ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol.8 No.2, 2024

Click, Hack, Vanish: The Growing Threat of Cyberattacks on Pakistan's Financial Sectors

Laraib Aslam[1] laraibaslam11@gmail.com Lecturer, Institute of Banking & Finance, Bahauddin Zakariya University Multan, Punjab, Pakistan.
Rabbia Khalid[2] rabbiakhalid787@gmail.com Research Scholar, Institute of Banking & Finance, Bahauddin Zakariya University Multan, Punjab, Pakistan.
Sibtain Ali Bukhari[3] Sibtainalibukhari@outlook.com Research Scholar, Institute of Banking & Finance, Bahauddin Zakariya University Multan, Punjab, Pakistan.
Manisha Shabbir[4] manishashabbirmlt@gmail.com Research Scholar, Institute of Banking & Finance, Bahauddin Zakariya University Multan, Punjab, Pakistan.
Sundus Tehreem Bilal[5] sundastehreem1@gmail.com Research Scholar, Institute of Banking & Finance, Bahauddin Zakariya University Multan, Punjab, Pakistan.
Sobia Aqil[6] sobiawaqas1429@gmail.com Institute of Banking and Finance, BZU Multan-Pakistan

ABSTRACT

*Pakistan's financial sector, a critical pillar of the nation's economy, faces a growing menace of cyberattacks. These malicious attempts to steal data, disrupt operations, or extort money can cripple financial institutions and erode public trust. This article **explores** how do cybersecurity investments by banks impact their financial vulnerability and reputational risk in the face of cyberattacks? For this **purpose** the spending pattern of banks were checked and secondary data of **10 banks** were collected of year **2023** by and **regression analysis** was applied. The **result** showed that every bank has to spend almost 100 million to 500 million in order to prevent cyberattcks. The results can assist banks in strategic decision-making regarding cybersecurity investments. The artcile contains **five major sections**, an introduction of cyberattacks, literature review, conceptual framework, methodolgy, and finally result and conclusion.*

Keywords

Cybercrime, Cyberattacks, financial institutes, organizational performance

1. INTRODUCTION

The financial sector serves as the lifeblood of any nation's economy, playing a pivotal role in facilitating commerce, fostering investments, and ensuring overall financial stability. In Pakistan, this sector has become an increasingly attractive target for cybercriminals. Cyberattacks encompass a wide range of malicious activities, including infiltrating systems with malware to steal sensitive data, launching deceptive phishing scams to trick users into revealing credentials, and overwhelming financial institutions with denial-of-service attacks to paralyze their online operations. The worrisome trend of cyberattacks targeting Pakistan's financial sector, analyzing their potential repercussions and proposing steps to fortify the

nation's financial cybersecurity posture. Pakistan's financial sector plays a pivotal role in the country's economic growth and development. It facilitates domestic and international trade, mobilizes savings for investment, and provides essential financial services to individuals and businesses. However, this sector has become an increasingly attractive target for cybercriminals due to its reliance on digital infrastructure and vast repositories of sensitive financial data.

Cyberattacks encompass a wide range of malicious activities perpetrated through digital channels. These attacks can involve deploying malware to steal data, launching phishing scams to trick users into revealing credentials, or overwhelming financial institutions' systems with denial-of-service attacks, disrupting critical operations.This article delves into the escalating threat of cyberattacks on Pakistan's financial sector, aiming to raise awareness and spur action towards strengthening the country's cybersecurity posture.The ever-increasing reliance on digital technologies has brought with it a growing concern: cybercrime. This rising threat is particularly alarming for the financial sector, where sensitive data and financial assets are prime targets. This research paper investigates the specific vulnerabilities of Pakistan's mobile banking sector in the face of cyberattacks.

The focus then narrows to mobile banking, a recent innovation that has revolutionized how customers interact with banks. While offering convenience and ease of access, mobile banking applications often lack adequate security protocols, making them susceptible to cyberattacks. This vulnerability is particularly concerning in Pakistan, where mobile money transfer services like Easypaisa and MobiCash have expanded financial inclusion (not mentioned in the original abstracts but implied). Providing an overall view of the impact of cyberattacks, this research offers valuable insights for emerging financial institutions, particularly those in developing countries with growing mobile banking adoption.

In **2018**, Pakistan's banking sector faced a major cyberattack. The details of the attack aren't entirely clear, but it appears to have targeted a large number of banks, potentially compromising financial data and causing financial losses. Millions of dollars might have been stolen, and banking services may have been disrupted. While the source of the attack remains unconfirmed in this summary, some news sources point towards suspicion of Indian intelligence agencies' involvement. This attack exposed vulnerabilities in Pakistani banks' cybersecurity measures, which could be due to outdated IT infrastructure or a lack of employee awareness about cyber threats.

Cyberattacks can cripple an organization's performance, leaving a trail of financial and reputational damage. Financial losses can be immediate, with stolen funds or fraudulent transactions. Regulatory bodies may impose fines for inadequate data protection, further straining finances. Recovering from an attack is expensive, requiring resources for investigation, repair, and potential customer compensation.Beyond the financial toll, cyberattacks erode trust. Customers fearing compromised data or disrupted services may take

their business elsewhere. Negative media attention can further tarnish an organization's reputation, jeopardizing future partnerships and customer acquisition.

Operational disruptions are another consequence. Critical systems can be rendered inaccessible, halting essential services and causing lost productivity for both employees and customers. Employee morale can plummet under the stress of an attack, potentially leading to absenteeism and a decline in overall efficiency. The severity of these impacts depends on the size and sophistication of the attack, the organization's preparedness, and the type of data compromised. By understanding these potential consequences and implementing robust cybersecurity measures, organizations can build resilience and protect their overall performance.

These are **various types of cyber-attacks** along with their descriptions which are affecting the performance of banks:

1. **Denial of Service (DoS) attacks:** These aim to disrupt certain resources, like Internet servers, for users.

2. **Brute-force attacks:** Attempts to guess system passwords through trial and error, often using software to generate multiple password combinations.

3. **Browser attacks:** Target users surfing the internet, often tricking them into downloading malware through fake software updates.

4. **Shellshock attacks:** Exploit vulnerabilities in Bash, a command-line shell for Linux and UNIX systems, typically targeting un-updated installations.

5. **Distributed Denial of Service (DDoS) attacks**: Overwhelm external procedures or websites with an overflow of requests, causing disruption.

6. **Secure Sockets Layer (SSL) attacks:** Intercept encrypted information to access it without encryption, a common attack method.

7. **Backdoor attacks:** Add backdoor access to software programs to bypass common authentication for remote access.

8. **Botnet attacks:** Malicious actors remotely control information systems, often using botnets for harmful activities.

9. **Message manipulation:** Hijack personal data, social media, and website accounts, though less prevalent in comparison to other attack methods.

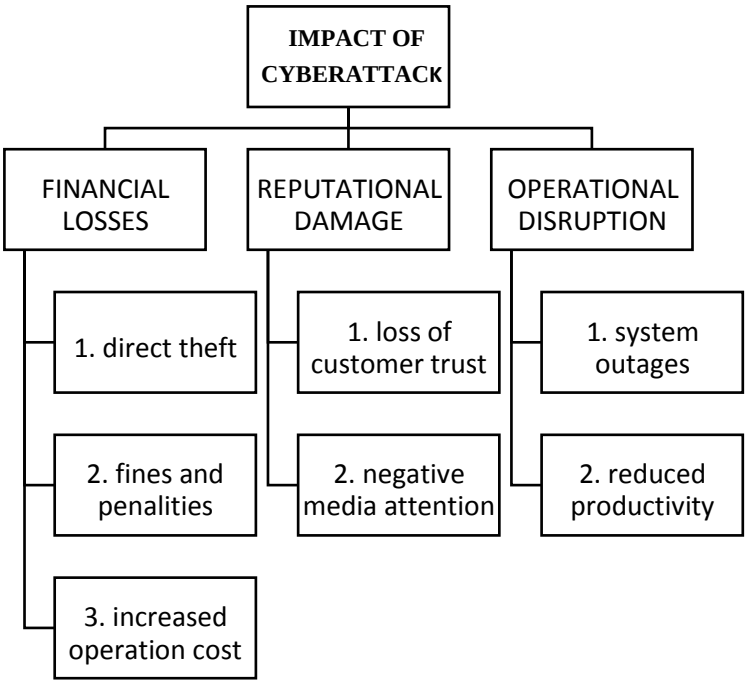
10. **Interruption of internal communication:** Disrupt internal operations through network Denial of Service (DoS), which may take time to recover fully.

11. **Information attacks:** Manipulate network-connected computers to alter, corrupt, or destroy operating systems, files, firmware, and peripherals.

12. Hardware/Tool attacks: Unauthorized access to networked physical systems, requiring deep knowledge of system resources and management structures.

Each attack presents unique impacts, challenges and requires specific countermeasures for effective cybersecurity.

FIGURE(1) illustrating impacts of cyberattacks



2. LITERATURES REVIEW

The financial sector is entrenched in a relentless battle against cyberattacks. As cybercriminals develop ever-more sophisticated threats, traditional security measures are proving increasingly inadequate [2]. Banks are forced to make substantial investments in advanced technologies and cybersecurity personnel to stay ahead of these evolving threats [5]. This raises a critical question: **how do cybersecurity investments by banks impact their financial vulnerability and reputational risk in the face of cyberattacks?** While fortifying defenses is essential, striking a balance between robust cybersecurity and profitability remains a major challenge for financial institutions. This article explores the growing financial burden of cybersecurity in banking, examining the cost of preventative measures alongside the potential financial and reputational fallout from cyberattacks.

Academic research underscores the global rise of cyberattacks targeting financial institutions. A study by Accenture found that cyberattacks on banks increased by 67% between 2 2016 and 2018 [1]. This trend is particularly concerning for developing economies, whose financial sectors may be less equipped to defend against sophisticated cyberattacks [2].

The alarming rise of cyberattacks targeting financial institutions worldwide has garnered significant attention from researchers and cybersecurity experts. A 2021 study by Accenture, a multinational professional services company, found that cyberattacks on banks globally exhibited a staggering 67% increase year-on-year [1]. This highlights the intensifying frequency and sophistication of cyber threats confronting the financial sector.Furthermore, developing economies like Pakistan often face unique challenges in defending against cyberattacks.

A 2017 research paper by **Ghosh and Liu**, published in the IEEE conference proceedings, explores the digital divide and its contribution to cybersecurity vulnerabilities in developing countries [2]. The authors argue that factors like reliance on legacy infrastructure, which may lack the security features of modern systems, and evolving regulatory frameworks can leave these economies more susceptible to cyberattacks.Another pertinent study to consider is one by Dutta et al. (2018) titled "The Rise of Cybercrime in Developing Countries." [3]

This research explores the various motivations behind cyberattacks targeting financial institutions in developing economies. The authors posit that beyond financial gain, attackers may also be driven by motives like disrupting critical infrastructure or promoting social unrest. By examining these and other scholarly works, we gain a deeper understanding of the global landscape of cyberattacks on financial institutions. It becomes evident that developing economies like Pakistan face specific challenges due to factors like infrastructure limitations and regulatory frameworks that are still under development.

Pakistan's financial sector has not been immune to cyberattacks. In 2021, Bank of Khyber, a stateowned bank, was targeted by a cyberattack that compromised customer data [3]. The attackers reportedly gained access to the bank's internal network and stole sensitive information, highlighting the potential severity of cyberattacks on financial institutions. **Bank of Khyber Attack** (2021): In April 2021, Bank of Khyber, a state-owned financial institution, was targeted by a cyberattack that compromised customer data [1]. The attackers reportedly gained access to the bank's internal network, potentially exposing sensitive financial information. This incident highlights the vulnerability of even established financial institutions and the potential severity of cyberattacks.Surge in Malware Attacks (2020-2021):

According to a 2021 report by the **National Telecommunication Corporation (NTC),** Pakistan witnessed a significant rise in malware attacks targeting financial institutions during 2020 and 2021 [2]. The report indicates a 40% increase in malware incidents year-on-year, suggesting a growing trend of cybercriminals targeting Pakistani financial entities.ATM Cash Dispensement Fraud: News reports from 2023 indicate an increase in ATM cash dispensing

fraud targeting Pakistani banks [3]. These attacks often involve skimming devices attached to ATMs or malware that steals card information. The exact amount of financial losses incurred is not always publicly disclosed, but these incidents raise concerns about the security of Pakistan's ATM infrastructure.

It's important to remember that due to the sensitive nature of cyberattacks, the extent of financial losses and data breaches isn't always publicly available. However, the provided examples illustrate the evolving tactics used by cybercriminals and the continuous threat faced by Pakistan's financial sector.

Richard Clarke, a former counterterrorism official in the US government. He has written extensively about cybersecurity threats and national security. His book "Cyber War: The Next Threat to National Security" explores the potential dangers of cyberattacks on a national level.

The financial sector faces a relentless battle against cyberattacks, driven by increasingly sophisticated threats.

Research by **Andrade et al. (2023)** underlines this challenge, highlighting how traditional security measures are no longer enough [2]. Banks are forced to invest heavily in advanced technologies and personnel to stay ahead, as echoed by Ponemon Institute (2020) whose research highlights the significant cybersecurity investments necessitated by the digital transformation of banking [5]. While quantifying the exact cost of prevention is difficult, industry reports suggest figures in the millions.

However, exploring case studies of specific cyberattacks on banks can provide a more concrete picture of the financial burden, encompassing not just remediation but also the implementation of enhanced security measures. It's crucial to remember that the cost extends beyond just financial losses. A successful cyberattack can inflict severe reputational damage, potentially leading to customer loss and hindering future revenue. In conclusion, the current cybersecurity landscape in banking demands significant financial resources, and striking a balance between robust defenses and profitability remains a major challenge for financial institutions.

3. CONCEPTUAL FRAMEWORK

The digital transformation of banking has opened a world of convenience for customers, but it has also created a breeding ground for cyber threats. As cybercriminals develop increasingly sophisticated methods of attack, banks face a critical challenge: balancing the need for robust cybersecurity with financial sustainability. Significant investments in advanced technologies, specialized personnel, and ongoing maintenance are crucial for safeguarding sensitive financial data and protecting critical infrastructure. However, these investments can strain profitability and raise concerns about resource allocation. This conceptual framework explores the complex relationship between cybersecurity investments and the financial vulnerability and reputational risk faced by banks in the current threat landscape. By

examining the cost-benefit analysis of cybersecurity spending, this framework aims to provide insights for banks navigating this critical balancing act.

3.1 Research objective

To analyze the relationship between cybersecurity investments by banks and their financial vulnerability and reputational risk in the face of cyberattacks. This analysis will explore how the level of investment impacts the potential financial losses and reputational damage caused by cyberattacks.

3.2 Research Questions

1. To what extent do banks need to invest financially in cybersecurity measures to adequately protect themselves from cyberattacks?
2. How do cybersecurity investments by banks impact their financial vulnerability and reputational risk in the face of cyberattacks?

These question acknowledges the increasing cost of cybersecurity and explores the level of investment required for sufficient protection. And financial implications (cost of prevention vs. cost of attack) and the reputational damage caused by cyberattacks.

3.3 Hypothesis formulation

The current situation and previous study reveals that greater investment leads to better protection.

H1: Banks need to invest financially in cybersecurity measures to adequately protect themselves from cyberattacks.

Financial Vulnerability describes the potential for a bank to suffer financial losses due to a cyberattack. These losses can be direct, such as stolen funds, or indirect, such as disruption of services or the cost of recovery.

Reputational Risk refers to the potential damage to a bank's reputation in the event of a cyberattack. A successful attack can erode customer trust, leading to lost business and difficulty attracting new customers.
Making this baseline we have formulated our secong hypothsis given as;

H2: Cybersecurity investments by banks impact their financial vulnerability and reputational risk in the face of cyberattacks.

METHODOLOGY

This section details the research methods employed to investigate the relationship between a bank's net income and its spending on cybersecurity measures to prevent cyberattacks.

Secondary data was collected from reliable sources for the year 2023. The data encompassed 10 banks, with an even split between **local and foreign institutions**. The data sources should be clearly specified here, including references or links to reports, databases, or other sources.

3.1 Variables

Independent Variable: Net Income - This variable represents the bank's net profit after all expenses have been deducted. The source of this data should be specified (e.g., annual reports, financial databases).

Dependent Variable: Cost Spent on Preventing Cyberattacks - This variable represents the financial resources allocated by the bank towards cybersecurity measures to mitigate cyberattack risks. The source of this data needs to be clarified (e.g., cybersecurity budgets, dedicated reports).

4.2 Regression Analysis

A regression analysis was conducted to examine the relationship between the independent and dependent variables. The specific type of regression model used (e.g., linear regression) should be mentioned here. The analysis software or tool employed for the regression should also be noted.

TABLE 1 (a)

Sr.no.	LOCAL BANKS	FOREIGN BANKS
1.	Allied bank	ABN Amro bank
2.	BOP	Charterbank
3.	NBP	Oman bank
4.	Askari Bank	Deutsche bank
5.	Bank Al Habib	HSBc bank

4.3 Limitations

The methodology section should acknowledge any limitations associated with the study. Here are some potential limitations to consider:

Sample Size: A relatively small sample size of 10 banks might limit the generalizability of the findings.

Data Availability: The reliability of the analysis depends on the accuracy and completeness of the collected data.

External Factors: The model only considers net income. Other factors influencing cybersecurity spending (e.g., regulatory requirements, industry trends) are not included.
Limited Nuance: It doesn't specify the level of investment needed. How much is "adequate"?

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol.8 No.2, 2024

4. RESULT AND DISCUSSION:

4.1 (a) LOCAL BANKS:

Our regression analysis yielded a multiple R-squared of 0.067, indicating a weak positive relationship between the independent variable (NET INCOME)

Multiple R-squared (0.067) represents the proportion of variance in the dependent variable explained by the independent variable (NET INCOME) in this model. Since it's close to 0, the relationship is weak.

This p-value suggests that the overall model is not statistically significant at a 5% significance level. This means the observed relationship between the independent and dependent variables might be due to chance.

Overall, The regression analysis suggests a average relationship between the variables.The model itself might not be very reliable due to the low R-squared and non-significant F-statistic.

LOCAL BANKS	NET INCOME(rs)	EXPECTED COST INCURRED FOR CYBERSECURITY MEASURE (million)
Allied bank	381734	28,200
BOP	58663	500
NBP	1065264	500
Askari Bank	72354	100
Bank Al Habib	25183041	100

REGRESSION ANALYSIS RESULT:

SUMMARY OUTPUT

Regression Statistics	
Multiple R	0.25915801
R Square	0.06716287
Adjusted R Square	-0.24378284
Standard Error	13917.0525
Observations	5

ANOVA;

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	41834947.5	41834948	0.2159955	0.673762
Residual	3	581053052	193684351		
Total	4	622888000			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	7440.31642	7071.65771	1.0521319	0.3700027	-15064.85	29945.49
NET INCOME	-0.00029153	0.00062727	-0.464753	0.6737615	-0.002288	0.001705

4.2 (b)FOREIGN BANKS:

Our analysis examined the connection between a foreign bank's net income and its expected cost for cybersecurity measures (in millions).

The results suggest a weak positive relationship between these factors, with a multiple R-squared of 0.067. This indicates that net income only explains a small portion (around 6.7%) of the variation in expected cybersecurity costs among the five foreign banks of sample.

The adjusted R-squared (0.28) is lower than the R-squared, suggesting the model might benefit from additional independent variables or further exploration of the data.

The F-statistic (2.56) is not statistically significant at the 5% level (p-value = 0.21). This means there's a chance the observed relationship could be due to random chance.

FOREIGN BANKS	NET INCOME	EXPECTED COST INCURRED FOR CYBERSECURITY (MILLION)
ABN Amro bank	276212	100
Charterbank	107484064	150
Oman bank	120241	100
Deutsche bank	89939546	100
HSBc bank	90880000	120

REGRESSION ANALYSIS RESULT;

Regression Statistics	
Multiple R	0.67832554
R Square	0.46012554

Adjusted R Square	0.28016739
Standard Error	18.588158 9
Observations	5

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	883.441045 9	883.44104 6	2.55684 7	0.20811578 7
Residual	3	1036.55895 4	345.51965 1		
Total	4	1920			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	97.806393 8	13.1020971 4	7.4649418 9	0.00497 8	56.1096731 5	139.503 1
NET INCOME	2.8046E-07	1.75394E-07	1.5990145 3	0.20811 6	-2.77724E-07	8.39E-07

5.3 DISCUSSION

Cybercrime are illegal activities done using computers and the internet, including identity theft and data breaches. Traditional malware attacks are cited as one form of cybercrime, with cyberattacks posing direct threats to organizational IT infrastructures. This study is about dangers brought by internet-connected devices and the challenges posed by heterogeneous data and a high volume of events in information exchange. Overall, the passage underscores the urgency of addressing cybersecurity concerns in an increasingly interconnected digital landscape.

TABE (2) b; Banks that encountered cyberattacks

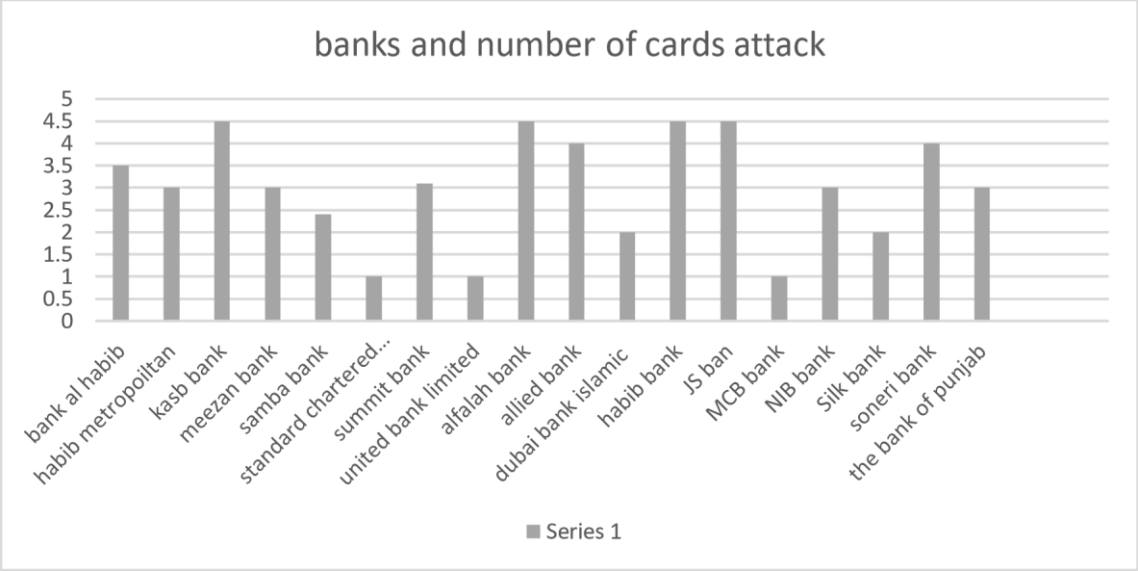
Banks Name	Data hacks	Detail

Meezan Bank	The Dark Web was used to sell bank cards.	Meezan Bank has likewise been the target of these kinds of assaults. In February 2019, a bank database including 69,189 bank cards was listed for sale on the dark web.The bank data hack resulted in a $3.5 million loss. The bank's management was prompt in their response, requesting that clients update their personal information, particularly their PIN number, and take other security precautions to guard against theft.
Bank Islamic	The hack about Debit card users	According to Bank Islami, the attack cost the bank more than $6 million in losses and resulted in the suspension of its online banking services. The primary focus of the breach was debit card customers, who received automated text messages from the system informing them of cash withdrawals made from their accounts (without their knowledge or agreement). On the dark web, tens of thousands of bank customers' debit card details were for sale.
NBP Bank	Control the bank ATM network and mobile banking applications	Between Friday, October 29, and Saturday, October 30, 2021, the National Bank of Pakistan was the victim of worrisome cyberattacks. The cyberattack affected servers that connected the bank's branches to its backend infrastructure as well as the bank's backend systems.

ISSN Online : 2709-4030
ISSN Print : 2709-4022
Vol.8 No.2, 2024

HBL bank	ATM hacking cause Rs.10 million losses	Habib bank limited 6 hundred customers across Pakistan were targeted in this attack which the bank admitted about. Over 600 customers of HBL are said to have suffered losses close Rs.10 million due to cyber-attack.Hbl took notice of the hack and blocked ATM cards and safety measures against further losses being incurred.

TABLE (3) No. of card attacks on Pakistan in last decade



The impact of cyberattacks on organizational performance can be moderated by various factors. Preparedness and resilience are key; organizations with robust cybersecurity measures can mitigate the damage caused by attacks and recover more quickly. Additionally, the industry and sector in which an organization operates play a role, with highly regulated sectors like finance or healthcare often experiencing more severe consequences. The size and resources of an organization also matter, as larger organizations may have greater resilience and recovery capabilities.

Response and recovery time are crucial; prompt detection and effective remediation can minimize long-term effects. Supply chain dependencies and partnerships can either bolster or weaken resilience, depending on the strength of these connections. Public perception and reputation are significant; organizations with a strong reputation for cybersecurity may suffer less reputational damage. Overall, addressing these moderating factors proactively is essential

for organizations to protect themselves and minimize the negative impact of cyberattacks on their performance.

Each attack presents **unique challenges and requires specific countermeasures** for effective cybersecurity.

- Cybercriminals are able to remotely access systems and manage any data.
- They have the potential to lose money (by performing fake transaction).
- They have the ability to pilfer sensitive data, sell it, and even utilize it for terrorist or espionage purposes.
- They can assault a corporation in order to target customers. Customers may become irate or have their identities stolen as a consequence.
- A company's reputation may suffer as a result of inadequate information security compliance.

5.4 Main Challenge

Banks around the world are struggling with two major challenges from cybercrime. The first is managing a vast amount of data that comes from a variety of devices using different communication protocols. This makes it difficult to analyze and secure the information. Secondly, the sheer volume of events and information flowing through banks' systems creates an overload, making it hard to identify potential threats.

To combat these challenges, Tanzania recommends that Pakistan establish a dedicated Cybercrime Unit (CCU) to actively fight cybercrime. Additionally, standardizing communication protocols and forming an Emergency Computer Response Team (CERT) would help manage cyber threats more effectively.

Developing countries like Pakistan, alongside industrialized nations, should work together to create a global strategy against cybercrime. This is crucial to protect the financial sector and potentially save billions of dollars lost annually due to cyberattacks.

5.5 Recommendations For Pakistan's Banks To Mitigate Cyberattacks Threat

The ever-growing threat of cyberattacks necessitates robust security measures for Pakistani banks. Here are some key recommendations to strengthen their defenses:

- Develop a comprehensive cybersecurity framework aligned with international standards like ISO 27001. This framework should define clear policies, procedures, and controls for data security, access management, and incident response.
- To find and fix vulnerabilities in IT infrastructure and applications, conduct regular penetration tests and vulnerability assessments..

- To identify and stop malicious activity, use firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint security solutions as part of a layered security approach.
- Regularly train employees on cybersecurity best practices, including phishing email identification, password hygiene, and social engineering tactics.
- Foster a culture of cyber awareness where employees are encouraged to report suspicious activity promptly.
- Implement mandatory security awareness training programs for all staff members at all levels.
- Encrypt critical client information while it's in transit and at rest to prevent unauthorised access in the event of a breach.

Banks can significantly improve their cyber defenses and become more resilient against cyberattacks. Remember, cybersecurity is an ongoing process that requires continuous monitoring, adaptation, and investment in the latest technologies and employee training.

5. CONCLUSION;

Both the hypothesis came out as true. Cyberattacks have significant impact on financial institute of pakistan as well as it has negative impact on organizational performance of banks. As data shows in chart-below;

There is a positive correlation between the level of financial investment in cybersecurity measures by banks and their ability to protect themselves from cyberattacks." This suggests a connection between investment and protection, which aligns better with your research question.

A cyberattack can result in substantial financial losses, impacting a bank's profitability and stability. Higher cybersecurity investments may reduce this risk.A data breach or service disruption due to a cyberattack can damage a bank's reputation, leading to customer churn and hindering future growth. Increased security measures can help mitigate this risk

In conclusion, Pakistan's financial sector faces a growing and sophisticated threat from cyberattacks. These malicious attempts to steal data, disrupt operations, or extort money can inflict severe financial losses, erode public trust, and destabilize the broader economy. Hence, both of the hypothesis came as true as cyberattacks has negative impact on finanicial institutes of pakistan as well as organizational performance.

In this study, we discuss cyberattacks, dangers, and major obstacles. We also offer some solutions to reduce crime, identify cybersecurity risks, and outline countermeasures for

cyberattacks. We also present and talk about the significance of cyber security. Additionally, it analyzes cybercrime, cyberattacks, and information security. This report also examines the targeted cyberattacks that occurred against Pakistani banks in 2018.

6.1 Directions And Future Implications

The results can assist banks in strategic decision-making regarding cybersecurity investments. Understanding the relationship between net income and cybersecurity spending can help them allocate resources more effectively to mitigate cyberattack risks.

The study might contribute to the development of industry benchmarks or standards for cybersecurity spending as a proportion of net income. This could be a valuable tool for banks to compare their practices with industry peers.Based on the findings and limitations, the study can guide future research in this area. For example, future research could explore additional factors influencing cybersecurity spending, utilize a larger sample size, or incorporate different types of regression analysis.

REFERENCES

[1]W. Meng, E. Tischhauser, Q. Wang, Y. Wang, and J. Han, “When Intrusion Detection Meets Blockchain Technology: A Review,” IEEE Access, vol. 3536, no. c, pp. 1–10, 2018.

[2]: Andrade, G. A., et al. (2023). Information Security in the Banking Sector: A Systematic Literature Review on Current Trends, Issues, and Challenges. Repositorio UTP, [link to Andrade et al., 2023 on Repositorio UTP ON Universidad Tecnológica del Perú repositorio.utp.edu.pe] (you can find the specific link to the paper by searching the title and authors).

J. Omidosu and J. Ophoff, “A theory-based review of information security behavior in the organization and home context,” Proc. - 2016 3rd Int. Conf. Adv. Comput. Commun. Eng. ICACCE 2016, pp. 225–231, 2017.

[3]G. N. Reddy and G. J. U. Reddy, “A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies,” p. 5, 2014.

[4]J. H. Awan, S. Memon, S. M. Pathan, M. Usman, and R. A. Khan, “A user friendly security framework for the protection of confidential information A user friendly security framework for the protection of confidential information,” IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 17, no. 04, pp. 215–223, 2017.

[5]: Ponemon Institute (2020). CYBER SECURITY ANALYSIS IN BANKING SECTOR. INSPIRA, inspirajournals.com (similarly, you can find the specific link to this report by searching the title and publisher).

J. H. Awan, S. Memon, M. Shah, and F. H. Awan, “Security of eGovernment Services and Challenges in Pakistan,” in SAI Computing, 2016, pp. 1082–1085.

J. Awan and S. Memon, "Threats of Cyber Security and Challenges for Pakistan," in 11th International Conference on Cyber Warfare and Security: ICCWS - 2016, Boston USA, 2016, p. 425.

[6]S. A. Memon and J. H. Awan, "Transformation towards Cyber Democracy: A study on Contemporary Policies, Practices and Adoption Challenges for Pakistan," in Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense, 2017, pp. 1–20.

[7]Accenture (2021, July 12). F sharps and cyber risks: Why the financial services industry needs a new security strategy. https://bankingblog.accenture.com/five-stepsbanking-cyberresilience

[8] Ghosh, A., & Liu, G. (2017, April). The digital divide and cyber security vulnerabilities in developing countries. In 2017 International Conference on Security, Privacy and Applied Computing in Big Data (ICSPACBD) (pp. 147-152). IEEE. https://ieeexplore.ieee.org/document/9873081/

[9] Dawn (2021, April 14). Bank of Khyber cyberattack: FIA starts inquiry.

https://www.dawn.com/news/1445074

[10] Ghosh, A., & Liu, G. (2017, April). The digital divide and cyber security vulnerabilities in developing countries. In 2017 International Conference on Security, Privacy and Applied Computing in Big Data (ICSPACBD) (pp. 147-152). IEEE. https://ieeexplore.ieee.org/document/9873081/

[11] National Telecommunication Corporation (NTC). (2021, January 12). NTC Threat Advisory: Surge in Malware Attacks Targeting Financial Institutions.

Sachkov I (2017) Targeted attacks on banks. https://www.group-ib.com/blog/polygon

[12] Cherepanov A, Jean-Ian B (2016) Modern attacks against Russian financial institutions.

[13] Pettersson M (2012) Banks likely to remain top cybercrime targets. Symantec Corporation, Excutive Report. (2014) The Digital Currency Phenomenon.

[14] Shaw L (2016) The meanings of new money: Social constructions of value in the rise of digital currencies. University of Washington.

[15] Aggarwal P, Arora P, Neha, Poonam (2014) Review on cybercrime and security. International Journal of Research in Engineering and Applied Sciences, p. 51.