IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

The impact of cyber attacks on financial institutions and the need for improved security measures.

Advay Khemka
Student
Pathways School, Noida

Abstract
The effects of cyber attacks on banks are investigated in depth in this research paper. Real-world instances of major cyber assaults on financial institutions have been examined, along with their financial, legal, and reputational fallout. Financial institution security measures also have been examined to determine their efficacy in reducing cyber threats. The study stressed the need to bolster security measures to meet the challenges of the ever-changing cyber threat scenario. Artificial intelligence, machine learning, and behaviour analytics have been discussed, along with other cutting-edge technologies and approaches that can potentially improve cybersecurity. To share information and best practices, the paper will also examine the value of cooperation among financial institutions, industry regulators, and cybersecurity professionals.

Table of Content

1.0 Introduction

Financial institutions now face constant danger from cyber attacks, which pose serious hazards to their operations, client data, and general financial stability. Increasingly complex and persistent cyber risks are a reality for the financial sector as the digital world develops. This research paper aims to investigate the effects of cyber assaults on banking institutions and the urgent need for better security measures to cope with these threats. Since so much money and sensitive information is at stake, cybercriminals have placed their sights on financial organisations, including banks, insurance companies, and investment corporations. Financial losses, lost client data, failure to comply with regulations, and reputational harm result from successful cyber attacks on these organisations.

2.0 Cyber Attacks' growth acceleration

In recent years, cyber dangers to financial institutions have multiplied. The number of cyberattacks that were state-sponsored and targeted the financial sector rose. These assaults were a part of the overall number of cyberattacks. The attack escalated in terms of frequency, level of sophistication, and level of destruction (Tawalbeh *et al.* 2020). The epidemic and a growing dependence on distant services were the primary contributors to cyberattacks' unanticipated and fast expansion (Hijji and Alam, 2021).

Hackers have their sights set on the financial services sector. According to the findings of the Modern Bank Heist 3.0 study, eighty per cent of the financial institutions polled have seen an increase in the number of cyberattacks (a thirteen per cent rise from 2019) (Tom Kellermann *et al.* n.d.). The poll of financial institutions found that 82 per cent of them believe that cybercriminals have gotten more clever and that malware is employed in longer and more complicated campaigns (Gabriel Bassett *et al.* 2021).

According to the findings of yet another study, the financial services sector was disproportionately impacted by ransomware assaults. The rise from the previous year to the beginning of the second half of 2021 was 1,318 per cent (M. Henriquez, 2021). The end goal is to leverage native operating system tools to remain invisible or gain a foothold on one system to island hop to a larger, more lucrative target," says the poll that was conducted for the Modern Bank Heist. Attackers enter a network and then utilise that network as a springboard to bounce into an affiliated network; in other instances, these systems exploit the supply-chain partners (Salahdine and Kaabouch,2019).

As per the research conducted by the Cyber Security Centre of the UK Government (2017), it was found that approximately 50% of companies in the United Kingdom experienced cyber breaches or attacks in the previous year (Al-Alawi *et al.* 2020). Notwithstanding this, the UK Government has committed to allocating $2.5 billion towards safeguarding the nation against cyber threats, aiming to enhance preparedness and establish the UK as the most secure environment for online activities and commerce (Al-Alawi *et al.* 2020). It is imperative for institutions to safeguard digital consumer data proactively. The organisation offers various cyber programmes to raise awareness, including e-Training, foundational cyber courses, and complimentary consultations.

3.0 Attack vectors

3.1. Social engineering and phishing

Phishing and social engineering are two of the most popular attack vectors. Phishing attacks directed at specific customers comprise the largest portion of these attacks. In most instances, the clients themselves are approached by hackers so that they verify their account information (Abraham *et al.* 2019). The employee-specific phishing attack comes next. According to Eurofins and personal experience, employee-targeted phishing attempts have grown since the pandemic due to the spread of remote working and the increased workload that directly or indirectly resulted from the epidemic (Bada and Nurse, 2020).

3.2. Ransomware attacks

During the last year, there was also a rise in the number of ransomware assaults. These assaults continue to be the third most typical kind of cybercrime. According to Eurofins, the number of ransomware attacks that targeted banks and financial institutions of all sizes and around the world was disproportionately higher than in previous years (Gulyás and Kiss, 2023). The number of assaults and the degree to which they were carried out were much higher than in previous years. According to specialists in cyber security, the degree of security awareness inside corporations is still quite low: the traditional techniques of attack are still in use, and new ways continue to emerge concurrently (Kshetri, 2019). Despite all the articles, education, and so on, victims still download malicious files by accident, either via attachments or by clicking on those that have been modified. According to the research published by Verizon, hackers were responsible for the installation of 30 per cent of the malware;

in 23 per cent of the incidents, the virus was sent through email; and in twenty per cent of the incidents, it was downloaded via an application (Gulyás and Kiss, 2023).

3.3. Increase in number and intensity

The significant shift that has occurred is the rise in the number of devastating assaults. The assaults are not carried out for the purpose of making monetary gains; rather, they are designed to damage data and files on certain systems in order to disrupt services or networks. In the year 2020, devastating assaults were directed against 25 per cent of the financial institutions that were examined (Tom Kellermann *et al.* n.d.). Cybersecurity professionals quickly point out that, sadly, the issue for financial institutions is not "if they will be attacked or not" but rather "when they will be attacked."

4.0 Large-scale attacks

The issue of whether or if the cyberattacks will expand to other sectors and impair other essential infrastructures is an important one. The faith that people have in the financial system and even the economy on a global scale is in danger from large-scale cyberattacks. Hackers target payment, clearing, or settlement systems in these situations (Milošević *et al.* 2019). Disruption of these services has the potential to dramatically impair the operation of financial markets by, among other things, hindering the flow of credit and liquidity. An assault on one or more institutions or vital infrastructures has major rippling consequences in the context of a financial ecosystem that is becoming more interconnected (Hijji and Alam, 2021).

5.0 The status of the cyber attack

The banking industry experiences a notable influence from digital technology. Financial institutions rely significantly on third-party technological and digital solutions to execute transactions and operations. As a result, financial institutions have implemented technological advancements in order to enhance their operational efficiency (Summerfield, 2014). Despite the advantageous impact of technology on the banking industry, several unfavourable consequences exist, such as the rise in cyber-crimes, which has been observed in recent times. The websites of the 50 leading banks worldwide have been subjected to attacks resulting in an annual loss of $1 billion (Cawley, 2017).

Enhancing cybersecurity measures can confer a competitive edge to banks, thereby underscoring the need for banks to bolster their security protocols to safeguard their data and engender trust among their clientele. The banking industry is facing challenges in keeping up with the rapid pace of technological advancements, particularly in relation to regulatory compliance within the banking system (Ayodeji *et al.* 2020). The presence of technological legacy systems poses a challenge to customers and entails significant security vulnerabilities for financial institutions and their clientele. The utilisation of two-factor authentication serves as a security measure to safeguard clients' bank accounts from cyber-attacks.

Financial institutions often utilise a security measure whereby clients are sent codes to their mobile devices prior to logging in (Ometov *et al.* 2019). This serves as an additional layer of protection, as potential attackers would require access to both the client's mobile device and computer in order to gain access to sensitive account information and conduct financial transactions. Despite the potential efficacy of the measure, a number of financial institutions have opted not to implement two-factor authentication to safeguard the banking accounts and sensitive information of their customers (Khando *et al.* 2021). The individual provided an account of the circumstances surrounding a financial institution in Bangladesh that exhibits weaknesses in its computerised infrastructure. Malware was detected in the computer system of the customers, which attackers utilise to circumvent risk controls and initiate the transfer of funds (Kuepper, 2017).

In the United States, the legislation mandates that banks are obligated to reimburse clients in the event of unauthorised theft of funds from their account, provided that the client has reported the loss to the bank within a period of 60 days following the transaction. In The Telegraph, financial cyber-attacks perpetrated against banking and financial services institutions resulted in a loss of over $10.5 billion for end-users in 2016, representing a 122% increase from the previous year (McGoogan, 2017). There was a 10% increase in online transactions during the corresponding period (Al-Alawi *et al.* 2020). Consequently, there is mounting pressure on online lenders to adopt more robust and sophisticated authentication protocols to expedite legitimate loan transactions and prevent fraudulent activities.

5.1 The most common Cyber-crime in the UK

No	Common cyber-crime	No of Reported Case	Remarks
1	Case of account fraud in bank	2,356,000	Customer open 'phishing mail cases amounting to 25 %
2	Fraud case on non-investment	1, 280,000	A Ponzi scheme is a fraudulent investment scheme that promises investors an exorbitant rate of return with minimal risk. The Ponzi scheme is a fraudulent investment scheme that promises high returns to initial investors by utilising funds from subsequent investors. This unsustainable model ultimately leads to the scheme's collapse.
3	Computer virus	1,340,000	Unsanctioned software, exemplified by Ransomware, demands payment in exchange for the restoration of system functionality.

Table 1: Cases of cyber crime

(Source: Al-Alawi *et al.* 2020)

6.0 Impact on Cyber Attacks

The considerable and far-reaching effects of cyberattacks on financial institutions underline the urgent need for enhanced security measures in this industry.

6.1 Financial Losses

Financial institutions are susceptible to suffering significant losses as a consequence of cyberattacks. It is possible for hackers to take advantage of weaknesses in order to get unauthorised access to sensitive financial data. This results in fraudulent financial activity, theft, or extortion. These accidents might result in direct monetary losses as well as legal responsibilities, which will have an effect on the bottom line of the organisation (Furnell and Shah, 2020).

6.2 Customer Trust and Reputation

Cyber attacks on computer networks, sometimes known as "cyber attacks," have the potential to do significant harm to the faith that customers have in their financial institutions. When clients find out that their personal or financial information has been stolen or compromised, they lose faith in the capacity of the organisation to keep their data secure. This breach of confidence causes clients to close their accounts or go elsewhere for the services they need, which negatively impacts the institution's finances (Alhayani *et al.* 2021).

6.3 Regulatory Compliance and Legal Consequences

Financial institutions are subject to stringent regulations such as GDPR and PCI DSS in order to ensure the safeguarding of customer data. In the event of a cyber attack that compromises this data, there are legal and regulatory consequences, including but not limited to financial penalties, litigation, and harm to the organisation's reputation. The aforementioned regulations

entail that financial institutions are required to adhere to stringent security protocols, protect confidential customer data, and uphold privacy standards (Tawalbeh *et al.* 2020). In the event of a cyber attack that results in the compromise of customer data, the institution is unable to fulfil regulatory requirements, thereby resulting in non-compliance.

Non-compliance can result in severe consequences, such as substantial financial penalties enforced by regulatory bodies. The breach of data privacy rights results in legal ramifications, including customer litigation aimed at obtaining compensation. Furthermore, the credibility of the organisation could be significantly damaged as clients lose confidence and opt to seek services from alternative sources (Tom Kellermann *et al.* n.d.).

6.4 Systemic Risks and Financial Stability

The interdependence among financial institutions engender a network externality that magnifies the ramifications of cyber assaults. In the event that a single institution experiences a successful attack, the repercussions have the potential to rapidly disseminate throughout the entirety of the financial system. The phenomenon of interconnectedness can be attributed to a multitude of factors, such as the utilisation of common infrastructure, interbank transactions, and reliance on external service providers (Gabriel Bassett *et al.* 2021).

A financial institution experiences significant disruptions to its essential services, including payment systems, clearing and settlement processes, and account management, as a result of a cyber attack. The occurrence of this disruption has the potential to cause delays in transactions, inaccuracies in financial records, and temporary cessation of operations (M. Henriquez, 2021). Consequently, entities such as businesses, individuals, and governments that depend on these services encounter financial setbacks, hindered access to monetary resources, and postponements in vital financial operations.

Furthermore, cyber attacks targeting financial institutions can have a substantial impact on the stock markets. Incidents that impact trading platforms or jeopardise the integrity of market data have the potential to diminish investor trust, resulting in market instability, hasty selling, and disruptions (Salahdine and Kaabouch,2019). In certain circumstances, the interdependence among financial institutions can result in systemic risks, whereby the collapse of a single institution initiates a domino effect, posing a threat to the soundness of the overall financial system. The aforementioned situation has the potential to yield significant ramifications at a national or international level, exerting influence on economies, governance, and the sustenance of individuals and enterprises (Al-Alawi *et al.* 2020).

6.5 Intellectual Property and Trade Secrets

Many times, financial firms have important intellectual property and trade secrets in their possession, such as their own unique trading algorithms or market research. Attacks against these assets through cyberspace result in their theft or unauthorised disclosure, which undermines the institution's competitive edge and even causes damage to the wider financial ecosystem (Abraham *et al.* 2019). Improved security measures need to be prioritised and invested in by financial institutions in order for these institutions to be able to solve these concerns.

7.0 Recommendation

7.1 Robust Cybersecurity Frameworks

For the purpose of providing adequate protection for their systems and data, financial institutions should develop comprehensive cybersecurity frameworks. This involves performing risk assessments on a regular basis in order to detect possible weaknesses and dangers. Institutions are better able to prioritise threats and distribute resources when they have a thorough grasp of the organisation's security environment (Bada and Nurse, 2020).

Audits should be performed on a regular basis in order to determine how well current security measures are working and where there is a need for improvement. The evaluation of security measures, the examination of access rights, and the verification of conformity with applicable rules are all possible aspects of these audits. Institutions are in a better position to proactively rectify any security holes and reduce risks when they perform audits (Gulyás and Kiss, 2023).

It is very necessary to have incident response procedures in place in order to effectively handle cyber threats. These plans provide an overview of the actions that are to be performed in the event that there is a breach in security. These actions include identifying the incident, isolating it, eliminating it, and recovering from its effects. Financial institutions lessen the effect of cyber assaults, cut down on the amount of time their systems are out, and secure their customers' data if they have clear-cut incident response processes in place (Kshetri, 2019).

7.2 Advanced Authentication and Access Controls

Robust authentication mechanisms are imperative for safeguarding confidential data. The implementation of multi-factor authentication (MFA) is recommended for financial institutions as a means of augmenting security measures. The MFA protocol necessitates the submission of various forms of identity verification, including but not limited to passwords, biometric data, and tokens, as a prerequisite for accessing systems or data (Tom Kellermann *et al.* n.d.).

Access controls are essential in restricting access rights according to job responsibilities and the principle of least privilege. The implementation of role-based access controls (RBAC) can enable financial institutions to guarantee that their personnel are solely authorised to access the systems and data that are essential for the execution of their professional responsibilities (Milošević *et al*. 2019).

7.3 Employee Education and Awareness

It is imperative for financial institutions to accord priority to cybersecurity training programmes aimed at equipping employees with knowledge of potential threats and optimal practices for safeguarding data. The training programme ought to encompass subject matters such as the ability to discern phishing scams, the aptitude to identify social engineering tactics, and the comprehension of the significance of robust passwords (Hijji and Alam, 2021).

Frequent awareness initiatives have the potential to strengthen the significance of cybersecurity within the organisational context. The implementation of email reminders, posters, or internal newsletters can facilitate the attainment of this objective by emphasising recent security incidents, emerging threats, and preventive measures (Summerfield, 2014).

7.4 Continuous Monitoring and Threat Intelligence

It is recommended that financial institutions implement advanced security measures to ensure ongoing surveillance and acquisition of threat intelligence. The implementation of real-time monitoring enables institutions to promptly identify potential cyber threats and take proactive measures in response. SIEM systems have the capability to gather log data from multiple sources and consolidate it in a centralised location (Cawley, 2017). This enables the system to generate notifications for any unusual or suspicious activities.

The process of threat intelligence entails the collection of data pertaining to nascent threats, susceptibilities, and modes of attack.

8.0 Conclusion

Cyber attacks have far-reaching consequences; financial institutions need to take a preventative stance when it comes to cybersecurity. Important measures towards protecting consumer data and privacy include the implementation of solid cybersecurity frameworks, the use of sophisticated authentication and access restrictions, and the provision of extensive staff education programmes. The financial system as a whole is more resilient when there is constant monitoring, cooperation, and information exchange. Vulnerabilities are reduced, and new attacks can be thwarted via timely testing, upgrades, and installation of security patches. Financial institutions defend themselves and their clients from the disastrous effects of cyber assaults by implementing these steps and therefore strengthening their security posture, as well as complying with regulatory obligations.**References**

Gabriel Bassett, C. David Hylender, Philippe Langlois, Alexandre Pinto, Suzanne Widup, 2021 Data Breach Investigations Report, Verizon, 2021.

Summerfield, R (2014). *Banking system faces cyber threat. Financier Worldwide Magazine, August 2014 Issue.* (2018). Available at. https://www.financierworldwide.com/banking-system-faces-cyberthreat#.W7dKcHszZdg (Accessed April, 22, 2018)

Kuepper, J (2017) Cyber Attacks and Bank Failures: Risks You Should Know, 21-01-2017, available at. Countering Terrorist Activities in Cyberspace, Z. Minchev & M. Bangladesh (eds)

Cawley, J. (2017). *The Impact of Cyber Attacks on the Banking System* (2017). Available at. https://www.researchgate.net/deref/https%3A%2F%2Fwall-street.com%2Fimpact-cyber-attacks-banking-industry%2F (Accessed December 22, 2017)

McGoogan, C. (2017). *Cyber Attacks against Financial Services Cost Consumers 8bn*, (2027). Available at. https://www.researchgate.net/deref/http%3A%2F%2Fwww.telegraph.co.uk%2Ftechnology%2F2017%2F02%2F27%2Fcyber-attacks-against-financial-services-cost-consumers-8bn%2F (Accessed April 22,2017)

Al-Alawi, A.I. and Al-Bassam, M.S.A., 2020. The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), pp.1523-1536.

Gulyás, O. and Kiss, G., 2023. Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, *219*, pp.84-90.

Tawalbeh, L.A., Muheidat, F., Tawalbeh, M. and Quwaider, M., 2020. IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), p.4102.

Salahdine, F. and Kaabouch, N., 2019. Social engineering attacks: A survey. *Future Internet*, *11*(4), p.89.

Abraham, C., Chatterjee, D. and Sims, R.R., 2019. Muddling through cybersecurity: Insights from the US healthcare industry. *Business horizons*, *62*(4), pp.539-548.

Kshetri, N., 2019. Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), pp.77-81.

Bada, M. and Nurse, J.R., 2020. The social and psychological impact of cyberattacks. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 73-92). Academic Press.

Milošević, J., Sandberg, H. and Johansson, K.H., 2019. Estimating the impact of cyber-attack strategies for stochastic networked control systems. *IEEE Transactions on Control of Network Systems*, *7*(2), pp.747-757.

Hijji, M. and Alam, G., 2021. A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. *Ieee Access*, *9*, pp.7152-7169.

Ayodeji, A., Liu, Y.K., Chao, N. and Yang, L.Q., 2020. A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. *Nuclear engineering and technology*, *52*(12), pp.2687-2698.

Ometov, A., Petrov, V., Bezzateev, S., Andreev, S., Koucheryavy, Y. and Gerla, M., 2019. Challenges of multi-factor authentication for securing advanced IoT applications. *IEEE Network*, *33*(2), pp.82-88.

Khando, K., Gao, S., Islam, S.M. and Salman, A., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, *106*, p.102267.

Furnell, S. and Shah, J.N., 2020. Home working and cyber security–an outbreak of unpreparedness?. *Computer fraud & security*, *2020*(8), pp.6-12.

Alhayani, B., Abbas, S.T., Khutar, D.Z. and Mohammed, H.J., 2021. Best ways computation intelligent of face cyber attacks. *Mater. Today Proc*, pp.26-31.

M. Henriquez, „Security Magazin," Reserved BNP Media, 20 10 2021. [Online]. Available: https://www.securitymagazine.com/articles/96128-banking-industry-sees-1318-increase-in-ransomware-attacks-in-2021.

Tom Kellermann, Ryan Murphy, „Modern Bank Heist 3.0," WMware Carbon Black, Paolo Alto, USA, May, 2020.