A REVIEW OF CYBERSECURITY AS AN EFFECTIVE TOOL FOR FIGHTING IDENTITY THEFT ACROSS THE UNITED STATES

Oloyede, Adekunle, Ajibade, Idris[1], Obunadike, Callistus[1], Phillips, Adeniyi[1], Shittu, Olayemi[1]; Taiwo, Esther[1] and Kizor-Akaraiwe, Somto[2]

[1]Department of Computer Science, Austin Peay State University,
Clarksville USA.
[2]School of Law, University of Washington, Seattle USA

ABSTRACT

The study is focused on identity theft and cybersecurity in United States. Hence, the study is aimed at examining the impact of cybersecurity on identity theft in United States using a time series data which covers the period between 2001 and 2021. Trend analysis of complaints of identity theft and cybersecurity over the years was conducted; also, the nature of relationship between the two variables was established. Chi-Square analysis was used to examine the impact of cybersecurity on identity theft in United States. Line graphs were used to analyze the trend in the variable. Time series data was used in the study and the data was obtained from secondary sources; Statista.com, US Federal Trade Commission, Insurance Information Institute and Identitytheft.org. Result from the study revealed that consumers' complaints on identity theft were on the increase every year. Total spending of the economy (both private and public sector) on cybersecurity was on continuous increase over the years. More than 100% of spending in 2010 was incurred in 2018. The Chi-Square analysis revealed that cybersecurity does not have significant impact on identity theft. The study recommended that the government increase the level of public awareness to ensure that members of the public protect their personal and other information to ensure that they are not compromised for fraud or identity theft. Organizations also need to invest more in the security system and develop policies that will support the security system. At the country level, international treaties and collaboration should be encouraged to prosecute the fraudsters hiding behind national borders.

KEYWORDS

Cybersecurity, Identity theft, Crime Prevention, Information Assurance and Security

1. INTRODUCTION

The Internet has become increasingly important in the last two decades as it contributes massively to nations' competitiveness, promotes innovation, promotes globalization, and makes life easy. As the importance and use of the internet continues to grow globally, there are growing cybersecurity threats and risks designed to take advantage of the usefulness of internet and how it connects different people from different countries [1]. Due to the structure of the computing environment, a security breach on one end providesa chance for exploitations elsewhere. Globally, cyber threats continue to move at a fast pace with cases of data breaches increasing yearly. Risk Based Security revealed that a shocking 7.9 billion records have been exposed by data breaches in 2019. That is way above double the number recorded in 2018 [2]. Governments across the globe have responded to rising cases of cyber threat by providing guidance to help organizations implement effective cybersecurity measures. In the U.S, a cyber-security

Dhinaharan Nagamalai (Eds): EMVL, EDUT, SECURA, AIIoT, CSSE -2023
pp. 31-42, 2023. IJCI – 2023 DOI:10.5121/ijci.2023.120504

framework was set up by the National Institute of Standards and Technology (NIST) to combat the spread of malicious code and early detection. The framework also emphasizes the continuous and real time monitoring of electronic resources. The importance of system monitoring was also emphasized in guidance provided by the U.K National Cybersecurity Centre and in Australian Cybersecurity Centre publications[2].

The phenomenon, identity theft, has been in existence for as long as humanity and crimes existed. With the emergence of the internet and e-commerce, identity theft evolved to online dimensions. In some countries, the scope of online identity theft is limited but its implications are significant across all countries and the growing risk of such theft erodes consumer confidence in the use of internet especially for e-commerce [3].Identity theft occurs when an individual, group of individuals or organization(s) acquire, transfer, own or utilize personal information of a legal entity in an unauthorized manner with purpose of personal gain which is usually in connection with fraud or other crimes [4]. There are two major types of identity theft: online and offline identity theft. The former is associated with misuse of computers and computer related crimes which are perpetrated using the internet. An example of this is that of a hacker that breached into profile or database of another entity to steal personal information. On the other hand, offline identity theft is usually committed through wallet theft and mail redirection. Identity theft related crimes in businesses have been on the increase over the last decade. KPMG, Kroll and CIFAS joint survey suggested that employees' fraud and identity theft related crimes cost more than $1.4 million per one billion US dollars of sales[5].

In recent years, the rate of identity theft has increased dramatically in United States, with criminals using varying methods to obtain and use Personally Identifiable Information (PII) to carry out malicious actions (National Security Agency, 2018).Findings of the U.S. Department of Justice in 2017 revealed that 17.6 million American or 7% of 16years or older were victims of identity theft, 86% of the country's population experience misuse of an existing credit card or bank account. The report also revealed that 7% experienced multiple types of identity theft while 14% of identity theft victims experienced an out-of-pocket loss, 49% of those suffered losses of more than $100 and 14% lost $1,000 or more[6].Governments have singly and collaboratively implemented policies to fight identity theft (both online and offline) at the domestic and international levels. The 1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce ("the 1999 Guidelines") and the 2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders ("the 2003 Guidelines"), for example, set out principles aimed at strengthening member countries' frameworks to fight offline and online fraud. Outside the OECD, international instruments such as the Council of Europe's Cybercrime Convention and the United Nations' Convention against Transnational Organized Crime have been developed to address the issue. With the growing menace caused by identity theft and losses incurred by victims of the crime, several measures and campaigns have been introduced by United States security agencies. One of which is cybersecurity. Personal protection from actors or criminals involved in identity theft is aimed to be dealt with on all fronts [3].

The United States faces threats from group of criminals who seek to exploit cyberspace to perpetrate different cybercrimes with motivation including financial gain, spying and political interest. It was observed that the criminal actors are highly empowered by modern and sophisticated information and communication technologies that enable them carry out their operations seamlessly [7]. Criminal organizations collaborate with each other through cyberspace. This makes it more complicated for the state, as they use proxies and other techniques that blur the distinction between state and non-state cyber activities. In several cases, malicious actors engaged in significant criminal cyber activity appear to have both criminal and nation-state affiliations. Threats from cyber criminals affect both federal and nonfederal information systems as threats and attempts to infiltrate government networks occur every day. The number of cyber incidents on federal systems reported to DHS increased more than ten-fold between 2006 and 2015. In 2015, a high-profile intrusion into a single federal agency resulted in the compromise of personnel records of over 4 million federal employees and ultimately affected nearly 22 million people [7].

The broad availability, relatively low cost, and increasing capabilities of cyber tools also affects trends and cybersecurity threats. For instance, Ransomware attacks both frontline systems and backup drives. Malicious cyber actors use this to compromise maritime, travel control, and healthcare systems. The Dark web facilitates the easy sale of illicit goods and services, from firearms and forged passports to malware, which actors may acquire and use. Malware kits and instructions are also readily available on Dark web. Malicious cyber tools sold on the Internet can be adapted to intrude into systems and otherwise commit criminal acts related to financial fraud, money laundering, intellectual property theft, or other illicit activities. The growing popularity of cryptocurrencies also presents challenges to countering money laundering and the work of law enforcement. Identity theft poses serious challenges and danger to individuals, businesses, and government. Cybersecurity measures undoubtedly need to be put in place for protection against identity theft. This study therefore aims to examine the impact of cybersecurity on identity theft. According to [8], it is vital to analyze the association and correlation between the variables (features), these variables are classified into PIE and DORT variables.

2. LITERATURE REVIEW

Cybersecurity can be said to be the act of providing protection to computers, mobile devices, network servers, electronic systems, databases, and data from malicious attacks. Cybersecurity can also to be referred to as information technology security and can be subdivided into different categories [2].

2.1. Network Security

This involves securing the computer network from attack or intruders or potential malware. Network security is a critical component of a successful business. It is important to ensure that all computers in a network are secure and that unauthorized access is not allowed. Security threats come in many forms, from viruses and malware to hackers and malicious software. To protect your network, you need to have a comprehensive security plan in place. The first step in network security is to create a secure environment. This involves using firewalls and antivirus programs to protect your network from outside attacks, using encryption and authentication methods to ensure that only authorized users can access your network. Additionally, you should keep all your software and hardware up to date, so that new threats can be quickly addressed. Another important part of network security is to monitor your network for any suspicious activity. You should be able to detect any suspicious traffic, such as unauthorized access attempts or denial of service attacks. You should also be able to detect any malicious software trying to infiltrate your network. Finally, you should create policies and procedures to ensure that all users are aware of the network security measures you have in place. This due diligence includes ensuring that all users are familiar with the security measures and understand the consequences of violation.

2.1.1. Operational Security

This includes operational decisions and lays down the processes for handling and protecting data assets. From the permission which users have when accessing the network to the process or procedures on how and where data is to be stored.

2.1.2. Information Security

Information security is another category of cybersecurity. It involves protecting information and protecting the integrity and privacy of data. This is done when information is moving from one person or medium to another and when information is in storage. Most organizations mandate staff to swear an oath of information security when joining as a new staff as a breach in information security could prove to be very costly.

2.1.3. Application Security

This has to do with providing security to application to prevent them from threats and compromise. A compromised application may become vulnerable and provide access to data that is meant to be protected. The process of application security starts from the beginning stages of an applications development.

2.1.4. Disaster Control

This explains how an organization responds to the threat of a cybersecurity incident or any situation that has led to a breach of the organization's cybersecurity infrastructure, loss of operations or data. This involves how an organization bounces back and returns to operational capacity and how the organization retrieves missing data in event of breach.

2.1.5. End User Education

This addresses the uncontrollable cybersecurity factor which is the end user. Some users of applications, devices or network servers are ignorant of threats to cybersecurity and may accidentally fall victim to breach in cybersecurity. The need for end user education is necessary to bring awareness to users of cybersecurity threats and how to protect their devices, emails, and servers [2].

2.2. Identity Theft

Traditionally, identity theft is committed by theft of personal belongings, gaining access to information acquired from public records, unauthorized use of databases, using credit cards of another entity for personal gains and misuse of personal information like demographic or financial information. Bad actors traditionally, steal identities from dumpster diving, pretexting, skimming, payment card theft and shoulder surfing to hacking, and business record theft. Identity theft is however, not majorly associated with one crime but composed of a wide variety of other crimes. Some other crimes with which identity theft is commonly associated are credit card fraud, other financial crimes, telemarketing and internet scams, auto theft, and robberies of various kinds. According to [9], the application of machine learning could be applied to tackle the problems of identity theft and cybersecurity across United States.

2.2.1. Stages of Identity Theft

All forms of identity theft are implemented through one or all ofthese three stages. They may include:

Stage 1:Identity is acquired through theft, hacking, fraud, trickery, force, redirecting mail or through legal means by buying victim's information online or from another party.

Stage 2: Use of identity for financial or other personal gain. The most common motivation for identity theft is financial gain. At this stage, the bad actor uses the identity acquired for personal gain. At this stage, the criminal also tries to avoid arrest from law enforcement or other authorities.

Stage 3: Discovery. This is the final stage of identity theft. At this stage, the theft of identity is discovered quickly depending on the amount of loss incurred by the victim. The loss at times may not be recovered [2].

2.3. Online Methods of Stealing Information

2.3.1. Malware

This is software code or program installed in an information system to cause damage to a system, breaking the defenses of the system it is installed in. The code or programis also installed into systems in some cases to undermine them for uses other than what their owner intended. Examples of malware include viruses, Trojan horses, spywares, backdoors, rootkits, Ransomware, Adware, and Botnets etc. Malware could be inserted into victims' system through removable drives or remotely through the download or installation of infected files.

2.3.2. Spam

This is the act of sending unsolicited and commercial bulk message over the internet. Spam messages or emails overload the network and occupy valuable memory space. Spam emails are sent to steal personal information by including compromised links for victims to click on.

2.3.3. Phishing

Phishing is a process of acquiring the personal or sensitive information of an individual or organization mostly via email while disguising as a trustworthy entity in electronic communication. This is when criminals target their victims with emails that appear to originate from legitimate sources, asking for personal or sensitive information. This is mostly used to obtain financial and other personal information from victims, especially credit card information. The email contains links that act as bait for victims to click.

2.3.4. Hacking

This is the practice of modifying computer hardware or software to achieve goals outside what the system was originally set up for. The purpose of hacking varies from demonstration of technical ability, to stealing, modifying, or deleting information for personal, political, social, or economic reasons. Corporate organizations hack their system to find and fix security vulnerabilities of their systems. Hackers are categorized into White Hat, Black hat, Grey Hat, and Blue Hat. White Hat hackers are hackers who find vulnerabilities in systems and inform the owner of the system, to fix the vulnerability. Black Hat hackers as opposed to White Hats hackers, hack systems with bad intentions. Grey hat hackers find out about security vulnerabilities through hacking, inform administrator and request for consultancy fee to fix a security bug. Blue Hat hackers are used to bug-test a system before they are launched [10].

2.3.5. Mitigation of Identity Theft

There are different methods adopted by individuals and organizations to prevent and tackle identity theft. Some of the measures include Network and Information Security: Organizations implement various methods at network and communication level to prevent identity theft. These measures include firewall security, network vulnerability analysis, encryption technology and anti-virus systems which mitigate identity theft [11].

It was indicated that among financial losses and losses of time, victims of identity theft also experience emotional (e.g., depression) and physical (e.g., poor health) symptoms, and withdrawal from certain transactions especially those involving their bank accounts. In addition to the rising incidence of identity theft, there is growing recognition of the negative emotional and physical health consequences of financial crimes[4].

Cybersecurity challenges and online fraud via the internet was studied by [12], the study revealed that assets and information that were once protected within the organization were now more easily accessible online; customer channels vulnerable to disruption; criminals have new opportunities for theft and fraud. With organizations growing organically and inorganically, the complexity of managing businesses & security operations is also becoming complex. It was also observed in the study that identity theft and online fraud will continue to increase as processing of transactions have mostly evolved to online mediums[12].

[13]investigated role of cybersecurity in minimizing crime rate in post-war Sierra Leone. The study focused on the establishment of the Cybercrime Unit at the Central Intelligence Department (CID), and the Office of the National Security (ONS). The study concluded that the use of CCTV cameras in certain quarters of both government and private entities minimized the crime rate and increased the bringing of perpetrators to justice by the ONS and CID departments. The study also highlighted some of the challenges of cybersecurity in security. Some of which include effective cooperation with neighboring countries such as the Republic of Liberia and the Republic of Guinea, high quality education among internet users and compliance with privacy and security guidelines as most telecommunication companies in third world countries were found to have breached their users' privacy, particularly because of the dearth of legal and legislative framework[13]. The approaches used in identity theft prevention were evaluated and guidelines suggested to overcome the weaknesses in mobile commerce (m-commerce). The result of the study showed that online organizations used the same approach to identity theft prevention for all online business transaction. While m-commerce has some unique characteristics with e-commerce, these arrangements are not evaluated for their effectiveness in m-commerce as a one glove fits all arrangement to identity theft protection is not effective[11].

3. METHODOLOGY

3.1. Data Sources and Descriptive Analysis

In this study, time series data spanning between years 2001 and 2021 was adopted. The data was sourced from secondary sources which included Statista.com, the US Federal Trade Commission and Insurance Information Institute.

3.2. Method of Analysis

The data collected was analyzed using Statistical Package for Social sciences (SPSS 20). Based on the objectives of the study, two major analytical methods will be adopted, they are Descriptive analysis and Chi-Square analysis. Descriptive analytical tools (graphs) are used to analyze the trend in the variables used in the study (identity theft and cybersecurity). Chi-square analysis will be used to examine the impact of cybersecurity on identity theft.

3.3. Analysis of Customers Complaints

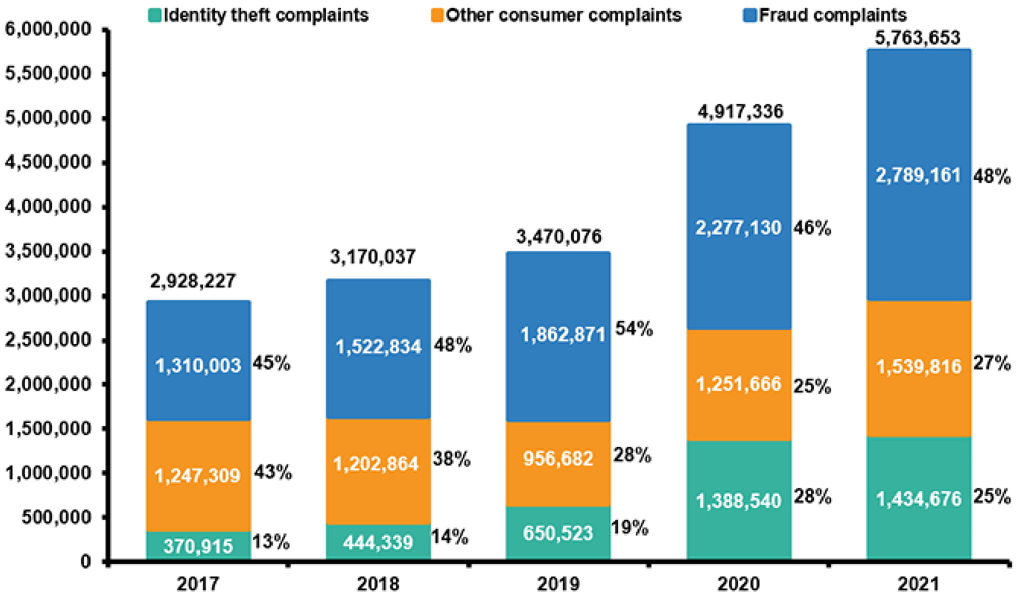

Figure 1. Consumers' Complaints (adopted from Insurance Information Institute (2023))

The graph above presents information about consumers' complaints between 2017 and 2021. It was observed in the graphical presentation that in 2017, identity theft accounted for 13% of consumer's complaints. Fraud complaints account for 45% of customers' complaints. In 2018, identity theft also accounts for the least of customers' complaints as it accounts for 14%. Between 2017 and 2019, the total increase in customers' complaints was on the increase. In 2020, the proportion of identity theft among customers' complaints was higher as it rose to 28% compared to less than 20% in previous years. In 2021, total customers' complaints rose rapidly while identity theft accounts for 25% of their complaints.

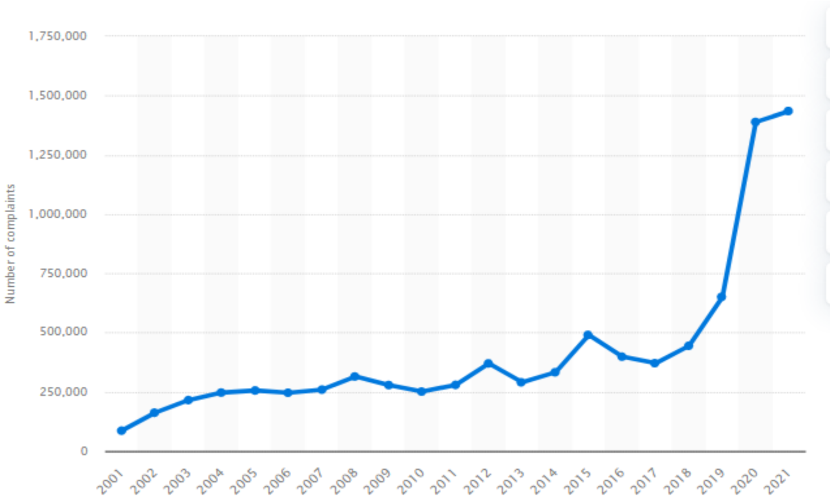

Figure 2: Number of Consumer Identity Fraud Complaints [14–16]

The graph above shows the trend in the number of consumers' complaints relating to identity theft in the US over the years. In the early 2000s, the number of complaints maintained a steady level with a slight increase year on year. This steady trend was maintained until 2008 when the number of identity theft complaints rose above 250,000 complaints. In 2009, there was a decline in the number of complaints, with the decline continuing until 2010 before a continued increase. Fluctuation was experienced between the years 2011 and 2017 when there was a sharp increase and decrease in the number of complaints. In 2015, the number of identity theft complaints from 2001 was at a peak of 500,000 complaints. From 2018 till 2021, the number of identity theft complaints rose to a significantly high level of about 1.5 million complaints in 2021.

3.4. Analysis of Cybersecurity Spending

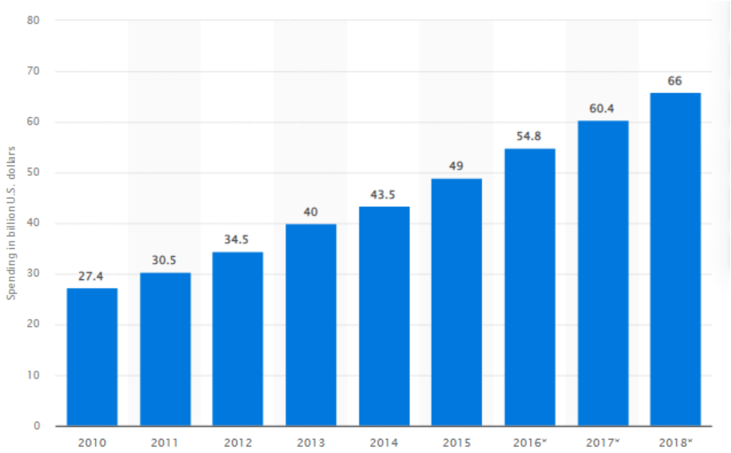

Figure 3: Spending on Cybersecurity in the United States from 2010 to 2018[14–16]

Figure 3 above presents information on the spending of the United States on Cybersecurity between 2010 and 2018. The graph shows that over the years, annual spending on cybersecurity has increased. In 2010, a total of 27.4 billion USD was spent on Cybersecurity, increasing to 30.5 billion USD in 2011. In 2013, total spending on cybersecurity increased to 40 billion USD and to 49 billion USD in 2015. In 2016, an additional 6 billion USD was spent on cybersecurity. Spending in 2018 increased by over 6 billion USD as compared to spending in 2017.

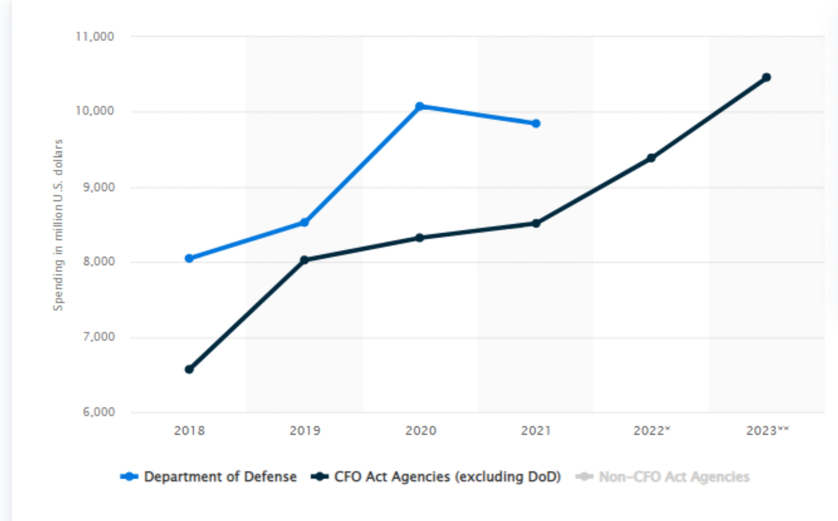

Figure 4: Total Government Spending on Cybersecurity[14–16]

Figure 4 shows the cybersecurity spending of the U.S. Government on CFO Act and non-CFO Act agencies from FY 2018 to FY 2023(in million USD). The diagram also presents the proposed spending on cybersecurity in 2023. In 2018, total government spending on cybersecurity for CFO Act agencies was about 6.5 billion USD while about 8 billion US dollars was expensed in US Department of Defense for cybersecurity. Government spending on CFO Act agencies increased massively in 2019 to 8 billion USD while the amount spent by Department of Defense was slightly above 8 billion USD. In 2020, much was spent by the Department of Defense on cybersecurity as over 10 billion USD was spent. Spending on CFO Act agencies increased slightly. In 2021, spending on Department of Defense for cybersecurity declined to less than 10 billion USD. Government spending on CFO Act Agencies continue to increase rapidly from 2021 to 2023.

3.5. Chi- Square Analysis

The test is used to analyze the relationship between cybersecurity and identity theft. The result of the analysis is presented in the table below.

Table 1: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	357.000[a]	340	.252
Likelihood Ratio	118.506	340	1.000
Linear-by-Linear Association	10.098	1	.001
N of Valid Cases	21		

a. 378 cells (100.0%) have expected count less than 5. The minimum expected count is .05.

The result of the Chi-square analysis showed that the Pearson Chi-square coefficient is 357 and the probability value is 0.252. The probability value is greater than 5% (0.05) significance level and therefore implies that there is no significant relationship betweencybersecurity and identity theft in the US.

4. RESULTS

Results from the analysis presented above, it was observed that consumers' complaints on identity theft were on the increase every year (see Figure 1). It was also revealed that in recent years, identity theft accounts for larger proportion of consumers' complaints relative to latter years (see Figure 2). Total spending of the economy (both private and public sector) on cybersecurity was on a continuous increase over the years (see Figure 3). More than 100% of spending in 2010 was incurred in 2018. Government spending on cybersecurity shows that in recent years, the government has injected more funds into other agencies (CFO Act Agencies) to combat cyber-crime and provide cybersecurity. It was also observed that between 2018 and 2023, government spending on cybersecurity has continued to be on the increase annually. The Chi-Square analysis revealed that cybersecurity does not have significant impact on identity theft as there is no significant relationship between cybersecurity spending and identity theft over the years.

5. CONCLUSION AND RECOMMENDATIONS

It can be concluded from the analysis above that more cases of identity theft are reported every year. It can also be concluded that both private and government spending on cybersecurity is on the rise. From the analysis, it can be concluded that cybersecurity does not have significant impact on identity theft. This is explained by the increased governmental and non-governmental spending on cybersecurity to ensure that the cases of identity theft are reduced but despite this increased yearly spending, cases of identity theft remain on a steady rise. From the conclusion of the study, it is recommended that the government increase public awareness to ensure that members of the public protect their personal and other information ensuring that they are not compromised for fraud or identity theft. Organizations on the other hand need to invest more in their security systems, developing policies and procedures that strengthen their security systems. With the heavy reliance of business processes on online systems, businesses should invest in their IT security infrastructure to protect their users and the organization from internal and external intruders. Consumer protection agencies should be adequately equipped with advanced technology to trace and track consumers' complaints. Prompt escalation should be made to relevant security agencies to be able to recover stolen funds from identity theft and protect potential victims who report suspicious activities.

Finally, at the country level, international treaties are needed to prosecute fraudsters hiding behind national borders. Countries should proactively reach agreements regarding the extradition of bad actors. End users should be encouraged to protect their personally identifiable information and on using additional authentication to prevent identity theft.

REFERENCES

1. The Department of Commerce, U.: Cybersecurity, Innovation and the Internet Economy. The Department of Commerce, Internet Policy Task Force., (2011)
2. Kaspersky: What is Cyber Security? Retrieved from Kaspersky, https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
3. OECD: OECD Policy Guidance on Online Identity Theft. (2008)
4. Li, Y., Yazdanmehr, A., Wang, J., Rao, H.R.: Responding to identity theft: A victimization perspective. Decis. Support Syst. 121, 13–24 (2019). https://doi.org/10.1016/j.dss.2019.04.002
5. Kroll Global Fraud Report: Global Fraud and Payments Report. (2023)
6. BJS: Victims of Identity Theft, 2014 Retrieved 0 from Bureau of Justice Statistics. (2014)
7. U.S. Department of Homeland Security: Cybersecurity Strategy. U.S. Department of Homeland Security. (2018)
8. I.Olufemi, C.Obunadike, A. Adefabi, D. Abimbola: Application of Logistic Regression Model in Prediction of Early Diabetes Across United States. Int. J. Sci. Manag. Res. 06, 34–48 (2023). https://doi.org/10.37502/IJSMR.2023.6502
9. Obunadike, C., Olisah, S., Adefabi, A., Abimbola, D., Oloyede, K.: Application of Regularized Logistic Regression and Artificial Neural Network model for Ozone Classification across El Paso County, Texas United States. Journal of Data Analysis and Information Processing. Vol. 11, No.3 (2023)
10. Jeetendra, P.: Introduction to Cyber Security. Uttarakhand Open University, Haldwani. (2017)
11. Mahmood, H.S., Javed, A., Zahoor, A.S.: INVESTIGATING THE IDENTITY THEFT PREVENTION STRATEGIES IN M-COMMERCE. Presented at the International Conferences ITS, ICEduTech and STE. (2016)
12. Krishan, T., Neenu, J.: CYBER SECURITY CHALLENGES & ONLINE FRAUDS ON INTERNET. International Journal of Advanced Research in IT and Engineering. 5(2), (2016)
13. Ibrahim, A.S.: The Role of Cyber Security in Minimizing CrimeRate in Post-War Sierra Leone: Durreesamin Journal. 3, 23–27 (2018)
14. Statista: Spending on cybersecurity in the United States:, https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/
15. Statista: Number of consumer complaints relating to fraud lodged with the U.S. Federal Trade Commission from 2001 to 2021:, https://www.statista.com/statistics/587350/fraud-complaints-frequency-in-the-us/
16. Statista: Cyber security spending of the U.S. government on CFO Act and non-CFO Act agencies. Retrieved 1 10, 2023, from Statista:, https://www.statista.com/statistics/1003402/us-cyber-security-spending-cfo-act-agencies/

AUTHORS

Kunle Oloyede has a B.Sc. in Geography and M.Sc. in Geographic Information System and is currently pursuing his second M.Sc. degree in Computer Science & Quantitative Methods. With 7 years of experience in the IT space. Kunle is passionate about using data to forecast and improve organizational metrics.

Idris Ajibade has an associate degree in Statistics, B.Sc. in Computer Science and M.Sc. in Computer Science & Quantitative Methods with over 8 years combined experience in Business & Sales Analytics, Product Marketing, Data Engineering and Systems Operations Engineering. Idris is always excited at the thought of exploring a pristine environment and making positive impacts

Callistus Obunadike holds three Master of Science degrees in geology, mining engineering, and computer science. Callistus combines his extensive knowledge of geosciences with data science. Callistus has a passion for applying machine learning algorithms to improve geological processes and predicting of future events.

Adeniyi Phillips is a highly skilled professional with a passion for leveraging data to drive innovation and improve business outcomes. Holding a master's degree in computer science, he has established himself as a proficient data engineer with a keen understanding of innovative technologies and their applications.

Olayemi Shittu is a highly skilled professional with a demonstrated ability to extract valuable insights from datasets and translate them into actionable strategies. Holding a B.Sc. in Finance and an M.Sc. in Computer Science & Quantitative Methods, he has a proven record of accomplishment of successfully designing and implementing data-driven solutions across diverse industries such as Finance and Technology industries.

Esther Taiwo a dedicated professional in the IT and data field holds a Bachelor of Science (BSc.) degree in Mathematics and Statistics. Currently, she is pursuing a Master of Science (MSc.) degree in Computer Science and Quantitative Methods. Esther's passion lies in utilizing data to foster innovation and enhance solutions that positively impact our world.

SomtoKizor-Akaraiwe is a trained attorney, data privacy and cybersecurity professional, holding a Bachelor of Laws (LL.B.) degree and dual Master of Lawsdegrees in Intellectual Property Law and Sustainable international Development. Somto is passionate about bringing the rapidly changing technological landscape up to par with global legal best practices.