Journal of Ecohumanism
2025
Volume: 4, No: 2, pp. 1508 – 1517
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i2.6526

Securing Financial Information in the Digital Age: An Overview of Cybersecurity Threat Evaluation in Banking Systems.

Md Abdullah Al Mahmud[1], Jannatul Ferdous mou[2], Al Modabbir Zaman[3], Sweety Rani Dhar[4], Anupom Debnath[5], Sadia Sharmin[6], Mahafuj Hassan[7]

Abstract

Financial information, especially in banking systems, requires robust security measures in the increasingly digital world. As technology evolves constantly, security threats also change, which highlights the need for a strong cybersecurity posture. In recent years, banks have been directly affected. Banks are susceptible to a variety of cyberattacks, such as ransomware attacks, DDOS assaults, phishing attacks, and malware attacks. It has been proposed in this paper how to improve financial system security by sharing real-life case studies and research. It includes a range of industries, such as banks, real estate companies, and investment or insurance corporations. The study identified banking regions that are more vulnerable to cyberattacks and ensured the modification and development of cybersecurity protocols. New researchers and those seeking to become deeply involved in cybersecurity in banking systems may find this material helpful as a guide.

Keywords: *Cyber-security, Bank, Cyber-attack, Threats, Business.*

Introduction

Globally, there are about 44,000 banks, according to S&P Global (S&P Global, 2024). In 2021, the Global Findex database of the World Bank estimated that 3.8 billion adults had bank accounts. In recent years, banks have been directly affected. Cyberattacks on digital technology and communication networks have sparked concern among ICT professionals and cyber security teams. Additional security officers are needed to improve security levels. Financial information in the digital era is a wide range of data on individual and business finances that is all handled and managed electronically. Securing financial information in the digital era is crucial due to the growing sophistication of cyber threats and the dependence on digital platforms for financial transactions. Cybercrime has a detrimental economic impact on South African society and impacts the whole planet. A breach in any cyber security system causes financial and non-financial damages for the victim company and its consumers; therefore, cyber security attempts to prevent these losses [1]. Non-monetary losses include the theft of intellectual property and sensitive customer information, such as identity and account numbers. Cybercrime is a worldwide problem with major economic consequences for South African society. Securing sensitive information is a significant problem for cyber security and privacy in the cyberbanking industry [2].It's critical to protect personal information. Cyberbanking-related worries about privacy and cyber security [2]. Banks are utilizing innovations to streamline operations, enhance security, and personalize customer experiences. One of the primary issues with cybersecurity and privacy in the field of cyberbanking is protecting sensitive data [2]. Additionally, it has been shown that companies must handle security threats methodically and with a high level of awareness rather than depending just on ad hoc approaches [3].By automating repetitive tasks, workers may concentrate on more difficult projects and provide better customer service. Strong encryption, which protects data during transmission and storage; multifactor authentication, which guarantees that only authorized users may access critical data; and the use of secure networks, like virtual private networks (VPNs), are important security measures.

[1] Department of Business Administration, International American University, #1000 Los Angeles, CA 90010, USA
[2] Department of Business Administration, International American University, #1000 Los Angeles, CA 90010, USA.
[3] Department of Business Administration, International American University, #1000 Los Angeles, CA 90010, USA.
[4] Department of Business Administration, International American University, #1000 Los Angeles, CA 90010, USA.
[5] Department of Business Administration, International American University, #1000 Los Angeles, CA 90010, USA
[6] Department of Business Administration, International American University, #1000 Los Angeles, CA 90010, USA
[7] Department of Business Administration, International American University, #1000 Los Angeles, CA 90010, USA

Journal of Ecohumanism
2025
Volume: 4, No: 2, pp. 1508 – 1517
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i2.6526

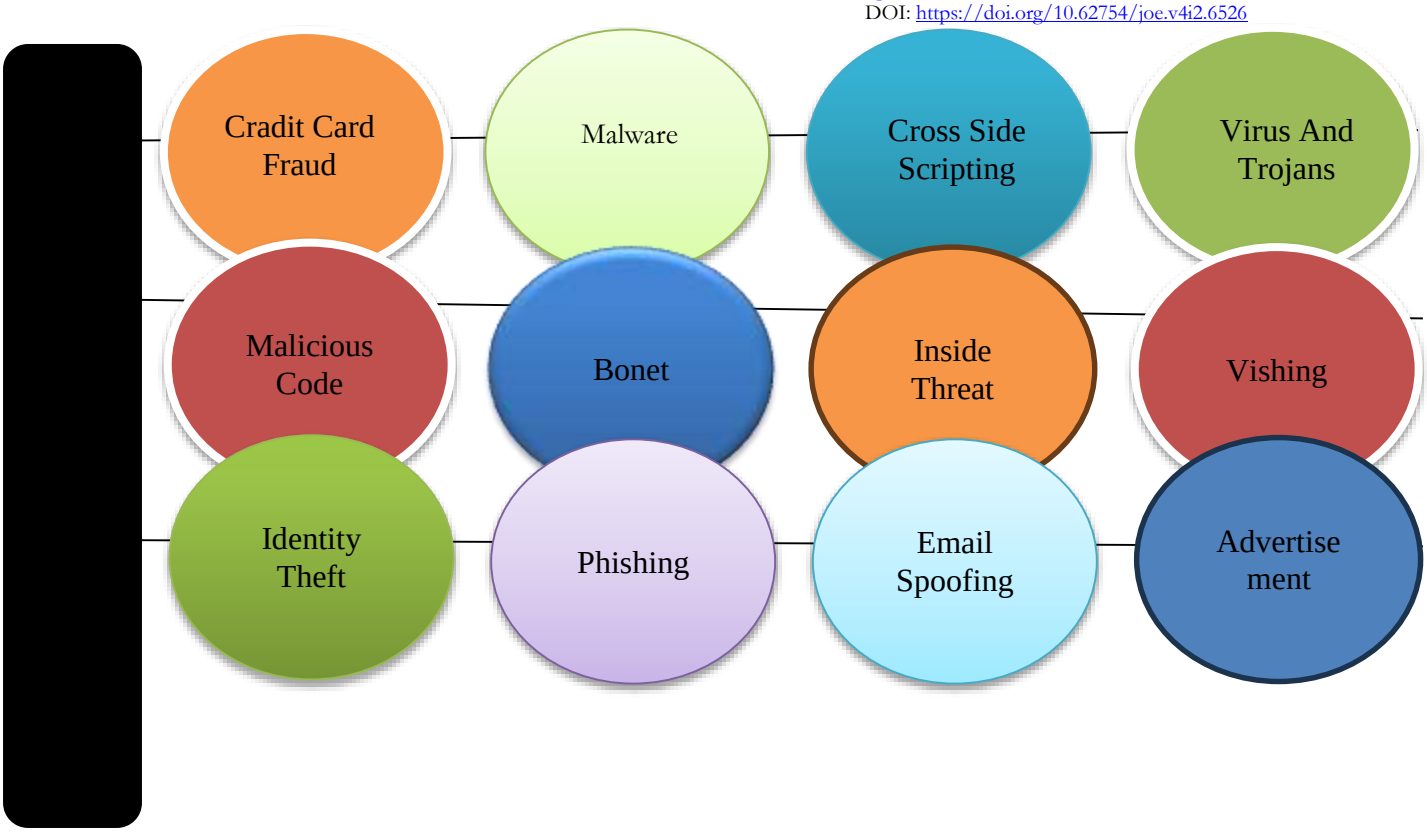
Cybersecurity vulnerabilities in banking systems are a major cause of concern, given the sensitive nature of financial data and the potential for significant financial loss and reputational injury. Common threats include phishing and social engineering, in which attackers deceive individuals into providing critical information, as well as malware or ransomware, which can penetrate networks, disrupt operations, or steal data. The banking and financial sector institution (BFSI) is a large industry with consumers all over the world. A nation's ability to serve its bank customers has been vital to its development, as banking has historically been one of the most important institutions in any given nation. Information networks and IT solutions play a significant role in our culture, economy, and essential infrastructure. The Internet is one of the most important inventions of the twenty-first century and has had a significant impact on our lives [4]. In 2021, the World Bank's Global Findex database estimated that 3.8 billion people had bank accounts. Financial institutions face a serious danger from cybercrime in the twenty-first century. Over time, the most vulnerable and impoverished segments of society have gained greater access to banking services. As the banking industry in USA uses more and more digital technology, protecting financial data in this day and age is crucial. Cybercrime includes, among other things, phishing schemes, investment fraud, identity theft, and coercion [5]. These risks have the potential to jeopardize private financial information, interfere with banking activities, and cause large losses. USA banks need to put strong cybersecurity measures in place to counter these attacks. Multi-factor authentication ensures that sensitive data is accessible by authorized persons only, and encryption is essential for protecting data during transmission and storage. Patches and software upgrades on a regular basis can protect systems from known vulnerabilities. In this present World where financial information security in the digital era is crucial due to the growing complexity of cyber threats and the increasing digitalization of banking institutions. Cybersecurity dangers that financial institutions must cope with include malware, ransomware, phishing, and advanced persistent threats (APTs). These risks include a high risk of serious financial losses, data breaches, and operational disruptions. End users, companies, and nation states are all worried about risks to the availability, confidentiality, and integrity of digital information [6]. As the banks are utilizing strong security measures to reduce these threats, including encryption, multifactor authentication, and constant monitoring. In order to further protect data privacy, local laws and standards, such the Payment Card Industry Data Security Standard (PCI DSS), must be followed. Examples of cutting-edge technology that are being used more and more for early risk detection and response include artificial intelligence and machine learning. Furthermore, information sharing and regional cooperation among the world improve the cybersecurity posture of the area as a whole and the financial institutions' resilience to assaults. Over time, a plethora of cybersecurity solutions and monitoring tactics have been developed in response to the growing threats facing regulatory bodies' cyberinfrastructure. We need to investigate cybersecurity opportunities and hazards since the number and complexity of cybersecurity events are becoming more and more apparent. Bankers' progress in adapting to cyber security is being examined [7].

Literature Review

Cybercrime has risen as a consequence of the emergence of a new age in banking technology, which has eliminated the need for a physical presence at the bank for many transactions and other financial services via the use of electronic devices. Cybercrime is a new kind of crime that has evolved as a consequence of the enormous opportunities that the advancement of computer technology and information and communication networks has provided society. Cybercrime is defined as any unlawful conduct carried out utilising a computer, network, or digital device. A wide range of unlawful online activities pose a risk to cybersecurity. Malware, viruses, denial-of-service assaults, SQL injection attacks, and zero-day exploits are among the crimes that directly target computer networks and devices. On the other side, there are crimes such as fraud, identity theft, phishing scams, information warfare, and cyberbullying that are made possible by computer networks or devices but are instead utilised for unrelated goals. Despite setting up a safe and secure VPN connection, they were unable to shield the data from several types of cyberattacks [8]. According to a consultant and the CEO of Cyberlaws.net, there are several kinds of cybercrime [9].

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

Journal of Ecohumanism
2025
Volume: 4, No: 2, pp. 1508 – 1517
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i2.6526



Cybercrime Types in the Banking Industry [10]

It is well known that phishing is an easy and inexpensive method of harming the victim. Regular emails from reliable sources are usually used to spread malware to a large number of systems. Because services like Dropbox, Office 365, Salesforce, and others are becoming more and more popular, hackers have more resources at their disposal to carry out annoying attacks [11]. Phishing techniques use a variety of communication channels, such as email, pop-up messages, websites, and instant chats [12]. Conventional malware attacks happen at one specific location on the surface between the network layer, software modules, and hardware devices. improperly using the current project [13]. Malware cybercrime involves the use of malicious software to infiltrate, damage, or exploit computer systems and networks. Common types include viruses, ransomware, spyware, and Trojans. Cybercriminals deploy malware to steal sensitive data, disrupt services, or gain unauthorized access to systems. These attacks can target individuals, businesses, and government entities, leading to financial loss, data breaches, and compromised security. Protecting against malware involves using robust cybersecurity measures like antivirus software, firewalls, regular updates, and user education on safe online practices. An attacker can gain unauthorized access to computer systems by introducing malicious software and taking advantage of security weaknesses. A significant financial or political benefit is the impetus behind the virus, which makes an attacker more eager to hack as many network devices as they can in order to accomplish their nefarious goals that they have set for themselves [14].

A Denial of Service (DoS) attack is a cybercrime where attackers overwhelm a system, network, or website with excessive traffic, rendering it unavailable to users. This flood of requests exhausts the target's resources, leading to slowdowns or complete outages. Common methods include flooding servers with superfluous requests or exploiting vulnerabilities to crash systems. DoS attacks disrupt services, cause financial losses, and damage reputations. Mitigation strategies involve using firewalls, intrusion detection systems, and rate limiting to filter malicious traffic and maintain service availability. These assaults are particularly utilized to neglect certain assets, such as a Web server for clients. These assaults are exceptionally common nowadays [15, 16]. Endpoint attacks target devices like computers, smartphones, and tablets that connect to a network. Cybercriminals exploit vulnerabilities in these devices to gain unauthorized access, steal data, or deploy

Journal of Ecohumanism
2025
Volume: 4, No: 2, pp. 1508 – 1517
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i2.6526

malware. Common tactics include phishing, exploiting software vulnerabilities, and using malicious downloads. Once compromised, endpoints can be used as entry points for larger network breaches or data exfiltration. Protecting against endpoint attacks involves using antivirus software, regular updates, strong passwords, and endpoint detection and response (EDR) solutions to monitor and secure devices against potential threats. Supply chain and third-party attacks target vulnerabilities in an organization's supply chain or through its third-party vendors.

Cybercriminals infiltrate less-secure networks of suppliers or service providers to gain access to the primary target. This can involve tampering with software updates, hardware, or services, leading to data breaches, malware distribution, or operational disruptions. These attacks exploit the interconnectedness of businesses, compromising security at multiple levels. Mitigating these risks requires thorough vetting of third parties, implementing strong security policies, continuous monitoring, and establishing robust incident response plans to protect the entire supply chain. An assault known as a "Man-in-the-Middle" (MitM) happens when a third party surreptitiously intercepts and relays communication between two parties, frequently without the participants' awareness. This gives the attacker the ability to intercept conversations, change messages, or take important data—such as bank account information and login credentials—and steal it. Common methods include spoofing Wi-Fi networks, DNS hijacking, and session hijacking. MitM attacks can compromise the confidentiality and integrity of data. Preventing these attacks involves using encryption (like HTTPS), secure VPNs, strong authentication methods, and ensuring the integrity of communication channels to protect against interception and tampering. By injecting malicious SQL code into input fields, SQL injection attacks take advantage of weaknesses in the database layer of an online application. This gives attackers the ability to edit or remove information, manipulate queries, obtain unauthorized access to data, and carry out administrative tasks. Data breaches, loss of data integrity, and compromised systems can result from SQL injection. In order to protect databases from harmful manipulations, SQL injection can be prevented by employing parameterized queries, prepared statements, and input validation to guarantee that user inputs are handled as data rather than executable code. Attacks using zero-day exploits target software flaws for which there are no patches or fixes available and which are unknown to the software manufacturer. Before developers can fix these vulnerabilities, cybercriminals take advantage of them, potentially causing serious harm. Unauthorized access, data breaches, and system compromises can result from zero-day attacks. They are particularly dangerous because they exploit unpatched vulnerabilities, leaving systems defenseless. Preventing zero-day attacks involves using advanced security measures like intrusion detection systems, regular software updates, threat intelligence, and employing a layered security approach to mitigate potential impacts. Browser attacks are directed at users who are browsing the web.

They may unknowingly download malware as a result of attacks. False software was employed in these assaults onswap out, or update. Malware can only be downloaded from websites. Avoiding browser-based network attacks in their entirety and regularly updating web browsers are excellent strategies [15]. Shellshock attacks target the flaws of Bash, a collective command-line shell for Linux and UNIX systems. The vulnerabilities on the Internet still remain because a lot of installations are never updated. The issue is that every network is aiming toward Shellshock [15].

Methodology

The first thing that springs to mind when thinking about cybersecurity is "cybercrimes or cyber-attacks," which are on the increase. This is because of the fact that cybersecurity is becoming more widespread. In the context of the fundamental concepts of burglary and instruction, the term "cybercrime" may be used to describe to any illegal behaviour that benefits from the usage of a computer. Cybercrime will expand with mechanical areas of interest in an individual's life since incremental innovation is something that is needed [17]. Traditional malware attacks happen at a single point on the surface between program regions, hardware, and the arrangement layer of the device, leading to improper use of the current venture [13]. Cyber-attacks are coordinated assaults through the internet on an organization that employs the Web through the clutter, devastation, deactivation, and pernicious control of the organization's IT foundation

Journal of Ecohumanism
2025
Volume: 4, No: 2, pp. 1508 – 1517
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i2.6526

[18]. Scanners, IPS, IDS, firewalls, and applications are examples of cybersecurity technology. Since most hackers do business over port 80 or 443 (SSL), current security solutions are not strong enough to fend off application-level attacks. Organizations use network firewalls for internal security, yet they are vulnerable to cybercrime. These options are summarized with their downsides [19].

Intrusion Prevention Systems

Intrusion Prevention Systems (IPS) act like digital bouncers on your network. They constantly monitor traffic for suspicious activity, comparing it to known attack patterns. If something seems fishy, the IPS can block it entirely, preventing harm. Unlike firewalls that control access, IPS actively stop threats in real-time. They come in two flavors: network-based, watching all incoming and outgoing traffic, and host-based, protecting individual devices. IPS are a vital layer of defense against cyberattacks, offering extra security for your valuable data.

Vaulnerbility Scanner

Vulnerability scanners are digital detectives for your systems. They crawl through software, hardware, and configurations searching for weaknesses like outdated software or misconfigured settings. These weaknesses, called vulnerabilities, can be exploited by attackers. The scanner compares these vulnerabilities to a database of known threats, prioritizing the most critical ones. This helps you identify and patch security holes before hackers find them, keeping your systems safe.

Intrusion Detection System

Intrusion Detection Systems (IDS) act as digital security guards. They monitor your network or individual devices for suspicious activity, like unauthorized access attempts or malware. Unlike IPS that block threats, IDS sound the alarm. They analyze traffic patterns and system behavior, comparing them to known attack signatures or baselines of normal activity. If something seems off, an IDS will alert you, allowing you to investigate and take action.

Cyber Security Cyclic Framework

There is no widely acknowledged "cyclic" framework in cybersecurity. However, the established NIST Cybersecurity Framework (CSF) has a cyclical approach. This framework outlines five functions: identification, protection, detection, response, and recovery. Organizations must go through these phases on a regular basis in order to successfully combat cyber threats. They identify critical assets, strengthen defenses, detect threats, respond to incidents, and recover from attacks. This cyclical strategy helps companies improve their entire cybersecurity posture. In short, the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is a continuous cycle that aims to improve the cybersecurity status of an organisation by identifying vulnerabilities, constructing defences, and actively reacting to attacks. When it comes to nations that have specific regulatory requirements for cyber risk, the first step that is often taken is to establish a documented cybersecurity program or policy for banks. Generally speaking, these criteria are structured in accordance with the risk management categories of governance, identification, protection, identification, response, and recovery, as can be seen in Figure 2.

Journal of Ecohumanism
2025
Volume: 4, No: 2, pp. 1508 – 1517
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i2.6526

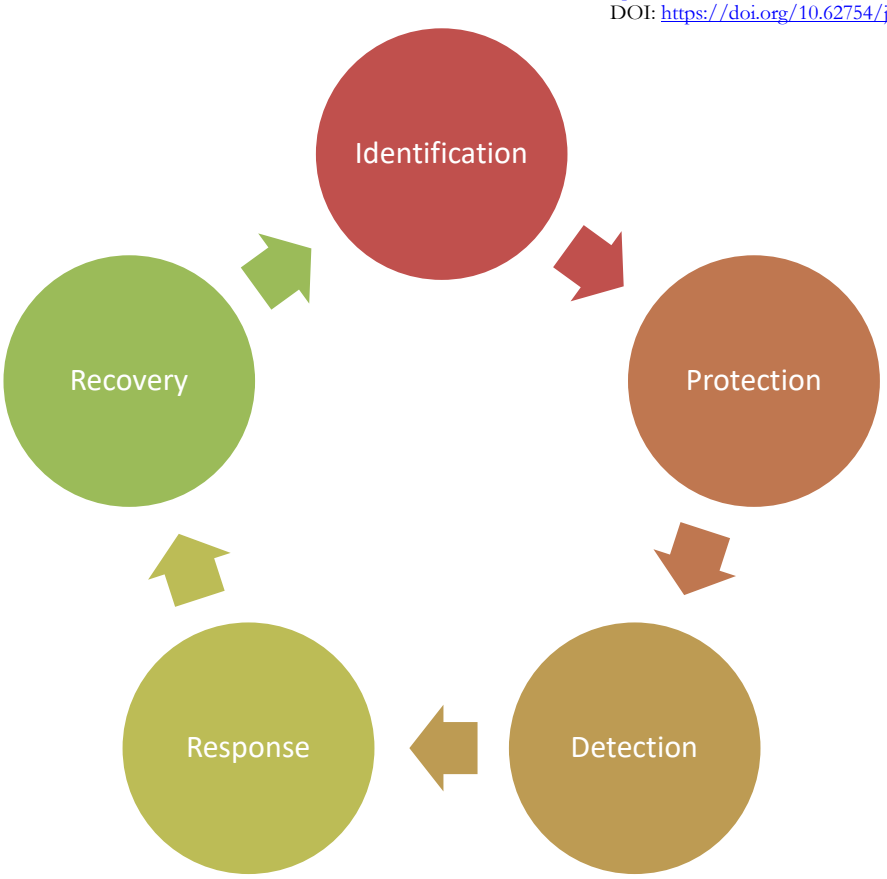


Fig.2. New Framework for Cybersecurity

This function focuses on understanding your critical assets, business environment, and regulatory requirements. It helps prioritize cybersecurity efforts based on potential risks. The baseline, the circumstances, the danger profile, the risk exposure, and the anticipated losses are identified. ISO offers a comprehensive set of control recommendations to safeguard information assets. These controls cover areas like physical security, access control, cryptography, and secure development practices. While not as explicit as NIST CSF, ISO encourages organizations to implement controls for continuous monitoring and anomaly detection to identify potential security breaches. ISO emphasizes the importance of having an incident response plan to address security incidents effectively. This includes procedures for containment, eradication, and recovery. Disaster recovery plans, corporate data recovery systems, and business continental strategies are linked as recovery measures [20].

Results and Findings

Data breaches in the United States and Italy, as well as trade issues in Russia, have all led to cyberattacks on New Zealand and Pakistan's central banks. In the United States, the bulk of the attacks were phoney, resulting in a loss of $117 million [10]. Table 1 depicts the World Central Bank's annual financial attack.

Table 1. Global Central Banks Target Financial Cases in Every Year

World Central Banks Yearly Cased Cyber Attack

Institutions	Years	Type of Attack	Details

Journal of Ecohumanism
2025
Volume: 4, No: 2, pp. 1508 – 1517
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i2.6526

Reserve Bank of New Zealand	2021	Data Breach	Unauthorised individuals gained access to the bank's data via one of its third-party file-sharing platforms.
South African Bank	2020	Data Breach	A credit analyst sold the personal information of 200,000 clients to third parties.
Hungarian Banks	2020	DDoS	A significant DDoS attack originating from computer systems in Russia, China, and Vietnam severely disrupted the service.
CIH Bank	2020	Theft	Breach consumer accounts, resulting in unlawful transactions.
SberBank of Russia	2019	Data Leak	60 million customer credit card details were exposed.
Bank Islami in Pakistan	2018	Data Breach	A cyber-attack was identified on a global payment network, leading to a system shutdown and resulting in losses amounting to Rs.2.6 million.
Bank of Italy	2017	Fraud	Hacking into the email accounts of two former executives.
Bank of Russia	2016	Fraud	The bank incurred a loss of $22 million as a result of 21 cyber-attacks and an additional $50 million from correspondent banks.
Central Bank of Azerbaijan	2015	Data Breach	Theft of thousands of bank customers' data
ECB	2014	Data Breach	A total of 20,000 email addresses and associated contact information were compromised.
Banco Central del Ecuador	2013	Fraud	The national bank account of Riobamba was compromised, resulting in a theft of USD 13.3 million.

Source: ORX News & Carnegie Endownment for international Peace.

Cyberattacks not only cause data breaches and fraud, but they may also put a person in a very difficult financial position. Data breaches(34%), fraud (43%), and disruptions (23%), according to the ORX News dataset. The data set is skewed since hackers' whereabouts and disclosure might take months or even years, in contrast to the rapidity of commercial impacts [12].

The latest SWIFT heist shows that cyberattacks may be utilised for illicit purposes (Table 2). Criminals online can obtain sensitive data, including customers' credit card details used for online purchases. Ninety percent of the losses recorded in the sample were caused by computer fraud.

Journal of Ecohumanism
2025
Volume: 4, No: 2, pp. 1508 – 1517
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i2.6526

Table 2. Cyber Attacks Cased via SWIFT Network

Institutions	**Date**	**Initial Losses (USD million)**	**Current Estimated Losses (USD million)**
Union Bank of India	Feb,2015	12.2	9.4
TP Bank (Vietnam)	May,2016	1	**0**
Bangladesh Centeral Bank	Feb,2016	171	0
Akbank (Turkey)	Dec,2016	4	4
Globex (Russia)	Dec,2017	1	0.1
NIC Ais Bank (Nepal	Oct,2017	4.4	0.6
City Union Bank (India)	Jan,2018	2	Unknown
Far Easter International Bank	Oct,2017	60	0.5
Banco del Austro (Eucador)	Jan, 2015	12.2	9.4

Sources: ORX & News , Financial Times. Estimated loss base on public info.

Using a weighted average of fourteen tokens related to anti-money-laundering and counter-financing-of-terrorism laws, operations, financial regulations, political transparency, and the rule of law, the Basel AML Index determines an aggregate risk score. A number of organisations provide the Basel Institute with statistics, such as the Financial Action Task Force (FATF), Transparency International (TI), the World Bank, and the World Economic Forum (WEF). This approach highlights the precarious position of a nation instead than concentrating just on money or illicit commerce.

Journal of Ecohumanism
2025
Volume: 4, No: 2, pp. 1508 – 1517
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i2.6526

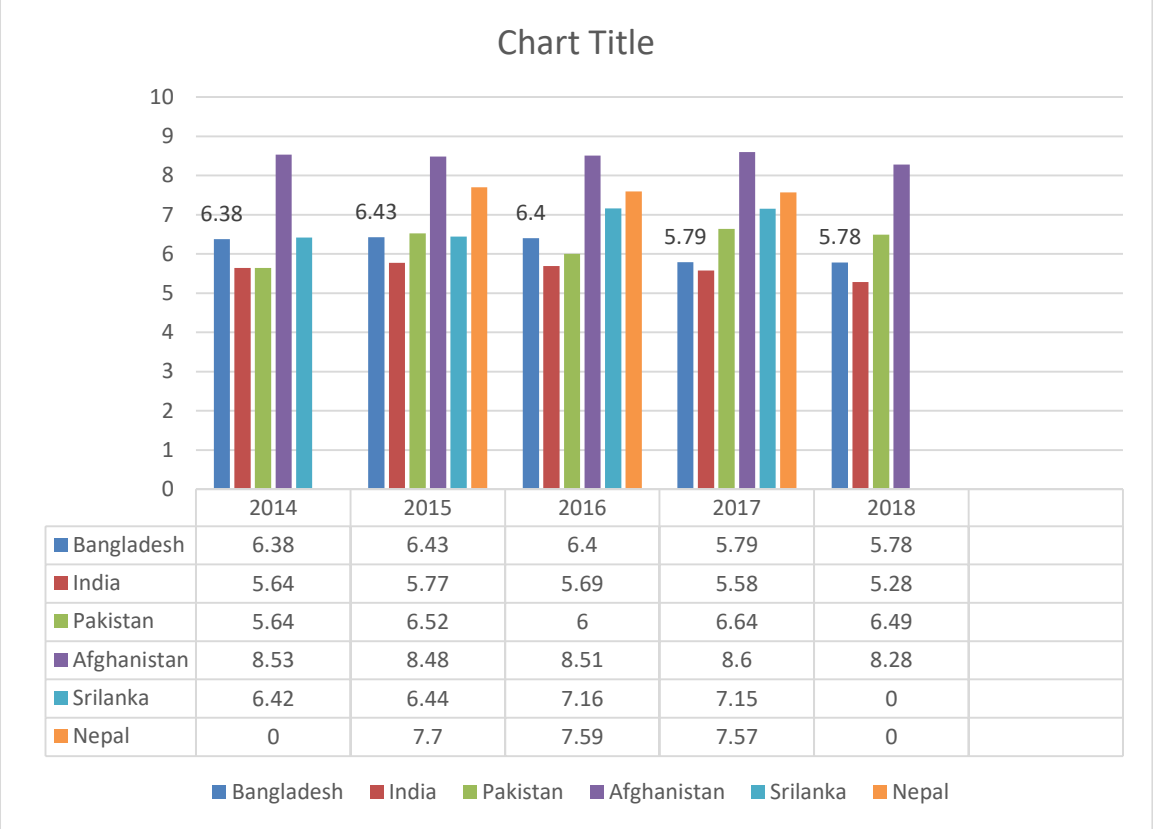


Fig .3. South Asian Nations Are Compared and Contrasted

Source: Cost of Cybercrime Study in the 2019 Financial Services Report.

Figure 3 shows that seven South Asian nations have done better than India in the past five years, with Bangladesh coming in at number five. Data from 129 nations with a high potential for terrorist funding and money laundering was used to generate the 2018 Basel AML Index. In 2018, India was rated 5.78 (51st), and Bangladesh was ranked 5.78 (68th). Afghanistan has the most impressive score, having broken the Basel AML record. In contrast, out of the six countries stated above, India has received the lowest score over the last five years.

Conclusions

Therefore, the concepts and techniques presented in this paper enable the development of efficient defenses against cyberattacks in banking systems. Globally, cybersecurity is a field intended to safeguard and keep an eye on computers, networks, data, and apps to prevent misuse or illegal access. A cyber-security analyst's primary responsibility is to prevent network harm. In this study, we express information that this article discusses cyber-attacks, risks, issues, crime control solutions, cyber security attacks, and tactics for overcoming them. We also highlight the necessity of cybersecurity. Furthermore, it investigates information security, cybercrime, and cyberattacks. This architecture ensures quick access and protects data from potential attacks. Future research will improve the model's security and usability by addressing potential risks. As cyberbanking evolves, managing massive amounts of data becomes increasingly important. Banks are the nation's financial engine and resources are available to both people and organizations. Nothing should jeopardize the soundness of a banking institution or bank credit in any way. Banks are rapidly seeing the need to collaborate with new technologies and viewpoints in order to mitigate or eradicate cyber hazards in the system. Doing so requires an in-depth familiarity with the systems' known vulnerabilities and the many forms of persistent assaults, as well as the consequences of each.

Journal of Ecohumanism
2025
Volume: 4, No: 2, pp. 1508 – 1517
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i2.6526

References

B. Panja, D. Fattaleh, M. Mercado, A. Robinson, and P. Meharia, "Cybersecurity in banking and financial sector: Security analysis of a mobile banking application," in 2013 international conference on collaboration technologies and systems (CTS), 2013, pp. 397-403: IEEE.

A. B. Jibril, M. A. Kwarteng, M. Chovancova, and R. Denanyoh, "Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study," in ICCWS 2020 15th International Conference on Cyber Warfare and Security, 2020, vol. 270: Academic Conferences and publishing limited.

D. Mohammed, "Cybersecurity compliance in the financial sector," Journal of Internet Banking and Commerce, vol. 20, no. 1, pp. 1-11, 2015.

Y. Perwej, S. Q. Abbas, J. P. Dixit, N. Akhtar, and A. K. Jaiswal, "A systematic literature review on the cyber security," International Journal of scientific research and management, vol. 9, no. 12, pp. 669-710, 2021.

M. S. Malik and U. Islam, "Cybercrime: an emerging threat to the banking sector of Pakistan," Journal of Financial Crime, vol. 26, no. 1, pp. 50-60, 2019.

T. Rid and B. Buchanan, "Attributing cyber attacks," Journal of strategic studies, vol. 38, no. 1-2, pp. 4-37, 2015.

T. F. N. Bukht, M. A. Raza, J. H. Awan, and R. Ahmad, "Analyzing cyber-attacks targeted on the Banks of Pakistan and their Solutions," IJCSNS International Journal of Computer Science and Network Security, vol. 20, no. 2, 2020.

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, pp. 163-180, 2021.

N. Joveda, M. T. Khan, A. Pathak, and B. Chattogram, "Cyber laundering: a threat to banking industries in bangladesh: in quest of effective legal framework and cyber security of financial information," International Journal of Economics and Finance, vol. 11, no. 10, pp. 54-65, 2019.

A. Q. Stanikzai and M. A. Shah, "Evaluation of cyber security threats in banking systems," in 2021 IEEE Symposium Series on Computational Intelligence (SSCI), 2021, pp. 1-4: IEEE.

A. Bouveret, Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund, 2018.

A. Razzaq, A. Hur, H. F. Ahmad, and M. Masood, "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," in 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), 2013, pp. 1-6: IEEE.

J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," Journal of computer and system sciences, vol. 80, no. 5, pp. 973-993, 2014.

C. Stevens, "Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet," Contemporary Security Policy, vol. 41, no. 1, pp. 129-152, 2020.

J. Jain and P. R. Pal, "A recent study over cyber security and its elements," International Journal of Advanced Research in Computer Science, vol. 8, no. 3, pp. 791-793, 2017.

M. Aamir and M. A. Zaidi, "A survey on DDoS attack and defense strategies: from traditional schemes to current techniques," Interdisciplinary Information Sciences, vol. 19, no. 2, pp. 173-200, 2013.

G. N. Reddy and G. Reddy, "A study of cyber security challenges and its emerging trends on latest technologies," arXiv preprint arXiv:1402.1842, 2014.

J. Omidosu and J. Ophoff, "A theory-based review of information security behavior in the organization and home context," in 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), 2016, pp. 225-231: IEEE.

S. K. Lim, A. O. Muis, W. Lu, and C. H. Ong, "Malwaretextdb: A database for annotated malware articles," in Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), 2017, pp. 1557-1567.

J. C. Crisanto and J. Prenio, Regulatory approaches to enhance banks' cyber-security frameworks. Bank for International Settlements, Financial Stability Institute, 2017.