as recorded from year 2010 have been analyzed from the data obtained from Statistia. The data shows that, since 2010, over 240,000 individuals have fallen victims of cybercrime in the US alone, over the past 10 years. When analyzed, it was found that, most victims were middle aged (Mean age 40) and with the higher percentage constituting of women (66%), belonging to the white

race (84.3%) and maintaining a single and employed status with 63.4% and 61% respectively. This is clearly described below with the help of a bar chart in figure 1.

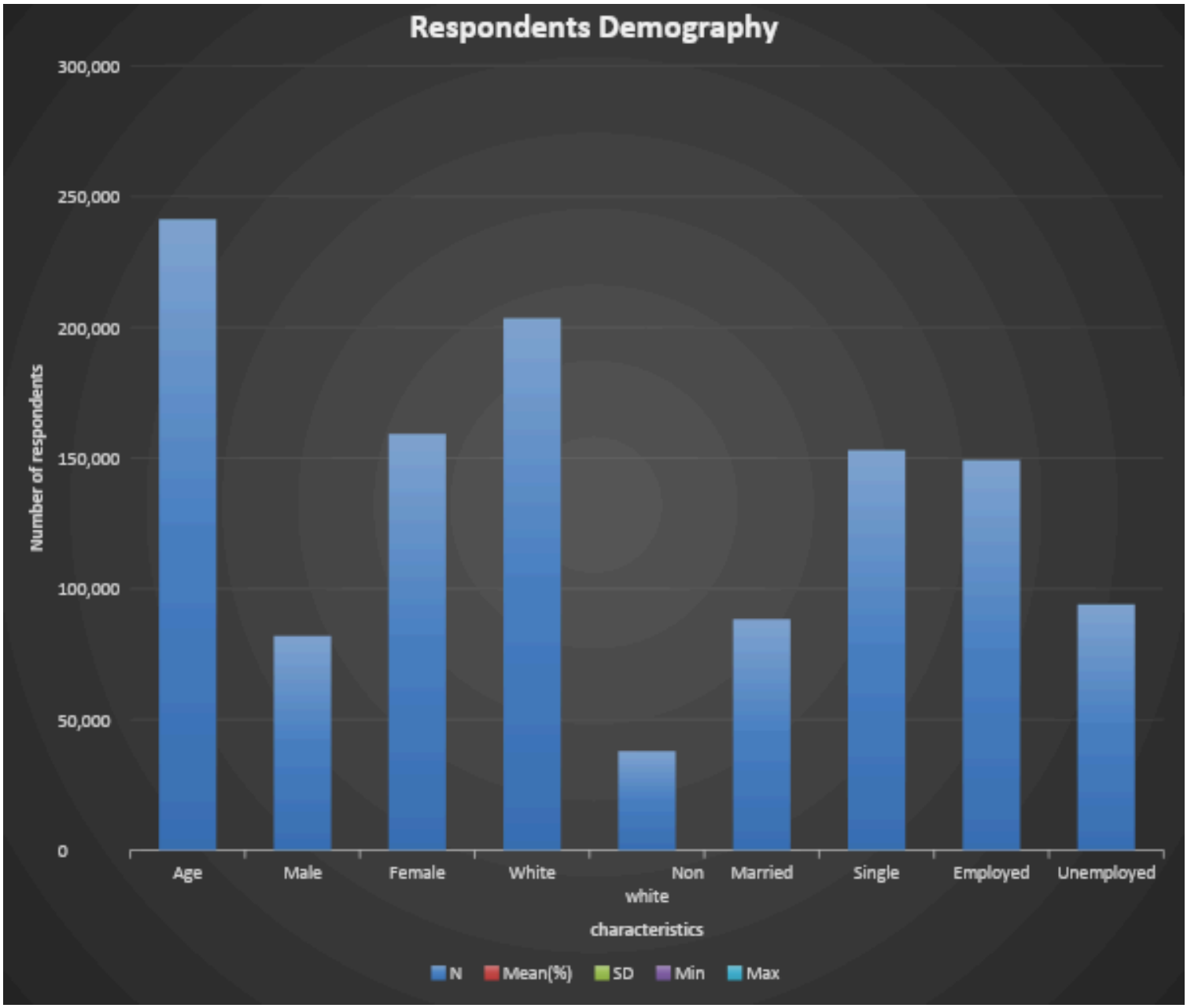

Figure 1. Respondent demography chart

While exploring the data to analyze the most frequent forms of cyberattacks experienced by the respondents, as reported, over seventeen forms of attack were shortlisted to rank the most frequent cybercrime victimization factors. All of the 241,324 victims to have reported a case on cybercrime explicitly marked out the forms of attacks ever experienced. Most victims have fallen for a minimum of 3 out of the seventeen shortlisted cybercrime attacks. The top 10 ranking factors were considered for this report. These factors are as shown in table 2 below.

Top 10 Factors	**Victims (n)**
Phishing	241,342
Non-Payment/Non-Delivery	108,869
Extortion	76,741
Personal Data Breach	45,330
Identity Theft	43,330

Spoofing	28,218
Misrepresentation	24,276
Confidence Fraud/Romance	23,751
Harassment/Threats of Violence	20,604
BEC/EAC	19,369

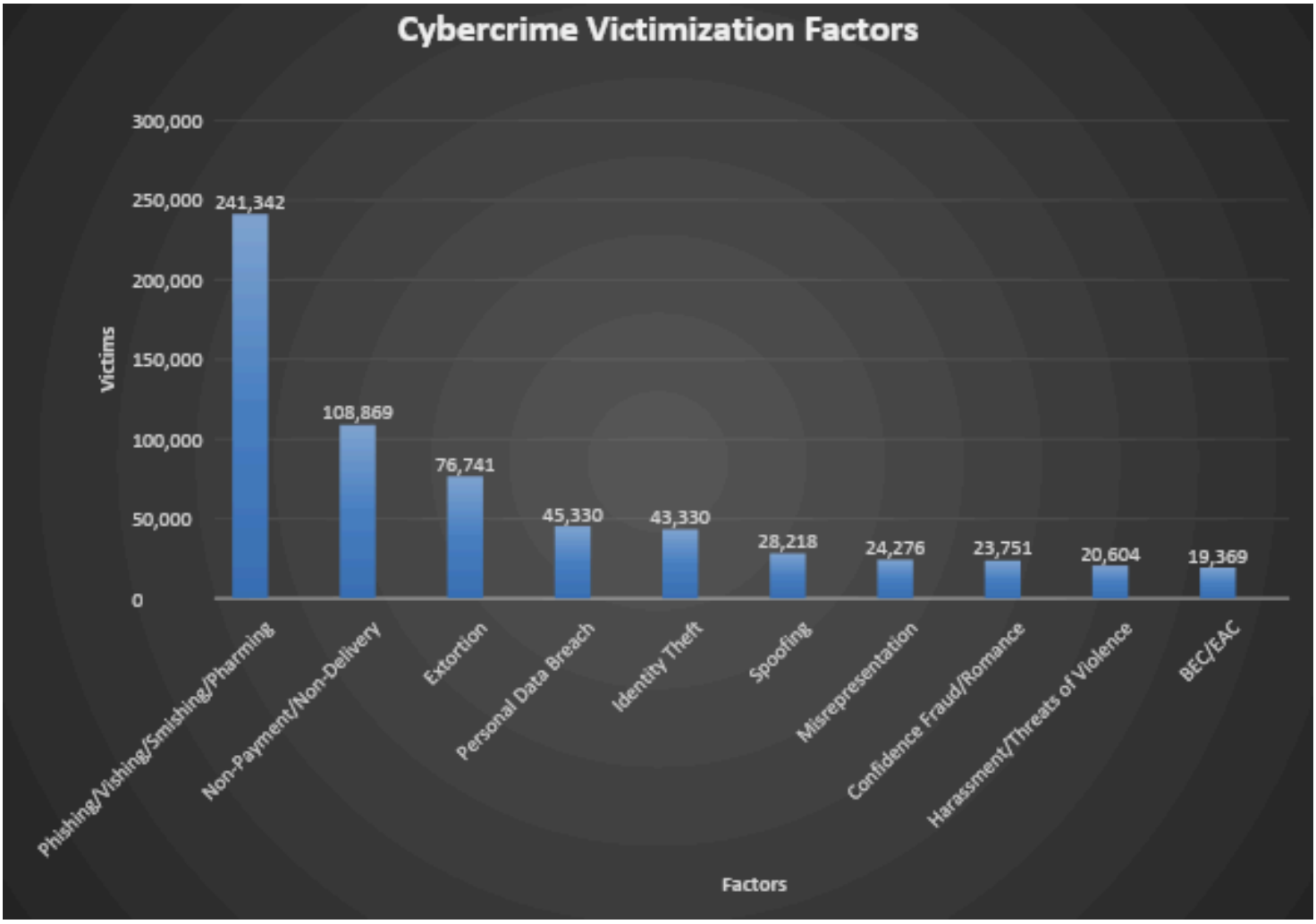

Figure 2. Most Frequent cybercrime since 2010

Conclusion

The identification of challenging factors of cybercrime victimizations is imperial to the security of online users. This research examined the prevalent cybercrime victimization factors and characteristics among teenagers, youth, and adults in the US.

As the results indicated, cybercrime victimization is a widespread phenomenon. In terms of the victimization factors, phishing, and non-payment/non-delivery were the most common types of crimes. And the characteristics of these crimes indicated that the middle-aged (Mean age 40) populace, with the higher percentage constituting of women (66%), belonging to the white race (84.3%) and maintaining a single and employed status with 63.4% and 61% respectively suffered most from cybercrimes. This may in fact relate to the nature of online interaction. The quantitative methodology applied to the underlying research questions has successfully and appropriately suggested the most common factors affecting cybercrime victimization.

References

[1] Ali, Maziah. (2015). Determinants of Preventing Cyber Crime: a Survey Research. *International Journal of Management Science and Business Administration*. 2. 16-24. 10.18775/ijmsba.1849-5664-5419.2014.27.1002.

[2] Ngo, Fawn T and Raymond Paternoster. “Cybercrime Victimization: An Examination of Individual Level Factors” *International Journal of Cyber Criminology* 5 (2011): 773.

[3] Philippsohn, Steven. (2001). Trends In Cybercrime — An Overview of Current Financial Crimes on The Internet. Computers & Security. 20. 53-69. 10.1016/S0167-4048(01)01021-5.

[4] Catherine D. Marcum and George E. Higgins Cybercrime in, Krohn, M. D., Hendrix, N., Penly Hall, G., & Lizotte, A. J. (Eds.). (2019). *Handbook on Crime and Deviance. Handbooks of Sociology and Social Research.*

[5] Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? Cyberpsychology, Behavior, and Social Networking, 21(2), 84–90.

[6] Meško, G. (2018). *On Some Aspects of Cybercrime and Cybervictimization. European Journal of Crime, Criminal Law and Criminal Justice, 26(3), 189–199.*

[7] Chang, Weiping & Chung, Wingyan & Chen, Hsiu-chin & Chou, Shihchieh. (2003). An International Perspective on Fighting Cybercrime. 2665. 379-384. 10.1007/3-540-44853-5_34.

[8] Sumanjit Das & Tapaswini Nayak(2013). *Impact Of Cybercrime: Issues And Challenges*. International Journal of Engineering Sciences & Emerging Technologies, October 2013. ISSN: 22316604 Volume 6, Issue 2, pp: 142-153

[9] Julian Jang-Jaccard, Surya Nepal, A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences, Volume 80, Issue5, 2014, Pages 973-993, ISSN 0022-0000,

[10] Baker, J. (2019, November 22). *Survey: Most Americans fear cybercrime but fewer take security measures*. Retrieved from PCWorld: https://www.pcworld.com/article/2066460/survey

[11] most-europeans-fear-cybercrime-but-fewer-take-security-measures.html

[12] Gibson, M. (2014, January 23). *Cell Phone Statistics: Updated 2013.* Retrieved from https://www.accuconference.com/blog/cell-phone-statistics Accessed-2021.

[13] Griffin, R. C. (2012). Cybercrime. *J. Int'l Com. L. & Tech.*, 136.

[14] McCusker, R. (2006). Transnational organised cyber crime: Distinguishing threat from reality. *Crime, Law and Social Change, 46*(4-5), 257-273.

[15] McGuire, M. (2012). *Organised crime in the digital age*. John Grieve Centre for Policing and Security.

[16] Lavorgna, A., & Sergi, A. (2016). Serious, therefore organised? A critique of the emerging" cyber organised crime" rhetoric in the United States. *International Journal of Cyber Criminology, 10*(2), 170.

[17] Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2016). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research, 23*(3), 287-300.

[19] Song, H., Lynch, M. J., & Cochran, J. K. (2016). A macro-social exploratory analysis of the rate of interstate

cyber-victimization. *American Journal of Criminal Justice, 41*(3), 583-601.