JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cybersecurity in the Banking Sector: Balancing Security and Privacy in the Digital World

Alexander Aruldoss, Sophia Rahaman
Student, Associate Professor
School of Engineering & IT, School of Engineering & IT

Manipal Academy of Higher Education, Dubai Campus, Dubai, U.A.E

Abstract : The development of digital technologies has brought numerous benefits, but it has also led to cyber-crimes, posing significant threats to people, organizations, and governments. As the digital landscape evolves, the challenge in balancing security and privacy becomes increasingly complex. In the swiftly changing digital economy, the banking industry confronts unparalleled cybersecurity challenges as it seeks to protect financial assets, customer information, and essential infrastructure. As cyber threats become more intricate and frequent, banks are making substantial investments in advanced security features such as multi-factor authentication, encryption, behavioral biometrics, and AI-based threat detection. Nevertheless, these advancements frequently lead to concerns regarding user privacy, compliance with regulations, and the ethical management of personal data. This paper explores the careful balance between providing strong cybersecurity and sustaining customer privacy within contemporary banking systems. It looks into the various types of cyberattacks typically aimed at banks—such as phishing, ransomware, and insider threats—and assesses the effectiveness of existing defense strategies. The paper also addresses the influence of international regulations like GDPR, PCI-DSS, and local data protection laws, on cybersecurity practices. Through case studies, industry evaluations, and expert interviews, this study presents insights into how financial organizations can improve cyber resilience while preserving public trust and transparency. The findings intend to provide a framework for securing both safety and privacy, emphasizing best practices that marry technological progress with ethical accountability in the banking sector.

IndexTerms - **Cyberattacks, Phishing, Ransomware, Cybersecurity, Security.**

I. INTRODUCTION

We currently exist in an era where digital technology impacts nearly every aspect of our lives. Whether we're using a smartphone to communicate with friends, submitting our assignments on the internet, browsing social media, or watching our favorite shows, we are continually connected online. This strong connection necessitates the need to safeguard ourselves and our personal information. This is where cybersecurity comes into play—serving as the barrier that helps secure our digital environment. Essentially, cybersecurity focuses on defending our devices, data, and online activities from threats such as hackers, malware, and scams. It represents a field that merges technology, awareness, and intelligent practices to protect against cybercriminals who are perpetually devising new methods to infiltrate systems and obtain information.

For students like us, cybersecurity may seem like a domain reserved for specialists, but it actually has implications for everyone. From ensuring the security of our school accounts to safeguarding personal information on social media, cybersecurity is vital in our day-to-day online interactions. Cyber threats are evolving and becoming increasingly sophisticated. An innocuously appearing email could be a phishing attempt designed to deceive you into revealing your password. A free app might covertly install spyware on your device. Public Wi-Fi networks can expose your personal information to individuals with malicious intent. Without caution, we can lose access to our accounts, have our data compromised, or even fall victim to identity theft. These aren't merely news stories—they represent real dangers that anyone can encounter, and it's not just individuals in jeopardy. Educational institutions, hospitals, banks, and even governments require robust cybersecurity measures to protect sensitive information and ensure smooth operations.

Consider the consequences if someone were to breach your school's system and erase all student data or disrupt online classes. This highlights why institutions are investing more in cybersecurity solutions—and educating students like us on how to be more vigilant and prepared. Surprisingly, cybersecurity encompasses more than just advanced technology; it's also about human actions. In actuality, many cyberattacks succeed because an individual clicked an incorrect link or employed a weak password.

Therefore, cultivating sound cyber practices is essential. Simple actions such as updating software, crafting complex passwords, avoiding oversharing online, and identifying suspicious communications can significantly enhance your protection. These minor measures can lead to substantial improvements. The domain of cybersecurity is also thrilling and filled with possibilities. As cyber threats continue to escalate, the need for individuals who can thwart them is also increasing. Careers in ethical hacking, network security, cybersecurity legislation, and digital forensics are gaining traction—and they offer attractive salaries as well. If you enjoy solving enigmas, engaging in critical thinking, and applying technology intelligently, cybersecurity could be an ideal path for your future. Ultimately, cybersecurity transcends mere technical understanding—it represents a crucial competency for life in our digital era. It ensures our safety online, fosters trust in the technologies we rely on daily, and paves the way for various career opportunities. For students, gaining knowledge about cybersecurity is not merely advisable—it equips you to utilize the internet confidently and take command of your digital existence in an ever-connected world. We will now explore how cybersecurity is applied in the banking and financial sectors, along with the types of attacks that occur.

In today's fast-paced and constantly changing digital environment, the finance industry finds itself at the intersection of trust and technology. Financial services—from mobile banking apps and digital wallets to investment platforms and insurance websites—are intricately woven into our everyday lives. Nevertheless, this convenience carries a significant obligation: ensuring the protection of sensitive financial data against cyber threats. This is why, in our digital age, cybersecurity has become a vital priority for the finance sector.

In finance, cybersecurity involves much more than just installing antivirus software or using robust passwords. It requires building and maintaining a secure environment that allows customers to make transactions, apply for loans, invest, and pay bills with assurance. Financial institutions, whether long-standing banks or innovative fintech firms, handle immense volumes of personal data and conduct high-value transactions around the clock. This situation makes them attractive targets for hackers, cybercriminals, and even state-sponsored threats.

The risks faced by these organizations are not only common but are also growing in complexity. Cyber attackers employ various tactics, including phishing schemes, ransomware, fake websites, insider threats, and specialized malware to breach systems. The goals of these attacks can vary—some aim to steal funds directly, while others focus on acquiring sensitive information, committing fraud, or causing disruptions for political or competitive reasons.

When a financial institution suffers a cyberattack, the consequences extend beyond simple monetary loss. Possible outcomes include stolen identities, accounts being frozen, damaged reputations, weakened customer confidence, and hefty penalties from regulatory authorities. In cases involving major financial entities like banks or stock exchanges, cyber incidents can undermine public trust and trigger broader economic effects.

To bolster their defenses, financial organizations are significantly enhancing their security measures. They are adopting encryption to protect data, implementing multi-factor authentication for secure logins, utilizing fraud detection systems to spot suspicious activity, and employing real-time monitoring to identify breaches as they happen. However, technological solutions alone are insufficient—compliance with regulations like GDPR and standards such as PCI-DSS is essential. These frameworks advocate for responsible and secure management of customer data, adding an extra layer of protection.

The challenge grows as the methods for accessing financial services rapidly change. Innovations like mobile banking, digital wallets, contactless payments, and blockchain solutions create fresh opportunities for interacting with finances, while also opening new routes for hackers to target. As the potential for attacks expands, financial organizations must stay alert, utilizing tools like artificial intelligence, ethical hacking, and threat intelligence to predict and counteract emerging cyber threats.

Ultimately, cybersecurity in finance goes beyond mere technical issues; it represents a crucial component of business and a key pillar of building trust. In a time when data breaches capture headlines and digital services are commonplace, safeguarding customers and their assets is essential. As the finance sector evolves and interconnects further, strong cybersecurity will remain a foundational element supporting the industry's future.

II. LITERATURE REVIEW

Cybercrime presents a major obstacle for society, yet it can be especially damaging to those who fall victim to it. This chapter offers an in-depth and relevant exploration of the cybercrimes aimed at individuals. It also delves into the motivations behind the criminals who carry out these attacks, as well as the crucial human factors and psychological elements that contribute to the effectiveness of cybercriminals.[1].This article will examine the many cyberattack types that frequently target banks, such as ransomware, phishing, and insider threats, and assess how well the defences in place are working. The influence of regional data protection legislation and global standards like GDPR and PCI-DSS on cybersecurity procedures will also be discussed. The introduction of contemporary banking technology, which enables numerous financial services and transactions to be carried out via electronic devices without the need to physically visit a bank, has contributed to the rise in cybercrime. The enormous opportunities brought about by developments in computer technology and information and communication networks have given rise to a new type of illegal conduct known as cybercrime. It is described as any unlawful behaviour done through a network or computer[2]. According to S&P Global, there are an expected 44,000 banks in the world (S&P Global, 2024). According to a 2021 projection from the World Bank's Global Findex database, 3.8 billion adults had bank account access. ICT experts and cybersecurity teams are concerned about cyberattacks that target digital technology and communication infrastructures. To

improve security measures, there is an increasing need for more security staff. Financial information, which is managed electronically in the digital age, includes a wide range of data pertaining to both personal and commercial accounts. Given the growing sophistication of cyberthreats and the dependence on digital platforms for financial transactions, safeguarding financial data is essential in the digital era.Any cybersecurity framework breach causes the impacted firm and its clients to suffer both monetary and non-monetary damages; therefore, cybersecurity efforts are made to reduce these risks[3].
These categories illustrate the wide variety of threats that banks encounter in the constantly changing cybersecurity environment, underscoring the necessity of strong security measures to safeguard sensitive information and uphold trust.
Banking is a crucial institution in any nation, and ensuring the safety of bank customers is essential for a country's proper functioning. Banks face numerous risks. The advent of computers significantly impacted the banking sector; however, it also led to new methods by which individuals could fall victim to various attacks. The dramatic rise in cybercrime is the primary challenge for financial institutions in the 21st century. In the early 1970s, criminals committed offenses through telephone lines, known as Phreakers, who discovered the sound patterns that operated the American telephone system. They replicated these tones to make free calls. Up until the 1980s, true cybercrime had not yet emerged. One entity hacked into another's computer to find, copy, or exploit personal data and information. The first individual convicted of cybercrime was Ian Murphy, also recognized as Captain Zap, in 1981. He compromised the American telephone corporation to manipulate the inner clock so that customers could make free calls during peak hours. Over time, hackers have continued to evolve in distinct ways. While the early targets were telecommunications providers, banks, online retailers, and private individuals soon followed.

These days, online banking is increasingly common and offers a lot of opportunities. For instance, hackers can obtain bank account and credit card passwords, as well as login credentials and addresses. As a result, they have the ability to either drain accounts or use someone else's account to make transactions online (Soni 2019). One of the most important and widespread types of crime in the world today is cybercrime. Because the internet is available to everyone, there are risks involved. It is dangerous to commit a crime using a network or device that is connected to the internet, and it is frequently difficult to find the offender. Cybercrime can take many different forms, such as identity theft, extortion, investment fraud, and phishing.
Due to corona,when lockdown started, online retail fraud has cost £16 million, and coronavirus-related schemes have cost over £5 million. Online sales of personal protective equipment (PPE), such face masks, that are never delivered account for the majority of coronavirus-related fraud. Phishing emails and SMS have even been sent by crooks posing as the army, HMRC, and health organisations in an attempt to trick people into opening links or attachments that reveal personal or financial information[4].

Cyberattacks on banking and finance in U.S.A

Cyber attacks are becoming a growing concern, particularly for financial institutions, which might face up to 300 times more cyber incidents annually compared to other businesses (Boston Consulting Group, 2019). Cyber attacks consistently rank among the top risks in nearly every financial stability assessment. Scholarly economists have recently begun to stress how critical it is to investigate and assess cyberattacks as a risk to financial stability. Nevertheless, there is still no universally accepted classification or definition of cyber incidents, not to mention thorough data gathering about the prevalence and nature of cyberattacks. The purpose of this study is to assess the potential for a cyberattack to be amplified throughout the U.S. financial system and to comprehend the threat that cyberattacks bring to it.[5]. Effective responses to cybersecurity incidents usually require cooperation between financial institutions, regulators, and other stakeholders. In the U.S., the Financial Services Sector Coordinating Council brings together financial organisations, regulatory bodies, and government entities to coordinate cybersecurity initiatives and share information about emerging threats, which helps to improve the sector's resilience and capabilities in responding to cybersecurity challenges. In the United States, financial organisations must follow the FFIEC's Cybersecurity Assessment Tool, which provides guidance on incident response readiness, and notify regulators and affected parties of cybersecurity incidents in compliance with applicable laws and regulations.
Similarly, in order to promote cooperation on cybersecurity issues, the European Banking Authority (EBA) works closely with national authorities and financial institutions inside the EU. To guarantee a coordinated response to cybersecurity breaches, the EBA has set rules for reporting occurrences and encouraging collaboration between national authorities and financial institutions.[6].
The banking and financial environment in the U.S. is shaped by elements such as competition, management of risk, the transmission of monetary policy, and the function of financial mediators. According to Diamond and Dybvig (1983), examining strategies for preventing bank runs and preserving market liquidity emphasises the vital roles that deposit insurance and liquidity play. Their analysis highlights how crucial regulatory efforts are to preserving the stability of the American banking system. Rajan assesses the impact of financial development on risk-taking and risk dissemination. The expansion of the financial industry has improved access to capital but also increased risk exposure.
However, this growth has brought to light new challenges, particularly the susceptibility to disturbances caused by the financial sector. This knowledge is essential for ensuring stability in the U.S. banking system[7].

Impact of Cyberattacks on Banking and finance

A. Financial losses

Cybercrime in the financial sector entails gaining illicit financial rewards through profit-focused criminal endeavors. This includes activities such as identity theft, ransomware attacks, internet and email scams, and attempts to access financial accounts, credit cards, or other payment information. It is essential for every individual to be aware that their personal data has likely been compromised, shrouded in secrecy, and utilized to facilitate and support nefarious activities. The scale of the deep web is greater than that of the surface web and continues to grow at an unprecedented pace[10]. Furthermore, operational loss information is typically not presented as a separate item in financial institutions' audited financial statements or other disclosures. This suggests that financial organisations are free to choose how they want to calculate operating losses. As a result, loss data is not a valid indicator of operational risk from an accounting perspective. Other risk categories might be impacted by similar reporting biases,

although in the case of cyber risk, there are situations where loss information is thorough because of mandated reporting requirements, such as those pertaining to data breaches in the US and the EU. Therefore, we do not claim that our estimating approach provides answers to the more general problems of operational risk management.
Rather, our analysis focusses on the characteristics that affect the severity of cyber losses and how those factors might be used to predict possible loss amounts.[17].
The banking sector often faces security threats, with DDoS attacks being some of the most prevalent, leading to considerable financial repercussions. Figure 3 illustrates the e-banking network of the sampled bank, highlighting the communication flow between various nodes during a transaction. The cardholder sends the first request message to the ATM, PoS, or Internet/Mobile gateway, which local acquirer switches then route to the CSS. Requests are logged in queues by the CSS before being sent to the CBS for recording and processing. Customers may experience discomfort and reception issues as a result of transactions not being registered in their accounts due to errors caused by failures in the CBS or CSS.
Financial institutions may incur substantial losses as a result of cyber threats. Hackers can exploit vulnerabilities to gain unauthorized access to sensitive financial information, leading to fraud, theft, or extortion. Such incidents can result in direct financial losses as well as legal liabilities, impacting the organization's financial performance[12].
If the CBS fails to address the requests, the CSS is required to log them and maintain them in its queue, potentially leading to an overflow of requests and causing the network to send error messages to the cardholder.

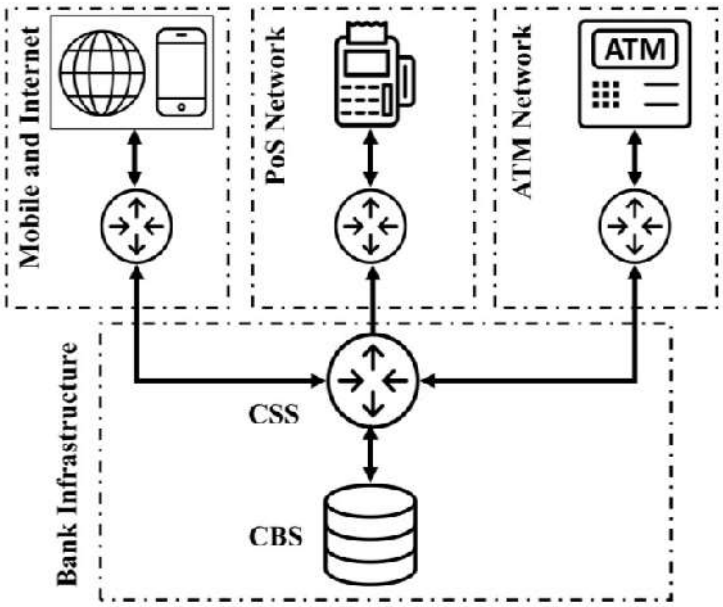


Fig 1

By altering the traffic's IP address to make it appear as though it is originating from a trustworthy source, spoofing techniques can be used to launch a Distributed Denial of Service (DDoS) assault on a banking network. The bank's security systems may find it difficult to identify and stop the fraudulent traffic as a result. DDoS attacks can be extremely harmful to the banking industry since they can prevent clients from using online banking services, accessing their accounts, or completing transactions. As a result, there may be significant monetary losses, reputational damage, and a decline in consumer trust. Banks should work with third-party security companies and put robust security measures like firewalls, intrusion detection systems, and content filtering into place to thwart these attacks.
In order to lessen the effects of the attack and facilitate the recovery process, banks must also create a thorough incident response strategy.[9].

B. **Reputation Damage**

A company's success and long-term viability in the market are greatly influenced by its reputation. It can be difficult to quantify intangible assets like reputation, which account for a significant portion of market value. Additionally, businesses with a solid reputation are seen as providing more value because the market believes they will continue to generate steady profits and expand in the future. Considering the important influence of the financial sector on the economy, the reputation of financial institutions is a primary concern for regulators, industry bodies, consultants, and the companies themselves, all of which need to develop thorough guidelines to assess and manage the risks linked with reputational damage.Regulators and the banking sector now fully understand the significance of operational risk in financial institutions' risk profiles as a result of significant operational events[11].
Cyber attacks on computer networks, often referred to as "cyber attacks," can severely damage the trust that customers place in their financial institutions. Customers lose faith in an organization's ability to protect their data when they learn that their financial or personal information has been compromised or stolen.
This erosion of trust leads clients to terminate their accounts or seek services elsewhere, adversely affecting the institution's financial situation[12].

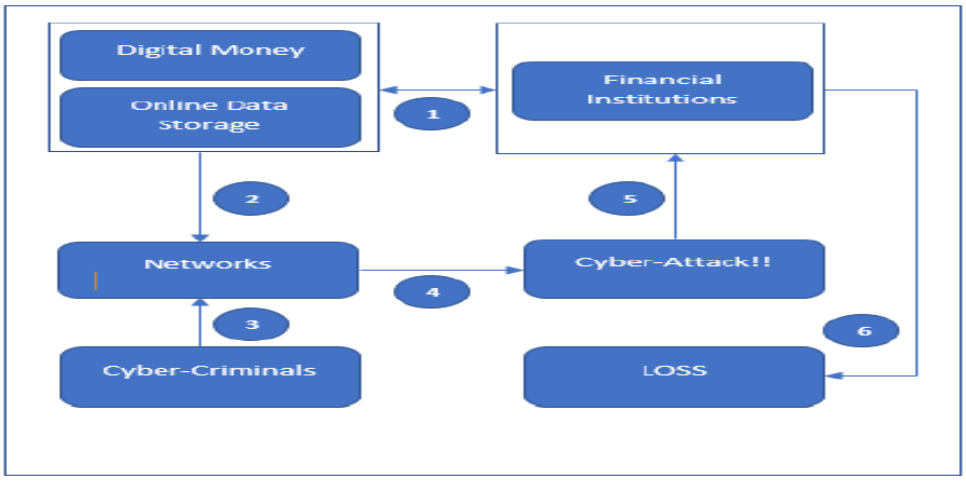


Fig2 :Demonstrating The consequences of cyberattacks on Financial Institutions.

The dependence on cyberspace in modern societies and businesses has increased dramatically [18]. There are disadvantages to the negligent use of computer and networking technologies, despite the fact that technology has provided many advantages for businesses to improve and streamline their operations.

[19]. One major disadvantage is that the organisation may suffer large material and immaterial financial losses as a result of inadequate security and inefficient business procedures. Although it is frequently possible to calculate the direct cash losses resulting from cyberattacks, it is more challenging to quantify the intangible damages associated with organisational sentiment, goodwill, and reputation. The socioeconomic competitiveness of an organisation can be significantly impacted by shadow pricing, which places a monetary value on currently unknown expenses in the absence of precise market prices. Payment diversion fraud, ransomware, data breaches, advanced persistent threats, cyber theft, security lapses, cyber espionage, and even cyberterrorism are among the many cyberthreats that organisations must contend with.[20,21]. Protecting user privacy and data is crucial to preserving customer trust, since people place a high value on the security of their personally identifiable information and other sensitive data[22].Since tangible and financial accomplishments are the primary indicators of success for firms, reputation management becomes essential to sustaining that success. An organization's reputation is an important intangible asset that affects all parties involved. Reputation can be influenced by a number of things, such as investor and customer confidence in the company and their perception of it as a reliable and trustworthy institution.[23].

Cyberattacks are increasing at an alarming rate, and their annual financial effect keeps rising. Additionally, the global pandemic has changed how organisations function, resulting in modifications to their risk and attack profiles [24]. As technology progresses, the severity of attacks likewise grows, causing substantial harm to corporate reputation and branding. The repercussions of these cyberthreats are unfortunately not well understood or anticipated by many public and private organisations. For instance, KPMG found that a cyber breach can significantly impact a company's reputation after surveying 1,000 organisations in the UK.[25]. More than 58% of the companies included in the survey failed to accurately assess the actual consequences a breach can have on their organization. Furthermore, 599 companies that had encountered a breach indicated that such incidents had an effect on their reputation.

C. Loss of customer trust

The research revealed a direct link between the perceived risks of cybersecurity and the level of trust customers have in digital banking. Consumer Surveys: Surveys conducted among users of digital banking showed that more than 60% of participants reported worries about the safety of their personal information. Numerous respondents indicated that these fears affected their choice to utilize digital banking services, with some choosing to stick with traditional banking methods instead. Trust Deficit: Discussions with industry professionals underscored a notable lack of trust among consumers, worsened by prominent cyber incidents highlighted in the media. Consequently, banks encounter difficulties in persuading customers to fully participate in digital banking platforms. Here is the graph depicting the effect of cybersecurity concerns on customer trust in digital banking in Uzbekistan for the year 2023[8].

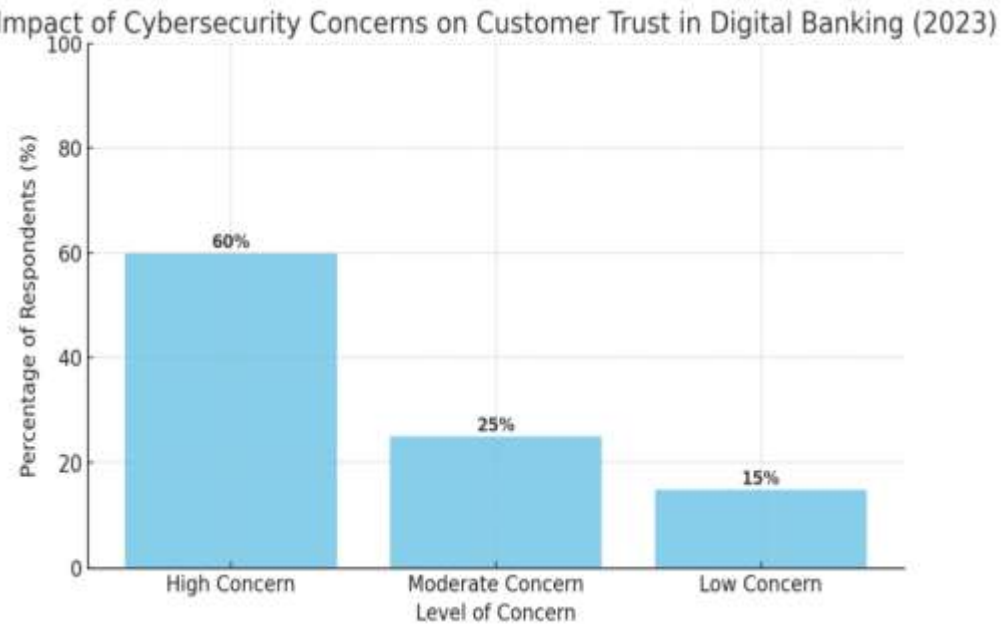


Fig3. Impact Of Cybersecurity Concerns On Customer Trust In Digital Banking (2023)

The bar chart illustrates the proportion of participants indicating high, moderate, and low levels of concern about cybersecurity, emphasizing the substantial effect these concerns have on customer trust[8].

The digital banking industry encounters numerous security issues and obstacles. As the banking system experiences various stages of digital evolution, driven by increasing competition among state-owned, private, and foreign entities, the need to ensure security becomes critical. The need to safeguard sensitive financial data and transactions must be balanced against the goal of making banking more affordable, effective, and accessible to all individuals[26].

D. Operational Disruption

These attacks target operational technology (OT), that includes the software and hardware in charge of keeping an eye on or managing machinery, assets, and procedures in industrial environments. The inter connectedness of OT with information technology (IT) introduces numerous additional risks related to operations and supply chains that necessitate thorough assessment and proper management to mitigate. The impacts of assaults on OT can lead to a loss of control over processes, malfunctioning equipment, interruptions in processes, shutdowns of facilities, and even safety incidents like explosions. These adjustments demand extra labor hours to carry out and often require the adoption of less optimal production methods, both of which result in increased costs. Table 1 provides a summary of cyberattacks on Colonial Pipeline, JBS, and Merck, highlighting the disruptions to their operations.

Company	Attack vector	Operational disruption
Colonial Pipeline	Broke into an outdated VPN system that did not have multifactor authentication by obtaining user credentials.	Cease the operation of a pipeline that delivers 45% of the fuel used on the East Coast, impacting 50 million consumers. After a week , more than 10,000 fuel stations remained without fuel and couldn't function.
JBS	Credentials of several JBS Australia employees have surfaced on the dark web before any data was stolen. TeamViewer was set up within the JBS network to maintain a continuous connection; 45 GB of data was transferred to Meg and 5 TB of data to holdings in Hong Kong.	JBS USA has been compelled to close all nine of its beef processing plants, which process over 22,000 cattle daily. The union that represents 25,000 meatpacking workers at JBS in the U.S. announced that all meatpacking facilities across the country faced some interruptions in their operations.
Merck	An upstream accounting software provider was targeted in a software supply chain attack, leading to the release of updates that infected Merck's servers with NotPetya. As a result, NotPetya propagated throughout 40,000 systems within Merck.	Experienced interruptions in the manufacturing of active pharmaceutical ingredients, formulation and packaging processes, as well as research and development activities.

Table 1. Cyberattacks on Operational Technology

One promising approach to reduce risks, which has received significant attention from the U.S. government over the last ten years and is increasingly being adopted within the industry, is the exchange of cyber threat information. Real-time communication of risks, occurrences, and vulnerabilities is thought to improve decision-making through teamwork. In fact, the National Cybersecurity and Communications Integration Centre is tasked with "engaging in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents" as part of Executive Order 13691, which encourages the establishment of information sharing and analysis organisations, such as information sharing and

analysis centres (ISACs). Guidelines are provided by the National Institute of Standards and Technology (NIST) to encourage voluntary information exchange in the fight against cyberthreats. Through safe and efficient information-sharing procedures, these guidelines aim to "enhance cybersecurity operations and risk management efforts, and assist organisations in planning, implementing, and sustaining information sharing."
To improve their current threat information capabilities, NIST advises organisations to think about joining public or private information-sharing associations. The Cyber Safety Review Board was created by Executive Order 14028 in the wake of the disruptive events at Colonial Pipeline and SolarWinds. Its purpose is to facilitate the sharing of information about critical incidents across industries and offer specific recommendations for organisations to prevent similar threats. Because they think that the public and commercial sectors will benefit from these exchanges, policymakers have pushed for the establishment of legal and procedural frameworks for exchanging information about cyber threats. But despite the government's earlier efforts to promote voluntary information sharing, many firms are still apprehensive because they fear taking advantage of other people's contributions.By issuing an Executive Order for Improving the Nation's Cybersecurity, the Biden administration has stepped up its efforts to promote information sharing[27].

E. Regulatory and Legal Consequences

In recent years, there have been significant transformations in the regulatory landscape of cybersecurity. The financial industry is at the forefront of these new cybersecurity measures that have emerged from a convergence of various factors. Firstly, the nature of cyber threats necessitates a different mindset (an ‘assume breach’ approach), based on the realistic expectation that preventing all attacks is impossible; therefore, greater focus should be placed on identifying and addressing threats rather than solely constructing impenetrable defenses. This mindset is influenced by several aspects, including the persistent, dynamic, intelligent, and adaptive nature of cyber threats, their ease of crossing national boundaries, and the inadequacy of certain preventive measures (like data mirroring on servers in different locations) in countering them. Given their inherently stealthy characteristics and potential for rapid escalation, cyber-attacks pose a genuine risk. Secondly, the financial sector is experiencing an unprecedented surge in data digitization. Few ways are:

i. Safe online channels for central banks to communicate
ii. creative ways to pay within payment systems (e.g., using wearable technology, phone numbers, or bar codes)
iii. activities (such as those utilising distributed ledger technology) that do not require paper documentation
iv. the adoption - smart contracts
v. the growing reliance on biometric data for client identification in financial institutions (from India’s ambitious Aadhaar project to Russia’s new biometric platform for bank identification)
vi. updated reporting formats for banks.

This trend is expected to persist with the rise of big data; as CFTC Chairman Christopher Giancarlo aptly stated during the announcement of the new office of data and analytics in November 2018, if data reigns supreme, then automating processes that previously required human input is essential work for the ‘King's Court.’ Thirdly, the financial ecosystem's increasing complexity and interconnectedness – resulting from an interdependent operational network encompassing a variety of stakeholders (such as banks and financial markets) – elevates the threat level. These traits arise from the nature of potential cyber threats, where attackers are often motivated and sophisticated. According to the BIS Committee on Payments and Market Infrastructures and the International Organisation of Securities Commissions, their report on ‘Guidance on Cyber Resilience for Financial Market Infrastructures’ highlights that these vulnerabilities heighten contagion risks and create fresh opportunities for intrusions, emphasizing the need for enhanced cybersecurity across the entire financial sector, not just among the largest institutions. The growing incorporation of new third-party services (like cloud service providers, which keep data outside regulated financial institutions) further escalates these dangers. Fourthly, the financial sector incurs substantial costs from cyber-attacks, as indicated by Accenture, which reported that in 2018, banks faced the highest average annual cybercrime expenses (exceeding USD 18 million per bank), with the insurance sector coming in fifth (over USD 15 million per company). Given that these costs are likely to be transferred to customers, regulators are motivated to mitigate the effects of cyber-attacks. Finally, recent incidents have clearly shown that not even the largest financial institutions or regulatory bodies are shielded from cyber threats, as evidenced by successful attacks on the central banks of Azerbaijan, Bangladesh, Ecuador, Italy, Russia, Sweden, and the US, along with the European Central Bank in recent years.[28].

F. Data Theft and Identity Fraud

Every individual who accesses the internet leaves behind a digital footprint of their personal information and identity. Some of the online activities we participate in lack sufficient security, attracting cybercriminals and fraudsters who seek new methods to acquire personal data. For cybersecurity professionals and users alike, it’s important to focus on preventing system breaches, but it’s even more crucial to quickly identify any breaches that do occur and minimize their impact to safeguard the system and its data, as attackers constantly adapt their tactics. On a global scale, identity plays a pivotal role in our daily lives, and it is a multifaceted topic. Establishing identity typically necessitates a comprehensive ecosystem that includes verifying what a person uniquely knows (such as a username, password, or PIN) along with what the person possesses (like a cell phone number or token generator) to either permit or deny that individual from completing a transaction or process[29].

The hours spent resolving fraud issues soared in 2023. In 2022, consumers averaged six hours to address identity fraud problems, but in 2023, this time surged significantly to nearly 10 hours, posing a significant challenge for both consumers and financial institutions.

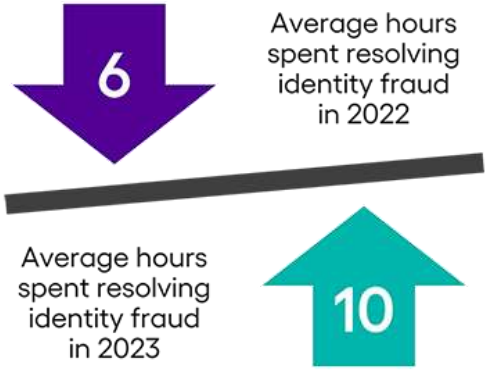


Fig4 Skyrocketing Resolution Hours Create Headaches for Consumers

Instances of traditional identity fraud in 2023 led to losses of nearly $23 billion, reflecting a 13% rise in overall financial damages for adult victims of identity fraud in the U.S. Since Javelin began monitoring financial losses linked to scams in 2021, there has been a gradual, though hardly noticeable, decline in financial losses. Criminally orchestrated scams resulted in more than $20 billion in losses for victims.

Javelin differentiates between traditional identity fraud losses and those resulting from identity fraud scams to offer a clearer understanding of the identity fraud landscape and to present accurate historical data along with pertinent recommendations for financial institutions, fintech companies, third-party fraud solution providers, and consumers. However, it's crucial to keep in mind that for victims of identity fraud, the method of analyzing and categorizing these losses is irrelevant.

What truly matters is how organizations manage the victim's experience after encountering fraud and scams, how they are treated during the resolution process, and how they feel after facing a financial loss and a breach of trust. This consideration should always be prioritized by organizations as they strive to enhance their strategies for detecting and preventing the further impact of identity fraud.[30].

Real-Time Fraud Detection - Systems powered by AI examine transactions to pinpoint and highlight suspicious activities. Tokenization - Substitutes sensitive data, such as credit card numbers, with distinct tokens during transactions. Cybersecurity Training - Instructing employees and customers to identify phishing and fraudulent behaviors. Collaboration and Information Sharing - Financial institutions working together and with government bodies to share threat intelligence. Safeguarding banking and financial services against cyber threats demands a proactive and flexible strategy. By utilizing cutting-edge technologies, enforcing rigorous security measures, and promoting collaboration throughout the financial sector, organizations can reduce risks and build trust in digital banking. Ongoing advancements in cybersecurity techniques will continue to be crucial in addressing emerging threats[31].

G. Market Instability

The true effect on financial stability will hinge on the resilience strategies, preemptive measures, and the decisions regarding business and technology that are implemented in the aftermath of the attack, along with the repercussions those decisions might have on other markets and firms. In a stable market environment, even a significant cyber disruption might not lead to financial instability. However, if the markets or the economy are particularly vulnerable—such as in situations of high leverage and declining asset prices—or if the attacker targets a notably weak point at a critical time, even a relatively minor incident could have far-reaching consequences for the financial system.

For instance, in 2020, teams likely affiliated with Russian intelligence executed an intrusion into SolarWinds, embedding a Trojan horse within the company's widely used network management software, which was subsequently downloaded by 18,000 other organizations, including banks and the U.S. Department of the Treasury. Although this was one of the most significant cybersecurity events in history, the supply chain incident did not result in any systemic financial repercussions because the Russian intentions appeared to focus on quietly gathering geopolitical intelligence rather than engaging in criminal activities against banks, similar to the North Korean attack on the Bank of Bangladesh, or attempting to create widespread disruption of U.S. financial institutions, as the Iranians aimed to do nearly a decade prior.

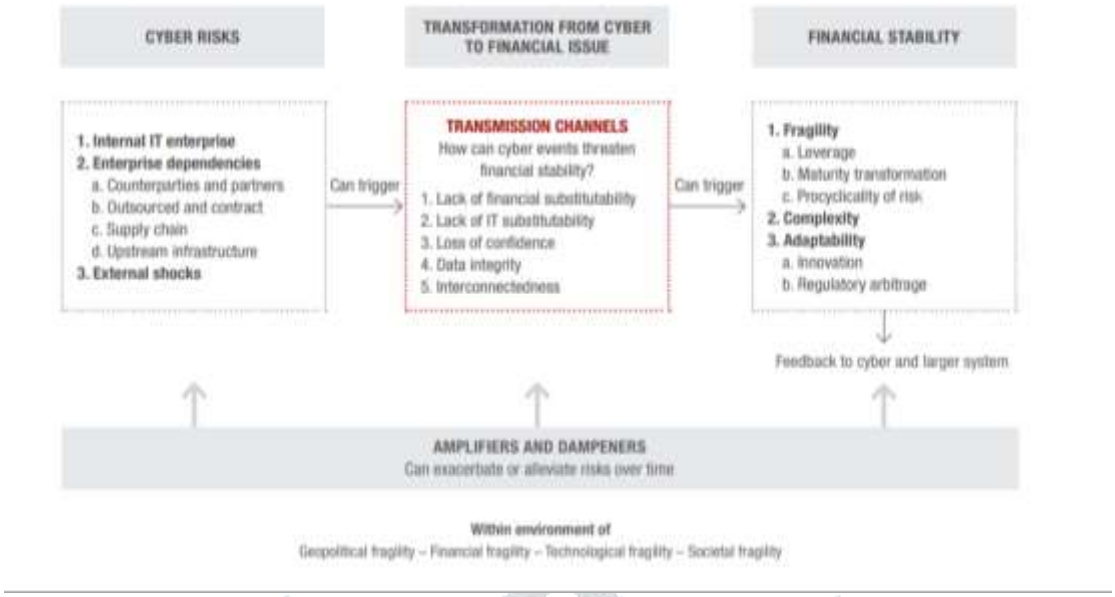


Fig5. Framework with Cyber risks

Figure 5 depicts the foundational structure, with risks flowing from the left to the right. Cyber risks can arise from various "aggregations" (on the left), which can then initiate a financial stability incident (to the right) via the transmission channels (in the center). Each category is influenced by amplifiers and dampeners that can either intensify or reduce the impact, all occurring within a context of inherent vulnerabilities (at the bottom). The cyber risks originating from the left can, through the central transmission channels, evolve into systemic financial risks. Nevertheless, the framework can be utilized in multiple ways based on the specific analytical requirements[32].

H. Psychological and Strategic Impact

A variety of potential consequences stemming from crime victimization—both in digital and physical environments—are documented in the research. These consequences encompass feelings of distress, irritation, anxiety, difficulties with concentration, trouble sleeping, diminished self-esteem, post-traumatic stress disorder, and a loss of trust in online transactions. Furthermore, victims may also lose their sense of invulnerability to becoming victims themselves. Nevertheless, accurately characterizing the specific effects of different crime types can be challenging due to their similarities. Thus, crimes involving fraud can also lead to significant repercussions for those victimized. The impact is tied to how intense the effects are perceived to be and how long they last, from the victim's subjective perspective. Although the exact effects and repercussions of victimization can vary across different crimes, they may also differ for individuals subjected to the same crimes, influenced by unique characteristics like age, gender, and income. For instance, women frequently experience more severe psychological impacts than men, particularly in the context of offline financial crimes.

The initial phase typically spans from several hours to a few days, during which individuals may feel numb, disoriented, in denial, disbelieving, and helpless. The second phase can last between three to eight months and includes varying emotions, transitioning from fear to anger, sadness to elation, and self-pity to guilt. In the final phase, victims work through their trauma by employing effective coping strategies. However, long-lasting effects can pose challenges to the victim’s well-being, potentially leading to issues such as depression, fear, guilt, low self-esteem, and difficulties in relationships, as shown in more recent studies. Once a person has experienced victimization and the corresponding effects outlined in the preceding section, they must exert effort to recover from the situation[33].Cyber-resilience in financial institutions has shifted from viewing security merely as a barrier against threats to adopting strategies that ensure operations continue despite such threats. The resilience frameworks explicitly acknowledge that absolute security is unattainable, thus emphasizing the importance of remaining vigilant to detect, counter, and contain threats while still performing essential business functions. This transformation moves away from preventive security approaches to what can be described as adaptable security paradigms, where security breaches are anticipated, and the focus is on minimizing their impact on the business. In the realm of cybersecurity, fundamental elements include safeguarding critical infrastructures and networks, distributing protective measures, promptly recognizing emerging threats and attack methods, as well as developing defenses against these and recovery strategies for any detrimental occurrences. Financial institutions implement layered defensive strategies and robust business continuity plans for cyber threats and attacks, indicating that effective resilience programs prioritize real-time threat intelligence, automation, and the validation of information security initiatives through regular testing[34].

Type of Attack	Description	Attack Method	Common Targets	Similarities With Other Attacks
Phishing / Spear Phishing	Phishing is a form of cyberattack in which attackers pose as a legitimate organization, such as a financial institution, to deceive individuals into disclosing sensitive information such as login details, credit card information, or one-time passwords (OTPs).	Fake emails, links, attachments	Employees, customers	Employs social engineering techniques such as Business Email Compromise (BEC); facilitates ransomware and SWIFT attacks through the theft of credentials.
Ransomware	Ransomware is a type of harmful software that locks a victim's files or systems and requires payment (typically in cryptocurrency) to regain access.	Malware from phishing or exploits	Servers, databases	Frequently occurs alongside phishing; similar to DDoS, it interrupts services and operations.
DDoS Attacks	A Distributed Denial of Service (DDoS) attack entails flooding a system, website, or network with enormous amounts of traffic from various origins, rendering it unavailable to legitimate users.	Flooding traffic via botnets	Websites, apps, ATMs	Similar to ransomware, it leads to system outages; often employed alongside other attacks to serve as a diversion.
SWIFT Network Attacks	SWIFT attacks involve deliberate intrusions into the banking systems linked to SWIFT. Attackers gain access to the bank's internal network, compromise the credentials or software that interacts with SWIFT, and issue fraudulent transfer instructions to siphon off significant amounts of money. They frequently conceal their activities to postpone detection.	Malware and stolen credentials	Internal SWIFT terminals	Depends on phishing or internal access similar to other sophisticated persistent threats (APTs)
Business Email Compromise	A Business Email Compromise (BEC) attack is a specific kind of phishing attack where scammers pose as a trusted individual (such as a CEO or finance director) to deceive employees into transferring money or providing confidential information. These BEC attacks do not depend on	Email spoofing, impersonation	Executives, finance departments	Similar to phishing but with a more focused approach; akin to SWIFT attacks in facilitating unauthorized transactions.

Type of Attack	Description	Attack Method	Common Targets	Similarities With Other Attacks
	malware; instead, they utilize social engineering tactics to achieve their goals.			
Credential Stuffing	Credential stuffing refers to a cyberattack method in which criminals utilize stolen usernames and passwords (often derived from different breaches) to automatically try logging into banking platforms and financial services.	Use of leaked credentials	Online banking users	Similar to phishing, it includes compromised login details; frequently results in fraud and unauthorized entry.
Insider Threats	An insider threat refers to a security hazard originating from within the organization, often involving current or former employees, contractors, or partners who either deliberately or accidentally jeopardize the integrity of systems or data.	Misuse of internal access	Employees with system access	Circumvents conventional protections such as SWIFT and sophisticated phishing initiatives.

Table 2. Types of cyberattacks on banking and finance

The categories of cybercrime in banking can be summed up as follows based on the literature analysis:

Fig 6. Threats in banking

These classifications underscore the varied types of threats that financial institutions encounter in the changing cybersecurity environment, stressing the necessity for strong security protocols to safeguard sensitive information and uphold trust.
Let's conduct a thorough examination of the nature, reasons, and methods behind these attacks.

- **Phishing/Spear phishing**

Phishing attacks and social engineering strategies continue to be among the most common cybersecurity risks within the digital banking industry, taking advantage of human weaknesses rather than system vulnerabilities. Phishing refers to a type of cyber

fraud where attackers employ misleading emails, messages, or counterfeit websites to deceive users into revealing confidential information, including login credentials, personal identification numbers (PINs), or financial data. Social engineering methods rely on psychological manipulation to take advantage of users' trust, persuading them to engage in actions that jeopardize their security, such as clicking on harmful links or downloading malicious attachments. Research conducted by Mehbodniya et al. (2021) indicated that phishing attacks have progressed beyond email-based tactics, now encompassing voice phishing (vishing), SMS phishing (smishing), and spear phishing methods aimed specifically at banking customers and staff. The success of phishing attacks stems from their ability to circumvent conventional security protocols, underscoring the importance for financial institutions to establish comprehensive security awareness training and effective authentication processes[13]. To comprehend the anatomy of a phishing attack, it is essential to have a clear and comprehensive definition that supports the previously existing definitions. Due to the combination of technical and social engineering tactics involved in a phishing attack, this article proposes a new definition (i.e., Anatomy) that outlines the entire process of a phishing attack. This offers readers a clearer comprehension since it explores phishing attacks thoroughly from various angles. Different perspectives on this could assist novice readers or scholars in this area. For this purpose, we characterize phishing as a socio-technical assault, where the assailant aims at particular assets by taking advantage of a present vulnerability to deliver a specific threat through a chosen medium into the victim's system, employing social engineering tactics or alternative methods to persuade the victim to perform a certain action that results in different kinds of harm[14].

Fig 7. Process of Phishing

Figure 7 illustrates the typical process involved in a phishing attack, which consists of four distinct phases detailed in Proposed Phishing Anatomy. As depicted in Figure 7, most phishing attacks begin with the collection of information about the target. Following this, the phisher selects the attack method to be employed in the planning phase. The second phase, known as the preparation phase, involves the phisher looking for vulnerabilities that can be exploited to ensnare the victim. In the third phase, the phisher executes the attack and anticipates a response from the victim. Finally, in the valuables acquisition phase, which is the last stage of the phishing process, the attacker collects the gains. For instance, an attacker might send a deceptive email to an internet user that appears to be from the victim's bank, asking the user to verify their bank account details or risk account suspension. The user may be led to believe the email is authentic as it mimics the branding, logos, and colors of their legitimate bank. The information provided will be sent directly to the phisher, who will then use it for various malicious activities, such as withdrawing funds, extorting the victim, or engaging in further fraudulent actions[14].

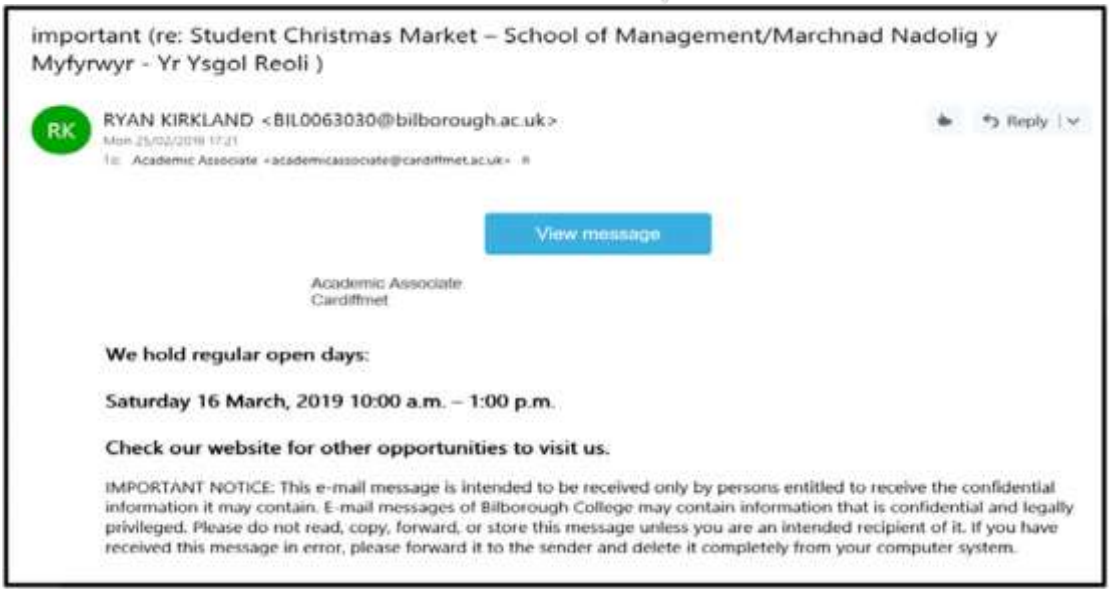


Fig 8. Screenshot of Phishing Email

This section highlights various real-world instances of phishing attacks to illustrate the complexity of some recent attempts. A suspicious phishing email that bypassed a university's spam filters and landed in the recipient's inbox is depicted in Figure 8. As indicated in Figure 8, the attacker instills a sense of urgency by using the term "important" in the subject line, which is designed to elicit a psychological response that prompts the recipient to click the "View message" button. The email features a dubious embedded button, and if one hovers over it, the URL displayed in the status bar is inconsistent. Additionally, the sender's address appears suspicious and is unfamiliar to the recipient. If the victim clicks the fraudulent attachment button, it could either lead to the installation of malware on their computer or redirect them to a counterfeit login page, resulting in the compromise of their credentials[14].
The types of Phishing attacks and techniques drawn upon existing phishing attacks:

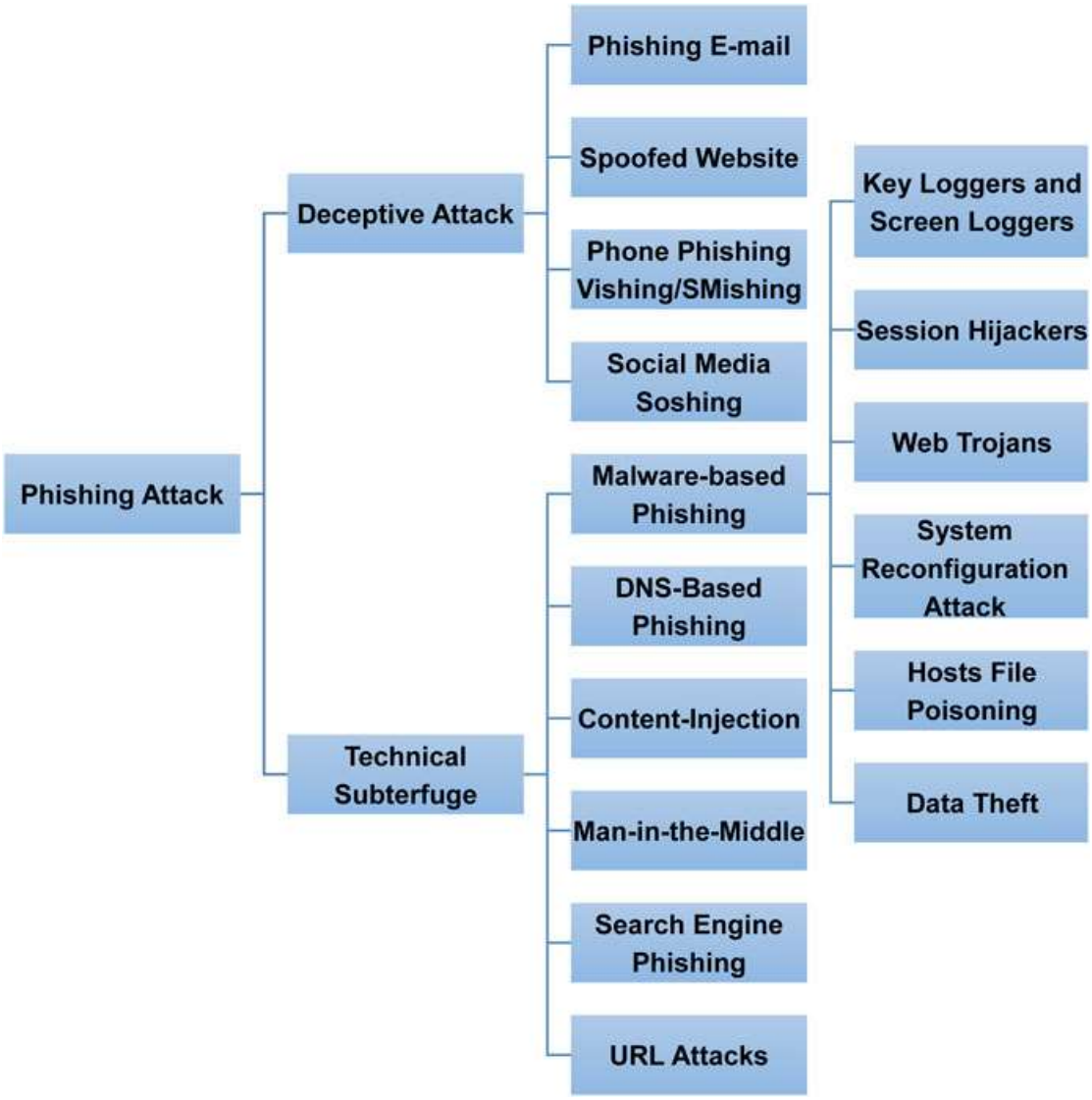


Fig 9. Types of Phishing Attacks

Along with collective experiences, we observe numerous variations across various sectors, departments, and groups of users. Comprehending what these distinctions imply for your organization enables you to more effectively address the specific methods attackers are using to target your personnel. You might be aware of the “six W’s” that serve as a guide for journalists, researchers, and investigators: who, what, where, when, why, and how. These questions are beneficial when trying to uncover the core of an issue. At the very least, we recommend that you initially respond to these three:

Who within my organization is being targeted by cybercriminals? The response is not merely a matter of examining the upper levels of your organizational structure.

What kinds of attacks are they encountering? Understanding the lures and traps employed by attackers can enhance your defensive strategies.

How can I reduce risk if these assaults do occur? The solution lies in utilizing the information you’ve collected to provide appropriate training to the suitable individuals at the right moment.

This exercise aids in protecting against your most urgent and relevant threats. Evaluating vulnerabilities on a more detailed level and aligning that with your threat intelligence allows you to identify where significant risks are emerging: the intersections of vulnerability and exposure[15].

TYPES OF PHISHING ATTACK

A. Deceptive Phishing
This is the most prevalent type of phishing, where attackers impersonate a legitimate organization to steal personal information or login credentials from individuals. They then attempt to blackmail the victims into complying with their demands.

B. Spear Phishing
A Wireless-based Intrusion Detection Prevention System analyzes the traffic on a wireless network by examining wireless protocol activities and taking suitable actions. It detects any unauthorized wireless local area network in operation. However, it cannot identify suspicious activities within the application layer, transport layer, or protocol activities. It is deployed within a specific range, allowing the organization to monitor the wireless network.

C. Clone Phishing
Clone phishing is a phishing attack that involves a legitimate or previously received email which contains an attachment and a link. The recipient's address is utilized to create an identical or cloned email, in which the original attachment or link is replaced with a malicious version. This altered email is then sent to the victim from an email address forged to appear as the original sender. This method can indirectly pivot from an infected machine, allowing the attacker to extract information or establish a foothold on another device.

D. Whaling
Whaling is a specific type of phishing where the attacker targets individuals of wealth and influence; the attacker gathers information about the victim via various sources, such as social media, before launching the attack. The targets of this attack are often referred to as “Whales” or “Big Phish.” Whale phishing utilizes similar tactics as those employed in Spear Phishing.

E. Link Manipulation
Link Manipulation is a category of phishing attacks wherein the phisher sends a link directing to a spoofed or malicious website. When the user clicks on the link, it redirects to the phisher’s website instead of the intended destination. Hovering the mouse over the link to view the actual address can help prevent users from falling victim to link manipulation.

F. Voice Phishing
Voice phishing is a type of phone-based criminal attack that employs social engineering through telephone systems to obtain personal and financial information for illicit financial purposes, and it is often referred to as “vishing.”

PREVENTION OF PHISHINGATTACK

Phishing attacks often manifest as spam or pop-up messages, making them challenging to identify. Once an attacker acquires your personal information, it can be exploited in various ways, including identity theft, which can severely damage your good credit. Given that phishing is one of the most insidious forms of identity theft, it’s crucial for us to understand the different types of phishing attacks and the preventive measures we can take against them. Some of these are detailed in the following sections.

1. Protect yourself against spam. In this method of prevention, attackers are typically unknown senders who request confirmation of personal or financial information online and solicit your details.
2. Only share personal information over the phone or through secure websites. When engaging in online transactions, users must ensure they see a secured sign on the browser's status bar or the “https” URL, where the “s” signifies “secure,” as opposed to “http.”
3. Avoid clicking on links, downloading files, or opening attachments in emails from unfamiliar sources. It is advisable to protect sensitive information, such as bank and social media details, in emails, and only open attachments when you are expecting them and know their content, even if the sender is recognized.
4. Establish sound security policies. In larger organizations or companies, it is essential to implement guidelines for how to respond to odd or unusual emails and requests. The company’s policy should also provide instructions on what to do in case something seems amiss.
5. Conduct Security Awareness Training: Educate employees on what legitimate emails look like and demonstrate how to recognize a phishing email. Manage and instruct staff about phishing attacks and their prevention. Ultimately, educating users will help reduce the success rate of these attacks, and assessments will ensure that security and management are prepared to respond appropriately.

.

DETECTION OF PHISHINGATTACKS

The internet serves as a vast resource for humanity to accomplish a wide range of tasks, but platforms like Facebook, Twitter, Gmail, Dropbox, PayPal, eBay, banking portals, and numerous other websites have counterfeit versions that are actually phishing attempts. “Phishing” refers to fraudulent websites that attempt to imitate legitimate sites you are familiar with and frequently visit. Some techniques for detecting phishing are outlined below:

Utilize custom DNS services. With this method of detection, users can take advantage of DNS resolution services that enable access to all the websites they typically frequent. Your computer may not know the exact internet address, or IP address, of Facebook, so it requests this information from a DNS resolution service. While standard DNS servers at ISPs primarily handle name resolution, several independent DNS companies offer additional features, such as filtering sites based on content, malware, or phishing threats.

Leverage your browser's phishing list. Many modern browsers now provide phishing detection lists. This feature allows the browser to assess any website you are about to visit or have recently accessed, checking for possible phishing attempts. Therefore, it’s wise to review this list before exploring new sites.

Use link-checking websites. Often, when navigating a site or using a program, you may encounter various types of links. If you come across a link that raises suspicion, you can copy it and verify it on multiple link-checking websites. This can help identify whether the site presents any dangers, such as malware or phishing.

Employ your own detective skills. While this might seem trivial, using your instinctive skills to identify potential phishing attacks can shield you from various kinds of malware or phishing sites that may not yet appear on your warning lists.

There are several indicators to consider when determining if you’re encountering a fake site:

1. Check for secure connections. This is typically indicated by a green section in the address bar and the presence of “https” in the URL.
2. Examine the URL's domain. Ensure that the domain has not been altered or modified.
3. Inspect the appearance of the site itself. If it doesn’t closely resemble the website you know well, it may be a scam. You can open the site in a new tab for further examination[16].

- **Ransomeware Attacks**

Ransomware is a category of malware that restricts or denies users access to their systems, frequently encrypting data in a way that makes recovery impossible. This type of malware compels victims to pay a ransom via specific online payment methods to regain access to their systems or restore their data. Ransomware has emerged as one of the most profitable business models in cybercrime today, severely impacting organizations such as banks worldwide. In a ransomware attack, cybercriminals utilize malware with encryption to seize vital data from victims, preventing them from accessing their systems until payment is made. Typically, cybercriminals initiate a ransomware attack through email, deceiving users into clicking on a malicious link or opening an infected attachment that disseminates malware throughout an organization’s network. The ease of executing ransomware attacks has increased significantly due to ransomware as a service, while cryptocurrency facilitates smooth financial transactions[35].

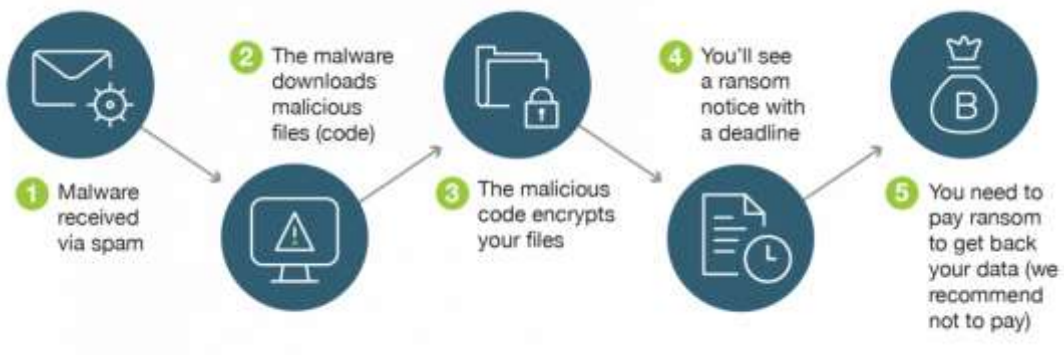


Fig 10. Process of Ransomeware attack

Ransomware remains a significant danger to the financial industry. The tactics employed by malicious actors have advanced from merely encrypting data to now incorporating methods like double and triple extortion, along with distributed denial of service (DDoS) attacks. For the financial industry, ransomware is more than just a monetary concern of paying to retrieve compromised data. It also poses an operational risk and, in some cases, threatens the very existence of the organization. Ransomware continues to adapt and will pose challenges to the financial sector for the foreseeable future. In the financial industry, ransomware transcends the financial aspect of paying a ransom or fees to regain access to stolen data. It also signifies an operational hazard

and, at times, a threat to the very continuity of the institution. Ransomware is constantly evolving and will continue to present risks to the financial sector for the coming times[36].

Types of Ransomware

There are essentially four classifications of ransomware: Crypto ransomware, Locker ransomware, Leakware, and Scareware. Crypto ransomware infiltrates the victim's computer via various attack methods, encrypting important files and rendering them inaccessible to the user while demanding a ransom for decryption. Locker ransomware, on the other hand, restricts access to the user's devices without encrypting files and requests payment to regain access. Leakware (also known as Doxware) gathers sensitive data from the victim's machine and then extorts them for ransom. Scareware is a milder version of ransomware that falsely warns users that their files are encrypted or locked, requesting payment despite not causing any actual harm and relying on intimidation. The following figure illustrates the diverse types of ransomware and their categories:

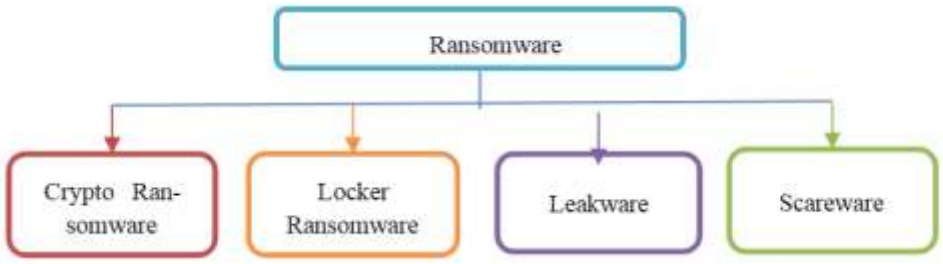


Fig 11. Types of Ransomware

Crypto Ransomware

Crypto ransomware is the most prevalent type of ransomware, both in terms of the number of attacks and the resulting damage. Figure 2 illustrates that well-known ransomware variants such as WannaCry, CryptoWall, Locky, Petya, CryptXXX, and notPetya fall under the crypto ransomware category, along with their market share. In 2017, the WannaCry ransomware infected 230,000 computers worldwide across 150 nations, leading to $4 billion in damages globally. This ransomware specifically targeted unpatched versions of the Microsoft Windows operating system in May 2017, utilizing a method known as EternalBlue, which was developed by the United States National Security Agency and later leaked by the Shadow Brokers group. Microsoft had issued a patch two months prior to the attack, but it impacted those systems that remained unpatched. Therefore, it is crucial to keep all software updated with the latest patches. All four of these ransomware types, along with most contemporary variants, belong to the Crypto ransomware category, and this study is concentrated on Crypto ransomware.

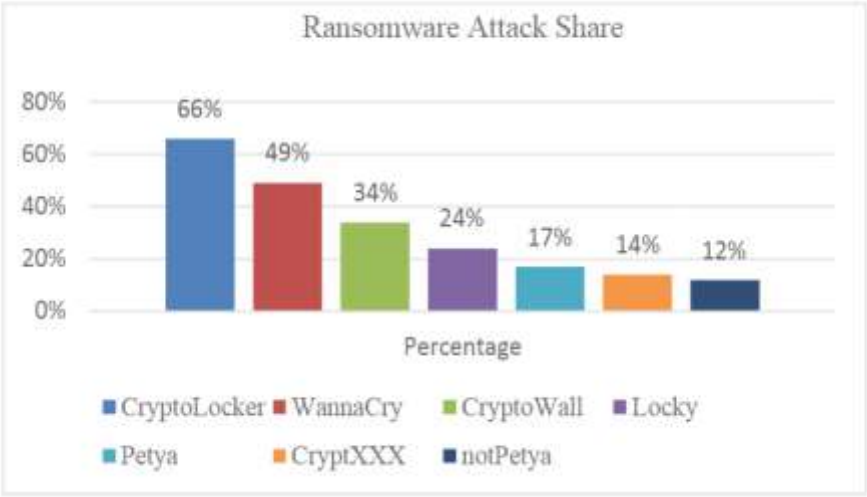


Fig 12. Shares of Ransomware attacks

Locker Ransomware

Locker ransomwares such as WinLock take control of the Windows screen, displaying pornographic messages or fake activation notices while demanding ransom for unlocking it. Another variant, Revton, similarly locks the Windows screen and shows a counterfeit message purporting to be from a law enforcement agency, demanding payment to regain access. Additionally, there is the Urausy Police ransomware, which also locks the screen and asks for money to release it. In 2013, a locker type known as Svpeng emerged, which locked Android devices, rendering them completely unusable; the only way to regain access is to reach out to the attacker. In this case, the attacker does not download or introduce further malware, such as programs that steal passwords.

Leakware (Doxware)

This type of ransomware is relatively new and is also referred to as extortionware. It targets individuals' private and valuable information, such as files and photographs, encrypts them, and holds them hostage while demanding a ransom. If the victim refuses to pay, the attackers threaten to publish their personal data online. Here, the attackers do not restrict access to the device, but instead, they move the encrypted files to a server or other compromised machines.

Scareware

Scareware, also known as fake ransomware, is not as intimidating as its name suggests. It is comparatively less frightening than other forms of ransomware, technically simpler, and relies primarily on fear tactics to pressure victims into paying a ransom.

Damages caused in the Banking and Financial Sector

Ransomware can arise from malicious websites that exploit known vulnerabilities, phishing emails, social engineering tactics, or web-based drive-by malware injections. When the exploit occurs, a downloader is installed on the system. This downloader quietly communicates with command and control servers to download and install the ransomware and secure an encryption key. The contacted C&C server then sends back the requested encryption key and provides payment options before the ransomware begins encrypting the entire contents of the hard drive, personal files, and sensitive data. A warning appears on the screen with instructions on how to pay for the decryption key. The primary motive behind most ransomware attacks tends to be financial gain. In certain instances, what may initially seem to be a ransomware attack could be a malicious attack intended to destroy digital assets and data instead of allowing for their recovery. A destructive attack uses malware to erase system components, corrupt data, and render enterprise devices inoperative. Another model of ransomware attack that has emerged recently is the blended attack mode. It starts like a traditional ransomware attack, demanding payment for encrypted files, but simultaneously, attackers have already exfiltrated data from the bank. If the ransom is not paid, they threaten to disclose or auction the data online. These blended attacks can bypass backup strategies since they effectively coerce the victim into paying even if backups are available. Such attacks can place enormous pressure on organizations to meet extortion demands. Some of the damages resulting from a ransomware attack are outlined below [38]:

• Loss of Data and Information

• Employee Downtime and Loss of Production

• Ransom Costs

• IT Consultant Time and Labor

• Forensic Investigation Cost

• Data Leak and Compliance Issues

• Regulatory FINES (HIPPA, etc.)

• Impact on Reputation and Loss of Business Relationships

• IT Infrastructure Upgrades/Overhaul

Detection of Ransomware Attacks

The method by which an organization initially detects a ransomware infection can differ based on the circumstances, but generally, an employee may find it impossible to access certain files, receive a ransom demand, or notice that a specific service is no longer available. The most urgent issue at the beginning of the attack is to identify all infected systems and those at immediate risk of infection. The primary objective is to contain the spread of the infection as quickly as possible and reduce the risk to the organization by isolating affected systems.

Analysis

The Analysis stage primarily concentrates on two areas, with the first objective being to contain the infection's spread as quickly as possible and to mitigate the risk to the organization by isolating infected systems.

1. Identifying the particular variant of ransomware involved

2. Understanding how the malware penetrated the organization (root cause analysis)

Containment

The Containment phase is a crucial element of the response strategy. Once a system has been identified as possibly infected with ransomware, the affected computer should be immediately disconnected from all networks (including WiFi connections) and either shut down or, ideally, hibernated to aid in forensic and sample analysis while reducing the risk of the ransomware continuing its encryption process. Delaying the quick isolation of infected systems from the network may lead to an escalation of the incident by allowing the malware to encrypt more files on the infected system or network shares, thus complicating recovery efforts.

Eradication

The Eradication phase focuses on eliminating the ransomware from all infected systems within the organization. Depending on the extent of the attack, this process may be time-consuming and could involve both user devices and critical machines and

services that have been affected. Systems identified as infected with ransomware should be restored from a trusted source, utilizing reliable templates and securely stored settings.

Recovery

After a bank has managed to contain the ransomware and pinpointed the root cause of the infection, there are several factors the organization should consider when initiating the recovery phase.

• Addressing vulnerabilities

• Restoring data from backups

Post-Incident Activities

Post-incident activities are a vital component of the response plan and should never be overlooked. Following any incident, whether large or small, it is advisable to convene with relevant stakeholders to review what worked well and analyze what did not. This type of "lessons learned" evaluation can assist banks in refining their processes over time and ensure that future incidents are dealt with more effectively, thereby minimizing potential impacts. Notify Authorities: Most organizations are aware of the compliance and regulatory obligations that apply to their operations. Generally, these requirements pertain to all instances of a data breach and the loss of private information belonging to customers and individuals. Banks may have more specific duties to report.

Recommendations for ransomeware attacks

Ransomware has garnered significant attention from cybersecurity professionals in recent years due to the rapid rise in its attacks and the emergence of new variants that can circumvent antivirus and anti-malware solutions. This type of malware is relatively recent but has captured the interest of cybercriminals because of its effective attacks and direct potential for financial gain. The primary goal of ransomware is to prevent its victims from accessing their own data by encrypting valuable files, such as photos, spreadsheets, and presentations. Banks are among the primary targets of ransomware incidents. The most common methods for deploying ransomware include phishing emails, compromised USB drives, usage of hacked accounts belonging to bank employees, and visiting harmful websites[35].

- **DDoS attacks**

A Distributed Denial of Service (DDoS) Attack is a significant and recognized threat in the field of cybersecurity that infringes upon the security principle of service "Availability." DDoS attack methods take advantage of various characteristics of internet protocols, many of which were created years ago without considering security implications. The dynamic between an attacker utilizing protocol features, such as the TCP connection establishment through the three-way handshake, and the target is inherently uneven. DDoS attacks are primarily divided into two main types: bandwidth depletion attacks and resource depletion attacks. In the first type, a large volume of seemingly legitimate traffic that isn't meant for actual communication is directed at the target. In the second type, the target is flooded with fake service requests that exhaust its resources, thereby hindering its ability to process genuine requests. Typically, multiple bots (network nodes that have been compromised and are under an attacker's control) are deployed to execute DDoS attacks. Direct attacks on a target usually involve flooding, where numerous packets are dispatched from various bots to the target; common examples include TCP SYN floods, UDP floods, ICMP floods, and HTTP floods[41].

Furthermore, attacks that exploit protocols, such as TCP SYN flooding, can be executed against the targeted infrastructure by leveraging the TCP connection setup process and inundating the victim's system with a barrage of TCP SYN packets without any accompanying ACK responses, thereby depleting the victim's resources. The attacker can also employ automated scripts to unleash floods of TCP flags, including ACK, PUSH, RST, and FIN packets, to overwhelm the communication channels within the victim's infrastructure. Another type of DDoS attack includes the ping of death and land attacks. The ping of death attack involves sending a Ping command with a packet size exceeding the maximum permissible size of 65536 bytes, which can lead to the crashing of the victim's system. In a land attack, an attacker may transmit spoofed packets with identical sender and destination IP addresses, causing the victim to send the packet back to itself, thereby creating an infinite loop that leads to the failure of the victim's machine[39]. A zero-day vulnerability can be exploited to take control of legitimate machines and effectively initiate a denial of service attack[40].

According to the latest FS-ISAC/Akamai report, DDoS attacks are rapidly emerging as one of the most common forms of cyber threats, showing significant increases in both frequency and scale throughout the past year, particularly notable in the second and third quarters of 2023. Organizations with larger sizes and banks that enjoy strong brand recognition tend to be the primary targets, as attackers seek to create an impression of widespread chaos and misinformation. Nonetheless, these entities are also more likely to possess robust defensive measures in place. Attacks from hacktivists and DDoS incidents can disrupt business functions, leading to diminished credibility, loss of customer trust, and financial losses. Furthermore, DDoS assaults can act as a diversion for other nefarious actions, such as data breaches or cyber espionage. In the EMEA region, the financial services industry was responsible for 66% of all DDoS attacks, in contrast to 28% in North America. In the Asia-Pacific region, financial services ranked as the third-most targeted sector, making up 11% of DDoS attacks. The prevalence of DDoS attacks in the EMEA region underscores its utilization for political reasons, hacktivism, and cyber conflict, particularly concerning the ongoing Russia-Ukraine War.

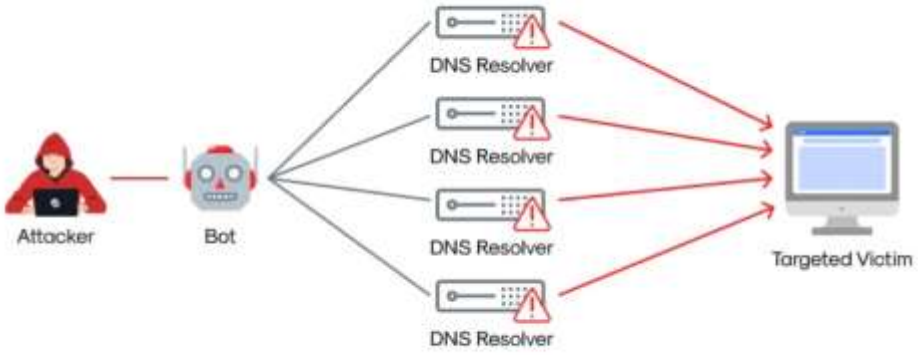


Fig 13. DDoS attack

A successful DDoS attack involves the formation of a botnet, target selection exploitation, and the generation of malicious traffic. Specifically, botnet creation consists of recruiting and coordinating the botnet. Attackers initially build a network of compromised machines, referred to as a botnet, by taking advantage of device vulnerabilities to install malware. Subsequently, the attacker utilizes command and control (C&C) servers to oversee the botnet, ensuring synchronized attack coordination. With the botnet in place, the attackers then focus on selecting targets to exploit. They may identify weaknesses in network protocols like HTTP, DNS, or TCP/IP to exploit during the attack. Specific characteristics and vulnerabilities of the target system (such as content caching) can also be exploited. Ultimately, the attacker determines the type of malicious traffic to create (e.g., SYN requests). They also design the traffic patterns to maximize disruption, potentially employing slow and low attacks to avoid detection or high-volume bursts to rapidly overwhelm the target. Adversarial tactics, such as using encrypted traffic, can be employed during the attack to evade traditional detection methods. Following this DDoS attack framework, we will begin by exploring advanced strategies for botnet recruitment and coordination, which act as the primary means for attackers to conduct DDoS campaigns. A visual depiction of the DDoS attack taxonomy and a summary overview are illustrated in Fig 2[43].

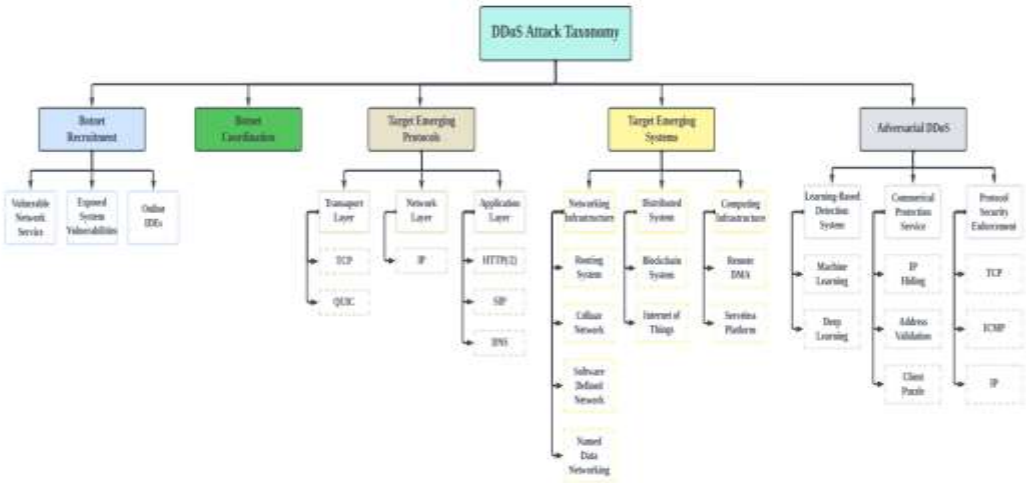


Fig 14. Taxonomy of DDoS attacks

Defense from DDoS attacks

DDOS DEFENSE

The critical nature of the DDoS issue, along with the rising frequency, complexity, and intensity of attacks, has prompted the suggestion of various defense strategies. However, despite the development of many solutions, the problem remains largely unaddressed, if not unresolved. What accounts for this situation? Several significant factors impede the progress of research into DDoS defenses. There is a necessity for a coordinated, distributed response at multiple points across the Internet. As previously discussed, there are numerous potential DDoS attacks, most of which cannot be managed solely by the victim. A distributed and, in some cases, coordinated response mechanism is often essential. Additionally, deploying the response across various locations

on the Internet to encompass different agents and victims is vital. Since the Internet is governed in a decentralized manner, widespread implementation of any defense system or even collaboration among networks cannot be enforced or guaranteed. This reality deters many researchers from even creating distributed solutions. Economic and social considerations come into play as well. A distributed response system has to be implemented by entities that do not face direct harm from the DDoS attack (source or intermediary networks). This leads to a peculiar economic model since those who bear the costs of deployment aren't the ones who benefit directly from the system. Historical instances of similar issues, akin to the Tragedy of the Commons, have been addressed through legislative actions, and it is possible that the DDoS challenge will eventually capture the attention of lawmakers and prompt a legislative response. Until such time, many effective distributed solutions may see only limited adoption and, therefore, have a minimal impact. There is also a deficiency in detailed information regarding attacks. A comprehensive understanding of DDoS attacks is crucial to creating innovative defenses against them. While some publicly available analyses exist for well-known DDoS attack tools, there remains a lack of information on the prevalence of different attack types (e.g., UDP floods, TCP SYN floods) and various attack parameters like speed, duration, packet size, number of agent machines, attempted responses and their effectiveness, damages incurred, etc. It is widely believed that publicizing attack incidents can harm the business reputation of the targeted network. Consequently, these attacks are typically reported solely to government bodies that are required to maintain confidentiality regarding the specifics. Some notable initiatives by researchers have aimed to deduce essential information from packet traces collected within their organizations. CAIDA's backscatter packet analysis technique has offered valuable insights into the occurrence, duration, and rate distributions of various attack types. This data was gathered by monitoring response packets sent to an unused range of IP addresses at CAIDA. Meanwhile, the ISI/USC analysis of attack traffic yielded estimates regarding the potential number of agents involved in specific attacks observed in Los Nettos packet traces. Both efforts represent progress, yet they still uncover only a fraction of the overall picture. There is also a lack of benchmarks for defense systems. Numerous vendors and researchers assert that their solutions entirely address the DDoS challenge. However, no benchmark suite exists for attack scenarios or any established evaluation methods that would allow for comparisons between different defense systems. This situation likely discourages networks from investing in DDoS protection, as they cannot be confident in the quality of the solutions they are purchasing. Additionally, large-scale testing poses challenges. DDoS defenses require evaluation in a realistic setting. This need is currently unmet due to the absence of large-scale testbeds, safe methodologies for conducting live distributed experiments across the Internet, or comprehensive and authentic simulation tools capable of supporting thousands of nodes. Claims about defense system performance are thus made based on small-scale experiments and simulations, and are not credible. This situation will likely change in the near future. The US National Science[44].

SWIFT network attacks

Over the years, there has been a consistent rise in cyber attacks targeting banks and the financial services industry as a whole, particularly concerning the creation and execution of advanced, targeted assaults on financial messaging systems like SWIFT. This trend is not surprising; attackers have recognized that allocating their resources to execute a low-profile, calculated, and refined strike on a financial institution offers a much greater potential reward, requiring less overall effort than repeatedly attempting to target individual customers. Consequently, these attacks have surged in frequency and complexity over the years; attackers are becoming more persistent and adaptable in their strategies to circumvent security measures and compromise essential financial systems to achieve their objectives. SWIFT (the Society for Worldwide Interbank Financial Telecommunication) is a secure messaging service utilized for sending financial messages between member institutions globally. SWIFT operates as a cooperative service exclusively for members, trusted by over 11,000 financial institutions across more than 200 countries and territories worldwide. Essentially, SWIFT provides access to the SWIFT messaging network (SWIFTNet) along with its four messaging services (FIN, InterAct, FileAct, and Browse). Additionally, it establishes the standards for financial messaging and offers various solutions for securing, creating, managing, processing, and validating these messages. However, SWIFT does not bear responsibility for the security of its customers' local SWIFT infrastructure, although it does offer support to help customers manage cyber attacks.

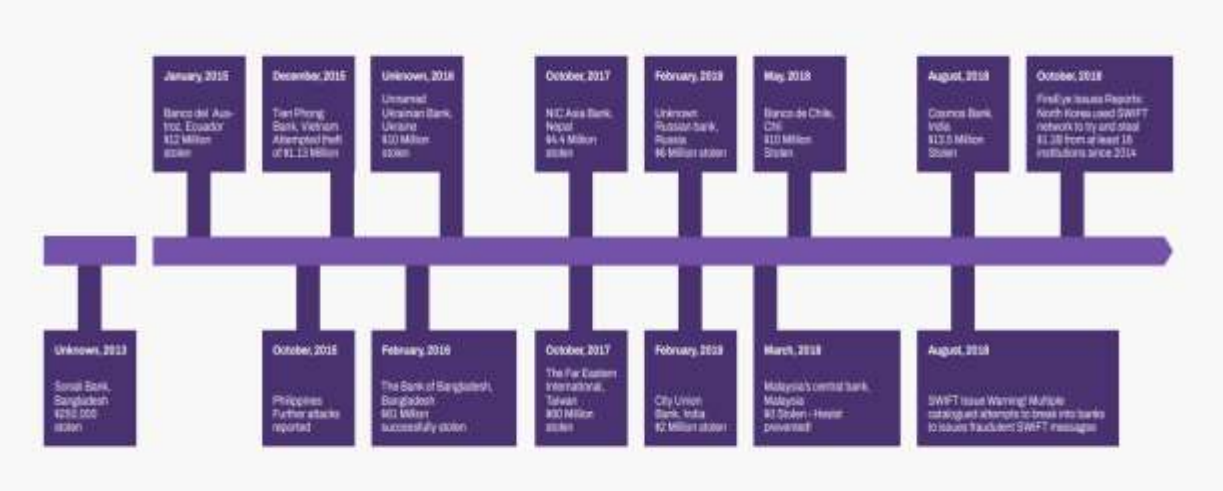


Fig 15 Swift network attacks across the world

A total of about $200,280,000 has been stolen as a result of these noteworthy attacks, with the 2016 cyberattack on the Bank of Bangladesh ranking among the biggest bank robberies in history. To fully recover the stolen monies from the financial system, $81,000,000 of the $951,000,000 that was attempted to be stolen in this incident was successfully moved to Philippine banks and then laundered through casinos. According to analysis, organisations with weaker policies and processes are frequently the target of attacks on SWIFT networks. However, there have been reports of attempted and successful attacks on institutions of different sizes and security readiness levels across the globe.[45].

Fig 16 Working of Swift Network Attack

Prediction and Prevention

Predict

Financial institutions must start by thoroughly comprehending and describing the several attack vectors that a hacker could use to compromise their local SWIFT infrastructure and corporate network. To identify which systems communicate with the SWIFT infrastructure and the administrative protocols associated with these systems, this process starts at the SWIFT systems and moves back towards the enterprise network's perimeter. Every system and application used by the company must also go through frequent penetration tests and security assessments.

Many attempts (and successes) of attacks on financial systems remain unreported to the public. Therefore, Organisations are urged to develop reliable connections with domestic and foreign financial institutions in order to share knowledge on approaches and resources.

Once potential attack vectors are recognized, it is crucial to analyze the steps an intruder would take to achieve their objectives. It is important to assess the security measures that surround each of these processes in order to confidently ascertain whether or not they would successfully prevent such operations. A comprehensive grasp of the acceptable use cases for each component should be part of this evaluation, as should security evaluations of every step in the process. Additionally, financial institutions should gain a thorough understanding of the actions and systems that privileged individuals can access, as well as how an attacker could abuse or exploit these privileges. Thorough monitoring and the detection of any harmful activity should be implemented if these lawful operations are necessary and cannot be stopped. Putting protections in place that stop malware from running should also be a top priority.

Moreover, these controls should be redundant to account for any failures or bypasses, for instance:

Mail gateway: extremely stringent controls, only allowing the appropriate file types, malware signature detection, and sandbox environments for malware explosion.

Endpoint devices: in order to prevent the execution of arbitrary binaries, scripts, and document macros, antivirus software must be implemented in conjunction with software whitelisting.

Account control involves limiting privileges whenever feasible and using multi-factor authentication in conjunction with a "just in time/minimal effective access" approach to authentication. The supervision of vital system access can be centralised with the use of Privileged Access Management (PAM) platforms.[45].

Business Email Compromise

In an era characterized by swift technological progress, individuals, businesses, and organizations are increasingly dependent on services such as digital communication, cloud services, social media platforms, and electronic money transfers, which has significantly expanded the opportunities for harmful cyberattacks[46]. Email, because of its widespread use globally as a communication method and work tool, is frequently exploited to disseminate malware attacks, spam attacks, and phishing attacks. Phishing is a form of cyberattack where an individual or entity sends messages impersonating a trustworthy person or organization to fool individuals into revealing sensitive information, clicking on harmful URLs, downloading dangerous attachments, or—most commonly—urgently requesting that they complete a financial transaction. Phishing, when executed through meticulously crafted emails and by collecting and spoofing information about the target, has become a highly profitable scam known as Business Email Compromise (BEC)[47].

As a man-in-the-middle email attack, business email compromise (BEC) is a type of cybercrime where an attacker uses carefully constructed emails or infiltration techniques to trick people into sending money without authorisation or disclosing private

company information. The attacker usually starts the process by looking through employee profiles, gathering information from social media and internet sources, and keeping an eye on internal conversations within the victim's company. Having this knowledge is crucial to writing an email that is very convincing. The content of BEC emails is typically written in a language context that is known to the recipient and is deliberately targeted.
Additionally, BEC emails are sent from spoof addresses, hacked accounts, or seemingly trustworthy sites, which makes it challenging for spam filters to identify them. Typically, BEC attacks take the following forms:
Spear phishing attack is a technique in which a hacker focusses on a particular individual or group, thoroughly researching the target to increase the possibility that the fraud would be successful.
A high-ranking executive, such as a CEO or CFO, is typically the target of a whaling attack, a type of spear phishing.[48].

Prevention: Non Technical Methods

Prevention can be the initial measure to avert BEC attacks, with a crucial element being the investment in ongoing employee training and the establishment of clear policies. To elaborate:

1. Ongoing employee training. Team members must be equipped to identify, report, and react to a BEC attack. Sensitive sectors within a firm, such as finance, should receive regular training on social engineering tactics and BEC strategies. Employees should maintain a cautious attitude toward hyperlinks, attachments, spelling errors in names, and sudden requests for wire transfers or account changes. It is also vital to encourage the validation of vendor information. All these practices should be approached with the understanding that social engineering and BEC tactics are continually evolving; hence, ongoing and updated training is essential.
2. Implementing fresh and creative training methods. The relevance of training content concerning technologies may vary within a company, just as it does across society. One shouldn't assume that an employee from the accounting team has the same level of technological knowledge as someone from the IT department. To properly comprehend the risks associated with online communication, new training approaches like theme and game-based analytical methodologies are therefore required.[49].

3. It is strongly advised that blue and red teams be established, especially for larger organisations. Red teams concentrate on probing security environments to find vulnerabilities, while blue teams are responsible for evaluating and protecting security environments.

4. Policy formulation: Create internal rules, policies, and guidelines that mandate enhanced protections for information sharing and financial transactions. Make sure that requests for money transfers via email are not allowed and that numerous people must participate in the transaction, or at the very least, verbal confirmation is required. To prevent unwanted data breaches, identity verification questions should be implemented for phone conversations.
Additionally, it is important to promote the creation of reports when incidents take place.

5. Assessment of fraud risk: Performing a fraud risk assessment can uncover and mitigate vulnerabilities that scammers may exploit.

6. Conduct frequent real-world assessments: Considering that employees have received comprehensive training on social engineering and BEC schemes, and that policies have been established, it is essential to conduct regular real-world assessments facilitated by professional partners such as penetration testers and social engineers.

7. Establishment of a social engineering section: For larger organisations in particular, a division devoted to workers with expertise in social engineering and Open Source Investigations (OSINT) is crucial. Workers might use OSINT technologies to look at prominent targets inside their company. Using internet services like "Have I Been Pwned," offered by Dehashed, a reputable company based on Market Street in San Francisco, CA, USA, they can use these tools to look for possible data breaches and leaks. Recognising the weaknesses and possible compromises in a company's profile is essential to preventing and identifying future BEC threats because any information collected could be used by an attacker to dox a victim.[50].

4.2. Technical Methods

While prevention is a good initial step, it alone cannot handle BEC attackers and their continuously changing tactics. The next layer of defense should include technical measures such as:

Anti-spam and anti-malware software: While anti-malware programs can detect harmful software, anti-spam solutions protect against spam and phishing attempts. Both kinds of assaults could be a component of a BEC plan.

Time-of-click protection: Using a variety of reputation services, this functionality alters URLs in emails and provides protection at the exact moment of click.

Executive tracking list: This automatically recognises users' real names in the header and envelope address fields by using data synchronised from an Active Directory.

neighbouring domains: This technique finds neighbouring domains, or those that differ by one or two characters, by comparing the sender's domain to valid domain names.

Preventing directory harvest attacks (DHAs): This tactic gets rid of emails sent to bogus or nonexistent email addresses[51].

A legitimate method of authentication that necessitates two or more verification elements in order to obtain access to a resource is multi-factor authentication (MFA) [55].

Email protocols: make sure they are up to date and forbid antiquated protocols (SMTP, POP, and IMAP) that could be able to get around MFA.

A cryptographic method called DomainKey Mail (DKIM) is used to confirm the authenticity and integrity of emails. The sender domain's private key is used to sign emails, while the receiver domain uses the sender domain's public key from DNS to verify the email's signature.

The Sender Policy Framework, or SPF, verifies that an email's IP address matches a pre-established list of permitted IP addresses.

DKIM and SPF are two techniques that are integrated into Domain-based Message Authentication, Reporting and Conformance (DMARC), which helps prevent attackers from posing as the company and domain. Its main drawback, though, is that it can be impersonated because it only looks at header data.

Encryption: By requiring that both the sender and the recipient have a set of cryptographic keys, encryption can help prevent data breaches.

Verifiers: By using apps like an invoice verifier, which can scan a QR code on an invoice, consumers can verify the authenticity of an invoice that was attached to an email[52].

Machine Learning (ML): This artificial intelligence-related technology uses algorithms to examine email data in order to build a classification model and identify any irregularities as possible indicators of BEC attempts.[55].

To successfully defend against BEC assaults, all of the aforementioned remedies are required, but machine learning (ML) is the most promising and quickly developing field. ML algorithms are able to recognise phoney email addresses, search for telltale signs like DMARC absence, and learn a user's usual behaviour from email databases. Four categories of machine learning algorithms can be distinguished ([53,54]), and the selection of one may be impacted by the different needs of every organisation:

Supervised learning: The machine learning algorithm is given a pre-defined dataset with known inputs and outputs by the operator, and its job is to figure out how to get those inputs and outputs.
In an effort to imitate the operator's outcomes, the algorithm models the connections between the input attributes and the intended output. This procedure keeps going until the algorithm's accuracy is adequate.

Semi-supervised learning: Semi-supervised learning uses labelled data, just like supervised learning, but it also uses unlabelled data, just like unsupervised learning. A model that is trained using a small quantity of labelled data may classify the dataset's remaining unlabelled data.

Unsupervised learning: In this method, the algorithm examines data to find trends without a human operator's help.
Reinforcement learning: The algorithm must use its own experiences to decide on the optimal course of action after being presented with a set of actions, parameters, and end values. With this method, the algorithm evaluates the value of the environment's state and modifies its approach to better suit the environment by rewarding desired behaviours and/or penalising bad ones[55].

Credentials Stuffing

Financial institutions are becoming prime targets for cyberattacks, with credential-stuffing attacks rising as a significant danger. These attacks leverage credentials obtained from earlier data breaches, capitalizing on users' tendency to reuse passwords across different platforms. After gaining unauthorized access, attackers can cause considerable harm, undermining both data security and customer confidence[55].Financial institutions are experiencing increasing pressure to protect sensitive data while facing cybercriminals who are constantly improving and automating their attack strategies. Credential-stuffing methods result in billions of login attempts each year, targeting banks on a large scale. Conventional security measures, such as Multi-Factor Authentication (MFA) and CAPTCHA, provide limited defense, often proving inadequate against the advancing tactics of attackers. The swift progression of these threats highlights the critical necessity for enhanced security solutions that can keep up[56,57].
By investigating AI/ML-driven methods such as anomaly detection, adaptive authentication, and real-time threat intelligence, the paper illustrates how these technologies can bolster cybersecurity measures. In addition, it examines the challenges of implementation and offers perspectives on future trends and research avenues to effectively address credential-based cyber threats. Credential-stuffing attacks pose a complex and prevalent risk to cybersecurity, aiming at login credentials acquired from extensive data breaches. These attacks take advantage of the frequent tendency to reuse passwords, as users often employ identical login credentials across various platforms. This behavior significantly elevates the likelihood of unauthorized access to confidential accounts, especially in sectors like banking, where financial and personal information is vulnerable [55,56].

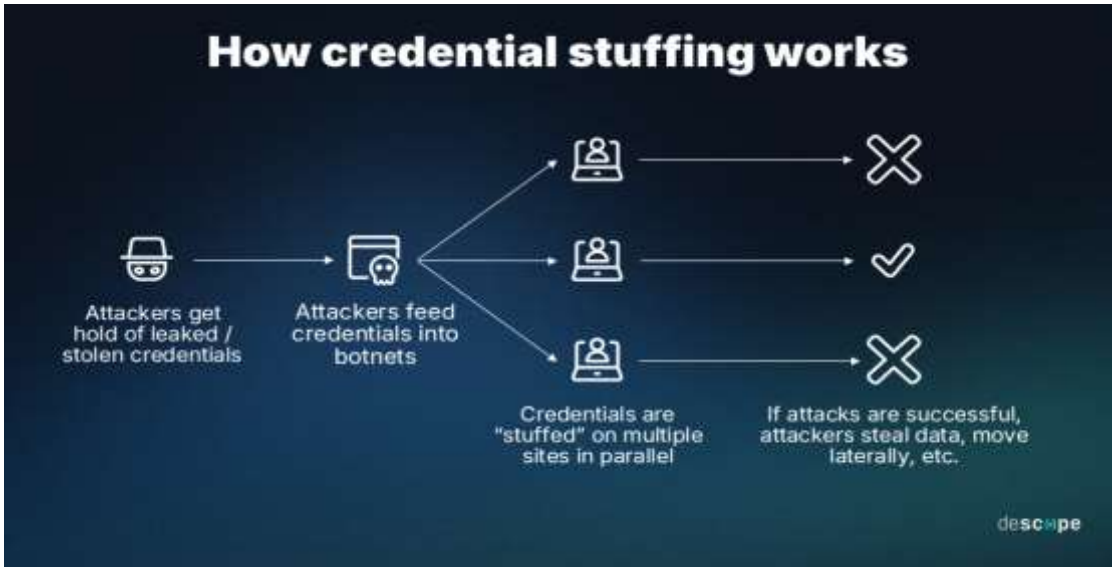


Fig 17 Working of Credential Stuffing

Impacts of credential stuffing

To thoroughly grasp the complete implications of credential-stuffing attacks, it is crucial to analyze their different effects on the banking industry. These attacks present considerable financial and operational difficulties while also eroding customer confidence and complicating regulatory compliance initiatives. For example, banks incur annual losses amounting to billions because of fraudulent transactions and the costs associated with recovery efforts, while penalties imposed by regulations such as the General Data Protection Regulation (GDPR) further increase their challenges [58]. Additionally, the harm to a company's reputation resulting from data breaches frequently results in a loss of customers, which exacerbates financial and operational pressures. The subsequent sections delve into these significant repercussions, demonstrating how credential-stuffing incidents impact banks and their customers.

Credential-stuffing attacks present a significant and growing threat to the banking sector, leading to financial losses, operational disruptions, and diminished customer trust. Traditional security measures, such as multi-factor authentication and CAPTCHA, have proven insufficient in countering the sophistication and scale of these attacks.The integration of AI and machine learning offers a proactive and robust solution.By leveraging AI-based solutions, banks can detect unusual login patterns, anticipate emerging threats, and respond swiftly to suspicious activities[58].

A preventive strategy

I.Taking care of all different type of attacks execution

II. Less intrusive for users

III. Cost effective so that small and middle size online portals can use it

IV. Easy to implement

V. Sending notifications to stakeholders when attack happens

VI. Providing automated mitigation In this paper, an algorithm will be discussed which will fulfill above criteria

Pre-Requisites

Store the below mentioned information associated with every login event (passed or failed) in a table:

I. IP Address

II. ISP (Internet Service Provider)

III. ASN (Autonomous System Number)

IV. Country from which login request was triggered

V. Username[60].

Insider threats

Insiders pose a significant threat because they have existing access to the organization as part of their roles. They might have the ability to view personally identifiable information (PII), comprehensive account details, or in-depth transaction histories, all of which are attractive to attackers and can be disastrous for the organization if misappropriated or taken. The consequences can be devastating, resulting in large financial losses, major damage to reputation, and hefty regulatory fines, particularly in the event of a data breach. What amplifies the danger of these threats is the difficulty in detecting them. They blend into regular data activities and engage in unusual behaviors that might not be obvious enough for detection.

Types of Insider Threats

Insider threats in an organization can take multiple forms, each demanding specific detection methods and proactive strategies.

a. Malicious Insiders – The most recognized type is the malicious insider, who willfully abuses their access to undermine systems, steal sensitive data, or otherwise harm the organization. Their actions are often intentional, presenting a serious risk to the security and integrity of corporate information.

b. Negligent Insiders – On the other hand, negligent insiders inadvertently contribute to security incidents through their carelessness or lack of knowledge. Typical errors include mishandling sensitive information, utilizing weak passwords, or succumbing to phishing attacks, which can unwittingly lead to breaches or data losses. Attackers can exploit these errors, gaining entry into otherwise secured systems.

c. Compromised Insiders – This category includes insiders whose credentials are stolen by external attackers. These credentials might be obtained through an attack on another organization with inadequate security measures. Regrettably, in workplaces where passwords are reused and multi-factor authentication is lacking, attackers can take advantage of these credentials to impersonate legitimate users, obtaining unauthorized access to systems and sensitive data[59].

While it is challenging to completely eliminate insider threat issues, there are several strategies we can implement to reduce them. It's a painful reality that we are often let down by those we trust the most. Nevertheless, businesses must continue to have faith in their employees to operate effectively. However, they can adopt these methods to limit the risks and monitor potential threats.

i. Companies should adhere to rigorous security policies and establish a team dedicated to monitoring harmful activities both internally and externally.

ii. The infrastructure should be safeguarded with appropriate security measures, and employees should have access to secure lockers for storing sensitive information and documents safely.

iii. The primary source of these issues often involves new employees; therefore, companies should invest in thorough screening of new hires and restrict their authority during the initial stages of their employment.

iv. We shouldn't solely hold individuals accountable for these breaches; our computer systems should be equipped with automatic shutdown features that activate during any signs of malicious activity or data breaches.

v. Monitoring employees directly can also be an effective method. When it comes to protecting your company's confidential information, it's better to be overly cautious. This can be achieved through the use of security cameras or the implementation of keystroke logging.

By applying these insider threat detection techniques, we can enhance the security of confidential data within our organization. Failing to embrace these tactics might lead to financial losses amounting to thousands of dollars due to persistent cyber-attacks, especially those involving insiders resulting in data leakage from within the organization rather than external sources[61].

III. NEEDS/PROBLEMS

As the financial services industry becomes increasingly digital, institutions face a growing array of cyber threats that jeopardize customer data, business operations, and public trust. Although digital banking, fintech applications, and mobile payment systems offer unquestionable convenience, they also expand the opportunities for cybercriminals to attack. These threats—from phishing and ransomware to insider threats and AI-driven social engineering—are becoming more sophisticated and prevalent, making traditional security measures insufficient. Moreover, the interaction between internal vulnerabilities and external attacks creates a complicated risk environment, complicating efforts for financial institutions to effectively detect, prevent, and address breaches. The core challenge is to design and implement a proactive, comprehensive cybersecurity strategy that not only minimizes technical weaknesses but also takes into account human and systemic factors to uphold financial stability and foster customer confidence.

3.1 Goals/Objectives

To identify and examine the prevalent cyber threats that target the banking industry which inlcudes phishing schemes, ransomware, insider threats, DDoS attacks, and various other cybercrimes that jeopardize financial information and systems. We must assess the effectiveness of existing cybersecurity measures and technologies utilized by financial institutions. This includes authentication mechanisms, encryption standards, intrusion detection systems, firewalls, and AI-driven fraud detection.

Investigating the challenges of preserving customer privacy while enforcing advanced cybersecurity protocols which will emphasize Cybercrime encompasses unlawful activities carried out through the use of computers, networks, or digital devices. Such crimes can impact individuals, corporations, and government entities, leading to significant financial losses, data breaches, and damage to reputation. Common forms of cybercrime include hacking, identity theft, phishing schemes, malware attacks, ransomware, and online fraud. We are investigating the various cybercrimes that can occur and are currently occurring in the banking and finance sectors. The banking industry is undergoing a substantial digital transformation, integrating online services, mobile banking, and cloud technologies to enhance customer service and operational efficiency. However, this digital advancement has also rendered financial institutions more susceptible to a growing array of cyber threats. With issues such as phishing scams, ransomware attacks, data breaches, and risks from insiders, banks are now facing sophisticated adversaries who aim not only for monetary gain but also to disrupt critical infrastructure and diminish public trust.

As security measures become more intrusive and data-dependent, a new challenge emerges: how to protect user privacy while ensuring robust cybersecurity. Achieving the right balance between safeguarding sensitive financial data and respecting customers' privacy rights is not purely a technical concern, but also a legal and ethical one. Regulatory frameworks such as the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI-DSS), and various national data protection regulations add additional layers of compliance that banks must carefully navigate.

This research paper explores the evolving cybersecurity landscape within the banking sector, concentrating on the tension between security and privacy. It examines the tactics used by cybercriminals, evaluates existing defense mechanisms, and critically analyzes the implications of excessive surveillance and data gathering. Ultimately, the goal is to identify best practices that empower financial institutions to remain resilient against cyber threats while maintaining transparency, accountability, and customer trust in the digital era.ata collection, concerns regarding surveillance, and the ethical issues related to privacy-infringing technologies. Analyze the influence of regulatory frameworks on cybersecurity and data privacy practices within the banking sector. This involves evaluating GDPR, PCI-DSS, Basel III, and local cybersecurity regulations and their impact on compliance and operations. Develop a strategic framework for achieving a balance between cybersecurity and privacy in digital banking contexts that aims to provide recommendations and best practices for ensuring both strong security and responsible data management.

3.2 Procedures/Scope of Work

In our fast-paced, digital-centric society, the financial sector stands at the crossroads of technology and trust. With services ranging from online banking apps and mobile wallets to investment and insurance platforms, financial services are intricately integrated into our daily routines. However, this convenience carries a significant obligation: safeguarding sensitive financial information from cyber threats. As a result, cybersecurity in finance has emerged as a critical focus area in the digital era.

For the financial industry, cybersecurity involves much more than simply employing antivirus programs or creating strong passwords. It encompasses establishing and upholding a secure atmosphere where customers can transfer funds, apply for loans, invest, and settle bills without apprehension. Financial entities—ranging from conventional banks to contemporary fintech companies—manage vast amounts of personal information and conduct high-value transactions continuously. This positions them as prime targets for hackers, cybercriminals, and even state-sponsored actors.The threats they encounter are not only frequent but are also becoming more sophisticated each day. Cyber attackers leverage tactics such as phishing emails, ransomware assaults, counterfeit websites, insider threats, and specialized malware to infiltrate systems. Their objectives differ sometimes the aim is to directly steal money, while on other occasions it involves gathering sensitive data, engaging in fraud, or even creating disruption for political or competitive motives.When a financial institution experiences a cyberattack, the repercussions extend far beyond financial losses. It can result in stolen identities, frozen accounts, tarnished reputations, diminished customer trust, and severe penalties from regulatory bodies. In particular, when significant banks or stock exchanges are targeted, cyberattacks can undermine public confidence and potentially affect the broader economy.To better safeguard themselves, financial organizations are enhancing their security measures. They are implementing encryption for data protection, multi-factor authentication for login security, fraud detection systems to identify unusual patterns, and real-time monitoring to detect breaches as they occur.

The challenge is intensifying due to the rapidly evolving nature of financial service use. With mobile banking, digital wallets, contactless payments, and even blockchain solutions providing more methods to manage finances, there are also increased opportunities for hackers to exploit. As the potential vulnerabilities grow, financial institutions must remain ahead by employing tools like artificial intelligence, ethical hackers, and threat intelligence to anticipate and thwart emerging cyber threats.

Ultimately, cybersecurity in finance transcends mere technical concerns—it is a vital, trust-building imperative for businesses. In an era where data breaches dominate headlines and digital services become standard, safeguarding customers and their assets is imperative. As finance continues to advance and interconnect, robust cybersecurity will serve as a fundamental support pillar for the industry's future.

Internal Threats: It is often hard to detect because of authorized access. Risk increases with lack of monitoring.

External Threats: Frequently it can be technical exploits or social engineering. Can be mitigated with perimeter defenses and awareness training.

Combined Threats: It is very common, where external attackers collaborate with or exploit internal actors (knowingly or unknowingly).

Defense Strategies

To reduce internal threats within the banking and finance industry, it is important to apply the principle of least privilege; this means granting employees access solely to the systems and information necessary for their roles. Organizations should also track user activity for any suspicious or unauthorized behavior that could suggest insider misuse. Consistent training for employees is important to enhance their understanding of cybersecurity best practices and potential risks. Moreover, utilizing data loss prevention (DLP) solutions can assist in identifying and preventing the unauthorized transfer of sensitive data.

For external threats, financial organizations should implement robust protective measures like firewalls, antivirus applications, and intrusion detection systems (IDS) to guard against and identify cyber attacks. The adoption of multi-factor authentication (MFA) provides an additional level of security against unauthorized access. Keeping all software and systems updated with the latest patches is crucial for addressing known vulnerabilities. In addition, performing regular phishing exercises can help employees learn to identify and react properly to social engineering tactics.

Cyberattack Type	Internal	External	Both	Description
Phishing/Spear Phishing		✓		External attackers trick employees into revealing credentials or sensitive information.
Ransomware		✓	✓	Usually external, but can spread internally via employee actions or insider planting malware.
Insider Threats	✓		✓	Malicious or negligent employees misuse or expose sensitive data.
DDoS (Distributed Denial of Service)		✓		External actors overload bank servers to take systems offline.
Privilege Misuse/Abuse	✓		✓	Employees with elevated privileges misuse their access; can be exploited by external actors.
SWIFT Network Attacks			✓	Attackers exploit the international SWIFT system, often with inside help.
Third-Party/Vendor Attacks	✓	✓	✓	Breaches occur via compromised service providers or outsourced functions.

Cyberattack Type	Internal	External	Both	Description
ATM Malware Attacks	✓	✓	✓	Malware is injected physically or remotely; often needs insider assistance for deployment.
Business Email Compromise (BEC)	✓	✓	✓	External attackers impersonate executives, but success often requires insider knowledge.
Credential Stuffing		✓		Attackers use leaked credentials from other breaches to gain access to financial systems.

Table 3. Cyberattacks by Origin in Banking & Finance

3.3 Case Study

Case Study 1

The Capital One data breach (2019)

One of the leading credit card companies, Capital One, suffered a data breach that affected more than 100 million individuals. By taking advantage of a poorly configured open-source web application firewall (WAF), the hacker gained access to the network.This cyberattack occurred in several stages, enabling the attacker to retrieve data stored in an AWS S3 storage bucket. According to Capital One, personal information such names, addresses, postal codes, phone numbers, email addresses, birth dates, and reported income made up the majority of the exposed data. In addition, about 1 million Canadian social insurance numbers, 140,000 social security numbers, and 80,000 associated bank account details were made public. Credit scores, credit limits, account balances, payment histories, contact information, and partial transaction records were among the data that was made available to the public.

Fig 18. The capital one databreach

Capital One holds the position of the fifth largest bank in the United States, employing nearly 50,000 people and generating $32 billion in revenue. It was among the pioneers in transitioning from on-premises data centers to a cloud-based infrastructure. The individual behind the attack was not affiliated with a nation-state but was Paige Thompson, a former employee of AWS. She breached the network by developing a scanning tool designed to identify misconfigured firewalls within cloud infrastructures. Capital One was not the only institution she targeted;Additionally, she made data from more than 30 organizations—including both government and private organizations—public. The FBI was able to locate her GitHub repository and social media activity thanks to an anonymous email made to Capital One, which ultimately led to her capture.

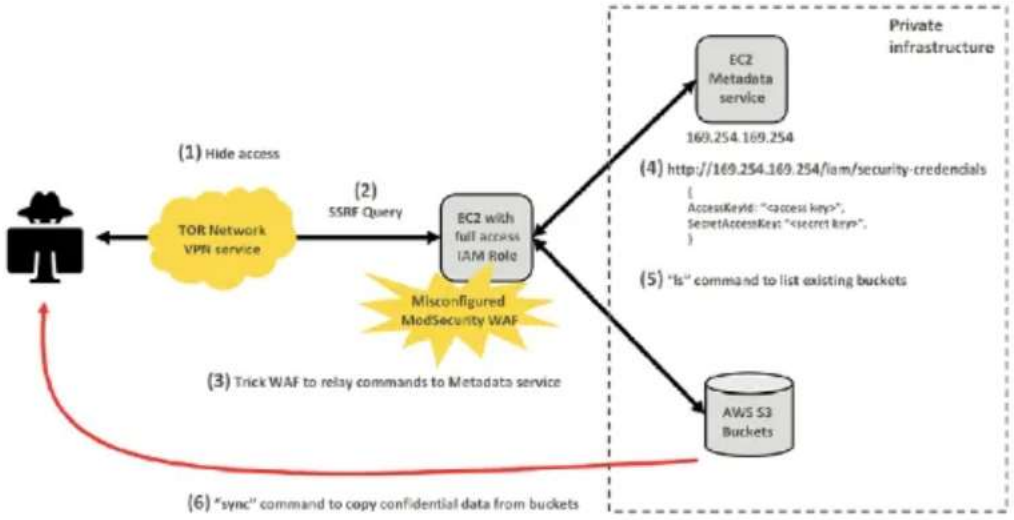


Fig 19 . Attack on AWS infrastructure

Figure 19 illustrates the method employed to infiltrate the system and extract data.

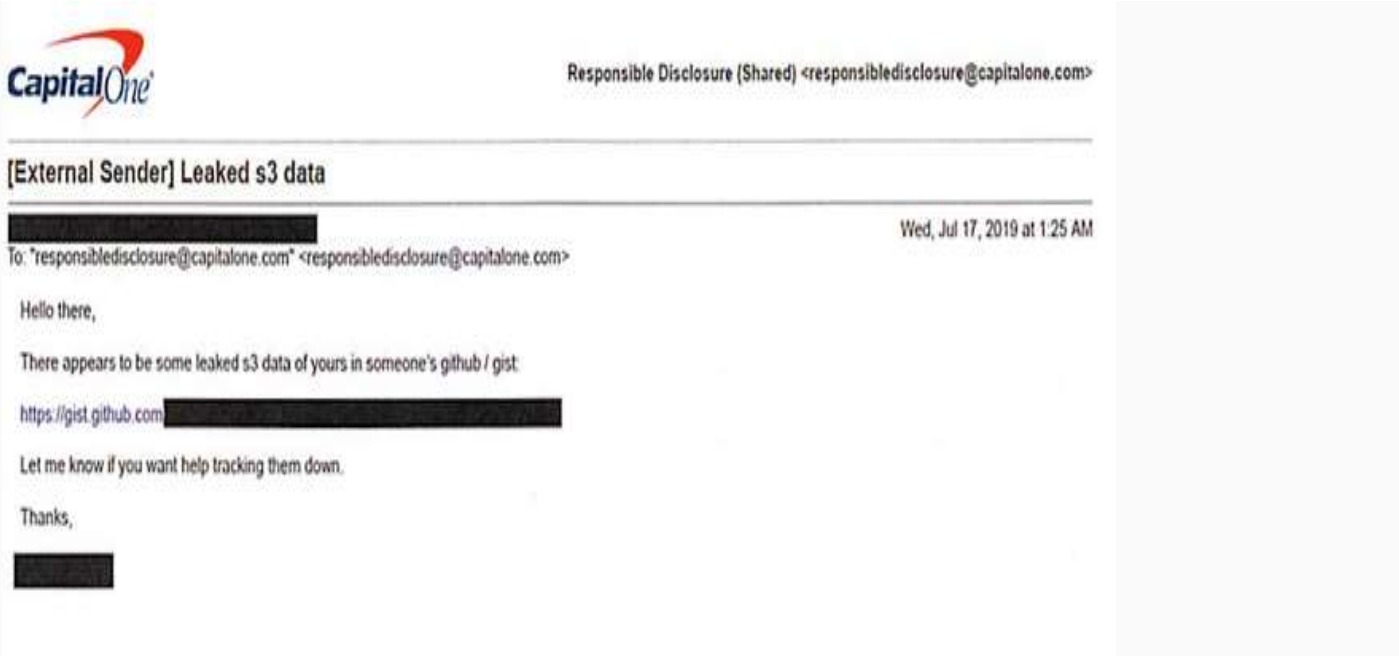
1. The hacker used anonymising technologies like TOR and VPN services to get access to the network.
2. They then carried out an attack known as server-side request forgery (SSRF), which tricked the server into carrying out commands that appeared to have come from a distant user.

3. A scanning tool later detected a poorly configured web application firewall (WAF) and sent commands to gain access to the AWS platform, which facilitated the retrieval of temporary credentials for the environment.
4. The combination of the SSRF attack and the WAF configuration error enabled the attacker to obtain valid credentials, allowing her to run commands through the AWS CLI.
5. She discovered that S3 buckets contained data.
6. She ultimately transferred 30 GB of client data among 700 distinct S3 buckets.

Response

Upon discovering the data breach, Capital One quickly took action to address the issues and notify customers regarding the security event. The promptness of this response can be attributed, in part, to the regulations and requirements within the financial industry that they are obligated to follow. Ultimately, they displayed quickness and openness about the security incident. They reached out to affected customers by sending notifications and providing two years of free credit monitoring and identity protection services. Due to the breach's extensive scope and seriousness, the hacker was quickly caught. This led authorities to uncover 30 additional security incidents associated with that individual. Throughout the process, Capital One was transparent and conducted a comprehensive review of the incident, which is incredibly useful.

Other businesses and people can use this knowledge to learn from past mistakes and make the required adjustments. Their website provides comprehensive information in the 2019 Cyber Incident Settlement, regular updates, and simple, unambiguous details concerning the data breach. Only after receiving an email tip from a member of the public did Capital One learn of the 106 million customer data leak.


Capital One

Responsible Disclosure (Shared) <responsibledisclosure@capitalone.com>

[External Sender] Leaked s3 data

[redacted] Wed, Jul 17, 2019 at 1:25 AM

To: "responsibledisclosure@capitalone.com" <responsibledisclosure@capitalone.com>

Hello there,

There appears to be some leaked s3 data of yours in someone's github / gist:

https://gist.github.com/[redacted]

Let me know if you want help tracking them down.

Thanks,

[redacted]

FIG. 20. AN EMAIL DATED JULY 17 NOTIFIED CAPITAL ONE THAT ITS DATA APPEARED TO HAVE BEEN COMPROMISED. CERTAIN INFORMATION WAS CONCEALED BY THE DEPARTMENT OF JUSTICE.

Prevention

In today's digital landscape, safeguarding your organization involves a proactive and extensive approach to cybersecurity. Begin by periodically assessing your cloud configurations—similar to verifying the security of your home—to make sure all digital "entrances and exits" are securely locked. Restrict employee access strictly to what is necessary for their job roles to minimize the risk of accidental or intentional misuse. Confirm that essential security tools like firewalls are not only appropriately set up but also regularly updated. Conducting routine security tests is crucial, serving as a health assessment to uncover system vulnerabilities before cybercriminals can exploit them. Remain alert to any unusual behavior within the organization, since threats can arise internally, and insider actions can be equally harmful. Encrypt critical information to prevent unauthorised individuals from accessing it, even in the event that it is intercepted or stolen. Adopting multi-factor authentication (MFA), which adds additional verification processes beyond passwords, can strengthen account security. Have a clear emergency response plan in place so that you can respond to a security breach promptly and efficiently. Finally, give your staff members continual cybersecurity training so they can identify phishing attempts and comprehend the significance of safeguarding private data.

Case Study 2

The Bangladesh Bank SWIFT attack (2016)

In 2016, a security breach at the Bangladesh Bank led to the loss of $81 million. This intricate attack is often considered the largest bank heist in history, later identified as the work of hackers with state backing. The scheme was carefully planned, starting a year prior to the actual theft of such a significant amount. It is suspected that employees of Bangladesh Bank received emails with seemingly harmless attachments that contained malware; once opened, these files released malicious software on the computers of the recipients. This granted the attackers access to the internal systems of the Bangladesh Bank. Concurrently, bank accounts were established globally in preparation for the later transfer of funds.

The attackers successfully infiltrated the SWIFT network via the Bangladesh Bank. The SWIFT network plays a crucial role in enabling international money transfers, and the aggressors displayed a deep knowledge of the system, indicating they may have executed similar schemes in the past. Gaining access to the SWIFT network permitted them to move funds from the Bangladesh Bank's account located in New York.

The operation was remarkably intricate, employing the various time zones relevant to global banking. Moving money from the Bangladesh Bank's New York account to banks in the Philippines required maneuvering through three separate time zones. The date was carefully planned so that the Bangladesh Bank would not be open on Thursday afternoon when the New York Federal Reserve began processing fraudulent wire transfer requests (since their weekend starts on Friday). The New York Fed was closed for the weekend when the Bangladesh Bank reopened on Sunday. Recognising this circumstance, the Bangladesh Bank attempted to contact Philippine banks, which were likewise closed because of the Chinese New Year. To increase the attackers' chances of success, the attack was purposefully carried out while banks were unable to communicate efficiently. It was too late by the time the concerned banks were able to get in touch.

Around $1 billion in transfer requests were made, but only $81 million was actually transferred since many requests were turned down by the New York Fed. Still, $81 million is a substantial amount. A part of the looted funds was quickly sent to a person in China, although the reason for this remains uncertain—potentially indicating their connection to the theft. It was necessary to launder the remaining funds, which were distributed to accounts across the globe, including those in Sri Lanka and the Philippines. In order to do this, the hackers transferred the funds to two Philippine casinos, where they played and eventually cashed out, thereby deleting any trace of the money.

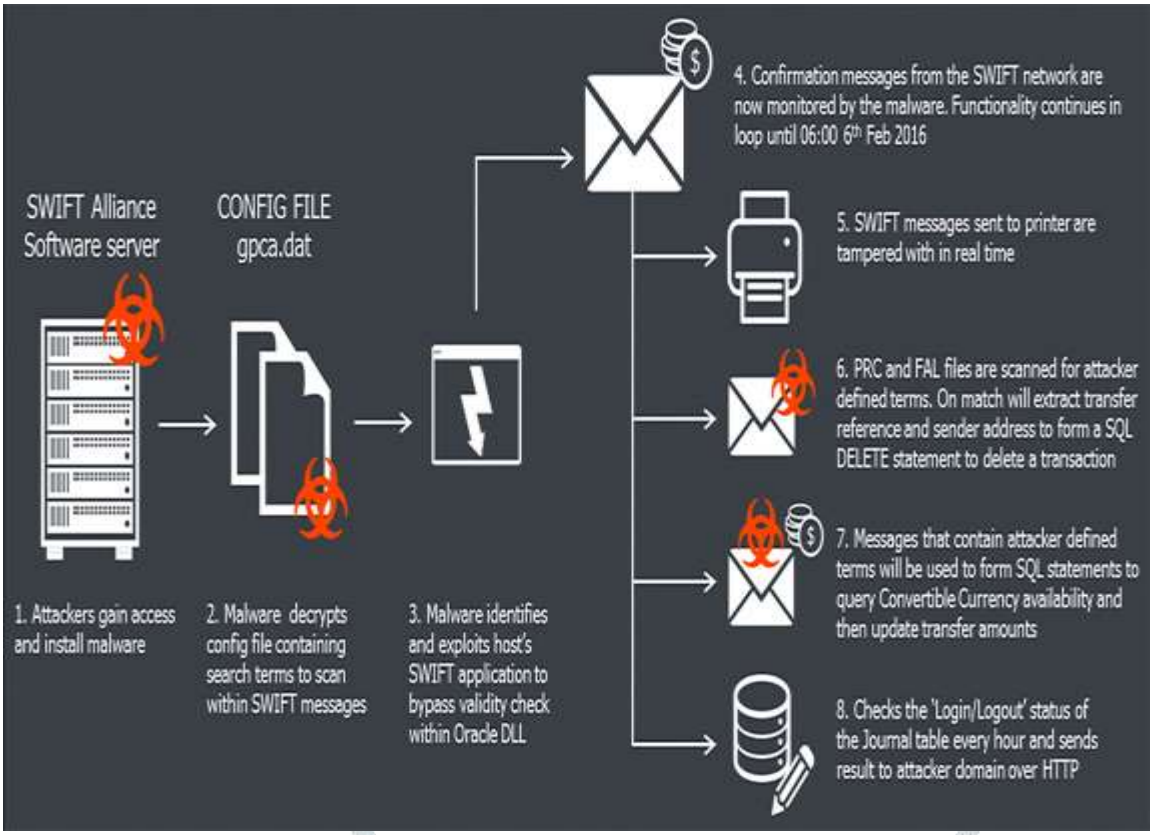


Fig21. How Bangladesh Bank's SWIFT software was hacked with malware.

The price of the violation

The attackers directed the Bangladesh Bank to release $951 million by taking advantage of the SWIFT network. $101 million worth of transactions were approved and carried out from the Bangladesh Bank's US Federal Reserve Bank of New York account. About $18 million of this total was finally recovered, of which $81 million was linked to the Philippines. Additionally, $20 million was linked to Sri Lanka; fortunately, the routing bank blocked it. For breaking banking laws and regulations, RCBC was fined roughly $52.92 million by the Bangko Sentral ng Pilipinas (BSP), the largest amount the BSP has ever imposed.
Dr. Atiur Rahman, a well-respected individual who was the Governor of Bangladesh Bank, resigned as a result of the government, media, and public of Bangladesh criticising the central bank for its failures after this incident. Following the incident, investigations were started in each of the participating countries to determine how the breach happened.
The Bangladesh Bank initially didn't know if its systems had been compromised. To manage the reaction to the security breach, carry out a vulnerability assessment, and carry out corrective actions, the governor of the central bank turned to the US-based company World Informatix Cyber Security. Mandiant, a forensic investigation agency, was hired by World Informatix Cyber Security to conduct the investigation. The investigators confirmed that there had been a system breach when they found evidence of malware and hackers. Additionally, they discovered that the hackers were not based in Bangladesh. The Bangladesh Bank opened an internal investigation on the matter.
According to Bangladesh Bank's forensic investigation, malware had entered the bank's systems in January 2016 and was collecting data on financial transfers and foreign payment procedures. The investigation also re-examined a hacking incident that occurred in 2013 at Sonali Bank, in which anonymous hackers took $250,000. According to reports, this crime featured illegal financial transfers over the SWIFT global payment network, just like the central bank loss that occurred in 2016. Before the remarkably identical 2016 robbery at the central bank was made public, Bangladeshi authorities had categorised this case as unresolved.
The Philippines' National Bureau of inquiry (NBI) has opened an inquiry into a Chinese-Filipino who is believed to have played a major role in money laundering. The nation's Anti-Money Laundering Council (AMLC) is one of the relevant government organisations with whom the NBI is working.
The AMLC started looking into a junket operator's bank accounts on February 19, 2016. A RCBC branch manager and five unidentified people who used fictitious identities in connection with the inquiry were the targets of a money laundering complaint that the AMLC submitted to the Department of Justice. On March 15, 2016, Senator Teofisto Guingona III, the head of the Congressional Oversight Committee and the Blue Ribbon Committee on the Anti-Money Laundering Act, led a Senate hearing. Then, on March 17, a closed session took place. An independent investigation was also initiated by the Philippine Amusement and Gaming Corporation (PAGCOR).

RCBC reportedly paid half of the ₱1 billion punishment levied by the Bangko Sentral ng Pilipinas (BSP) on August 12, 2016. The bank has already reorganised its board of directors, adding seven independent directors instead of the previous four. On January 10, 2019, a regional trial court in Makati City found former RCBC manager Maia Santos Deguito guilty of eight charges of money laundering and sentenced her to four to seven years for each count. Bangladesh Bank was accused by RCBC of participating in "a massive ploy and scheme to extort money from the plaintiff RCBC

through public defamation, harassment, and threats aimed at damaging RCBC's reputation and image" in a lawsuit filed against the bank on March 12, 2019.
Deguito's appeal was denied by the Court of Appeals' First Division on February 6, 2023, which upheld the Makati City Regional Trial Court's 2019 decision. The New York Supreme Court rejected three charges against Rizal Commercial Banking Corporation and defendants Ismael Reyes, Brigitte Capiña, Romualdo Agarrado, and Nestor Pineda in a decision pertaining to the February 29, 2024, Bangladesh Bank heist: conversion, aiding and abetting conversion, and conspiracy to commit conversion. The court cited a lack of personal jurisdiction. On other grounds, though, such as the recovery of funds, it allowed the lawsuit against Bangladesh Bank in relation to the $81 million cyber crime to proceed.
According to investigations, five Bangladesh Bank employees' carelessness caused computer system flaws that made it possible for malware to be installed. Subsequent enquiries revealed that these officials had introduced flaws in the system that allowed SWIFT transactions with the bank. Almost 100 Bangladesh Bank employees were interrogated, and several were barred from leaving the nation. Federal prosecutors in the United States have indicated that North Korea was engaged in the heist, despite the fact that the hackers have not been named.

Similar Incidents

The 2016 cyberattack on the Central Bank of Bangladesh was a very complicated and important event. Associated assaults consist of:

I. From 2013 to 2015, the Carbanak group, also called Anunak, targeted banks in the United States, Russia, and Ukraine, among other financial institutions worldwide. Millions of dollars were stolen by this gang, which first gained access to the banks' computers through spear-phishing techniques before using malware to track and alter their activities.
II. The Lazarus Group, which has been active since 2016 and is purportedly associated with North Korea, has participated in other cyberattacks against financial institutions, such as the Bangladesh Central Bank robbery.
III. A number of incidents have been connected to SWIFT, and the SWIFT system is constantly being attacked by hackers. One such example is the 2015 hack of Ecuador's Banco del Austro, in which hackers obtained the bank's SWIFT credentials and transferred money to multiple foreign accounts without authorisation.
IV. Financial institutions have been the target of cyberespionage and attacks by a number of Russian APT groups, including APT28 (Fancy Bear) and APT29 (Cosy Bear). These organisations are linked to a number of noteworthy events, such as attacks on financial institutions and banks.

Prevention

Prevention involves establishing a strategic, layered defense for systems that manage financial transactions. Start by treating crucial systems related to fund transfers—especially those linked to financial messaging platforms—as high-security areas, equipping them with strong, regularly updated antivirus solutions. Separate these vital networks from standard office networks to reduce the chance of malware spreading. Financial transfers should be monitored closely with real-time detection tools that identify suspicious activities and enforce multi-person approvals for sensitive transactions. Enhance login security by using additional identity verification methods, such as one-time codes or secure access devices, rather than relying solely on passwords. Access to core banking platforms should be limited to essential, well-trained staff, with comprehensive logs maintained to track user actions. Employees must receive regular training to recognize and respond to cyber threats like phishing and fraudulent communications, acting as the first line of defense. Conduct regular security evaluations and independent audits to identify vulnerabilities proactively. Each organization should also have a well-structured, actionable incident response plan in place to ensure prompt and effective measures in the event of an attack. Finally, aligning security measures with established frameworks like SWIFT's Customer Security Programme (CSP) aids institutions in adhering to industry standards and being better prepared against emerging threats.

Case Study 3

The LoanDepot ransomware attack (2024)

A ransomware attack that started on January 4 was made public by LoanDepot on January 8. The publicly traded company disclosed that hackers had broken into its network, encrypted data, and obtained unauthorised information. LoanDepot responded by taking a number of systems offline while it looked into the situation.

Founded in 2010 and based in Irvine, California, the company, often referred to as loanDepot, manages loans amounting to over $140 billion and has a workforce of around 4,500 employees. For the third quarter of 2023, the company announced revenue

of $266 million and an adjusted profit of $18 million.

Fig. 22Hackers using ransomware broke into the systems of LoanDepot, a major non-bank mortgage lender.

"This incident is the latest in a series of cyberattacks targeting the mortgage industry over the past six months, underscoring the urgent need for cybersecurity in mortgage practices," commented William Fricke, a senior credit officer at Moody's Investors Service, which evaluates residential mortgage-backed securities. In a filing to the U.S. Securities and Exchange Commission on Monday, LoanDepot first revealed the estimated number of victims of the data breach. The company stated that although its investigation is ongoing, it currently believes that the attackers obtained "sensitive personal information" belonging to roughly 16.6 million customers. LoanDepot stated that it will personally contact anyone impacted and provide them with free identity theft protection and credit monitoring services. Regarding whether it has linked the attack to a particular ransomware gang, whether a ransom was asked, and whether any ransom was paid in connection with the event, the business chose not to comment.
In order to look into and deal with the fallout from the attack, LoanDepot enlisted the help of outside cybersecurity and digital forensic specialists after the network breach and illegal access. The business said it is working to get its systems back up "as quickly as possible" and is posting updates on a special webpage. The business announced on Thursday that consumers may now manage or keep an eye on their online loan applications thanks to the restoration of its MyloanDepot client site.
The next day, it announced that both its customer portal and mobile application "are now entirely operational." LoanDepot had previously indicated that "recurring automatic payments continue to be processed as expected" and assured that it remains capable of accepting ACH payments. Customers had been venting on social media for days by the time LoanDepot admitted to the ransomware attack, expressing their annoyance at not being able to get in touch with the company—one of the largest mortgage lenders in the United States—or access its website or payment portal to make their mortgage payments.

The business suggested that consumers mail their payments or call its debt servicing contact centre as other options. Moody's stated that they were "closely monitoring" the attack on January 11 and that "it's possible
implications for around 50 Moody's-rated US RMBS transactions, where loanDepot manages part or all of the collateral." "Due to the cyber incident, borrowers are currently unable to access their online portal on the company's website, impacting their ability to make one-time payments through that portal," stated Fricke of Moody's at that time. "It remains uncertain what impact, if any, this may have on loan delinquency rates in the near future." This is not the first time that hackers have gained access to LoanDepot's servers and stolen information. The business revealed in May 2023 that hackers had obtained 1,361 clients' personal data in August 2022. Those impacted were notified immediately by LoanDepot that a small number of internal accounts had been accessed without authorisation, potentially leading to the theft of files containing Social Security numbers and other personal information.

Impact on employees

So far, no employees have publicly commented on the breach as of January 2024, apart from the statements issued by the company.

Impact on customers

In the proposed class-action lawsuit, customers asserted that the incident put them at a higher risk of fraud and identity theft.

Prevention

Routinely Backup Data

Regularly save copies of your critical files in a safe and distinct location to guarantee that you can recover everything if your systems are compromised.

Keep Software and Systems Current

Implement updates and security patches immediately when they become available to close vulnerabilities that cybercriminals may exploit.

Utilize Advanced Security Software

Employ threat detection applications to keep an eye on devices for suspicious or risky actions that could suggest a ransomware attack.

Be Wary of Emails

Educate employees to recognize phishing attempts and utilize email security solutions to filter out harmful communications and attachments.

Restrict User Access to Necessities

Ensure that employees only have access to the systems and data essential for their job functions. Confine administrative privileges to trusted individuals.

Isolate Critical Network Segments

Structure your network so that different departments or systems are separated. This measure hinders attackers from moving freely through your network.

Activate Multi-Factor Authentication

Implement an additional layer of login security to verify user identities with something beyond just a password.

Develop a Cyberattack Response Strategy

Formulate and practice a clear response plan to rapidly address and recuperate from a ransomware incident without paying the attackers.

Encrypt Confidential Information

Utilize encryption to safeguard sensitive data. If attackers gain access, they won't be able to utilize it without the decryption keys.

Monitor Network Activity Continuously

Keep a close watch on all system activities to identify abnormal behavior early. This approach assists in detecting ongoing attacks and enables a response before they escalate.

CASE STUDY 4

Phishing Attack Powered by AI on an Indian Financial Institution (2024)

As artificial intelligence technology progresses, its usage in cybercrimes globally has become increasingly prominent, especially within financial institutions. This report analyzes a significant event that took place in early 2024, where a notable Indian bank fell prey to a sophisticated phishing attack enhanced by AI. The assault utilized AI's natural abilities in data analysis and persuasive techniques, leading to a serious compromise of the bank's internal systems. The perpetrators employed AI to design messages that closely mirrored the internal communications shared among employees. By evaluating content from social media platforms like Facebook and Twitter, blog posts, LinkedIn connection histories, and the email styles of the bank's

executives, the AI was meticulously refined to imitate these emails. Several of these correspondences included formal formatting, specialized internal jargon, and the CEO's distinct writing style, which enhanced their believability. In addition, it featured phishing emails containing links that directed users to a fraudulent internal portal intended to capture their login credentials. Given their sophistication, the targeted individuals perceived the emails as legitimate and willingly entered their login details into the bank's system, thereby allowing the attackers access. The incident had a profound effect on the bank across all sectors. Numerous executives fell victim to phishing emails, leading to the compromise of several financial databases housing customer account and transaction records. This breach enabled criminals to disrupt various online services of the financial institution, resulting in operational interruptions for several days for both the bank and its clients. Moreover, they suffered a significant loss of customer confidence as the breach revealed the bank's vulnerabilities to contemporary cyber threats. Besides addressing immediate operations to mitigate the breach, the financial institution was also confronted with a long-term reputational damage.

Technical Analysis and Findings:

1. The AI techniques employed in generating phishing emails are as follows:
Advanced natural language processing (NLP) technologies were used in the attack; these technologies were probably based on large-scale transformer models such as GPT (Generative Pre-trained Transformer). To produce convincingly realistic emails, these models are trained on large datasets using examples from emails, social media, and daily language.

Key Technical Features:

Contextual Understanding: The AI adeptly considered the context of earlier communications and created follow-up emails that seamlessly matched previous discussions.

Style Mimicry: The AI replicated the writing style of the CEO by analyzing existing emails and extrapolating elements such as tone, language, and signature format.

Adaptive Learning: The AI evolved based on past mistakes and feedback, modifying the generated emails for future attempts, making detection more difficult.

2. Advanced Spear-Phishing Tactics

This attack was not an ordinary phishing scheme; it employed spear-phishing, concentrating on specific individuals through personalized emails. The AI applied social engineering techniques that significantly improved the chances of particular recipients responding to certain emails based on machine learning algorithms.

Key Technical Features:

Targeted Data Harvesting: The attackers pinpointed the organization's employees and sent focused messages by collecting information from publicly available profiles and messaging services.

Behavioral Analysis: The AI examined recent user behavior patterns from social networks and other online platforms to anticipate probable actions, such as clicking links or opening attachments.

Real-Time Adjustments: There were occasions when the AI assessed the need for responses to phishing emails, modifying the timing and content of subsequent emails accordingly.

3. Enhanced Evasion Strategies

The attackers effectively carried out this operation by utilizing AI to bypass typical filters employed in email systems. These methods involved altering the content of the emails in such a way that they went unnoticed by spam filters while preserving the message's core meaning.

Key Technical Features:

Dynamic Content Modification: The AI made subtle adjustments to various parts of the email message to produce different versions of the phishing email, which in turn compromised various detection algorithms.

Polymorphic Attacks: In this case, polymorphic code was utilized during the phishing attack, signifying that the actual payloads of the links changed frequently, making it harder for antivirus software to recognize and block these as threats.

Phantom Domains: Another tactic used involved the AI generating and distributing phantom domains, which are seemingly legitimate websites that are transient and created solely for this phishing attempt, increasing detection difficulties.

4. Exploitation of Human Vulnerabilities

The effectiveness of this type of attack is not only due to AI but also to human weaknesses, a dependency on familiar phrasing, and the tendency to comply with authority figures.

Key Technical Features:
Social Engineering: With regard to the second component, artificial intelligence identified specific psychological concepts—particularly those of familiarity and urgency—that ought to be used to increase the likelihood that the intended recipients will engage with phishing emails.
Multi-Layered Deception: The AI was able to successfully execute a two-part strategy in which the emails were designed to guarantee that, after the targeted individuals opened the first one, they would subsequently receive a second one that was posing as a follow-up message from a genuine business or individual.

Prevention

1. Enhanced Email Security Measures

AI-Driven Email Screening: Implement security measures that detect and block phishing emails through behavioral analysis, natural language processing, and pattern recognition.

Attachment & Link Evaluation: Automatically assess links and attachments in a secure sandbox before they reach users.

2. Staff Training & Awareness

Simulated Phishing Drills: Regularly conduct tests with realistic phishing emails to assess and improve employee awareness.

Deepfake Education: Educate employees about manipulation techniques involving voice and video in deepfake phishing attacks.

Incident Reporting Encouragement: Promote a culture where employees can report suspicious emails or requests without fear of repercussions.

3. Multi-Factor Authentication (MFA)

Mandate MFA across all internal platforms, especially when accessing sensitive information and performing financial transactions.

Consider phishing-resistant MFA solutions such as hardware tokens (e.g., YubiKeys) or biometric verification.

4. Identity and Access Management (IAM)

Role-Based Access Control (RBAC): Limit access to critical systems and data only to those who need it.

Zero Trust Framework: Continuously authenticate every user and device trying to access resources.

5. Threat Intelligence and Surveillance

Subscribe to real-time threat intelligence alerts that inform you of new phishing tactics or campaigns.

Utilize Security Information and Event Management (SIEM) systems to spot unusual user behavior or network trends.

6. AI Against AI Security

Utilize your own AI and machine learning models to detect patterns in vast quantities of communication that may evade human recognition.

Train models to identify indicators of social engineering, such as urgency, fear-inducing language, or false authority.

7. Policy and Compliance Adherence

Develop and routinely update cybersecurity policies in line with RBI, CERT-IN, and international standards like ISO 27001 or NIST.

Conduct regular penetration tests and third-party assessments to identify weaknesses.

8. Incident Response Strategy

Establish a comprehensive incident response plan for phishing incidents, outlining steps for containment, recovery, and customer notification.

Case Study 5

JPMorgan Chase Breach (2014)

The issue of cyberattacks is becoming more pressing as technological advancements continue. Attention to this matter is increasing, as cybercrimes have risen to the forefront of priorities for law enforcement. A particularly notable recent cyberattack targeted JPMorgan Chase, one of the leading banking firms in the country that offers financial services in over 100 locations. With a legacy of more than two hundred years, it is not surprising that JPMorgan Chase caters to millions of clients, including individuals, businesses, institutions, and government bodies (JPMorgan Chase & Co., 2017).

In the summer of 2014, specifically during July and August, the company faced multiple cyberattacks. As a result, a significant amount of data was compromised, including information regarding checking and savings accounts. This breach affected over 80 million households and small businesses. The exposure of their account information raised serious security concerns within JPMorgan Chase. Fortunately, there were no signs of fraud or misuse of the compromised data. The hackers primarily accessed email addresses, home addresses, and phone numbers, which are generally not viewed as highly sensitive since such information is readily available to the public.

The attack initially began in the spring about two years earlier. Experts believe that the hackers first acquired the login credentials of a bank employee, allowing them to penetrate the network and retrieve customer contact information. However, the bank only became aware of the breach in August when its sponsors were also targeted. Ultimately, this group of criminals managed to compromise more than 90 servers belonging to JPMorgan Chase. Nonetheless, they were captured before they could access sensitive financial information of customers.

The company faced challenges in securing its network due to its interconnection with customer networks. Experts suggest that the attack could have been prevented at an early stage had the system been better protected. One of the bank's network servers was neglected and had unaddressed vulnerabilities. The failure to update its software left it vulnerable. A more advanced authentication method could have helped alleviate this problem.

The precise source of this cyberattack remains unknown; however, Goldstein, Perlroth, and Corkery (2014) indicated that both Russia and Brazil were being investigated. The rationale for suspecting Brazil as the origin of the attack was not revealed and lacked corroborating evidence. Nonetheless, Russia was viewed as a potential adversary given the economic sanctions imposed and U.S. involvement in matters related to Russia and Ukraine. Ultimately, however, the FBI announced that Russia was not culpable. I think this hypothesis seemed somewhat credible, although it was weakened by insufficient evidence.

Regardless of the perpetrating nation, the operation was complex and well-organized, despite not employing any groundbreaking software exploits. If Russia was indeed responsible for the attack, it may have been an attempt to weaken U.S. influence in global affairs, particularly in relation to Ukraine. Given that the U.S. is a key player in the global market and a principal supporter of other nations, Russia might have believed that by targeting one of its major banks, it could divert U.S. attention inward and away from international issues. In doing so, Russia could have sought to bolster its own power and influence, aiming to eclipse the U.S. and establish itself as a future world leader.

Nevertheless, it cannot be asserted that the attack was a success. While many bank clients were affected, the accessed information was not critical and did not provide the hackers with the ability to adversely impact them.

In addition, the investigation did not reveal any cases of fraud, which supports this viewpoint. While other organizations were targeted by the same group, the actions of the adversary prompted the U.S. to focus on internal matters. However, the level of threat was insufficient to divert attention away from international issues.

Consequences and Actions Taken

JPMorgan has significantly increased its cybersecurity budget to $500 million.

All critical systems will now utilize two-step verification.

Improved technologies for detecting anomalies have been implemented.

Network segmentation is in place, along with enhanced training for employees.

Prevention

To prevent a cyberattack akin to the 2014 JPMorgan Chase incident, numerous vital cybersecurity practices should be established. That breach exploited fundamental security gaps, notably the lack of two-factor authentication and other vulnerabilities within the network. Below is a summary of essential preventative measures financial organizations can adopt:

1. Strong Access Controls

Implement Multi-Factor Authentication (MFA) across all systems, especially for admin access.

Adhere to the Principle of Least Privilege (PoLP): Users should only have access to the data and systems required for their specific functions.

2. Enhancing and Segmenting Networks

Segment internal networks to restrict lateral movement if intruders breach the system.

Fortify servers and endpoints by disabling unnecessary services and closing inactive ports.

3. Regular Security Audits and Penetration Testing

Conduct routine vulnerability assessments and penetration tests to identify and remediate weaknesses.

Employ both automated scanning tools and manual evaluations for thorough assessment.

4. Endpoint Detection and Response (EDR)

Adopt EDR solutions that provide real-time monitoring and reactive capabilities.

Detect unusual activities such as atypical login locations, elevated privileges, or large-scale data access attempts.

5. Secure Integrations with Third Parties

Carefully evaluate third-party vendors and impose stringent security standards.

Use contractual requirements to ensure that vendors comply with cybersecurity best practices.

Embrace Zero Trust Architecture, which assumes that no user or device is automatically trustworthy.

6. Comprehensive Security Protocols and Training

Continuously train employees on phishing, social engineering, and secure access practices.

Establish cyber hygiene policies (e.g., regular password changes, device encryption, secure remote operations).

7. Immediate Monitoring and Incident Response

Utilize Security Information and Event Management (SIEM) systems for instant analysis of security notifications.

Maintain a well-structured incident response plan and regularly test it through exercises.

8. Management of Patches and Software Updates

Ensure that all systems, particularly critical servers, receive the latest security updates.

Whenever possible, use automated tools for patch management.

9. Data Protection and Encryption

Encrypt sensitive information both during storage and transmission.

Monitor data flows to detect unauthorized access or data exfiltration attempts.

10. Compliance with Regulations and Frameworks

Ensure that security practices conform with established frameworks such as:

NIST Cybersecurity Framework

ISO/IEC 27001

FFIEC (for financial institutions within the U.S.)

RESEARCH METHODOLOGY

This research utilizes a case study analysis to investigate the impact of cyberattacks on the banking and financial sectors, focusing specifically on the various types of threats, the strategies employed in response, and the implications for security and privacy. The case study approach allows for a comprehensive examination of real cybersecurity incidents and the organizational reactions that resulted. Numerous cyberattacks have occurred globally. The selected notable cases of cyberattacks were chosen due to their magnitude, effect, and relevance to ongoing cybersecurity challenges within banking and finance.

REFERENCES

1. CYBERCRIME AND YOU: HOW CRIMINALS ATTACK AND THE HUMAN FACTORS THAT THEY SEEK TO EXPLOIT BY JASON R. C. NURSE. HTTPS://ARXIV.ORG/PDF/1811.06624
2. T. ur Rehman, "Cybersecurity for E-Banking and E-Commerce in Pakistan: Emerging Digital Challenges and Opportunities," Handbook of Research on Advancing Cybersecurity for Digital Transformation, T. ur Rehman, pp. 163-180, 2021.
3. Securing Financial Information in the Digital Age: An Overview of Cybersecurity Threat Evaluation in Banking Systems. Md Abdullah Al Mahmud, Jannatul Ferdous mou, Al Modabbir Zaman, Sweety Rani Dhar, Anupom Debnath, Sadia Sharmin, Mahafuj Hassan,2025. https://ecohumanism.co.uk/joe/ecohumanism/article/view/6526
4. Ali, L., Ali, F., Surendran, P. and Thomas, B., 2017. The effects of cyber threats on customer's behaviour in e-Banking services. International Journal of e-Education, e-Business, eManagement and e-Learning, 7 (1), 70-78 https://www.ijeeee.org/vol7/414-IM023.pdf
5. CYBER RISK AND THE U.S. FINANCIAL SYSTEM: A PRE-MORTEM ANALYSIS. HTTPS://WWW.NEWYORKFED.ORG/RESEARCH/STAFF_REPORTS/SR909.HTML.
6. CYBERSECURITY COMPLIANCE IN FINANCIAL INSTITUTIONS: A COMPARATIVE ANALYSIS OF GLOBAL STANDARDS AND REGULATIONS. HTTPS://DOI.ORG/10.30574/IJSRA.2024.12.1.0802
7. CYBERSECURITY IN U.S. AND NIGERIA BANKING AND FINANCIAL INSTITUTIONS:REVIEW AND ASSESSING RISKS AND ECONOMIC IMPACTS. HTTP://DOI.ORG/10.26480/AIM.01.2023.54.62
8. CYBERSECURITY IN DIGITAL BANKING: SAFEGUARDING CUSTOMER TRUST IN UZBEKISTAN. HTTP://EPRINTS.UMSIDA.AC.ID/14284/1/13-18%2BCYBERSECURITY%2BIN%2BDIGITAL%2BBANKING%2BSAFEGUARDING%2BCUSTOMER%2BTRUST%2BIN%2BUZBEKISTAN.PDF
9. QUANTIFYING THE FINANCIAL IMPACT OF CYBER SECURITY ATTACKS ON BANKS: A BIG DATA ANALYTICS APPROACH. HTTPS://WWW.RESEARCHGATE.NET/PUBLICATION/375009516_QUANTIFYING_THE_FINANCIAL_IMPACT_OF_CYBER_SECURITY_ATTACKS_ON_BANKS_A_BIG_DATA_ANALYTICS_APPROACH
10. A LITERATURE REVIEW OF FINANCIAL LOSSES STATISTICS FOR CYBER SECURITY AND FUTURE TREND HTTPS://WWW.RESEARCHGATE.NET/DEREF/HTTPS%3A%2F%2FDOI.ORG%2F10.30574%2FWJARR.2022.15.1.0573?_TP=EYJJB250ZXH0IJP7IMZPCNN0UGFNZSI6INB1YMXPY2F0AW9UIIWICGFNZSI6INB1YMXPY2F0AW9UIIWICG9ZAXRPB24IOIJWYWDLQ29UDGVUDCJ9FQ
11. REPUTATIONAL RISKS IN BANKS: A REVIEW OF RESEARCH THEMES, FRAMEWORKS, METHODS, AND FUTURE RESEARCH DIRECTIONS. HTTPS://PAPERS.SSRN.COM/SOL3/PAPERS.CFM?ABSTRACT_ID=3844453
12. THE IMPACT OF CYBER ATTACKS ON FINANCIAL INSTITUTIONS AND THE NEED FOR IMPROVED SECURITY MEASURES.
13. ASSESSING THE INFLUENCE OF CYBERSECURITY THREATS AND RISKS ON THE ADOPTION AND GROWTH OF DIGITAL BANKING. HTTPS://WWW.RESEARCHGATE.NET/PUBLICATION/390058447_ASSESSING_THE_INFLUENCE_OF_CYBERSECURITY_THREATS_AND_RISKS_ON_THE_ADOPTION_AND_GROWTH_OF_DIGITAL_BANKING_A_SYSTEMATIC_LITERATURE_REVIEW_CITATION
14. PHISHING ATTACKS: A RECENT COMPREHENSIVE STUDY AND A NEW ANATOMY. HTTPS://DOI.ORG/10.3389/FCOMP.2021.563060
15. STATE OF THE PHISH. HTTPS://WWW.PROOFPOINT.COM/SITES/DEFAULT/FILES/GTD-PFPT-US-TR-STATE-OF-THE-PHISH-2020.PDF

16. Study on Phishing Attacks. https://www.researchgate.net/publication/329716781_Study_on_Phishing_Attacks
17. Heterogeneity in cyber loss severity and its impact on cyber risk measurement. https://link.springer.com/article/10.1057/s41283-022-00095-w#Sec1
18. Arcuri, M.C.; Brogi, M.; Gandolfi, G. Cyber risk: A big challenge in developed and emerging markets. In Identity Theft: Breakthroughs in Research and Practice; IGI Global: Hershey, PA, USA, 2016; pp. 292–307. [Google Scholar]
19. Aydin, F.; Pusatli, O.T. Cyber attacks and preliminary steps in cyber security in national protection. In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications; IGI Global: Hershey, PA, USA, 2018; pp. 213–229. [Google Scholar]
20. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput. Secur. 2021, 105, 102248. [Google Scholar] [CrossRef]
21. Edwards, B.; Hofmeyr, S.; Forrest, S. Hype and heavy tails: A closer look at data breaches. J. Cybersecur. 2016, 2, 3–14. [Google Scholar] [CrossRef] [Green Version]
22. Poremba, S. The Cyber-Risk Paradox: Benefits of New Technologies Bring Hidden Security Risks; Security Boulevard: Boca Raton, FL, USA, 2019. [Google Scholar]
23. Adeosun, L.P.K.; Ganiyu, R.A. Corporate reputation as a strategic asset. Int. J. Bus. Soc. Sci. 2013, 4, 220–225. [Google Scholar]
24. FireEye. M-Trends Report 2021; FireEye, Inc.: Milpitas, CA, USA, 2021. [Google Scholar]
25. Raineri, E.M.; Resig, J. Evaluating Self-Efficacy Pertaining to Cybersecurity for Small Businesses. J. Appl. Bus. Econ. 2020, 22, 13–23. [Google Scholar]
26. A Study on the Customer Awareness on Security Issues and Threats in Digital Banking in Chennai.Dr. Sankararaman G1 , Dr. Suresh S2 , Dr Thirumagal PG3 , Priyadharshini V4 and Dr. Rengarajan.
27. Cyberattacks, Operational Disruption, and Investment inResilience Measures. https://pubsonline.informs.org/doi/epdf/10.1287/mnsc.2022.00430
28. CYBERSECURITY REGULATION IN THE FINANCIAL SECTOR: PROSPECTS OF LEGAL HARMONISATION IN THE EU AND BEYOND. https://dx.doi.org/10.2139/ssrn.3533664
29. Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends. https://doi.org/10.1016/j.techsoc.2021.101734
30. 2024 Identity Fraud Study: Resolving the Shattered Identity Crisis. https://javelinstrategy.com/research/2024-identity-fraud-study-resolving-shattered-identity-crisis
31. Cybersecurity in Banking and Financial Services: Protecting Digital Transactions and Combating Identity Theft and Fraud. https://ijrpr.com/uploads/V6ISSUE1/IJRPR37656.pdf
32. The Ties That Bind: A Framework for Assessing the Linkage Between Cyber Risk and Financial Stability. https://www.capco.com/Capco-Institute/Journal-53-Operational-Resilience/The-Ties-That-Bind?utm_source=chatgpt.com
33. COPING WITH CYBERCRIME VICTIMIZATION: AN EXPLORATORY STUDY INTO IMPACT AND CHANGE.
34. Strengthening cyber resilience in financial institutions: A strategic approach to threat mitigation and risk management.
35. A Review of Ransomware Attacks and its Impact on the Bank Sector. https://www.ijfmr.com/papers/2024/3/21458.pdf
36. Ransomware: Lessons Learned by Banks That Suffered an Attack. https://www.csbs.org/sites/default/files/other-files/Ransomware%20Lessons%20Learned%20by%20Banks%20That%20Suffered%20an%20Attack%20-%20Final%2023.10.24.pdf
37. Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques. https://www.academia.edu/127537558/Anatomy_of_Ransomware_Attack_Stages_Patterns_and_Handling_Techniques
38. Definitive guide to ransomware 2022. https://leadcomm.com.br/wp-content/uploads/2022/06/Definitive-guide-to-ransomware-2022.pdf
39. A Srivastava, B B Gupta, A Tyagi, Anupama Sharma, and Anupama Mishra. A Recent Survey on DDoS Attacks and Defense Mechanisms. Technical report, 20.
40. Catalin Cimpanu. DDoS botnets have abused three zero-days in LILIN video recorders for months. https://tinyurl.com/c32ja6w, 2020.
41. The role of Blockchain in DDoS attacks mitigation : techniques, open challenges and future directions. http://arxiv.org/pdf/2202.03617
42. DDoS: Here to Stay. https://www.fsisac.com/hubfs/Knowledge/DDoS/FSISAC_DDoS-HereToStay.pdf
43. Modern DDoS Threats and Countermeasures: Insights into Emerging Attacks and Detection Strategies. https://arxiv.org/pdf/2502.19996
44. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. https://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/DDoSmirkovic.pdf

45. Analysis: Attacking and Defending Swift Systems. https://www.withsecure.com/content/dam/with-secure/en/resources/withsecure-consulting-analysis-attacking-and-defending-swift-systems-en.pdf
46. Saud Al-Musib, N.; Mohammad Al-Serhani, F.; Humayun, M.; Jhanjhi, N. Business email compromise (BEC) attacks. Mater. Today Proc. **2021**, 81, 497–503. [**Google Scholar**] [**CrossRef**]
47. Europol. Internet Organized Crime Threat Assessment Report. 2020. Available online:**https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020** (accessed on 25 April 2023).
48. Maleki, N. A Behavioral Based Detection Approach for Business Email Compromises. Available online: **https://unbscholar.lib.unb.ca/islandora/object/unbscholar%3A10122** (accessed on 25 April 2023).
49. Yasin, A.; Fatima, R.; Liu, L.; Yasin, A.; Wang, J. Contemplating social engineering studies and attack scenarios: A review study. Secur. Priv. , 2, e73. [**Google Scholar**] [**CrossRef**]
50. Bazzell, M. Open Source Intelligence Techniques: Resources for Searching and Analyzying Online Information, 9th ed.; Amazon Digital Services: London, UK, 2022. [**Google Scholar**]
51. Bitdefender. GravityZone Email Security Repor. 2019. Available online: **https://www.bitdefender.com/content/dam/business/b2b/white-papers/Bitdefender-GravityZone-Email-Security-Report.pdf** (accessed on 25 April 2023).
52. Teerakanok, S.; Yasuki, H.; Uehara, T. A Practical Solution Against Business Email Compromise (BEC) Attack using Invoice Checksum. In Proceedings of the 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C), Macau, China, 11–14 December 2020; pp. 160–167. [**Google Scholar**] [**CrossRef**]
53. Choi, R.Y.; Coyner, A.S.; Kalpathy-Cramer, J.; Chiang, M.F.; Campbell, J.P. Introduction to Machine Learning, Neural Networks, and Deep Learning. Transl. Vis. Sci. Technol. **2020**, 9, 14. [**Google Scholar**] [**CrossRef**]
54. Atlam, H.F.; Oluwatimilehin, O. Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review. Electronics **2023**, 12, 42. [**Google Scholar**] [**CrossRef**]
55. HHS Cybersecurity Program. (2019). Credential stuffing. https://www.hhs.gov/sites/default/files/credential-stuffing.pdf
56. Security Intelligence. (2021). The state of credential stuffing attacks. https://securityintelligence.com/articles/credential-stuffing-attacks-2021/[3]
57. N. K., et al. (2023). AI in cybersecurity: Threat detection and response with machine learning. Tuijin Jishu/Journal of Propulsion Technology, 44(3), https://doi.org/10.52783/tjjpt.v44.i3.237[4]
58. Artificial Intelligence and Advanced Cybersecurity to Mitigate Credential-Stuffing Attacks in the Banking Industry. https://ijcesen.com/index.php/ijcesen/article/view/754/557
59. Preventing Insider Threats in the Financial Sector: A Zero-Trust Approach.
60. Credential Stuffing Attack: Countermeasures using Patterns and Machine Learning. https://www.irjet.net/archives/V9/i9/IRJET-V9I9203.pdf
61. A systematic literature review on insider threats. https://doi.org/10.48550/arXiv.2212.05347