Dissertation on

Types of Cyber Attack in Global Financial sectors and its threats to Financial System with Solution

[This dissertation report submitted in partial fulfillment for the degree of Master of Business Administration with a major in Finance and Banking]

Submitted By

Md. Zobaidul Islam Jabed

ID: R222212, Summer 2023

Submission Date: 20th May 2024

Department of Business Administration

Faculty of Business Studies

International Islamic University Chittagong

Dissertation on

Types of Cyber Attack in Global Financial sectors and its threats to Financial System with Solution

[This dissertation report submitted in partial fulfillment for the degree of Master of Business Administration with a major in Finance and Banking]

Submitted By

Md. Zobaidul Islam Jabed

ID: R222212, Summer 2023

Supervised By

Mohammad Emdad Hossain

Associate Professor, DBA, IIUC

Signature of Supervisor

Submission Date: 20th May 2024

Department of Business Administration

Faculty of Business Studies

International Islamic University Chittagong

Letter of Transmittal

14-05-2024

The Convener
MBA Dissertation Committee 2023
Department of Business Administration
International Islamic University Chittagong

Subject: Submission of Dissertation Report

Dear Sir,
It is great pleasure to submit the dissertation report (DISS-5500) titled **"Types of Cyber attack in global financial sectors and its threats to financial system with solution"** which has been prepared as an integrated part of the course requirement of my MBA Program. It will be highly appreciated if you kindly accept the dissertation report. Your positive action regarding this matter would be very much helpful for my professional career. If you need any further clarification or information in interpreting this study, I will be glad to answer your queries.

Thankfully,

Md. Zobaidul Islam Jabed
ID: R-222212

Acknowledgement

Al-hamdu-lillah, I whole heartedly express my gratitude to my “ALMIGHTY” for His blessings showered upon me for completion of the dissertation paper and for every moment of my life. I like to acknowledge gratitude from my deepest heart to my parents.

Many references and data have contributed to the research process that has led to the thesis. Without these support, and encouragement, it would have been very difficult to finalize my dissertation with the required rigor and enthusiasm.

First, I would like to express my deepest thanks to my supervisor **Mohammad Emdad Hossain,** Associate Professor, Department of Business Administration, IIUC for his invaluable guidance and supervision during the entire dissertation process. His continuous support has been crucial for the completion of this thesis.

My deepest gratitude goes to my parents and sisters for their interest and support, understanding and encouragement during this journey. I would also like to express my deepest gratitude to my friends and cousins for their continuous encouragement.

At last, I shall be grateful to those persons who will read this paper and who will get benefit from this paper at present and in future.

List of Used Abbreviation

WB	World Bank
IMF	International Monetary Fund
DDoS	Distributed Denial of Service Attack
SQL	Structured Query Language Attack
Web	Web Attack
DNS	Domain Name System Attack
UEBA	User and Entity Behavior Analytics
SIEM	Security Information and Event Management
AI	Artificial Intelligent
SD	Standard Deviation
SE	Standard Error

Abstract

Cybercrime is a threat that spans a wide range of online criminal activity in a broad range of settings. In the twenty-first century, financial institutions were most concerned about the rapid rise of cybercrime. The outcomes of attacks on financial institutions were compared throughout the year. When it comes to cybercrime, companies need to be aware of its impact to adopt suitable measurements.

The best method to keep financial institutions safe is to implement comprehensive internal and cyber security analyses and cyber defense training. As a result, the present study looked at the influence of cybercrime tactics on online banking use and the potential benefits of big data. Based on quantitative cross-sectional surveys, the researchers concluded that the financial system is negatively impacted by cybercrime approaches. Financial institutions (24.90%) are the most vulnerable to cybercrime, followed by social media (23.60%).

When it comes to cybercrime, webmail accounts for 19.60% of the attacks; e-commerce accounts for 8.50%; logistics accounts for5.80%; crypto currencies account for a total of 8%. The negative effect was caused by security vulnerabilities in some cybercrime tactics, which might lead to the theft of customer data. For example, consumer trust and performance were negatively affected by vishing schemes that robbed banks of their security credentials.

Keywords: Cybercrimes, Cyber Attack, Financial sectors.

Table of Contents

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

As the importance of protecting a network, device and the privacy of personal and confidential data is a national concern, cyber attacks are a significant issue to address. A cyber attack is an attempt to gain unauthorized access to a device, operating system, or computer network to cause damage. Cyber attacks are designed to disable, interrupt, kill, or take control of computer systems and modify, block, erase, exploit, or steal the data contained within them (Pratt, M. K. Pratt, 2021. [Online]. Available: https://searchsecurity.techtarget.com/definition/cyber-attack., 2021). Cyber-attacks can impact financial institutions through confidentiality, integrity, and availability issues, leading to disruptions and financial losses.

Data on cyber incidents is scarce, with underreporting in the financial sector. The cyber security issue was officially recognized worldwide in 2012 during the Global Economic Forum. That year, cyber security was named one of the five critical threats to humanity, ranking fourth on the scale of threats. Because of the constant increase of cyber-attacks worldwide every year and the financial and non-financial losses these attacks cause, the focus on creating methods and measures to identify, control, and prevent cyber risks is highly increased. Cyber-attacks constantly grow and are becoming more frequent. Hackers consistently improve their techniques, which usually happens much more rapidly than IT security evolves regarding cyber risks ((Cebula)).The growing risk of cybercrime is also recognized by increasing investments in cyber defense tools.

According to the KOVRR report (kvorr, n.d.), financial institutions have steadily increased their investments in cyber security. The investments are forecasted to reach $150 billion globally in 2022. Various factors could encourage increased attention and budget dedication to cyber security, for example, challenges in IT support growing awareness, and rising cyber-attack statistics. Research conducted by Deloitte (2020) proves a significant increase in investments in cyber security among financial institutions and that those institutions are already considering cyber security costs as part of permanent IT functions and budgets. This survey shows that in recent years institutions have been spending approximately 11% of their IT budget on cyber security tools. It is noted that this number is expected to be significantly growing in the future, considering the growth of cyber breaches. By choosing the right investment direction, financial institutions must understand the forces that affect and define the landscape of cyber threats. Understanding the significance of cyber threats and evaluating of most possible and harmful cyber attacks could guarantee the success and efficiency of potential investments that the company dedicates to cyber security.

1.2 Problem of the Statement

The problem that might be addressed in this study is that there have been security breaches inside the Financial System specially on online banking system, which is causing a decrease in total clients as a result of cybercrime. The study needs to explore the different cyber-attack techniques that might help to reduce these cyber threats to the banking system and financial sectors.

1.3 Objectives of the Study

The main objective of the study is to examine the types of cyber-attack in global financial sectors and its threats to financial system with solution. The related specific objectives are as follows:

i. To know about the types of Cybercrimes on Banking and Financial sectors;

ii. To analyze what are the impacts of Cybercrimes on banking and financial sector;

iii. To forecast the financial losses for upcoming years that will give some intuition to many financial organization like World Bank, IMF so that these organization can take necessary policy or strategy to overcome cyber hazard;

iv. To suggest a model to mitigate the cyber risk;

v. To suggest some recommendations according to findings;

1.4 Scope

The findings had a wide range of consequences for policymakers and responsible authorities in terms of taking real action against cybercrime and reducing it through the use of Time Series Analysis . The study would help to reduce the cybercrime attacks on the banking system and financial sectors. The study might help bankers to avoid cybercrime attacks on their systems. This new study would be extremely beneficial to cybercrime prevention in the online banking sector. Stakeholders and decision-makers must take immediate action in this area.

1.5 Limitation of the study

Every study has some limitation. This study has also some limitation including:

1. Limited sample size: This study will consider only few years data of cyber attack on financial sectors of the entire world.
2. Not applicable only for a particular country or economy as it consider the global financial records.
3. Availability of data is limited as many website do not publish it for safety reasons.

1.6 Organization of the Thesis

The whole thesis divided into five chapters. The first chapter gives an Introduction, Objectives, Scope and Limitations. The second chapter is review of theoretical literaure related cyber crimes or attack happened in financial sectors and the impact of these globally.The third chapter presents the Methodology, Variable description and model specification. Chapter four presents the analysis and the dicussion of the results. Recommendation, Findings and Conclusion is the last chapter that means fifth chapter of the study.

CHAPTER 2

LITERATURE REVIEW

2.1 Literature on topic

Cyber Attacks and the impacts on financial sectors specially banks are the main discussed topic in literature review. The most important operational risk in e-Banking is security. According to Sokolov (2007), A security breach that allows unauthorized access to customer information might be classified as risk management, but still the bank is also exposed to legal and reputational risk as a result customers should be educated about security threats, procedures, and the use of intelligent technologies to protect themselves and their reputations. According to Azhar, Shahi, and Chhapola (2020), the goal of E-Banking is to "provide consumers access to their bank accounts through a website and enable them to conduct specific activities on their account, subject to strict security checks." The words "PC banking," "online banking," "Internet banking," "telephone banking," and "mobile banking," according to Vrîncianu and Popa (2010), clients may reach the banks in several ways without actually visiting a bank facility.

Customers may perceive risks while making purchases online, particularly if they are paying with their hard-earned cash. Computerized financial services are often seen to be riskier than their manual counterparts. e-Banking security is deemed vital since it directly impacts the activities of its users. Consider how one of the most major obstacles to the expansion of electronic services has been customer views about online transaction security. Bakare and Commerce (2015) A survey is being conducted to find out how consumers feel about online banking today and in the future. He concluded there were universal views about online banking that was unaffected by demographic, geographical, or psychological characteristics. Internet banking security and lack of knowledge are two of the main "non-adoption" areas, according to him. e- Banking is characterized by a high degree of automation.

Aribake and Finance (2015) defined 17 service quality aspects, with security being among them. Banks are not as frequently looted in modern times since money is no longer housed only in bank vaults. A bunch of cash exists within cyberspace thanks to contemporary computer technology and data networks. Banks must adapt to contemporary trends of conducting business online ((Akinbowale, n.d.)) while also protecting themselves from cyber-crime. The first "cybercrime" was committed in the year 1820! Abacus, which is a computer, has been utilized in India, Japan, and China since at least 3500 BC.In contrast, it was Charles Babbage's analytical engine that ushered in the modern era of computers. The United States' first outward sign of electronic innovation, according to Saini, Rao, Panda, and Applications (2012) occurred in the Automatic teller machines (ATMs)were first deployed in the early 1990s by Standard Chartered Bank and the Central African Building Society (CABS) (ATMs). E-banking has grown significantly in recent years. The amount of internet transactions and mobile money transactions has grown dramatically during the last several years. E-banking fraud is a global problem that continues to cost both banks as well as customers money. There have been millions of dollars in financial transactions across network connections due to e Commerce, online banking, as well as associated technologies. However, as banks extend their online services to customers, the danger of internet computer fraud (ICF) increases, and the risk landscape alters. E-banking services are gaining in popularity throughout the globe and are likely to take over during the near future, leading to a rise in high-profile financial-motivated attacks. To reduce the risk of a significant security breach, several factors have been identified and need to be addressed. (Wang, 2020). A bank may indeed give customers and companies electronic banking services via the use of electronic techniques like a fixed and mobile phone or the Internet.

Modern e-banking services are much different from their predecessors because of the tremendous advancements in internet technology over the years. There are several types of E-Banking services accessible today, including online banking, automated teller machines (ATM), electronic payments, electronic check conversion, and money transfer, including web ATM services. These services have several security problems, and so this article will analyze relevant studies to identify elements that may be essential in preventing fraud in the e-banking sector (Popa, 2010).Financial services may be delivered more cheaply and conveniently via online banking when an account has been set up. Because of this, banks all around the globe are moving toward electronic banking. There are a few known elements that contribute to the enormous security problem that must be addressed with the rise in popularity and predicted dominance of expanding banking. This research emphasizes and synthesizes several variables that may be crucial in reducing e-banking fraud, including an increase in money supply, change management, rapid access to information, and strict internal controls. Such features may assist bank regulators and management teams in identifying areas in need of more focus and improvement (al, 2020).

2.2 Techniques of Cyber Crime

Following are some different types of cybercrime techniques that are influencing the banking
system:

Ddos Attack

Distributed Denial of Service is kind of attack when Attacker send multiple request to the suver of a particular organization to hang their server so that their server will not be able to respond to the actual customer request. By that reputation of that particular organization will be decreased. Distributed denial of service (DDoS) attacks poses a significant threat and are extremely difficult to protect against. Distributed denial of service (DDoS) defense mechanism can be divided based on activity deployed or location deployment (A. M. Christos Douligeris).Based on activity, Distributed denial of service (DDoS) defense system can be further categorized.

Phishing

Personal information, such as credit card or debit card numbers, online banking login credentials, and account numbers, may be obtained by using this kind of fraud. Email phishing is a misleading method of stealing personal data. It's very uncommon to get phishing emails pretending to be from a well-known organization and asking for personal information like your credit or debit card number, PIN code, expiry date and CVV code, mobile phone number, and other login credentials to online banking. Sites, services, and companies with someone you have no connection with may be the source of phishing attempts. In phishing emails, the user is instructed to click on a link that directs them to a website that requests personal information. An email from a legitimate company asking for this information would never be sent to you.

Password Login

Password attacks are one of the most common forms of corporate and personal data breach. A password attack is simply when a hacker trys to steal your password. In 2020, 81% of data breaches were due to compromised credentials. Because passwords can only contain so many letters and numbers, passwords are becoming less safe. Hackers know that many passwords are poorly designed, so password attacks will remain a method of attack as long as passwords are being used. (onelogin, n.d.)

Vishing

Vishing is criminal conduct that involves utilizing the telephone network to gather sensitive personal and financial information from the general public, most often via the use of Voiceover Internet Protocol (VoIP) as well as mobile phones. Portmanteau’s words "voice phishing “are used to describe a kind of scam that uses the words "phishing" and "voice". As part of Vishing, scam artists call innocent bank customers/consumers pretending to be from a bank ora merchant and inform them that they have issues with their bank accounts/online shopping but that they need to verify their account, KYC, or online order but also request the victim's payment credentials because once they commit fraud. Today, virtually all financial cyber crimes are committed using a method known as phishing, a kind of social engineering attack.

Spam Emails

Attcker sends email to the targeted computer. If user click the email then some malicious code run to the system and takes the authority of the system computer.

Cyber squatting

the practice of registering names, especially well-known company or brand names, as internet domains, in the hope of reselling them at a profit.

DNS

DNS attacks are any type of attack that involves the domain name system (DNS). There are many different ways that attackers can take advantage of weaknesses in the DNS. Most of these attacks are focused on abusing the DNS to stop internet users from being able to access certain websites.

SQL injection Attack

Structured Query Language injection (SQLi) is a form of web hacking technique in which an attacker inserts code to manipulate a SQL query to obtain unauthorized access to a database. As exchanging information over the Internet through various channels and web applications became a fairly widespread phenomenon, these applications and their related databases are vulnerable to all sorts of threats to information security since they can be accessed through the Internet. To better understand SQL injection attacks, a website that allows users to log in by entering their username and password can be used as an example. Following is the query constructed in case of an authorized login attempt where the username is 'user' and password '123'. SELECT * FROM users WHERE name = 'user' and password = '123'. However, it is also possible to type the following input into the website's username with 'user' and password field with" or '1’=’1' by a user with malicious intent *SELECT * FROM users WHERE name = 'user' and password = "or '1’=’1'.* Here, this user will always be logged into the website because 1=1 will always be valid. Hence, unauthorized access to the account details of authentic users is gained by the attacker and ownership of this data may have significant implications for the individual who is the authentic account owner. This is known as fraud and data privacy infringement. This is a straightforward example of a SQL injection attack just for understanding (Pratt, 2021).

2.3 Cyber Attack impact on financial sector

Cyber attacks in the financial sector or banking operations can have significant and wide-ranging impacts, both financially and in terms of reputation. Here are some key areas where these attacks can impact:

1. Financial Losses: Cyber attacks can lead to direct financial losses through theft of funds, fraudulent transactions, or ransom demands. These losses can occur through various means such as unauthorized access to accounts, manipulation of financial data, or exploitation of vulnerabilities in payment systems.
2. Disruption of Services: Many financial institutions rely heavily on digital systems to provide services to customers. A cyber attack can disrupt these services, leading to downtime in online banking, ATM services, or payment processing systems. This not only affects customer experience but can also result in lost revenue for the institution.
3. Reputational Damage: The trust of customers and investors is crucial in the financial sector. Cyber attacks can damage the reputation of a financial institution, leading to loss of confidence among customers and shareholders. Even if the financial losses are recovered, the reputational damage may have long-term consequences.
4. Regulatory Compliance Issues: Financial institutions are subject to strict regulations and compliance requirements to ensure the security and confidentiality of customer data. A cyber attack can result in violations of these regulations, leading to fines, legal actions, and increased regulatory scrutiny.
5. Data Breach and Identity Theft: Cyber attacks often involve the theft of sensitive customer information such as personal and financial data. This can lead to identity theft, fraud, and other forms of financial crimes. The financial institution may be held liable for failing to protect customer data, resulting in legal and financial repercussions.
6. Operational Disruption and Recovery Costs: Recovering from a cyber attack can be costly and time-consuming. Financial institutions may need to invest in cyber security measures, forensic investigations, and system upgrades to prevent future attacks. Additionally, there may be costs associated with restoring operations, compensating affected customers, and addressing legal liabilities.

7. Systemic Risk: In some cases, cyber attacks targeting key financial infrastructure or institutions can pose systemic risk to the entire financial system. Disruptions in payment systems or trading platforms can have cascading effects, leading to market instability and economic consequences beyond the affected institution.

Overall, cyber attacks in the financial sector can have profound and multifaceted impacts, highlighting the importance of robust cyber security measures and incident response strategies for financial institutions.

CHAPTER 3

METHODOLOGY AND MODEL

3.1 Introduction

The word method comes from the Greek words "Meta" and "Hodes" meaning a way. Broadly, a methodology is the underlying principles and rules of organization of philosophical system or inquiry procedure. Methodology is a process or technique in which various stages or steps of collection of data or information are explained and the analytical techniques are defined. A dictionary of social science observes, "Methodology is a systematical and logical study of the principles guiding scientific investigation". In general a method is the way of doing something. Mainly the methodologies used in making this study are consultation with the several relevant information from the company profile, different journals, annual report and internet, gone through the books on banking written by wise writers.

3.2 Sample and Data Collection

Sampling

In this study purposive sampling method has been used. Among many cyber attack few attacks information have been taken for this study. They are: DdoS, SQL or Password Login, Web, DNS, Malware, Brute Force.

Data Collection Process

In order to make the study more meaningful and presentable it will be based on secondary data. For this research Quantities data undertaken from multiple documentation, Websites, and article.

Secondary Sources of Data

The secondary sources of data have been collected from:

I. Article of Raymond Pompon
II. Annual report of FBI's Internet Crime Complain Center (IC3).

3.3 Methodology and Research Approach

First of all many types of attack have been selected and also how they are effecting in many financial sectors of the world Like: Banks, Stock exchange, credit unions, Insurance companies, Government sponsored financial institutions. I have shown in a parcentage manner like which types of attack affecting a particular sector with what parcentage. Then for cyber incidents how much losses happened in last five years have been shown and Time series Analysis done by the method of Least Square method to calculate a trend line equation for both complaints and losses. After that a forecast of next five years losses also have been calculated with the help of Trend line equation. The method of least square can be used either to fit a straight line trend. The straight-line trend method represents the equation Yc = a+bx. In this equation, Yc denotes the trend values to distinguish them from the actual Y value. "a" represents Y intercept. "b" is the slope of the line of the amount of change in Y variable that is associated with a change of one unit in x variable. "x" variable in the time series analysis represents time. Least squred method used to find trend equation. With that trend equation forecasted losses have been shown. Similarly I have calculated trend equation for complaints, with that trend equation I have forecasted complaints for next five years(2024-2028) Microsoft Excel has been used to make the analysis. After the analysis and interpretation, some findings have been found and those findings result in some conclusion. Then correlation between top two attacks will be calculated so that the similarities of these two attack can calculated it will help to understand if one particular attack is occurred on particular financial sector is it possible of being attack of another particular attack or what is the similarities between these attack. By analysing these I have recommendated a solusion how this problem can be mitigated.

3.4 Multi-Layered Model

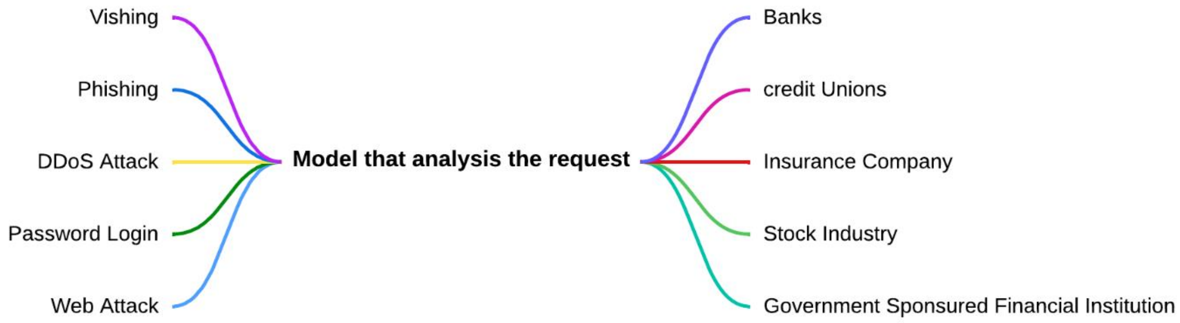


Figure 3.4: Flow chart for solution of cyber Attack in Financial sectors

In the solution part a multi layered model is suggested that can filter requested to the financial service like suppose a request in bank server it will analyses whether this is a legitimat customer request or it’s a cyber attack. If it is cyber attack it will block the requested. By that it can filter all request and maintain a safe online customer service. Above shown Model should be multi layered. Here are some several recommendation for this multi layerd model.

1. Implement Strong Security Measure implementing Multi-Factor Authentication(MFA) can add a security layer beyond just password. And also having Intrusion Detection system can be helpful.
2. Regularly Update software, website can be effective.
3. Employ advanced threat detection technologies such as Security Information and Event Management (SIEM) systems, User and Entity Behavior Analytics (UEBA), and artificial intelligence (AI)-based solutions to detect and respond to anomalies and threats in real-time.

If the above described model can serve this functionality then it can mitigate the problem of cyber threats.

CHAPTER 4

DATA ANALYSIS AND INTERPRETATION

In an article, noted that financial services organizations experienced the highest ratio of incidents attributed to password login attacks (46.2%) compared to all other sectors. They were third in the percentage of denial-of-service (DoS) incidents (36.1%). The last largest category was web-related attacks, at 6.3%. Figure 4.1 breaks down the categories of incidents at financial organizations.

4.1 Cyber incident in all financial sectors

Cyber Attack Name	Parcentage
Password Login Attack	46.2%
DdoS Attack	36.08%
Web Attack	6.33%
DNS Attack	1.90%
Malware Attack	1.27%
Unknown Attack	3.80%
Other Attacks	4.43%

Table 1: Cyber Attack incidents at all types of financial organizations(2018-2020)

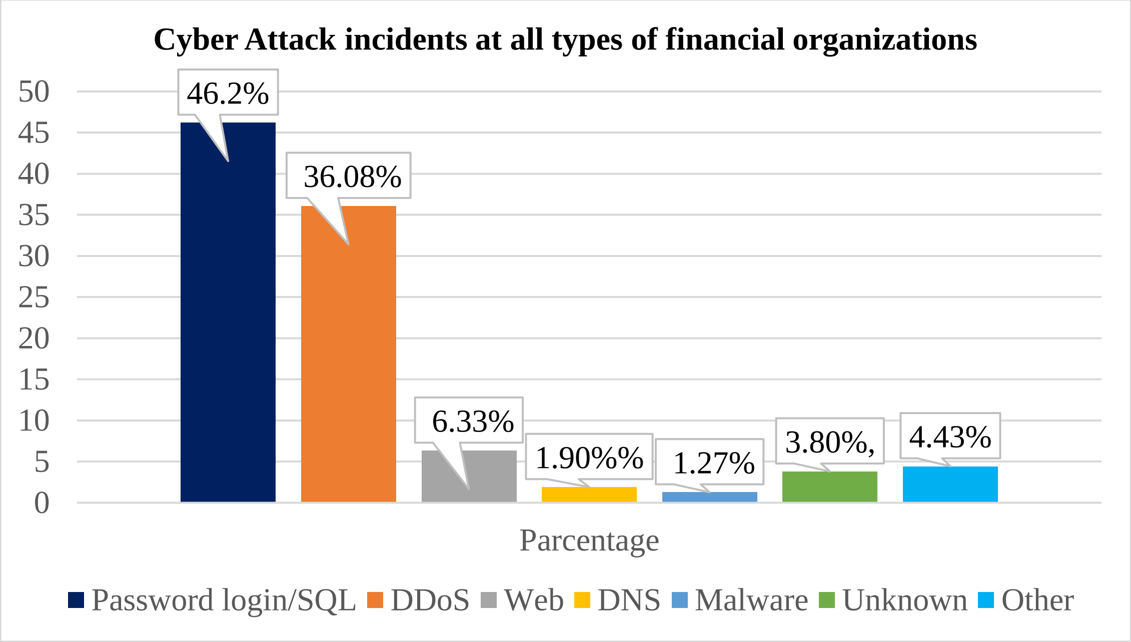


Figure 1: Types of reported incidents at financial organization 2018-2020

A wide variety of organizations fall under financial services, including banks of varying sizes, credit unions, insurance companies, government-sponsored financial institutions, stock exchanges, investment funds, payment processors, consumer finance lenders, brokerages, and companies that service the financial sector. We'll look at all of these and note the differences in the data, starting with the largest category, banks (Pompon, n.d.).

4.2 Cyber incident in Banks

Cyber Attack Name	Parcentage
Password Login Attack	41%
DdoS Attack	41%
Brute Force Attack	10%
DNS Attack	1.3%
Other Attack	6.7%

Table 2: Cyber attack incidents at Banks(2018-2020)

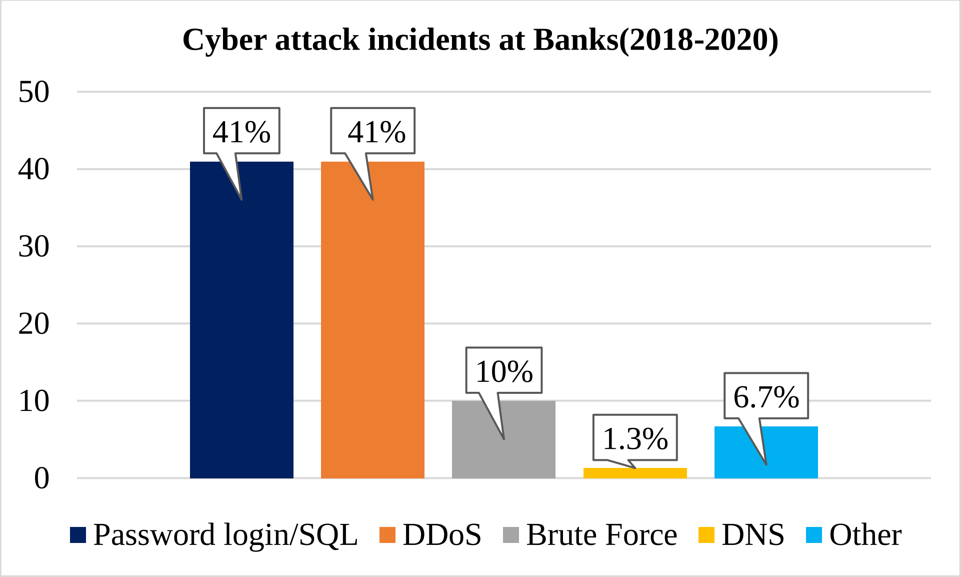


Figure 2: Cyber attack incident at Banks

Banks are the largest segment in the 2018-2020 financial services incident data, representing 40% of the records. Out of financial services organizations, banks saw more DoS attacks (41%), which is five points above the average of 36%. However, they also saw fewer password login attacks (41%), which was five points below the average of 46%. One possible reason for this is that banks have better anti bot controls in place, which mitigate password login attacks, and thus see fewer attacks than the average financial organization. Web attacks make up 6% of the reported bank security incidents, which is on par with the average. Of the password login attacks against banks, the majority of incidents were reported as brute force (77%), with the remainder (23%) reported as credential stuffing bot net attacks. The DoS attacks that could be classified were mostly web application, or layer 7, attacks (36%), followed by network volumetric attacks (24%) and DNS DoS (14%) attacks, with the rest uncategorized (Pompon, n.d.).

4.3 Cyber Attack incidents at Large Banks and Small Banks

Cyber Attack Name	Large Banks	Small Banks
Password Login Attack	36%	48%
DDoS	44%	37%
Web	6%	7%

Table 3: Attack comparison at Large and small Banks(2018-2020)

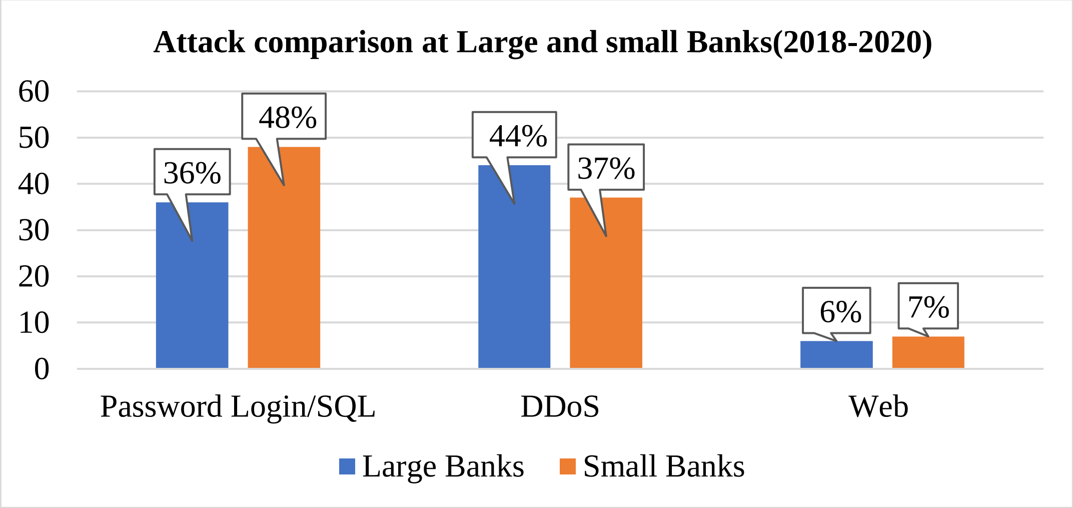


Figure 3: Cyber attack incident at Small and Large Banks

4.4 Cyber Attack Incident at Credit Unions

Cyber Attack Name	Parcentage
Password Login Attack	88%
DdoS Attack	8%
Web Attack	3%

Table 4: Incidents at Credit Unions(2018-2020)

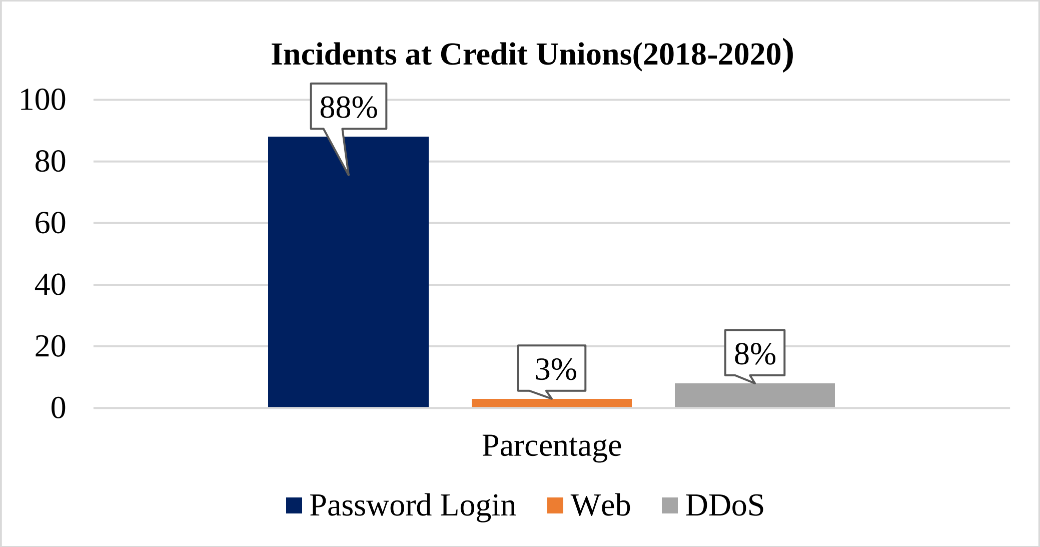


Figure 4: Cyber attack incident at Credit Unions

Some may think that credit unions are like small banks, but they are far different. For one, credit unions are owned by their customers, so they are far more focused on individual consumers than the average bank. This consumer focus shows up in the cyber-incident data as well, with 88% of incidents reported as password login attacks. This is nearly double the average and far higher than banks see. Credit unions provide a lot more customer services, which means more user-friendly logins that attackers are eager to exploit with credential stuffing and brute force attacks. Do attacks are also far below the average at credit unions, showing up as only 8% of reported incidents. It could be that credit unions are less of a target for DoS because they are perceived as having less money to pay ransom. Or perhaps they aren’t as unloved as banks or they’re simply not seen as a potential target. Credit unions also saw about half the average of web attacks, at 3%.

4.5 Cyber Attack incidents at insurance companies

Cyber Attack Name	Parcentage
Password Login Attack	27%
DdoS Attack	60%
Web Attack	7%

Table 5: Incidents at Insurance(2018-2020)

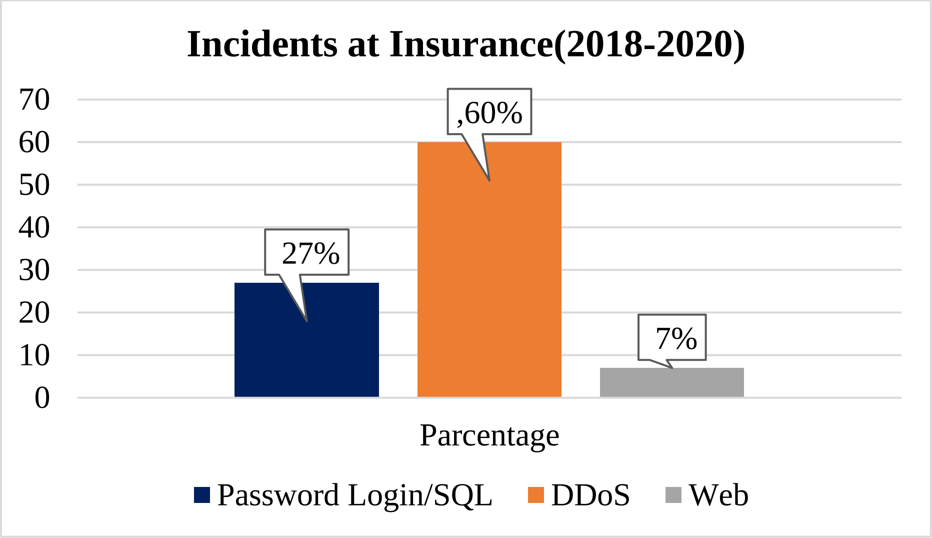


Figure 5: Cyber attack incident at Banks

Many don’t think of insurance companies as financial institutions, but they handle large amounts of money and confidential financial data. They also deal with fraud and have experienced some large cyberattacks as well as subsequent compliance investigations.[1] Insurance companies reported higher-than-average DoS attacks (60%), but their password login attacks were below average, at 27%. They reported a little bit more than average for web attacks, at 7%

4.6 Incidents for Government Sponsored Financial institution

Cyber Attack Name	Parcentage
Password Login Attack	32%
DdoS Attack	44%
Web Attack	6%

Table 6: Incidents for Government Sponsored Financial institution(2018-2020)

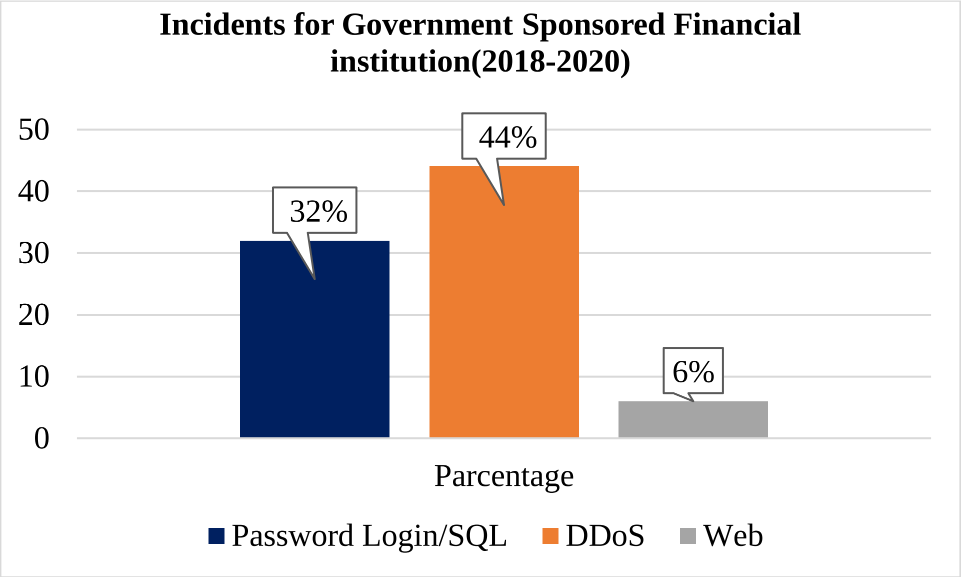


Figure 6. Cyber attack Incidents for Government Sponsored Financial institution

This category looks at large government- or public-sponsored financial organizations, usually established to promote borrowing by augmenting credit to particular industry sectors. Overall, their reported cyber incidents look pretty close to the average for password login attacks (32%). Their reports of DoS attacks are 8 points higher than average, at 44%. They saw an average number of web attacks (6%). (Pompon, n.d.)

4.7 Cyber Attack Incidents for Stock Exchanges

Over the years, stock exchanges have been the target of a few notable massive DoS attacks. Therefore, it should be no surprise that reported DoS attack incidents at stock exchanges clocked in at 80%, way above the average. Although there were no reported password login attack incidents, they did report more than three times the average in web attacks, at 20%.

Cyber Attack Name	Parcentage
DdoS Attack	80%
Web Attack	20%

Table 7: Incidents for Stock Exchanges(2018-2020)

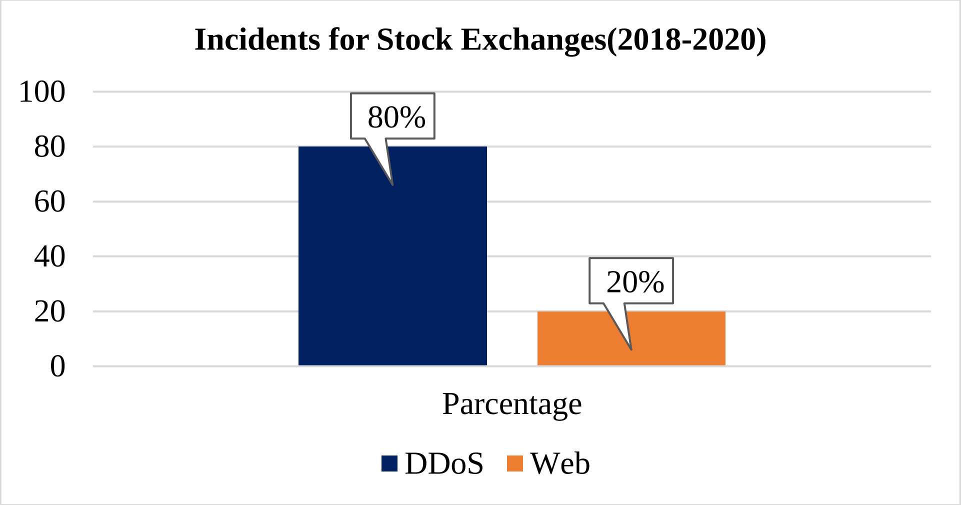


Figure 7. Cyber attack Incidents for Stock Exchanges(2018-2020)

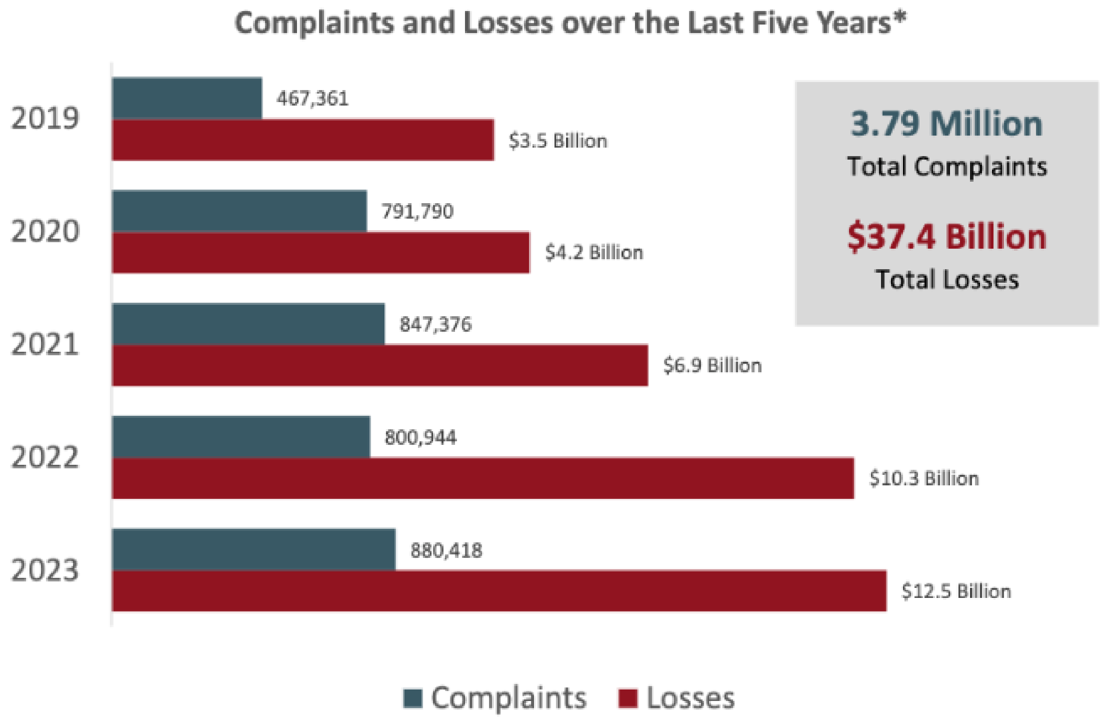
4.8 Losses over Last Five Years

Form web site a last five years financial losses against complaints is shown. From this report total 3.79 Million Complaints wear occurred from there $37.4 Billion Losses happened. And also if the graph is being seen it can be seen that the losses is gradually touching the top of the head. (IC3Report, n.d.)

Year	Complaints	Losses(Billion)
2019	467361	$3.5
2020	791790	$4.2
2021	847376	$6.9
2022	800944	$10.3
2023	880418	$12.5

Table 8.1: Complaints and Losses over last five years(2019-2023)

Source: FBI's internet crime report



Source: FBI's internet crime report

Figure 8.1: Compaints and Losses over the last Five years(2019-2023)

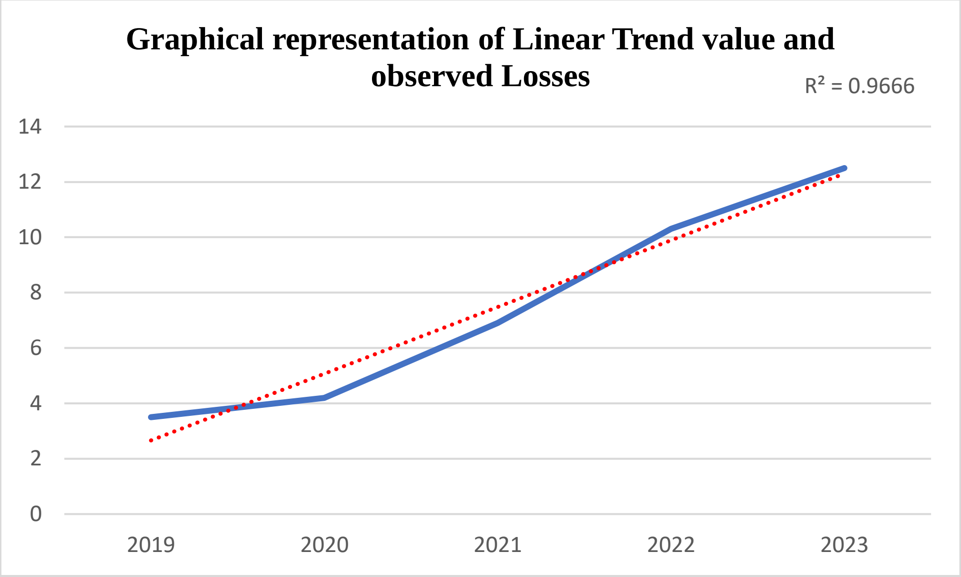


Figure 8.2: Losses over the last Five years with respect to Trend Line(2019-2023)

Doing Time series analysis by using Least Square method I found the trend equation for Last Five(2019-2023) years of losses is Y_c = 7.48+2.41x and the value of R square is 0.96. Also trend equation found for complaints is Y_c = 757577.8+83526.8x.

Trend Equation	R square	Mean	Standard Deviation	Standard Error
Y_c = 7.48+2.41x	0.96	7.48	3.87	1.73

Table 8.2: Trend equation and R square, Mean, standard Deviation for losses

Year	Losses(Billion)	Trend Equation Value(y = a+bx)
2019	$3.5	$2.66
2020	$4.2	$5.07
2021	$6.9	$7.48
2022	$10.3	$9.89
2023	$12.5	$12.3

Table 8.3: Trend equation value for losses over the last five years

Interpretation: This Trend table shows the observed losses with respect to trend equation value of Y_c = 7.48+2.41x. which R square is 0.96, mean is 7.48, standard deviation is 3.87 and Standard Error is 1.73.

4.9 Forecasting Complaints and Losses of Next Five Years

Year	Forecasted complains (Next five years)	Forecasted Losses (Next Five years)
2024	1008158	$14.71
2025	1091685	$17.12
2026	1175212	$19.53
2027	1258739	$21.94
2028	1342265	$24.35

Table 9.1: Forecasting of Losses over the Last Five years

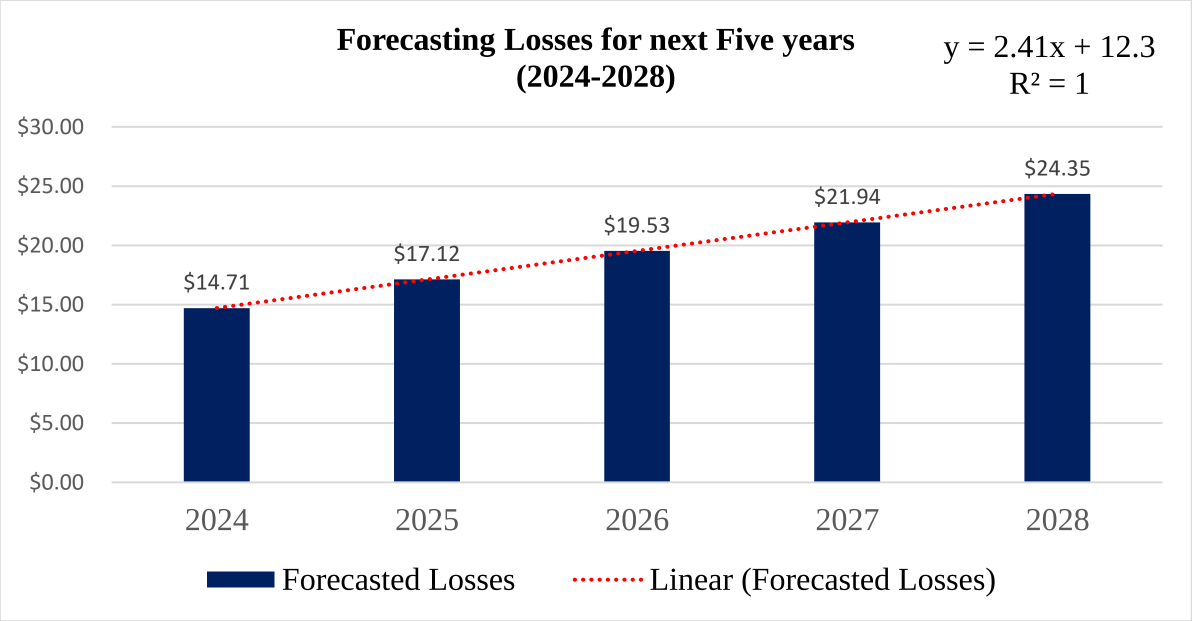


Figure 9.1: Predicted loss for next Five Years

By using the trend equation of $Y_c = 7.48+2.41x$, losses for next five years (2024-2028) has been forecasted. Also usign the trend equation of complaints $Y_c = 757577.8+83526.8x$ I calculated future complaints for next five years(2024-2028).

Trend Equation	R square	Mean	Standard Deviation	Standard Error
$Y_c = 12.3+2.41x$	1	19.53	3.81	1.70

Table 9.2: Trend equation and R square, Mean, standard Deviation for forecasted loss

Interpretation: Here goodness of fit of all predicted lossed is abjectly 1. That means it is very much linear then observed losses of table 8.1.

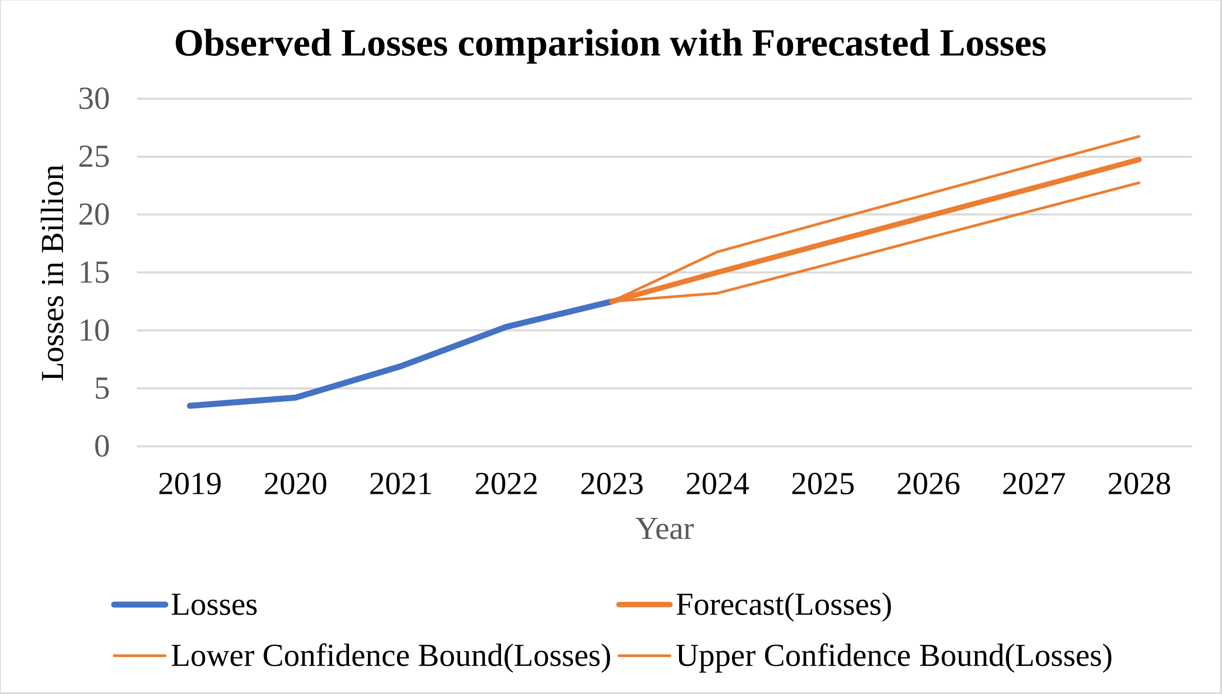


Figure 9.2: Loss comparison of predicted loss and observed losses

Interpretation: Both figures shows that prediction for next five years is very much linear with respect to observed Losses data. Where squared value of R is abjectly 'one' Which means linear line fitted very well with forecasted values.

4.10 Correlation between DdoS Attack and Password Login Attack

Correlation: Relation between Correlation is a statistical measure that expresses the extent to which two variables are linearly related (meaning they change together at a constant rate). It’s a common tool for describing simple relationships without making a statement about cause and effect. Here we have calculated correlation between DdoS Attack and Password Login Attack by Kerl Pearson method.

$$\mathrm{r}_{\mathrm{x\&y}} = \frac{\mathrm{n(xy)} - \frac{\mathrm{n(x)} * \mathrm{n(y)}}{n}}{\sqrt{\{n(x2) - \frac{\mathrm{n(x)2}}{n}\}\{n(y2) - \frac{\mathrm{n(y)2}}{n}\}}}$$

$$\mathrm{r}_{\text{DdoS \& Password Login}} = 0.20$$

As there is a possitive correlation between Ddos attack and Password Login Attack. If any financial sector has a high number of chance of being Ddos attack there is also a high chance of Password Login Attack.

CHAPTER 5

FINDINGS , RECOMMENDATION & CONCLUSION

5.1 Findings

1. In figure 4.1 it can be seen that cyber incident in all sort of financial organization Password Login is most vulnerable for every organization then Distributed Denial of Service attack holds the second position.
2. Out of financial services organizations, banks saw more DoS attacks (41%), which is five points above the average of 36%. However, they also saw fewer password login attacks (41%), which was five points below the average of 46%.
3. Credit unions, with 88% of incidents reported as password login attacks. This is nearly double the average and far higher than banks see. Credit unions provide a lot more customer services, which means more user-friendly logins that attackers are eager to exploit with credential stuffing and brute force attacks. DoS attacks are also far below the average at credit unions, showing up as only 8% of reported incidents. Also of 3% of Web attack has been seen.
4. Many don’t think of insurance companies as financial institutions, but they handle large amounts of money and confidential financial data. They also deal with fraud and have experienced some large cyber attacks as well as subsequent compliance investigations. Insurance companies reported higher-than-average DoS attacks (60%), but their password login attacks were below average, at 27%. They reported a little bit more than average for web attacks, at 7%.
5. Over the years, stock exchanges have been the target of a few notable massive DoS attacks. Therefore, it should be no surprise that reported DoS attack incidents at stock exchanges clocked in at 80%, way above the average. Although there were no reported password login attack incidents, they did report more than three times the average in web attacks, at 20%.
6. Form report of FBI’s Internet Crime Complain Center (IC3) annual report financial losses against complaints is shown. From this report total 3.79 Million Complaints wear occurred from there $37.4 Billion Losses happened. And also if the graph is being seen that the losses is gradually touching the top of the head.

If I find the trend equation for this then it will be Y_c = 7.48+2.41x where a = 7.48 and b = 2.41 and also value of $r^2$is 0.96. Mean is 7.48, Standard Deviation 3.87 and Standard Error is 1.73.

7. In Figure 4.9 I have forecasted complaints and losses for next five years(2024-2028). For which I found Trend equation of Y_c = 12.3+2.41x and the value of r^2 is 1 that means data is well fitted. For which mean is 19.53, standard deviation is 3.81, standard error is 1.70 So special focus should be given for upcoming future. Also usign the trend equation of complaints Y_c = 757577.8+83526.8x I calculated future complaints for next five years(2024-2028).
8. Correlation between DdoS and Password Login or Sql Attack is 0.20 which is positive but not strong possitive. That means the rise of Ddos Attack also increase the opportunity that there is also a chance of being Password Login Attack at that particular financial sector.

5.2 Recommendations

If we buid a model which is trained and that is capable of recognizing of different types of attacks and able of blocking these types of attacks can be a great helpful for financial sectors.

1. Implement Strong Security Measures: Require MFA for accessing sensitive systems and data to add an extra layer of security beyond just passwords. Use encryption for data at rest and in transit to protect sensitive information from unauthorized access. Deploy advanced firewalls and IDS to monitor and block suspicious activities and potential intrusions.
2. Ensure that all software, hardware, and firmware are regularly updated and patched to
3. protect against known vulnerabilities. Implement a robust patch management process. Provide ongoing cybersecurity training for employees to recognize and respond to phishing attempts, social engineering attacks, and other common threats. Create a culture of security awareness within the organization.

4. Perform regular security audits and penetration testing to identify and address vulnerabilities in the network and systems. This helps to proactively detect and fix security weaknesses.
5. Join industry groups such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) to share threat intelligence and best practices with other financial institutions. Collaboration enhances collective cybersecurity defense capabilities.
6. In 4.10 pera I calculated correlation between Password Login Attack and DdoS attack which is 0.20 so that policy maker can have an intuition that if any particular financial sector has a threat of Password Login Attack then there is also a high chance of being attacked by DdoS attack.

5.3 Conclusion

In conclusion, enhancing financial security in the face of evolving cyber threats requires a proactive, multi-faceted approach. Financial institutions must implement robust security measures, regularly update and patch systems, and conduct frequent security audits and penetration testing. Employee training and awareness are crucial in recognizing and mitigating phishing and social engineering attacks.

Strong access controls, well-developed incident response plans, and advanced threat detection technologies are essential for rapid threat identification and response. Collaboration with industry peers and compliance with regulatory requirements further strengthen the overall security framework. Adopting a Zero Trust architecture and securing third-party networks help ensure comprehensive protection, while cyber insurance can provide financial mitigation in case of an incident.

By integrating these strategies, financial institutions can build a resilient cybersecurity posture that not only safeguards sensitive data and systems but also maintains customer trust and confidence in the financial sector's integrity and reliability.

References

A. M. Christos Douligeris. (n.d.). DDOS ATTACKS AND DEFENSE MECHANISMS: A CLASSIFICATION.

Akinbowale, K. &. (n.d.). Retrieved from https://www.emerald.com/insight/content/doi/10.1108/JFC-03-2020-0037/full/html

al, A. e. (2020). An innovative approach in combating economic crime using forensic accounting techniques.

Cebula. (n.d.). A Taxonomy of Operational Cyber. Retrieved from https://insights.sei.cmu.edu/documents/2273/2014_004_001_91026.pdf

Kovacs, E. (n.d.). Retrieved from https://www.securityweek.com/fbi-cybercrime-losses-exceeded-12-5-billion-in-2023/#:~:text=Cybercrime%20victims%20in%20the%20United%20States%20filed%20more,3.8%20million%20complaints%20over%20losses%20totaling%20%2437.4%20billion.

kvorr. (n.d.). *kvorr*. Retrieved from https://www.kovrr.com/blog-post/what-is-cyber-risk-quantification-crq

onelogin. (n.d.). Retrieved from https://www.onelogin.com/learn/6-types-password-attacks

Pompon, R. (n.d.). *f5*. Retrieved from https://www.f5.com/labs/articles/threat-intelligence/cyberattacks-at-banks-and-financial-services-organizations

Popa, V. &. (2010). Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests.

Pratt, M. K. (2021). Retrieved from https://searchsecurity.techtarget.com/definition/cyber-attack

Pratt, M. K. (2021). *M. K. Pratt, 2021. [Online]. Available: https://searchsecurity.techtarget.com/definition/cyber-attack*. Retrieved from https://searchsecurity.techtarget.com/definition/cyber-attack.

Wang, N. J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability.