World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

Check for updates

A literature review of financial losses statistics for cyber security and future trend

Md Haris Uddin Sharif * and Mehmood Ali Mohammed

School of Computer and Information Sciences, University of the Cumberland, Williamsburg, Kentucky, U.S.A.

World Journal of Advanced Research and Reviews, 2022, 15(01), 138–156

Publication history: Received on 13 May 2022; revised on 20 June 2022; accepted on 22 June 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.15.1.0573

Abstract

Cybercrime directs to any criminal activity taken out utilizing computers or the internet. Attackers have chosen strategies such as social engineering, phishing, and malware as part of their cyber-attacks. A cyber-attack can lead to various effects, ranging from stealing individual data to extortion money or losing helpful information. Society and systems depend on critical infrastructures like power plants, hospitals, and financial services companies. This paper analyzes financial losses statistics for cyber security and future trends. The cost of cybercrime prevention is increasing day by day. Financial losses refer to damages to the wealth of an organization. This includes organizational losses, compensation, and legal fees. By financial loss, we mean increased costs or reduced income caused by the threat. We collect data from various datasets and information from sources. After collecting data, we analyze the data and create a different chart to identify the growth of cyber-attacks, cyber security, and cybercrime costs. We analyze global and worldwide cybercrime status. We also investigate state-wise cybercrime and the cyber security status of the United States of America. Our main objective of the analysis is to find out the financial losses and future trends of cybercrime and cyber security. From our study, we noticed that the number of cybercrimes and their management and prevention costs are rapidly increasing in the USA and worldwide.

Keywords: Cyber risk; Open data; Datasets; Cyberattacks; Cyber threats; Financial Losses

1. Introduction

Cybercrime in finance obtains financial gain through profit-driven criminal activity, including identity fraud, ransomware attacks, email and internet fraud, and attempts to steal financial accounts, credit cards, or other payment card information. Every citizen should know that their data has been stolen and is in the dark, deliberately concealed, and used to cover up and promote heinous activities. The size of the deep web is stronger than the surface web and is increasing at a rate that defies measurement.

In 2021, the United States gained unprecedented experience in malicious cyber activity and cyber-attacks. Many businesses and the American public negotiate these types of cyber-attacks. Cyber threats and classic foreign intelligence threats are increasing day by day. It is becoming increasingly involved with emerging technologies. The F.B.I. uses individual authority and partnerships to assess risks and impacts on U.S.A. cyber adversaries [7]. FAUCFA compiled the result of F.B.I. internet offense statistics from 2015 to 2020. In these reports there are eight internet crimes identified for study: (i) Theft Identity, (ii) Fraud Investment, (iii) Email Account Compromise/Business Email Compromise/ (EAC/BEC), (iv) Fraud/Romance Confidence, (v) Spoofing, (vi) Rental/Real Estate, (vii) Non-Delivery/Non-Payment, and (viii) Fraud of Tech Support. The highest online crime - BEC/EAC was with documented victim losses in 2020 of $1.9 billion. BEC/EAC explained one-third to three-quarters of all online victim losses during 2020 in the six top states. It accounted for 76% of all online victim losses in Ohio, 65% in New York, 59% in Illinois, 43% in Texas, 39% in Florida, and 35% in California. The ratio of victim losses from this scam to all online crime losses for 2020 increased in Florida,

* Corresponding author: Haris Uddin Sharif
School of Computer and Information Sciences, University of the Cumberland, Williamsburg, Kentucky, U.S.A.

Illinois, New York, and Texas and declined in California and Ohio [8]. Cyber risks are "Functional risks to data and technology wealth that impact the secrecy, vacancy, and probity of data or information systems." [9]. Distinguished cyber risks contain data breaches and cyber-attacks [10]. A contemporary industry report highlights potential impacts and rising exposure to cyber risks. The Global Risk Report, produced by the World Economic Forum, ranks cyber-attacks on vital infrastructure 5th.

The trend and intensity of cyber-attack have multiplied due to intelligent technology, digitization, and globalization. Research, potential fields, and robust cyber security defense systems are essential in industrial development. Cyber-attack has been focused at the corporate, individual, and national levels. It is estimated that the lack of cyber security in the global economy has cost $945 billion by 2020. Cyber threats create huge corporate risks, privacy breaches, trade obstacles, and economic losses [1]. Despite the increasing relevancy of cyber risk, there are constraints to the availability of cyber risk data for the international economy. There are many reasons: it is an evolving and emerging risk; consequently, limited data sources [2]. The second reason: hacked institutions don't want to disclose incidence [3]. The shortage of required data poses challenges for multiple issues such as risk management, analysis, and cyber security [4]. In April 2021, The European Council declared that a Center of Excellence for Cyber Security (CESC) would be established to pool technology, research, and industrial development funding. The center aims to improve the security of virtual networks, information systems, and the internet [5].

Besides the benefit of risk-adjusted costing, the source of open datasets supports institutions in benchmarking their inner cyber attitude and cybersecurity measures. The analysis can even assist in enhancing risk awareness and associate manners. Multiple companies still ignore their cyber risk [11]. Though companies are bound to report data breaches to the respective supervisory management in many countries, this data is generally unavailable to the analysis community. Also, the economic effect of these breaches is usually in the dark.

This study works from a risk management perspective considering the role of cyber security and cyber insurance. It focuses on cyber risk and contributes to risk mitigation and risk transfer. We review existing literature and open data sources related to cybersecurity and cyber threats, highlighting the datasets utilized to enhance academic performance and increase the existing state-of-the-art in cybersecurity. Therefore, significant data about the available datasets are presented, and cyber risk data is standardized for educational analysis comparability and transcript. The following section explains the literature review regarding cybersecurity and cyber risks. The results of the 3rd section outline the data source. The fourth section describes the output of the data analysis. 5t section described future trends of cybercrime. The 6th section presents Steps Taking in Advance to Avoid Cyber Risks Findings; further discussion is shown in the 7th section. And the final section concludes.

2. Literature Review

Due to the importance of cyber risks, different literature studies have been conducted in this field. We studied the published literature on cyber risk from a financial perspective. One hundred forty-seven papers with the term 'cyber risk' were identified and classified into various categories. [6] Publishes cybersecurity forecasts and reports. The report was published in Cyber Crime. By 2021, the loss of cybercrime will cost $6 trillion annually, up from $3 trillion in 2015, according to the editor-in-chief of the annual cybercrime report. The published Ransomware report focuses on the fact that the financial loss of Global Ransomware will reach $20 billion by 2021, which is 57% more than in 2015. Cybersecurity Market Report - Global expense on cybersecurity services and products will exceed $1 trillion from 2017 to 2021. Women In Cybersecurity Workforce – In 2019, Women represented 20% of cybersecurity workers globally. The Data Attack Report – The world will reserve 200 zettabytes of information by 2025. 50% of data will preserve in the cloud. Cybersecurity Almanac – figures, 100 facts, Cybersecurity Ventures predictions, and statistics published by Cisco. C.M.W. – By 2021, more than 70% of all cryptocurrency trades yearly will be for criminal activity.

2021 was an extremely trying year for cybercrime in so many places. There were high-profile breaches such as Solar Winds, Colonial Pipeline, and dozens of others with significant economic and security-related impacts. Ransomware became an act of revenge targeting multiple small and medium businesses [31]. The specified open information can help cyber insurers endeavor sustainable product development. Standard risk analysis processes have been vulnerable for insurance companies due to the lack of recorded claims data [30]. [12] All industrial internet of things (IIoT) attacks happen at the information transmission layer, contrary to most references.

In IIoT, ML and DL approaches are utilized for creating the I.D.S. and models to identify the attacks at any level of its architecture. Minimizing the attacks could be a fundamental goal of cybersecurity while understanding that we can't entirely ignore them. The number of people preventing the attacks and defense approaches is smaller than those ready for the attacks. [13] According to the 2018 PwC's Global Economic Crime and Fraud Survey, U.S. organizations encountered more economic defeats in every class (from $0.5 to $100 million) due to fraud likened to their global opponent. The previous review on cyber-attacks and their economic effects show separated outcomes on the primary goal and victims. As per the 2016 F.I.C. Report, cyber-attacks are the second-highest financial crime resource in global economic associations [16]. Many are large-scale attacks, frauds, and heists, as the economic sector is the primary target of cyber criminals [15]. For instance, in 2016, Bangladesh Central Bank surrendered to SWIFT hackers. Hackers steal $81 million [14]. In 2013, cyber hackers used South Korean economic networks for many days [18]. In 2012, Bank of America, Wells Fargo, P.N.C. Bank, and JPMorgan Chase faced a denial-of-service (DDoS) attack [18]. At the same time, different agents deliver additional losses for the banks globally. I.M.F. calculates that the annual financial could be about USD 97 billion, which amounts to about 9% of the global banking net profits in 2016 [19]. Thus, economic organization and banks have persistently improved their security systems to overcome growing cybercrime that controls their fixed functioning costs [20]. Deloitte's report displays that banks' techniques costs (as a percentage of total revenue) rise to 7.16%, the highest prices among all categories of the global economy [21]. Therefore, it recommends that the global economic industry is adversely affected by direct losses from cybersecurity breaches and additional cyber overhead costs.

The 2017 Norton Cyber Security Insights Report [37] shows a growing trend in cyber-attack and resulting losses globally. According to the report, the total population of 20 countries in 2017 was 3.2 billion. Out of 3.2 billion, 98 million people were affected, and 44% of consumers were affected by cybercrime. One of the 2017 Norton Cyber Security Insights Report [37] highlights that most consumers think cybercrime is a mistake and a criminal act. They also recognize it as a reality of life and consider that data is not theft online. Theft of 'real life' things is awful. Although such crimes constantly affect consumers worldwide, an exciting and perhaps unexpected result of the report is that American consumers ranked third in 2017, after China and Brazil, with a total loss of $19.4 billion due to cybercrime. In 2018, the World Economic Forum stated that fake and economic crime was a trillion-dollar industry reporting that private organizations independently spent about $8.2 billion on anti-money laundering (A.M.L.) controls in 2017 [22].

Several systematic reviews have been published on cybercrime [38]; [39]; [40]; [41]. In these articles, the authors focused on an exact area or sector in the context of cybersecurity. This article adds to this existent literature by concentrating on data availability and its importance to risk control and insurance stakeholders. With an emphasis on healthcare and cybersecurity, [38] directed an organized literature study. The authors determined 472 articles containing ransomware, cybersecurity & healthcare, and security risk in Cumulative databases. Associate Health Literature Indicators, Nursing, PubMed, and ProQuest. The articles were worthy of this review. Three criteria are considered here:

- They were published between 2006 and 2016.
- The full text of the paper was available.
- The publication is an equivalent-reviewed or scholarly journal.

The authors saw that technical improvement and federal policies (in the U.S.) are the significant characteristics revealing the health sector to cyber risks. Loukas et al. (2013) directed a study emphasizing cyber risks and cybersecurity in crisis control. The authors supplied a summary of cyber threats in transmission, detector, data managing, and vehicle techniques utilized in crisis control and displayed places for which there is no explanation in the publications. Also, [41] studied the publications on cybersecurity threats in higher education organizations. For the publication's study, the authors utilized the keywords' cyber', 'information threats' or 'vulnerability' in relationship with 'higher education, 'university' or 'academia.' The same publications study focused on the Internet of Things (IoT) cyber threats was executed by [39]. The study indicated that qualitative techniques concentrate on high-level frameworks, and quantitative approaches to cybersecurity risk control focus on risk inspection and quantification of cyber threats and effects. Moreover, the results showed a four-step IoT cyber threats control framework that identifies, quantifies, and emphasizes cyber threats.

Network intrusion detection (N.I.D.) methods found malicious network activity settlement a network's secrecy, availability, and integrity. A method for categorizing distributed denial of service (DDoS) and identifying it together was created by [23]. In [24], the authors showed a Fog layer-based DDoS threats identification technique to determine malicious nodes in the IoT network. The offered resolution utilizes clustering and an entropy-based approach and is executed on the OMNeT++ simulator. Social spamming is a severe cyber risk, which depends laboriously on huge messaging, fraud I.D., and the circulation of harmful links. [25] The focus is that attackers utilize social media to make phishing attacks, advertise affiliate websites and propagate malware. Datasets are a fundamental element of cybersecurity analysis, highlighted by these works. [27] Analyzed different cyber threats datasets in detail. The reality inspired the research that with the proliferation of the internet and innovative technologies, the way of attacks is also developing. Therefore, to prevent this attack, one must first detect them; cybersecurity datasets' propagation and development are critical. The authors followed analyses of datasets utilized in I.D.S. in their work. [28] Determined the demand for a new database in cybersecurity. The researchers presented a taxonomy of current intrusion detection systems, a comprehensive review of notable recent work, and an overview of the datasets commonly used for assessment purposes.

The IoT botnet threat is a different class of DoS threats. The authors created an I.D.S., a mixture of ANN, NB, and D.T., to ignore botnet threats against the message queuing telemetry transport (MQTT) and domain name system (DNS). There are Chose ANN, NB, and D.T. as they could categorize these vectors skillfully due to the relative chronology weights between the malicious and benign vectors. Every single algorithm regarding out-false-positive and detection ratio performance parameters is performed in this ensemble model. The result was that the accuracy of the UNSW and NIMS datasets was 99.54% and 98.29%, respectively [26]. C.P.S. from being utilized to resolve real-world difficulties, despite all the fraud adjacent to them. It is essential to perform in real-time. Because of this anticipation, methods might run to network challenges, such as pauses, so C.P.S.s have strict conditions. Also, compared to traditional information technology (I.T.) techniques, the loss that a defeat fetches to human life and infrastructure is more extreme in this issue [29].

2.1. Summary of the Cost of Cyber Crime in 2021 [42]

- Due to COVID-19 Pandemic, Cybercrime up 600%
- It is estimated that cybercrimes will cost $10.5 trillion annually worldwide by 2025.
- The global estimated cybercrime annual cost will be $6 trillion.
- Cybercrime cost makes up a value worth 1% of the global G.D.P.
- Average cyber-attack costs a company over 2.5 USD
- Ransomware is 57% more destructive in 2021 than in 2015.
- The average cyber-attack cost of a small business ranges from $120,000 to $1.24 million.
- Zero trust security policies saved $1.76 million per attack.
- Enterprises experienced an average of 130 security breaches per year per organization.
- Enterprises saw the annual cost of cyber security increase by 22.7% in 2021.
- The annual number of security breaches in enterprise organizations increased by 27.4%.
- 71.1 million people fall victim to cybercrimes yearly.
- Individuals lose USD 4,476 on average.
- Individuals lose USD 318 billion to cybercrime.
- Individuals of phishing scams lost USD 225 on average.
- The top 5 cybercrimes in 2021 were:
  - Extortion
  - Identity theft
  - Personal data breach
  - Non-payment
  - Phishing attacks

Cyber Security Ventures predicts that the cost of global cybercrime will increase by 15% per year over the next five years. If this continues to grow, the expense will reach 10.5 trillion U.S. dollars by 2025, 3 trillion more than in 2015. This describes the most significant transfer of financial assets in history, risks the inspirations for novelty and investment, is exponentially more extensive than the harm imposed from natural disasters in a year and will be more beneficial than the global business of all unlawful drugs [6]. Therefore, it is essential to take the needed steps to control cyber-attacks.

3. Data Source

We collect data from Consumer Sentinel Network Data Book 2021 (Federal Trade Commission), 2021_IC3Report (Internet Crime Repost 2021 of Federal Bureau of Investigation), Cybercrime Magazine, and published articles in reputed journals, Chapters, and websites. We got some information in CSV dataset format, some in excel files, and others in the text. The F.B.I. receives internet-related fraud complaints through its Internet Crime Complaint Centre IC3. The IC3's website www.IC3.gov is a website for victims to file suspected internet-related crimes. Filing a complaint requires the victim or complainant to provide detailed information on the internet crime. The detailed information requested when filling a complaint includes:

- Victim's personal information (name, address, telephone, and email)

- Financial trade information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and I.P. address
- Specific details on the person were victimized
- Email header(s)

It is essential to remember that the F.B.I. reports include reported internet crimes, only a portion of the actual number of internet crimes committed yearly in the United States of America.

Cybercrime Magazine formulates its ground-up research plus synthesizes and repurposes research from the most credible sources (analysts, researchers, associations, vendors, industry experts, and media publishers) to provide readers with a bird's-eye view of cybercrime and the cybersecurity industry. Its sponsor's name, "KnowBe4," provider of the world's most effective security awareness training and simulated phishing platform — recently announced it had launched a new research arm called KnowBe4 Research, with the branch's first "Security Culture Report."

4. Data Analysis

This report covers twelve years from 2010 to 2021, as these years contain comparable information for crime types in F.B.I. data, F.T.C. data & reposts. They used different data formats. Our report herein shows the reported internet crime in absolute numbers of victim losses and numbers of victims, and relative loss rates and victim rates accounting for population. The loss rate is defined as the number of monetary victim losses divided by millions. Similarly, the victim rate is defined as the number of victims divided by the population in millions. Further, our report uses internet crime and internet fraud interchangeably.

4.1. Number of Complaints of Cyberattacks last twelve years (2010-2021), U.S.A.

We collect data from Federal Trade Commission (F.T.C.), U.S.A., and Infosec Insights. The F.T.C. published data book, namely Consumer Sentinel Network Data Book. The data provided by the public. The databook focuses on fraud, identity theft, other consumer problems, and financial losses. Unwanted phone calls are written in the Do Not Call Data Book. Infosec Insights collects data from the Center for Strategic & International Studies (CSIS), Kaspersky, and the Federal Bureau of Investigation (F.B.I.) Internet Crime Report. F.T.C. and F.B.I. are government organizations. CSIS and Kaspersky are reputed and trusted sources. The Federal Bureau of Investigation (F.B.I.) enforces federal law. It investigates various criminal activities, including terrorism, cybercrime, white-collar crimes, public corruption, civil rights violations, and other significant crimes. CSIS is a non-profit policy research organization dedicated to advancing practical ideas to address the world's most critical challenges. Kaspersky is an anti-Virus that provides comprehensive protection against various information security threats. Multiple functions and protection components are available as part of Kaspersky Anti-Virus to deliver complete protection. A dedicated protection component handles every kind of threat.

We collect financial data. Financial Data means any economic and market data, price quotes, news, analyst opinions, research reports, signals, graphs, or other data or information available through the Trading Platform. Since these data have been collected from the F.B.I., F.T.C., CSIS, and Kaspersky, these data are reliable.

After collecting the data, we create an excel table. There are two columns and 13 rows in the table. The first column shows reporting years, and 2nd column shows no complaints. There is a different figure each year. We use the summation formula to get the total number for the relevant year. We gather and calculate the data for creating a bar chart. We created a horizontal bar chart using the data in figure 1.

We are analyzing financial losses in this article. We gather year-wise complaints data to create this bar chart. Here we present a comparative statement for no. of complaints last 12 years from 2010 to 2021.

We select the table and then click on the insert bar chart. We choose a horizontal bar chart. Microsoft Excel generates a horizontal bar chart. Then we add Axes, Axis Title, Chart Title, Data Labels, Guidelines, and Legend. We also changed the chart style and color. Microsoft excel uses internal chart-creating procedures to generate the chart.

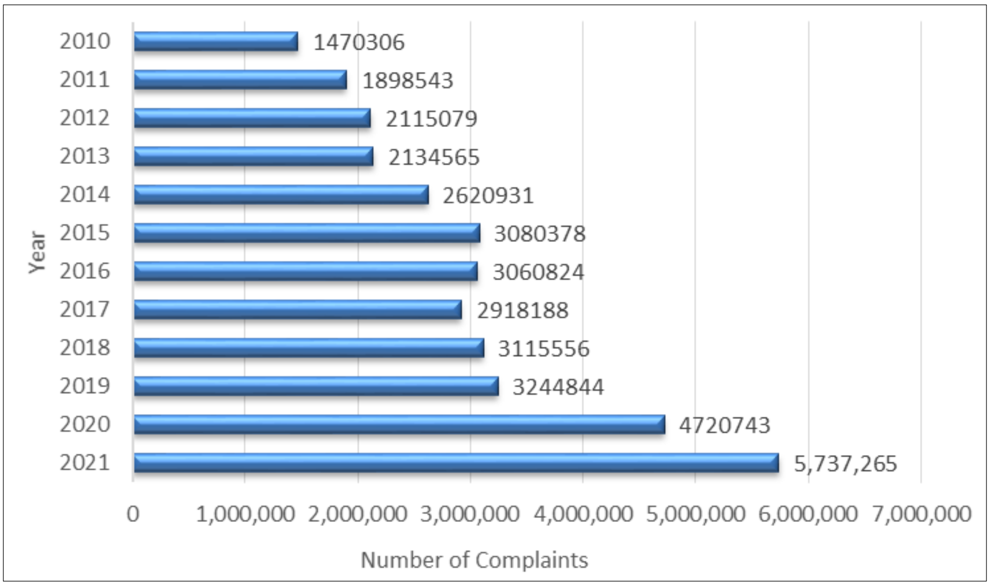

Figure 1 Number of Complaints of Cyberattacks last twelve years (2010-2021), U.S.A.

The bar chart shows the number of cybercrime complaints for the last 12 years, from 2010 to 2021. The X-axis represents the number of complaints in this chart, and the Y-axis represents years. In 2010, the total complaints were 1,470,306 which increased in 2021, the value is 5,737,265. Growth rate 290.21%. Details are shown in Figure 1. Hackers are getting smarter, cybercrime prevention is expensive, everything is automated, vulnerabilities are everywhere, and companies' processes have become automated; more of their infrastructure is rooted in technology. Moreover, every automated system is created by code that can be accessed when cybercriminals break in.

4.2. Amount of Losses of Cyberattacks last twelve years (2010-2021), U.S.A.

We collect data from the Federal Trade Commission (F.T.C.) and the Federal Bureau of Investigation (F.B.I.). The F.T.C. published data book, namely Consumer Sentinel Network Data Book. The data provided by the public. The databook focuses on fraud, identity theft, other consumer problems, and financial losses. The Federal Bureau of Investigation (F.B.I.) enforces federal law. It investigates various criminal activities, including terrorism, cybercrime, white-collar crimes, public corruption, civil rights violations, and other significant crimes. F.T.C. and F.B.I. are government organizations.

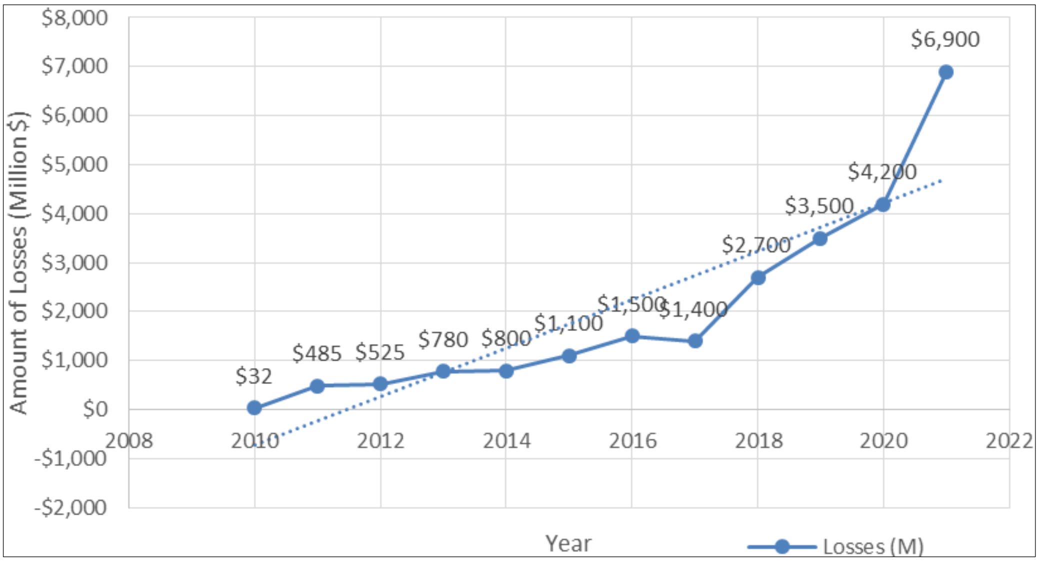

Figure 2 Amount of Losses of Cyberattacks last twelve years (2010-2021), U.S.A.

We collect financial data. Financial Data means any economic and market data, price quotes, news, analyst opinions, research reports, signals, graphs, or other data or information available through the Trading Platform. Since these data have been collected from the F.B.I. and F.T.C., these data are reliable.

After collecting the data, we create an excel table. There are two columns and 13 rows in the table. The first column shows reporting years, and 2nd column shows the number of losses (in a million $). There is a different figure each year. We use the summation formula to get the total number for the relevant year. We gather and calculate the data for creating a 2D line chart. We created a 2D line chart using the data in figure 2.

We gather year-wise financial losses data to create this 2D line chart. Here we present a year-wise statement for the last 12 years from 2010 to 2021 U.S.A.

We select the table and then click on insert 2D line chart. We choose a 2D line chart. Microsoft Excel generates a 2D line chart using the data. Then we add Axes, Axis Title, Chart Title, Data Labels, Guidelines, Legend, and Trendline. We also changed the chart style and color. Microsoft excel uses internal chart-creating procedures to generate the chart.

The 2D line chart shows the amount of cyber-attack losses for the last 12 years, from 2010 to 2021. The Y-axis shows the number of losses for cyber-attacks, and the X-axis shows the year. In 2011 the cost increase 21.53%; 45.48% in 2012 and 29.13% increase in 2021. Details are shown in Figure 2.

4.3. Number of Fraud, No. of Identity Theft, and No. of Other Cyber Attacks from 2010 to 2021, U.S.A.

We collect data from Federal Trade Commission (F.T.C.). The F.T.C. published data book, namely Consumer Sentinel Network Data Book. The data provided by the public. The databook focuses on fraud, identity theft, other consumer problems, and financial losses.

We collect year-wise fraud, identify theft, and other data from F.T.C. data. Since these data have been collected from F.T.C., F.T.C. is a U.S. government department, so these data are reliable.

Table 1 Number of Fraud, No. of Identity Theft, and No. of Other Cyber Attacks from 2010 to 2021, U.S.A.

Year	Fraud	Identity Theft	Other
2010	820,072	251,074	399,160
2011	1,041,517	279,191	577,835
2012	1,112,693	369,958	632,428
2013	1,159,115	290,098	685,352
2014	1,526,365	332,545	762,021
2015	1,165,393	490,085	1,429,676
2016	1,228,865	398,356	1,435,874
2017	1,310,003	370,915	1,247,309
2018	1,522,834	444,339	1,202,864
2019	1,862,871	650,523	956,682
2020	2,277,130	1,388,540	1,251,666
2021	2,789,161	1,434,676	1,539,816

After collecting the data, we create an excel table shown in Table 1. There are four columns and 13 rows in the table. The first column shows reporting years, 2nd column shows the year-wise number of frauds, 3rd column shows year-wise identify theft, and column four shows other threads. There is a different number each year. We use the summation formula to get the total number for the relevant year. We gather and calculate the data for creating a 2D line chart. We created a 2D line chart using the data in figure 3.

We gather year-wise data breaches number to create this 2D line chart. Here we present year-wise data breaches statements for the last 12 years from 2010 to 2021 U.S.A.

We select the table and then click on insert 2D line chart. We choose a 2D line chart. Microsoft Excel generates a 2D line chart using the data. Then we add Axes, Axis Title, Chart Title, Data Labels, Guidelines, Legend, and Trendline. We also changed the chart style and color. Microsoft excel uses internal chart-creating procedures to generate the chart.

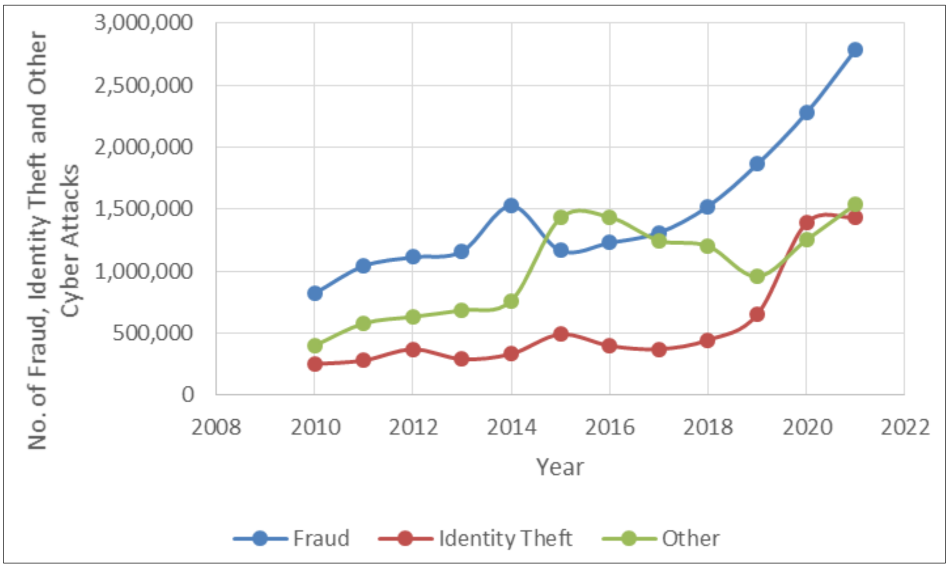

Figure 3 Number of Fraud, No. of Identity Theft, and No. of Other Cyber Attacks from 2010 to 2021, U.S.A.

Table 1 [43] and Figure 3 show the number of Fraud, identity theft, and No. of Other Cyber Attacks from 2010 to 2021 U.S.A. In 2010 there was no. of fraud 820,072; identity theft 251,074; and other cyber-attacks 399,160. In 2021, we saw that the number increased significantly compared to 2010. 2021 has come no. of fraud 2,789,116; no. of identity theft 1,434,676 and other cyber-attacks 1,539,816. The growth rate compared to 2010: fraud by 240.11%, Identity theft by 471.42%, and Other cyber-attacks increased by 285.76% [43]. X-Axis represented the number of Fraud, No. of Identity Theft, and No. Of Other Cyber Attacks, and Y-Axis represented the year. Hackers are getting smarter, cybercrime prevention is expensive, everything is automated, vulnerabilities are everywhere, and companies' processes have become automated; more of their infrastructure is rooted in technology. Due to these frauds, identity theft and other cyber-attacks increased.

4.4. The number of Records Breaches from 2010-2021, U.S.A.

We collect data from Federal Trade Commission (F.T.C.). The F.T.C. published data book, namely Consumer Sentinel Network Data Book. The data provided by the public. The databook focuses on fraud, identity theft, other consumer problems, and financial losses.

We collect year-wise reports of breaches data from F.T.C. data. Since these data have been collected from F.T.C., F.T.C. is a U.S. government department, so these data are reliable.

After collecting the data, we create an excel table. There are two columns and 13 rows in the table. The first column shows reporting years, 2nd the column shows the year-wise number of report breaches. There is a different number each year. We use the summation formula to get the total number for the relevant year. We gather and calculate the data for creating a bar chart. We have created a bar chart using the data shown in figure 4.

We gather year-wise report breach numbers to create this bar chart. Here we present a year-wise report breaches statement for the last 12 years from 2010 to 2021 U.S.A.

We select the table and then click on the insert bar chart. We choose a bar chart. Microsoft Excel generates a bar chart using the data. Then we add Axes, Axis Title, Chart Title, Data Labels, Guidelines, Legend, and Trendline. We also changed the chart style and color. Microsoft excel uses internal chart-creating procedures to generate the graph.

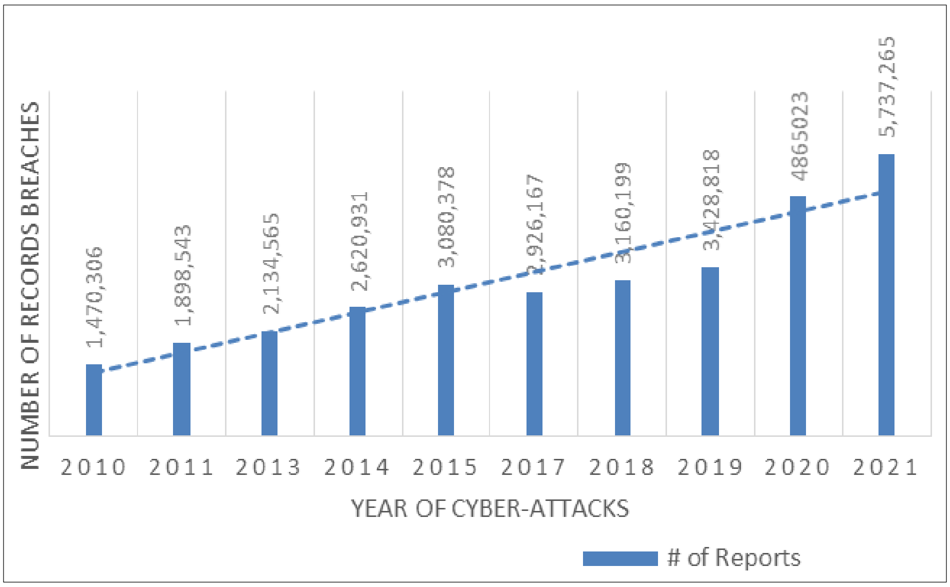

Figure 4 Number of Records Breaches from 2010-2021, U.S.A.

The bar diagram shows the Number of Records Breaches from 2010-to 2021, U.S.A. In 2010, the total records breached 1,470,306, which increased in 2021, and the number is 5,737,265. Growth rate 290.21% [43]. Details are shown in Figure 4

4.5. Top 10 Fraud Categories 2021, U.S.A.

We collect data from Federal Trade Commission (F.T.C.). The F.T.C. published data book, namely Consumer Sentinel Network Data Book. The data provided by the public. The databook focuses on fraud, identity theft, other consumer problems, and financial losses.

We collect year-wise fraud, identify theft, and other data from F.T.C. data. Since these data have been collected from F.T.C., F.T.C. is a U.S. government department, so these data are reliable.

After collecting the data, we create an excel table. There are four columns and 30 rows in the table. The first column shows rank, 2nd column shows categories, 3rd column shows no report breaches, and 4th column shows %. There is different value in each category. We use the summation formula to get the total number for the relevant category. We gather and calculate the data first. Then sum 3o categories at the bottom of the category column. Select the table, use the short & filter formula, and select short largest to smallest. We got top 10 categories. In column four calculate % i.e., column 4 (%) = no. of reports ÷ sum of categories x 100. We calculate % of the top 10 categories. We have created a pie chart using the data shown in figure 5.

We gather category-wise report breach numbers, calculate % for relevant categories, and generate the pie chart. Here we present the top 10 fraud categories 2021, U.S.A.

We select 11 rows and three columns from the table, then click on the insert pie chart. Microsoft Excel generates a pie chart using the data. Then we add Chart Title, Data Labels, and Legend. Microsoft excel uses internal chart-creating procedures to create the graph.

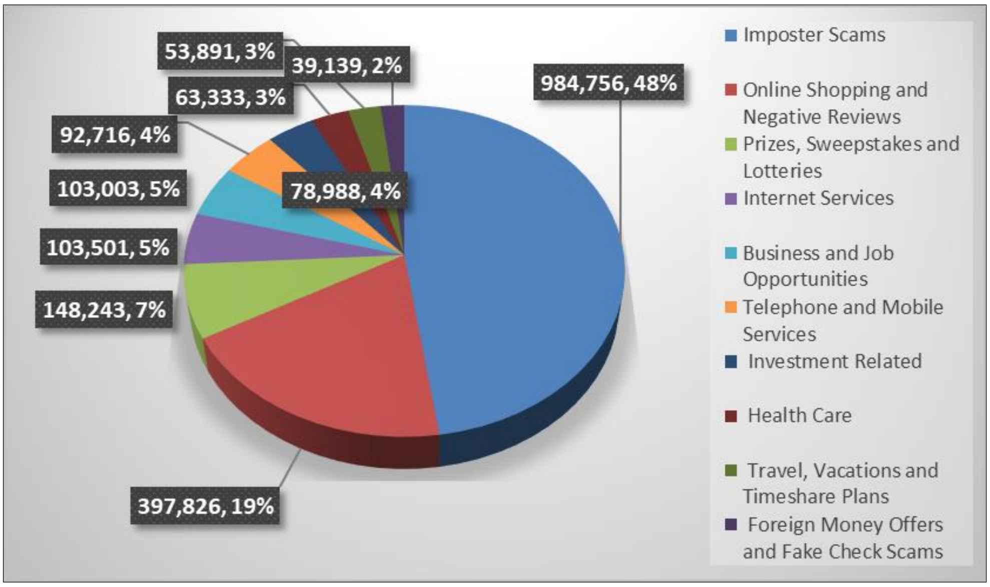

Figure 5 Top 10 Fraud Categories 2021, U.S.A.

The pie chart is showing to 10 fraud categories in 2021 U.S.A. The highest fraud happened in Imposter Scams, 984,756 (48%), and the lowest copy happened in Foreign Money Offers and Fake Check Scams, 39,139 (2%) [43]. Details in figure 5.

4.6. Victims by Age Group 2021, U.S.A.

We collect data from IC3. The IC3's website www.IC3.gov is a website for victims to file suspected internet-related crimes. Filing a complaint requires the victim or complainant to provide detailed information on the internet crime. The detailed information requested when filling a complaint includes:

- Victim's personal information (name, address, telephone, and email)
- Financial trade information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and I.P. address
- Specific details on the person were victimized
- Email header(s)

We collect age-wise losses and complaints data from IC3 reports. Since these data have been collected from IC3. IC3 is a U.S. government department F.B.I., so these data are reliable.

After collecting the data, we create an excel table. There are three columns and seven rows in the table. The first column shows ages, 2nd column shows complaints number, and column three shows age-wise losses. There is a different number for each generation. We use the summation formula to get the total number for the relevant age. We gather and calculate the data for creating a bar chart. We have created a bar chart using the data shown in figure 6.

To create the bar chart, we gather victims' data by age group complaints and losses. Here, we present victims' complaints by age group and losses ($ million) 2021, U.S.A.

We select the table and then click on the select bar chart from the Insert menu. We choose a bar chart. Microsoft Excel generates a bar chart using the data. Then we add Axes, Axis Title, Chart Title, Data Labels, Guidelines, and Legend. We also changed the chart style and color. Microsoft excel uses internal chart-creating procedures to generate the chart.

In 2021, U.S. age-based cybersecurity analysis showed that there had been 42.8772 million complaints this year. Whose losses amounted to S5.5998 billion. The lowest breach was for people under 20 (record number 14,919, and damage was $101.4 million). The highest breach was for people over 60 (record number 92,371, and the amount of damage was $1680 million) [7]; figure 6 shows the details.

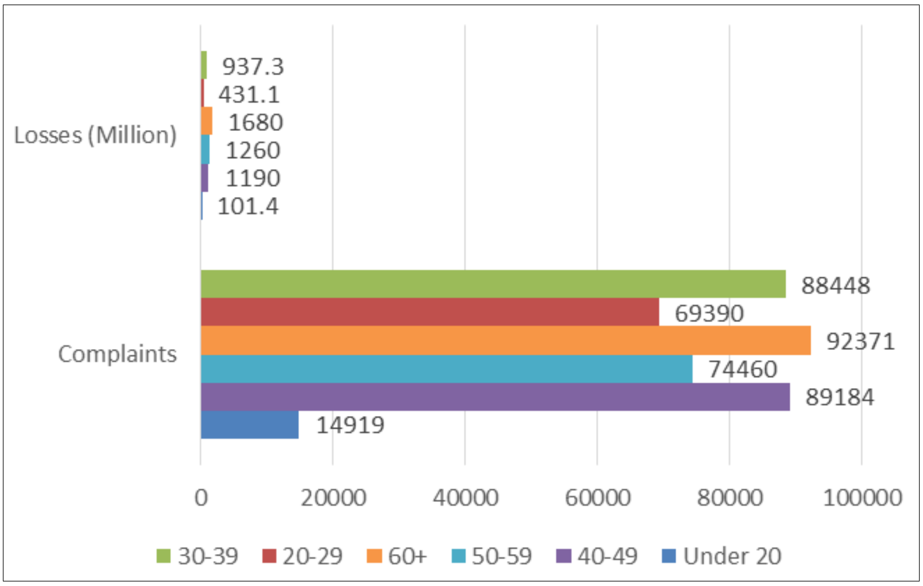

Figure 6 Victims by Age Group Complaints and Losses ($ million) 2021, U.S.A.

4.7. Top 15 Crime Types by Losses U.S.A. 2021

We collect data from IC3. The IC3's website www.IC3.gov is a website for victims to file suspected internet-related crimes. Filing a complaint requires the victim or complainant to provide detailed information on the internet crime. The detailed information requested when filling a complaint includes:

- Victim's personal information (name, address, telephone, and email)
- Financial trade information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and I.P. address
- Specific details on the person were victimized
- Email header(s)

We collect crime types by losses data from IC3 reports. Since these data have been collected from IC3. IC3 is a U.S. government department F.B.I., so these data are reliable.

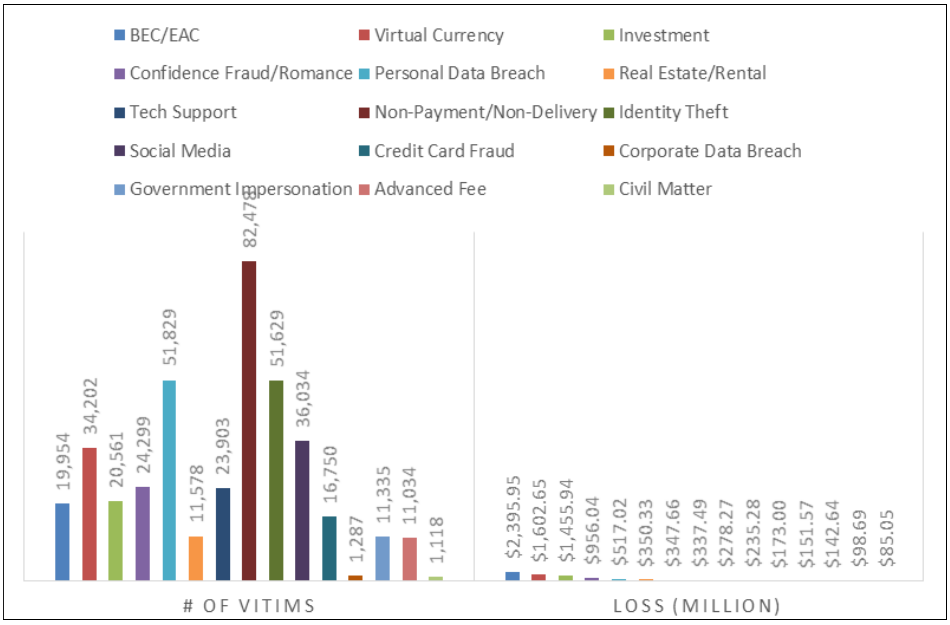

Figure 7 Top 15 Crime Types by Losses 2021, U.S.A.

After collecting the data, we create an excel table. There are four columns and 33 rows in the table. The first column shows rank, 2nd column shows crime types, 3rd column shows no. Victims and the 4th column show losses ($ million). There is a different value for each kind. We use a summation formula to get the total number for the relevant type. We gather and calculate the data first. Select the table, use the short & filter formula, and select fast most significant to the most minor. We got the top 15 types. We have created a bar chart using the data shown in figure 7.

We gather crime types by losses data to create the bar chart. Here we present the top 15 crime types by losses 2021, U.S.A.

We select the table and click on the bar chart from the Insert menu. We choose a bar chart. Microsoft Excel generates a bar chart using the data. Then we add Axes, Axis Title, Chart Title, Data Labels, Guidelines, and Legend. We also changed the chart style and color. Microsoft excel uses internal chart-creating procedures to generate the chart.

Here we discover the Top 15 crime types in 2021 in the U.S.A. There have been breaches, a total of 3,97,991 million complaints this year. Whose losses amounted to S9,128.00 billion. The lowest breach was for people under the age of 20 (record number 14,919, and the amount of damage was $101.4 million). The highest breach was for people over 60 (record number 92,371, and the amount of damage was $1680 million) [7]; figure 7 shows the details.

4.8. Top 10 States by Victim 2021, U.S.A.

We collect data from IC3. The IC3's website www.IC3.gov is a website for victims to file suspected internet-related crimes. Filing a complaint requires the victim or complainant to provide detailed information on the internet crime. The detailed information requested when filling a complaint includes:

- Victim's personal information (name, address, telephone, and email)
- Financial trade information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and I.P. address
- Specific details on the person were victimized
- Email header(s)

We collect states by victim data from IC3 reports. Since these data have been collected from IC3. IC3 is a U.S. government department F.B.I., so these data are reliable.

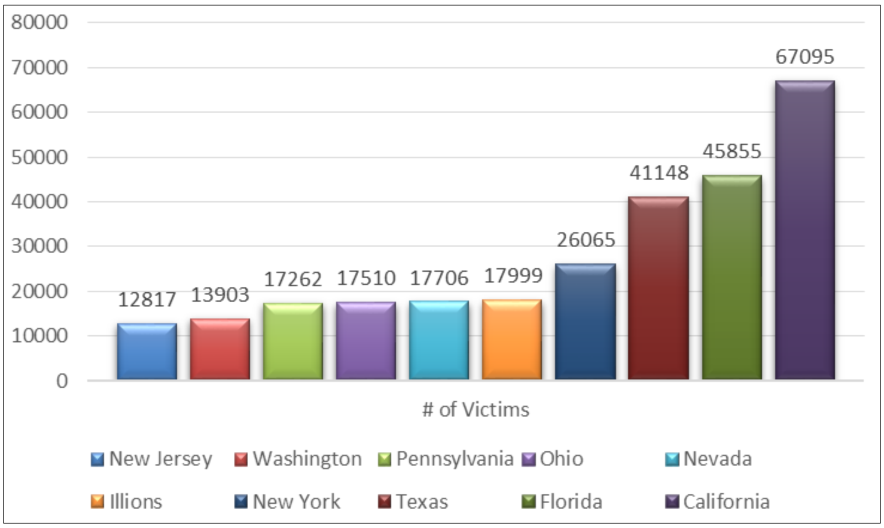

Figure 8 Top 10 States by Victim 2021, U.S.A.

After collecting the data, we create an excel table. There are three columns and 51 rows in the table. The first column shows rank, 2nd column shows the state's name, and 3rd column shows no. Victims. There is different value in each state. We use the summation formula to get the total number for relevant conditions. We gather and calculate the data first. Select the table, use the short & filter formula, and select fast most significant to the most minor. We got the top 10 states. We have created a bar chart using the data shown in figure 8.

We gather states by victim data to create the bar chart. Here we present the top 10 states by victim 2021, U.S.A.

We select the table and then click on a bar chart from the Insert menu. We choose a bar chart. Microsoft Excel generates a bar chart using the data. Then we add Axes, Axis Title, Chart Title, Data Labels, Guidelines, and Legend. We also changed the chart style and color. Microsoft excel uses internal chart-creating procedures to generate the chart.

The highest breaches happened in California (67095), 2nd position in Florida (45855), and the lowest violations were found in New Jersey (12817) [7]; figure 8 shows the details.

4.9. Top 10 States Losses 2021, U.S.A.

We collect data from IC3. The IC3's website www.IC3.gov is a website for victims to file suspected internet-related crimes. Filing a complaint requires the victim or complainant to provide detailed information on the internet crime. The detailed information requested when filling a complaint includes:

- Victim's personal information (name, address, telephone, and email)
- Financial trade information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and I.P. address
- Specific details on the person were victimized
- Email header(s)

We collect state losses data from IC3 reports. Since these data have been collected from IC3. IC3 is a U.S. government department F.B.I., so these data are reliable.

After collecting the data, we create an excel table. There are three columns and 51 rows in the table. The first column shows rank, 2nd column shows the state's name, and 3rd column indicates the number of losses ($ million). There is different value in each state. We use the summation formula to get the total losses for relevant states. We gather and calculate the data first. Select the table, use the short & filter formula, and select fast most significant to the most minor. We got the top 10 states. We have created a bar chart using the data shown in figure 9.

We gather state losses data to create the bar chart. Here we present the top 10 states' losses 2021, U.S.A.

We select the table and then click on a bar chart from the Insert menu. We choose a bar chart. Microsoft Excel generates a bar chart using the data. Then we add Axes, Axis Title, Chart Title, Data Labels, Guidelines, and Legend. We also changed the chart style and color. Microsoft excel uses internal chart-creating procedures to generate the chart.

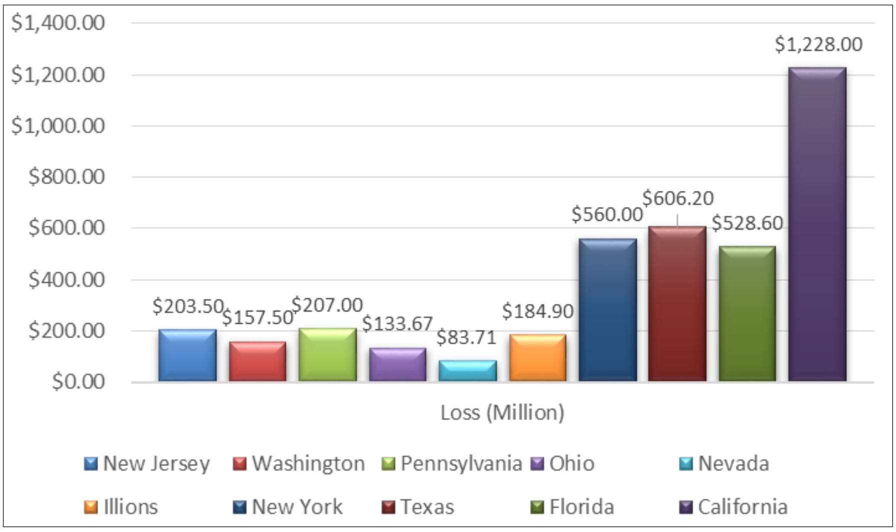

Figure 9 Top 10 States Losses 2021, U.S.A.

In 2021 labeled the top 10 states based on the number of Losses. These include California, Florida, Texas, New York, Illinois, Nevada, Ohio, Pennsylvania, Washington, and New Jersey. The highest losses happened in California ($1,228.00 million), 2nd position in Texas ($606.00 million), and the lowest breaches cost in New Jersey ($83.71 million) [7]; the difference between the lowest and highest amount is $1144.29 million. The X-axis represents States name in this chart, and Y-axis represents cybersecurity losses. Figure 9 shows the details.

Hackers are getting smarter, cybercrime prevention is expensive, everything is automated, vulnerabilities are everywhere, and companies' processes have become automated; more of their infrastructure is rooted in technology. Moreover, every computerized system is created with code that can be accessed when cybercriminals break-in.

4.10. Top 20 International Victim Countries in 2021

We collect data from IC3. The IC3's website www.IC3.gov is a website for victims to file suspected internet-related crimes. Filing a complaint requires the victim or complainant to provide detailed information on the internet crime. The detailed information requested when filling a complaint includes:

- Victim's personal information (name, address, telephone, and email)
- Financial trade information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and I.P. address
- Specific details on the person were victimized
- Email header(s).

We collect country no. of victim's data from IC3. Since these data have been collected from IC3. IC3 is a U.S. government department F.B.I., so these data are reliable.

After collecting the data, we create an excel table shown in Table 2. There are two columns and 42 rows in the table. The first column shows the country name, and 2nd column shows no. of victims. There is different value in each state. We use the summation formula to get the total losses for relevant states. We gather and calculate the data first. Select the table, use the short & filter formula, and select short smallest to largest. We got the top 20 countries. We have created a waterfall chart using the data shown in figure 10.

Table 2 Top 20 International Victim Countries in 2021

Country	# Of Victims
Japan	419
Turkey	422
Malaysia	443
Italy	517
Pakistan	530
Argentina	538
Spain	560
China	571
Greece	585
Netherlands	675
Philippines	1051
Brazil	1053
Mexico	1326
Germany	1429
South Africa	1790
France	1972
Australia	2204
India	3131
United Kingdom	303949
United States	466501

We gather country-wise no. of victim data to create this waterfall chart. Here we presented the Top 20 International Victim Countries in 2021.

We select the table and then click on insert waterfall chart. Microsoft Excel generates a waterfall chart using the data. Then we add Axes, Axis Title, Chart Title, Data Labels, Guidelines, and Legend. We also changed the chart style and color. Microsoft excel uses internal chart-creating procedures to generate the chart.

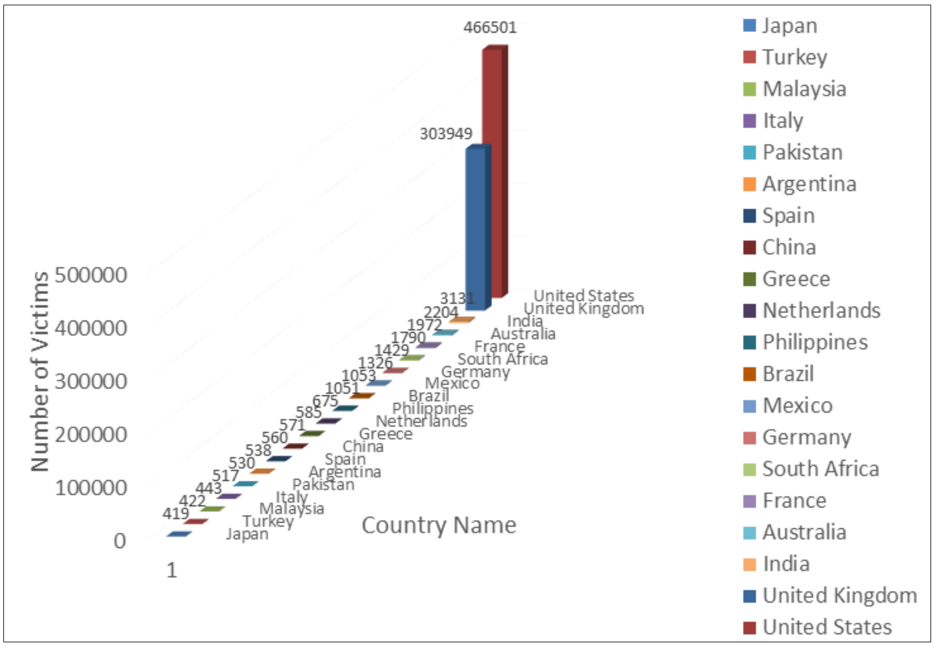

Figure 10 Top 20 International Victim Countries in 2021

Table 2 and figure 10 show the top 20 countries by several total victims. In 2021 highest breaches were found in the United States (out of 20), 2nd position in the U.K., and the lowest place in Japan [7].

5. Results

Our study shows that the United States has the most cyber-attacks. The cost of cyber security is increasing day by day. Number of attacks: 21.53% in 2011; 45.48% in 2012, 4.15% in 2013; Cyber-attacks increased by 7.6% in 2014. In 2015 and 2016, the number of cyber-attacks was relatively low. Cyber-attacks decreased by 4.6% in 2015 and 0.63% in 2016. The cost of cyber security is increasing day by day. 21.53% in 2011; 45.48% in 2012, 4.15% in 2013; Cyber-attacks increased by 7.6% in 2014. In 2015 and 2016, the number of cyber-attacks was relatively low. Cyber-attacks decreased by 4.6% in 2015 and 0.63% in 2016. In 2016, the number of attacks increased by 16.53%. In 2016, the attack rate increased to 22.89%. In 2019, the attack rate decreased by 0.92%. The Corona epidemic has led to a worldwide lockdown and a slowdown in trade and commerce, leading to fewer attacks this year. In 2020, it will increase again by 11.41%. In 2021 it increased by 29.13%. In terms of financial expenditure, the cost increased by 7.25% in 2012. In 2013, the expenditure increased manifold to 48.56%. Although the number of attacks increased in 1018, expenditure decreased by 7.6%. In 2021, the amount of expenditure will reach the highest level. Expenditure increased by 74.29% compared to 2020. Category-based analysis shows that in 2021, the highest fraud happened in Imposter Scams, 984,756 (48%), and the lowest copy happened in Foreign Money Offers and Fake Check Scams, 39,139 (2%). State-wise analysis shows the highest losses happened in California ($1,228.00 million) and the lowest breaches cost in New Jersey ($83.71 million); the lowest and highest amount is $1144.29 million. Country-wise analysis shows the 2021 highest breaches found in the United States, 466,501, and the lowest position in Japan (419). Hackers are getting smarter every day, everything turns to automation, and cybercrime prevention is expensive; for this reason, the number of cyber-attacks and the protection costs increase. Moreover, every computerized system is created with code that can be accessed when cybercriminals break-in.

6. Future Trends of Cybercrime

- The projected cost of staff safety awareness training will reach $10 billion by 2027 [32].

- The number of Internet utilizers will reach 6 billion by 2022, increasing to more than 7.5 billion by 2030 [33].
- By 2022, global spending on I.A.M. products and services will exceed $ 16 billion [34].
- By 2025, smartphones will account for 55% of total IP. Traffic [35].
- From 2017 to 2021, global healthcare cybersecurity spending will gradually exceed $ 65 billion [36].

7. Steps Taking in Advance to Avoid Cyber Risks Findings

- Restrict all confidential information that is shared online.
- Don't utilize location features.
- Modify privacy settings.
- Keep operating system and software applications up to date.
- Create strong passwords. Utilize two factors of password validation.
- Use a Wi-Fi network and a secure Internet connection.
- Passwords or P.I.N.s don't share with anyone.
- Be careful about sharing personal financial information with your social security number, credit card number, or bank account number.
- Only share personal information on secure sites, starting with HTTP
- Use anti-malware and antivirus solutions and use firewalls to block threats.
- Regularly back up your files to an encrypted file storage device.
- Scammers can create fake links to websites. So, don't click on the text or email links from people you don't know.

8. Research Findings

In this study, we have analyzed various data sets from open source. There is a shortage of free datasets online. We have collected the necessary information from various government and non-government reports on the financial loss for cyber security and analyzed them. The data used in our research is more accurate.

8.1. Significant Findings are as follows.

- Cybersecurity is endless fighting. It will not find a permanently powerful solution to the problem in the foreseeable future.
- Advancements to the cybersecurity pose of someone, businesses, government agencies, and the government have significant measures in decreasing the defeat and damage incorporated with cybersecurity breaches.
- Advancements in cybersecurity call for two types of activity: (a) steps to more actually and more widely utilize what is known about enhancing cybersecurity, and (b) steps to acquire new learning about cybersecurity.
- Generally available data and guideline efforts have been inadequate to inspire a satisfactory feeling of quickness and privilege of cybersecurity issues in the U.S. as a nation.
- Cybersecurity is essential to the United States, but the nation has different attractions and few disputes with critical.
- Cybersecurity. Tradeoffs are unavoidable and must be received through the nation's political and policy-making procedures.
- The benefit of improper functions in cyberspace as a tool to extend U.S. attractions increases numerous essential technological, lawful, and policy questions which have yet to be circulated publicly by the U.S. government.

9. Challenges

Lack of historical data and dynamic nature, knowing and evaluating cyber threats is a big challenge for stakeholders. To manage this challenge, a more significant source of cyber data is required to help researchers with cyber threat management and cyber risk-related problems. Institutes could integrate this new understanding into their associated culture to decrease cyber threats. In addition, it could acquire standard explanations of cyber threats from new data.

Proposed Acronyms

- C.P.S. : Safety and security concerns prevent
- CSIS : The Center for Strategic and International Studies
- DDoS : Distributed Denial-of-Service (DDoS)

- FAUCFA: Florida Atlantic University's Center for Forensic Accounting
- E.A.C. : Email Account Compromise
- B.E.C. : Business Email Compromise
- W.E.F. : World Economic Forum
- A.M.L. : Anti–Money Laundering
- P.R.C. : Privacy Rights Clearinghouse
- M.E.D. : Medical Dataset
- B.S.O. : Block Storage Option
- F.B.I. : Federal Bureau of Investigation
- CESC : Center of Excellence for Cyber Security
- DL : Deep Learning
- ML : Machine Learning
- N.I.D. : Network intrusion detection
- C.M.W. : Cryptocurrency Market Watch
- F.I.C. : Financial Industry Cybersecurity Report
- IMF : International Monetary Fund IMF

10. Conclusion

This paper analyzes Financial Losses Statistics for Cyber Security and Future Trends. We collect and analyze available datasets, literature, eBooks, reports, journals, and websites on cybercrime, cyber security, cyber-attacks, cyber risks, and economic losses. After analyzing the data, we created year-based, country-based, U.S. state-based, organization-based, and category-based tables and charts. These charts will benefit readers, researchers, various organizations, and stakeholders. Other investigation areas may include the integrity and conformation of cybersecurity and cyber threats databases. From the tables and charts obtained in our analysis, we found that the number of cyber-attacks and the amount of financial loss is increasing day by day in different countries of the world, including America. Many people must be recruited and trained to prevent and protect against cyber-attacks. As a result, the cost of this sector is increasing rapidly. We also analyze future trends of cybercrime and financial losses. In the analysis, we also noticed that the number, cost, and growth rate of cyber-attacks are different among the states of the U.S.A. due to financial activity and transactions. In some states, the number and price of cyber-attacks are growing at an alarming rate. We have analyzed the data for the last 12 years and found the future trend of cyber-attacks. It shows that the number of cyber-attacks and costs is increasing rapidly. From this literature review, decision-makers and planners can get an idea of what should be done next. Our literature review is also helpful for planners planning to prevent cyber-attacks or risks and financial losses.

Compliance with ethical standards

Acknowledgments

This Research paper analysis the statistical analysis of Cybersecurity losses and future trends. The authors wish to thank online source owners according to their data availability.

Disclosure of conflict of interest

The authors said there is no conflict of interest concerning this article's research, authorship, and publication.

Funding

The authors received no financial support for this article's research, authorship, and publication.

References

[1] Sheehan, B., F. Murphy, M. Mullins, and C. Ryan. Connected and autonomous vehicles: A cyber risk classification framework. Transportation Research Part a: Policy and Practice. 2019; 124: 523–536.

[2] Biener, C., M. Eling, and J.H. Wirfs. Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance—Issues and Practice. 2015; 40 (1): 131–158.

[3] Eling, M., and W. Schnell. What do we know about cyber risk and cyber risk insurance? Journal of Risk Finance. 2016; 17 (5): 474–491.

[4] Falco, G. et al. Cyber risk research impeded by disciplinary barriers. Science (American Association for the Advancement of Science). 2019; 366 (6469): 1066–1069.

[5] Cybersecurity: how the E.U. tackles cyber threats. European Council; 2021. Available from: https://www.consilium.europa.eu/en/policies/cybersecurity

[6] Morgan, S. Cybersecurity research: All in one place. Cyber Crime Magazine; 2020. Available from: https://cybersecurityventures.com/research/

[7] Abbate, P. Internet crime report 2021. Federal Bureau of Investigation; 2021. Available from: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[8] Crain, D. M. A. Computer crime statistics—2020. College of Business; 2020. Available from: https://business.fau.edu/images/business/centers/center-for-forensic-accounting/files/fbi_analysis_2020.html#fnref2

[9] Cebula, J.J., M.E. Popeck, and L.R. Young. A Taxonomy of Operational Cyber Security Risks Version 2 (Technical Report CMU/SEI-2014-TN-006). Pittsburgh: Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=91013

[10] Agrafotis, I., J.R.C. Nurse, M. Goldsmith, S. Creese, and D. Upton. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity. 2018; 4(1), tyy006, https://doi.org/10.1093/cybsec/tyy006.

[11] Leong, Y. Y., & Chen, Y. C. Cyber risk cost and management in IoT devices-linked health insurance. The Geneva Papers on Risk and Insurance—Issues and Practice. 2020; 45 (4): 737–759

[12] Alshaibi A, Al-Ani M, Al-Azzawi A, Konev A, Shelupanov A. The Comparison of Cybersecurity Datasets. Data. 2022; 7(2):22. https://doi.org/10.3390/data7020022

[13] Kamy, F., Conrad, S., & Jay, V. Cybersecurity indices and annual cybercrime loss and economic impacts. Journal of Business and Behavioral Sciences; San Diego. 2020; 32(1): 63-71.

[14] Gladstone, R. Bangladesh Bank chief resigns after cyber theft of $81 million. The New York Times. 2016. Available from: https://www.nytimes.com/2016/03/16/world/asia/bangladesh-bank-chief-resigns-after-cyber-theft-of-81-million.html

[15] Ashford, W. Financial services top cyber-attack target. Computer Weekly. 2019; Available from: https://www.computerweekly.com/news/252467639/Financial-services-top-cyber-attack-target

[16] SecurityScoreboard. Financial industry cybersecurity report. New York: SecurityScoreboard. Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? Business Horizons. 2016; 55, 349

[17] Schwartz, M. J. South Korea Bank hacks 7 key facts. Dark Reading. 2013; Available from: https://www.darkreading.com/attacks-breaches/south-korea-bank-hacks-7-key-facts

[18] Goldman, D. Major banks hit with biggest cyberattacks in history. CNN Business. Atlanta. 2012. Available from: https://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html

[19] Bouveret, Antoine, Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment (June 25, 2018). Available at SSRN: https://ssrn.com/abstract=3203026 or http://dx.doi.org/10.2139/ssrn.3203026

[20] Euromoney. Technology investments drive up banks' costs. Euromoney magazine. London. 2017. Available from: https://www.euromoney.com/article/b143rj4dz3cd92/technology-investments-drive-up-banks-costs

[21] Kark, K., Shaikh, A., & Brown, C. Technology budgets: From value preservation to value creation. Deloitte Insight. London. 2017; 1-11. Available from: https://www2.deloitte.com/us/en/insights/focus/cio-insider-business-insights/technology-investments-value-creation.html

[22] Hasham, S., Joshi, S., & Mikkelsen, D. Financial crime and fraud in the age of cybersecurity. McKinsey & Company. 2019; 1-11. Available from: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity

[23] Sedjelmaci, H., & Feham, M. Novel hybrid intrusion detection system for clustered wireless sensor network. Int. J. Netw. Secure. Its Appl. 2011; 3: 1–14.

[24] Gaurav, A., Gupta, B. B., Hsu, C. H., Yamaguchi, S., & Chui, K.T. Fog layer-based DDoS attack detection approach for internet-of-things (IoT) devices. In Proceedings of the 2021 IEEE International Conference on Consumer Electronics (ICCE). 2021; 1–5.

[25] Proper C, Engel D, Green R.C. Anomaly detection in smart grids with imbalanced data methods. IEEE Symposium Series on Computational Intelligence (SSCI). 2017; 1-8.

[26] Kolias, C., Kambourakis, G., Stavrou, A., Gritzalis, S. Intrusion Detection in 802.11 Networks: Empirical evaluation of threats and a public dataset. IEEE Commun. Surv. Tutor. 2016; 18: 184–208.

[27] Kilincer, I .F., F. Ertam, & Abdulkadir, S. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks. 2021; 188: 107840

[28] Christ, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. 2019; Cybersecurity 2 (1): 20.

[29] Kang, J.; Yu, R.; Huang, X.; Maharjan, S.; Zhang, Y.; Hossain, E. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Trans. Ind. Inform. 2017; 13, 3154–3164.

[30] Sheehan, B., F. Murphy, A.N. Kia, and R. Kiely. A quantitative bow-tie cyber risk classification and assessment framework. Journal of Risk Research. 2021; 24 (12): 1619–1638.

[31] Brooks, C. Cybersecurity in 2022 – A fresh look at some very alarming stats. Forbes. 2022; Available from:https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=33d8d10b6b61

[32] Mello, J. P. Security awareness training explosion. Cybercrime Magazine. 2017; Available from: https://cybersecurityventures.com/security-awareness-training-report

[33] Morgan, S. Humans on the internet will triple from 2015 to 2022 and hit 6 billion. Cybercrime Magazine. 2019; Available from: https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030

[34] Morgan, S. Identity & access management report. Cybercrime Magazine. 2017; Available from: https://cybersecurityventures.com/identity-and-access-management-report

[35] Zurkus, K. (2017). Wi-Fi and mobile devices predicted to account for 80 percent of I.P. traffic by 2025. Cybercrime Magazine. Available from: https://cybersecurityventures.com/mobile-security-report-2017

[36] Mello, J. P. Healthcare Security $65 Billion Market. Cybercrime Magazine. 2017; Available from: https://cybersecurityventures.com/healthcare-cybersecurity-report-2017

[37] Norton Cyber Security Insights Report: Global results. Norton by Symantec. 2017: Available from:https://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf

[38] Kruse, C.S., B. Frederick, T. Jacobson, and D. Kyle Monticone. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care. 2017; 25 (1): 1–10.

[39] Lee, S.J., P.D. Yoo, A.T. Asyhari, Y. Jhi, L. Chermak, C.Y. Yeun, and K. Taha. IMPACT: Impersonation attack detection via edge computing using deep Autoencoder and feature abstraction. IEEE Access. 2020: 8: 65520–65529.

[40] Loukas, G., D. Gan, and Tuan Vuong. A review of cyber threats and defense approaches in emergency management. Future Internet. 2013: 5: 205–236.

[41] Ulven, J.B., and G. Wangen. A systematic review of cybersecurity risks in higher education. Future Internet. 2021; 13 (2): 1–40.

[42] Cost of cyber security. (n.d.). Purples. Available from: https://purplesec.us/resources/cyber-security-statistics/#CyberCrime

[43] Consumer sentinel network data book 2021. Federal Trade Commission. 2022; Available from: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021.