ASJP
Algerian Scientific Journal Platform

Review MECAS **V° 22/ N° 1une 2026**

Cybersecurity Strategies and their role in achieving Financial Stability in the Banking Sector

BADRAOUI Chahinez[1]
MIFMA Laboratory / Lecturer A / Abu Bakr Belkaid University of Tlemcen (Algeria)
badraoui.chahinez@gmail.com

Received date: 25.03.2026, Accepted date : 06.05.2026, Publication date: 02.06.2026

Abstract :

This research paper aims to highlight the role of Cybersecurity Strategies in achieving Financial Stability in the Banking Sector, which has become one of the most vulnerable sectors to Cyber Risks in light of the rapid Digital Transformation and increasing reliance on Electronic Banking Services. The study discusses the theoretical framework of both Cybersecurity and Financial Stability, analysing Cyber Threats and their impact on bank performance and stability. It also highlights key Cybersecurity Strategies, such as Cybersecurity Governance, Risk Management, and Operational Resilience, and their role in protecting bank assets, enhancing trust, and reducing Systemic Risk. The study concludes that adopting effective Cybersecurity Strategies is essential to supporting the stability of the Banking Sector and ensuring its sustainability in the digital age. It also contributes to enhancing banks' ability to respond quickly to cyber incidents and minimise the resulting Operational Losses and Financial Losses.

Keywords: Cybersecurity, Cybersecurity Strategies, Financial Stability, Cyber Risks, Banking Sector.

Jel Classification Codes: K24, G21, G28, O33.

Introduction:

The modern era has witnessed tremendous developments in the fields of technology and communications, with the World Wide Web (the Internet) has become an integral part of the daily lives of individuals and institutions alike. With the increasing use of technology and the expansion of electronic networks, growing Cyber Threats targeting banks and Financial Institutions have emerged, making Cybersecurity a vital element in ensuring the protection of information and financial assets. Banks are strategically important within the Financial System as they are a key pillar of the digital economy and rely heavily on banking information systems and Digital Banking in their daily operations. The widespread use of digital technologies in banking operations is associated with increased Cyber Risks, as hacking banks and Data Theft or customer identity theft can lead to significant Financial Losses and negatively impact public confidence in the banking system and the economy as a whole, which directly affects Financial Stability and Economic Stability.

[1] Corresponding Author.

In this context, cybersecurity has become a strategic necessity for banks and Financial Institutions, not only to avoid potential risks, but also to ensure the ability to deal with their effects and address them quickly and effectively. World Bank reports indicate that the Financial Sector is one of the most vulnerable to Security Breaches, which calls for the development of integrated strategies at the level of central banks and Financial Institutions that play a pivotal role in maintaining the reliability of financial operations, protecting customer assets, and strengthening trust between institutions and investors. This directly contributes to supporting Financial Stability, achieving sustainable economic growth in the digital age, and enhancing resilience to increasing Cyber Attacks. However, despite the importance of Cybersecurity, many banks still face challenges in implementing effective strategies that ensure prevention and rapid response to Cyber Attacks. Based on the above, the main issue is:

How can Cybersecurity Strategies contribute to Financial Stability in the Banking Sector?

The importance of this research paper lies in highlighting the vital role of Cybersecurity Strategies in protecting the Banking Sector and ensuring its Financial Stability by reducing digital risks, safeguarding customer assets, and strengthening trust between banks and investors. The article also highlights how Financial Institutions can remain resilient and sustain economic growth in the face of increasing cyber threats, making it an important reference for policymakers in developing effective security policies.

Accordingly, this study aims to:

- Enrich theoretical knowledge in the field of Cybersecurity and Financial Stability by clarifying the conceptual framework of both concepts.
- Analyse the nature of Cyber Risks and Cyber Threats facing the Banking Sector and their potential impact on bank performance and Financial System stability.
- Highlight the role of Cybersecurity as a strategic tool in reducing Operational Risk and Financial Risk and enhancing the resilience and continuity of banking institutions.
- Review the most important Cybersecurity Strategies and policies adopted in the field of Cybersecurity, and explain their contribution to enhancing the confidence, Cybersecurity Governance and Operational Resilience of banks.
- Provide an analytical framework that can assist decision-makers and regulators in developing effective Cybersecurity policies that support the stability of the Banking Sector.

I. Cybersecurity - Theoretical Background:

The rapid development of information and communication technology has led to profound changes in the way activities and organisations are managed, with the digital space becoming an essential element in the execution of operations and the exchange of information. This transformation has been accompanied by an increase in the risks and threats associated with the use of electronic systems and networks, which has necessitated the adoption of protection mechanisms capable of addressing these challenges. In this context, Cybersecurity has emerged as one of the key areas

of focus for ensuring the safety and continuity of digital systems, especially in light of the rise in Cyber Attacks and the diversity of their methods.

1. The concept of Cybersecurity:

Cybersecurity is not just an electronic shield that protects systems, but rather an ambassador for Digital Transformation that encompasses a variety of concepts and technologies that form the first line of defence against Cyber Attacks, representing a philosophical framework characterised by interaction with advanced technologies and ongoing security challenges. The concept of Cybersecurity branches out into many dimensions, one of which is its diverse components, ranging from encryption technologies to advanced detection methods. It is based on principles of diversity and speed of adaptation, where the constant challenge is seen as an opportunity to enhance protection. Despite the importance of this concept and the global debate and discussion it has sparked, there is no agreed-upon general definition. This is perhaps because it encompasses many issues for different parties, even though they all revolve around the protection of digital information security, where:

- The US Cybersecurity Agency (CISA) defines Cybersecurity as 'the art of protecting networks, devices and data from unauthorised access or criminal use, ensuring the confidentiality, integrity and availability of information.'
- The 2011 report by the International Telecommunication Union (ITU) defines Cybersecurity as "a set of activities that include a combination of tools, policies, security safeguards, guidelines, Risk Management approaches, training, best practices, and technologies that can be used to protect the cyber environment and the assets of organisations and users." **(ABDELKADER, 2024, p. 46)**
- The Information Security Glossary defines cyber as an attack through cyberspace aimed at disrupting, destroying or causing damage by controlling computing environments in order to compromise or steal information**. (Al-Shaikh, 2023, p. 103)**

By using expert systems to match different definitions, a study by Gains and Al (2022) concluded that the definition of Cybersecurity provided by the National Initiative for Cybersecurity Careers and Studies (NICCS) is the most comprehensive, defining Cybersecurity as 'the strategy, policy, and standards related to the security of cyberspace and operations therein, encompassing a full range of policies and activities for threat reduction, reduction of weaknesses, deterrence, international engagement and Incident Response, resilience, and Recovery, including computer network operations and information assurance.' It can therefore be said that the role of Cybersecurity is not limited to prevention strategies, but also extends to mitigating the damage and losses that occur in the event of Cyber Attacks and repairing the damage caused by these attacks as quickly as possible. **(Khamiss, 2024, p. 911)**

2. Cybersecurity objectives:

Numerous studies have shown that Cybersecurity has many objectives, which can be summarised as follows: **(Elbardony, 2025, pp. 15-16)**

- Strengthening the protection of information technology systems, including devices, networks, software, and databases, as well as identifying and addressing weaknesses and gaps in these systems.

- Countering cyber attacks targeting government agencies and business establishments of all types and across all sectors.
- Develop a plan for recovery from the effects of cyber attacks and ensure business continuity.
- Providing a secure cyber environment for conducting financial and non-financial transactions in light of the global trend towards Digital Transformation and the integration of digital technology in all areas of business.
- Providing the necessary training for employees on how to protect information technology systems from any Security Breaches or unauthorised use, across all sectors and at all levels.
- Enhance the protection of society from all types of cybercrime committed through internet networks and technologies.

In this regard, standard **(ISO/IEC 27032: 2012)** on Cybersecurity in business organisations, issued by the International Organization for Standardization **(ISO)**, that the Cybersecurity framework is based on four main areas that reflect the objectives and importance of having a Cybersecurity system in business organisations, particularly banks, as follows: **(ISO, 2012)**

- **Prevention:** This involves adopting policies, controls and Preventive Measures aimed at reducing the chances of Electronic Attacks and limiting the impact of potential Cyber Threats.
- **Detection and protection:** This involves activating Cybersecurity management mechanisms and continuously monitoring security activities and events, enabling attacks and Cyber Threats to be detected at an early stage and measures to be taken to protect systems and information.
- **Response and communication:** This includes preparing in advance for security incidents and implementing appropriate Incident Response Plans when Electronic Attacks occur, while ensuring data confidentiality, integrity and availability, as well as documenting and reporting incidents and coordinating effectively with relevant parties.
- **Recovery and learning:** This involves focusing on restoring information systems, technologies and related services to their normal operational state after a Cyber Attack, as well as analysing the causes of incidents and taking appropriate corrective measures to prevent them from recurring in the future.

3. Cybersecurity challenges in the Financial and Banking Sector:

Cybersecurity is a serious challenge for the Financial Sector due to the rapid shift towards Digital Transformation, with the aim of improving the quality of financial services and increasing financial access opportunities as part of a strategy to promote Financial Inclusion. These challenges are represented by the following factors: **(Djeghel Djamila, 2023, p. 309)**

- **Lack of awareness:** Awareness of the importance of Cybersecurity among the general public is very low, and many companies do not invest in training and improving public awareness of Cybersecurity.
- **Inadequate budgets and lack of management:** Cybersecurity is often given low priority and a low budget, and senior management's focus on Cybersecurity

remains low in most banks, with its projects given low priority. This may be because senior management is indifferent to the impact of Cyber Threats.

- **Weak Identity and Access Management:** Identity and Access Management is a fundamental component of Cybersecurity, as a single breach of identity and access is enough to compromise and damage an entire bank network.
- **Increase in Ransomware:** The threat of Ransomware is growing, as cybercriminals have begun to use methods that avoid detection by focusing on executable files and causing damage to them.
- **Mobile devices and applications:** Most banking institutions have adopted mobile phones as a means of conducting business, and with the increase in the use of mobile devices and the volume of transactions conducted through them, these devices are becoming a target for hackers.

4. Cyber Threats:

Concepts of Cyber Attacks vary, but they all agree on the need to deter and counter them by modernising security systems and raising awareness about the nature of these attacks. 'Cyber Attacks are one of the most dynamic types of armed conflict or conflict. They differ from traditional forms of conflict and can occur invisibly and unnoticed, such as when the intelligence services of any country launch attacks using cyber weapons to sabotage the information infrastructure of another country.' **(Azzeddine, 2022, p. 114)**

Cyber Attacks have a negative impact on banks themselves, on customers, on the Financial Sector and on the economy in general. Among the negative effects of Cyber Attacks on banks are the following: **(Abdullelah Saeed Al Mohayya, 2025)**

- Loss of information, data, money, resources, time, and opportunities.
- Disruption of services, operations, systems, networks, applications, and platforms.
- Reduction in efficiency, quality, innovation, competitiveness, growth, and profitability.
- Damage to reputation, brand, trust, loyalty, satisfaction, experience, and relationships with customers, partners, regulators, competitors, and the community.
- Increased risks, threats, liabilities, costs, losses, penalties, claims, lawsuits, investigations, audits,reports, recommendations, and regulations.
- The impact of Cyber Attacks on banks is not limited to banks alone, but extends to customers who may be exposed to theft, fraud, loss, disruption, inconvenience, frustration, anxiety, fear, anger, resentment, or discontinuation of banking services.

In this context, the banking and financial services sector experiences 71% more Cyber Attacks than other sectors, according to World Bank estimates released in December 2021. The cost of Cyber Attacks in this sector could reach an estimated $360 billion annually if they become more widespread, according to estimates by the International Monetary Fund. This has prompted Arab central banks to tighten regulatory instructions, requiring banks to establish a set of instructions to secure electronic applications, the most important of which is the installation of protection

software against hacking. As information and communication technologies continue to innovate in finding and providing new ways to reach users, these banks, especially electronic ones, are exposed to a range of risks, as the malicious use of information and communication technology can disrupt financial services that are essential to national and international financial systems, undermine security and trust, and jeopardise Financial Stability and economic stability. Cyber Attacks pose a threat to the entire Financial System, a fact confirmed by reports issued on this matter at the international, regional and local levels. The percentage of users who suffered Cyber Attacks in 2016 reached about 65%, an increase of about 29% compared to 2015.

according to a report issued by the World Bank on this matter. As a result of the above and in recognition of the Cyber Threats, there is a need to continuously strive to address and mitigate these risks and to establish effective mechanisms to enhance the ability of banking institutions to withstand and hedge against these risks, especially after regulatory authorities around the world took regulatory and supervisory steps aimed at avoiding the impact of these Cyber Risks on banks. **(Jabr, 2023, pp. 54-55)**

II. Financial Stability – theoretical introduction:

Financial Stability is a fundamental component of economic soundness, reflecting the ability of the Financial System to operate efficiently and continuously without experiencing disruptions that affect its performance. It is achieved when Financial Institutions and markets are able to implement Risk Management and withstand shocks, ensuring the continued provision of financial services and support for economic activity, which contributes to strengthening confidence in the Financial System and protecting the economy from crises and severe fluctuations.

1. Definition of Financial Stability:

Economic literature has included multiple concepts of Financial Stability, many of which have focused on defining it as the opposite of Financial Instability, which is characterised by a failure or disruption in the Financial Sector's ability to perform its financial intermediation function according to ideal principles and standards. Another group of economists has criticised this approach, pointing out that the Financial Sector's optimal performance of its financial intermediation function does not necessarily mean that it is capable of withstanding financial crises that spread from one country to another and cannot be avoided in a world that has become a small village linked by highly intertwined and complex financial and economic relationships. It is therefore clear that there is no single concept or definition of Financial Stability among economists. Some express it in terms of the repercussions of its failure in the Financial Sector, while others believe that ensuring it is not linked to the good performance of the Financial Sector because it is subject to uncontrollable and unpredictable variables. The following is a presentation of the most important definitions of Financial Stability, where:

- It is defined as ensuring that elements of the Financial System do not enter into a series of cyclical imbalances that threaten economic efficiency, because Financial Stability is a necessary condition within economic mechanisms for the purpose of evaluating and determining Financial Risk Management for economic efficiency. **(Senoussaoui Fatna, 2022, p. 208)**

- The Bank for International Settlements considers Financial Stability to be a state in which there are no factors that could cause sudden and unjustified fluctuations in the prices of financial assets or affect the ability of Financial Institutions to meet their contractual obligations. In other words, stability is achieved in an economic situation that is calm and stable in terms of the level of transactions between Financial Institutions in the Financial System. **(Crockett, 1997)**
- Economist Mishkin linked Financial Stability to the symmetry of information in Capital markets and its impact on them. In a different context, economist Crochett defined Financial Instability and banking instability as: 'A situation in which economic performance falls below its original level, leading to a loss of confidence in the Financial System in general and banks in particular, as they are unable to meet their obligations on a continuous basis and without external (government) assistance, with sharp price fluctuations in financial and banking markets that may not reflect the reality of economic fundamentals.' **(Farida Mouhoub, 2022, p. 38)**

After reviewing some of the points of view, Financial Stability can be defined as: "A situation in which the Financial Sector is able to hedge against internal and external crises and, if they occur, continues to perform its function of directing financial resources to investment opportunities and continuing to make payments efficiently, quickly and in a timely manner, without compromising the mechanisms for mitigating the risks associated with the credit and liquidity process, Market Risk and Operational Risk, taking into account the proportionality of the growth of financial asset values with the growth of the Real Economy and the growth of productive and sustainable employment opportunities. The degree of Financial Stability can be determined by the Financial System's ability to mitigate the impact of crises on the Real Economy, as well as its speed and effectiveness in restoring Financial Stability. **(Boudayar, 2023, p. 50)**

2. Financial Stability objectives:

The general framework for developing Financial Stability policies aims to achieve several objectives, the most important of which are: **(Amamra Yasmine, 2020, p. 39)**

- Achieving an efficient Financial Sector that contributes to high and sustainable economic growth and a highly efficient infrastructure that enjoys the confidence of users.
- Enabling policymakers and financial decision-makers to identify potential vulnerabilities early on, before financial crises occur.
- Encouraging the adoption of timely preventive and remedial policies to avoid Financial Instability, while strengthening the capacity to restore Financial Stability in the event of a disruption.

3. Conditions for achieving Financial Stability:

Vasy lenko and Androsova believe that the following conditions must be met to ensure Financial Stability: **(Androsova, 2016, p. 124)**

- The banking system must be able to withstand negative impacts and dynamic market conditions, and be able to absorb shocks without giving rise to

cumulative processes that hinder the allocation of savings to investment opportunities.

- Banks must be safe repositories for depositors' funds, protecting their interests and meeting their obligations quickly to ensure Financial Stability.
- Banks must be able to increase their capital in response to rising market power, because banks with higher market power due to higher Capital Ratios can offset Non-Performing Loans, reducing the risk of Bank Insolvency, which leads to increased Financial Stability.
- The government and central banks implement regulatory policies through their supervisory measures on commercial banks to determine the extent of credit these institutions provide and the amount of risk they are willing to take, thereby assessing, pricing, identifying and managing financial risks in order to mitigate Financial Contagion.
- The Financial System must be able to transfer resources efficiently and smoothly from savers to investors, with efficient management of the geographical distribution of economic resources. Financial risks must be assessed and priced with reasonable accuracy and must be managed relatively well. In addition, the Financial System must be in a position to comfortably absorb real economic and financial surprises and shocks.

4. Factors affecting Financial Stability:

There are several factors that can affect the stability of any country's Financial Systems, making them more vulnerable to financial and economic shocks and fluctuations. The most important of these factors are as follows: **(Al-Obaidi, 2023, p. 36)**

- **Inflation Rates:** Fluctuations in inflation rates between highs and lows have a clear impact on the work of the central bank, but the general trend in inflation is upward, due to the loss of revenues and significant growth in the Money Supply.
- **Exchange Rate**: The continuous decline of the national currency against foreign currencies leads to a loss of foreign exchange revenues and a widening of the Balance of Payments Deficit, which negatively affects Financial Stability Indicators.
- **Money Supply**: A very large increase in the Money Supply leads to a significant rise in Inflation Rates, which affects the operations of many banks around the world.
- **Balance of Payments**: The widening of the Balance of Payments Deficit is affected by the loss of oil revenues from foreign exchange and the increase in the volume of imports compared to the volume of exports in general, which negatively affects the Exchange Rate of the national currency against foreign currencies.

III. Cybersecurity and Cybersecurity Strategies for enhancing the stability of the Banking Sector:

The Financial Sector is more vulnerable to Cyber Risks due to the sensitivity of the data it handles, such as bank accounts, credit cards, and Financial Transfers. A report by the International Monetary Fund indicated that Cyber Risk losses have quadrupled since 2017. Incidents affecting this sector could threaten Financial Stability and Economic Stability if they erode confidence in the Financial System or disrupt essential services. With the rapid Digital Transformation of banking services,

Cybersecurity has become an urgent necessity to protect customer assets and ensure the stability of financial systems. Any security vulnerability could lead to huge financial losses, a decline in customer confidence, and even the collapse of Financial Institutions. This undoubtedly requires the development of adequate national Cybersecurity Strategies to protect Cybersecurity, accompanied by effective Regulatory Frameworks and Supervisory Capabilities to ensure the strengthening of the Financial Sector.

1. General Cybersecurity Policy to Mitigate Cyber Risks:

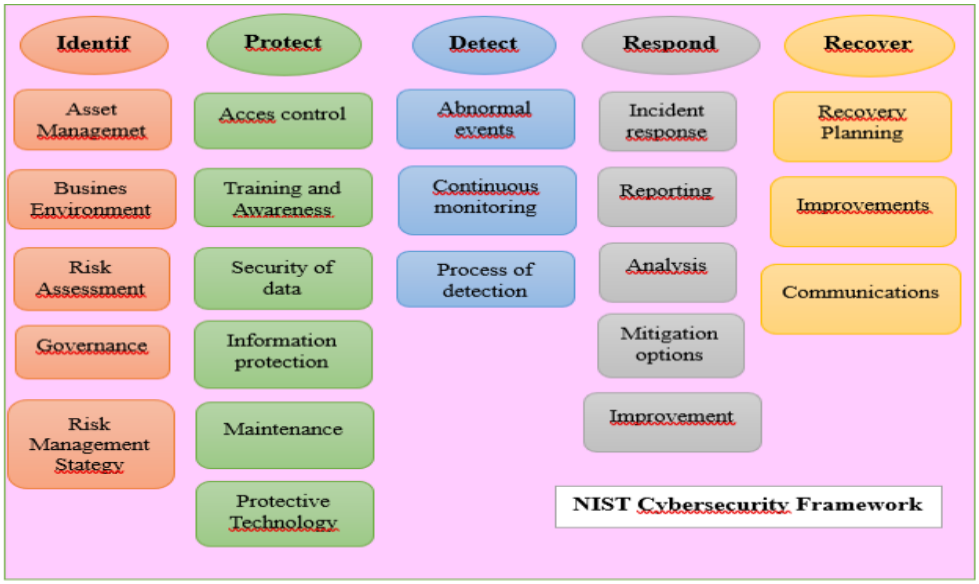
Controlling IT risks for any organisation means developing a strategy for their implementation from an executive and operational perspective. The general policy on Cybersecurity translates the concept of risk and its impact into specific security measures for implementation in the field. It facilitates both prevention and remedial measures taken in response to security problems. It also helps to reduce risks and their impact. Although it is impossible to eliminate all risks and difficult to prepare for all possible threats, it is important to reduce the exposure of the environments and resources that need to be protected. The organisation's security policy should specify, among other things, the resources, form, measures and plans for defence to reduce risks to an acceptable level in order to ensure that Operational Risk and technological risks can be controlled.

Practices to reduce perceived risks include the following: **(Souag Abdelkader, 2023, pp. 359-360)**

- Take the necessary measures to verify the identity of customers.
- The bank should rely on optimal procedures to ensure the validity and security of electronic banking operations.
- Using means to protect electronic payment systems and customer accounts and data.
- Adopting effective control methods for electronic systems, as well as access rights to the information system, data and various application programmes.
- Taking a set of measures and methods to maintain the confidentiality of banking information and data, including: preventing access to customers' personal information and data and their accounts except by persons and entities authorised to do so.
- Protecting information from unauthorised access, modification or copying.
- Reviewing all electronic banking transactions and information to ensure their integrity.

The National Institute of Standards and Technology (NIST) has developed a framework for improving Cybersecurity infrastructure to help companies reduce the potential impact of Cyber Risks. The framework consists of the following key pillars: identification, protection, detection, response, and Recovery. Each phase consists of a set of different activities for Cyber Risk Management, as shown in the following figure:

Figure : NIST Cybersecurity Framework



Source : Henock Mulugeta Melaku, 2023, Context-Based and Adaptive Cybersecurity Risk Management Framework, Risks, 11 (101), P 07.

2. The role of Cybersecurity in promoting Financial Stability in the Banking Sector:

Cybersecurity in the Banking Sector is essential to ensuring the stability of Financial Institutions and protecting the Financial System from growing digital risks and Cyber Threats, especially in light of the rapid Digital Transformation and banks' reliance on modern technologies. Below, we discuss the most important roles that Cybersecurity plays in supporting the stability of the Banking Sector:

- **Protecting bank assets and preventing direct losses:**

Cybersecurity is the first line of defence for protecting banks' financial and information assets. When banks are exposed to attacks such as card data theft, illegal financial transfers, and System Disruption, they face direct financial losses that weaken their ability to maintain bank liquidity and meet short-term obligations. Good cybersecurity management allows banks to prevent Cyber Attacks before they occur, quickly detect Security Breaches, and limit their Financial Losses, ensuring Financial Stability. The literature also shows that banks' increasing reliance on digital services has significantly raised the level of risk, making Cybersecurity a necessity rather than an option. **(VIEWPOINT, 2017, pp. 1-12)**

- **Enhancing governance, Disclosure and Transparency in banks:**

Cybersecurity is an essential part of Risk Governance and Institutional Stability Management in banks, as its implementation within a Cybersecurity Governance framework leads to:

- Regulating internal information policies
- Improving Cybersecurity Risk Disclosure
- Promoting periodic review of security incidents
- Increasing management transparency to shareholders and customers

Studies have shown that banks that implement strong cyber governance become more capable of performing Risk Management for both financial and non-financial risks, particularly those related to information technology. Disclosure of Cyber Risks also contributes to improving transparency and raising investor confidence, which has a positive impact on the bank's financial position, as investors prefer banks that take global threats such as Electronic Attacks seriously. **(Dalia Hussein Elsayed, 2024, pp. 1-15)**

- **Reducing Liquidity Risk and Operational Risk arising from Cyber Attacks:**

Cyber Attacks, especially those targeting payment systems, can lead to the suspension of Banking Transactions or prevent customers from accessing their accounts, which directly affects: the bank's ability to meet withdrawals, manage daily liquidity, and maintain interbank transfers.

The Office of Financial Research (2017) report noted that Cyber Risks are not limited to technical aspects, but can also translate into Operational Risk and Liquidity Risk if they lead to System Disruption or disrupt vital financial services. The report also explained that System Disruption can cause immediate liquidity pressures and negatively affect the stability of Financial Institutions, especially if it coincides with a loss of customer confidence or deposit withdrawals. Consequently, Cyber Risks have become closely linked to Liquidity Risk, making Cybersecurity an important element in supporting Financial Stability for banks. Weak protection systems may also prompt some banks to increase their risk levels to offset losses, exposing them to greater financial risks. Conversely, effective protection systems and Incident Response Plans help to limit the operational impact of Cyber Attacks and reduce their repercussions on Bank Liquidity and banking operations. **(VIEWPOINT, 2017, pp. 1-12)**

- **Supporting internal review and Cyber Resilience to enhance bank stability:**

Cybersecurity plays a vital role in enhancing bank stability through internal review and security audits, as well as strengthening their resilience and ability to achieve Recovery from Cyber Attacks, where:

- Internal audit units assess the effectiveness of technical controls, detect Security Vulnerabilities before Security Breaches occur, monitor employee compliance with security policies, and ensure the implementation of Incident Response Plans, thereby supporting the stability of banking operations.
- At the same time, these measures contribute to building Cyber Resilience, enabling the bank to absorb the effects of Cyber Attacks, quickly restore systems, and ensure uninterrupted service delivery, thereby reducing financial impact and strengthening customer confidence.

Studies have shown that the quality of internal auditing is linked to lower Cyber Risks and faster Recovery from them, and that banks with advanced auditing units are more financially stable because they reduce potential Operational Losses and increase the bank's Cyber Resilience. The combination of effective internal auditing and the development of Disaster Recovery plans is a fundamental pillar for protecting the Financial System and the resilience of banks against Cyber Attacks. **(Ibtihaj Ismail Yaqoub, 2025, pp. 265-280)**

- **Supporting Digital Transformation and Financial Inclusion in a secure manner:**

Digital banking contributes to increasing the efficiency of the Banking Sector and the number of users, but at the same time it raises risk levels. Therefore, Cybersecurity is the key factor in ensuring that Digital Transformation does not lead to:

- Security Breaches that threaten customer confidence
- Disruption of digital channels
- Data Leakage of sensitive data belonging to e-service customers

Recent studies have confirmed that increased reliance on digital services in banks is accompanied by a rise in Cyber Threats, and that achieving Financial Inclusion and stability in digital services requires strong Cybersecurity measures, because any security breach leads to people shying away from digital services, thereby reducing bank revenues and undermining Financial Stability. **(Benaini Rahima, 2025, pp. 107-126)**

- **Enhancing trust and reducing reputational risk within the banking system:**

Any major cyber breach can lead to: loss of customer confidence, withdrawal of deposits, decline in the value of the bank's shares, and deterioration of its reputation locally and internationally. However, if a bank implements robust protection systems and clearly states its Cybersecurity policies, it sends a message to investors and customers that the bank is secure, which increases its Financial Stability. Some studies have shown that Cybersecurity Disclosure has a strong positive impact on banks' performance, profitability, and stability. **(Md. Waliullah, 2025, pp. 226-257)**

3. Cybersecurity Strategies to enhance the resilience and stability of banks:

With the aim of enhancing the resilience of the Financial Sector in general and the Banking Sector in particular, authorities should develop adequate national Cybersecurity protection strategies, accompanied by effective Regulatory Frameworks and supervisory capabilities, including the following: **(Jennifer Elliot, 2020, p. 01)**

- **Preparation of cyber maps and quantification of Cyber Risks:** A better understanding of the interdependencies in the global Financial System can be gained by mapping the most important operational and technological interconnections and critical infrastructure. Better integration of Cyber Risks into Financial Stability analysis would improve the ability to understand and mitigate system-wide risks, and quantifying the potential impact would help focus the response and encourage stronger commitment to this issue. Work in this area is still in its infancy, partly due to a lack of data on the impact of cyber events and the challenges of modelling, but it needs to be accelerated in line with its growing importance.

- **Regulatory convergence and Cybersecurity Governance:** Enhancing international convergence in cybersecurity regulation and Regulatory Supervision reduces compliance costs and improves the efficiency of oversight of cross-border banking institutions. These efforts are most effective when complemented by strengthening Cybersecurity Governance within banks, by integrating Cyber Risks into the Enterprise Risk Management framework and ensuring that senior management boards oversee them as a direct source of financial and Systemic Risk. Coordination between international bodies such as the Financial Stability Board and

the Basel Committee on Banking Supervision, and national authorities, is a key pillar for establishing uniform standards that promote Financial Stability.

- **Resilience and operational robustness:** With Cyber Attacks becoming more frequent and complex, the banking system's ability to respond quickly, achieve Recovery and resume critical functions is crucial to protecting Financial Stability and maintaining confidence. Incident Response and business continuity strategies are an integral part of the concept of operational resilience, which focuses on ensuring the Continuity of Banking Services even in the event of System Disruption. However, these strategies remain underdeveloped in many developing economies, calling for technical and institutional support, as well as clear international arrangements to support Recovery in cross-border Financial Institutions and services.
- **Advanced testing and Operational Risk and technical risk management:** Enhancing cyber preparedness in the Banking Sector requires the adoption of advanced periodic tests, such as Cyber Stress Testing, Simulation Exercises and virtual attacks, and linking their results to financial stress tests to measure the potential impact on capital and liquidity. It is also important to adopt modern technical approaches, such as the 'Zero Trust Model,' and to use advanced analytics and artificial intelligence for Early Detection of Cyber Threats, thereby reducing the likelihood of cyber incidents turning into large-scale financial crises.
- **Willingness to collaborate and share information:** Enhancing the exchange of information on Cyber Threats, Cyber Attacks and responses between the public and private sectors contributes to raising the level of deterrence and improving Systemic Risk Management. However, such cooperation faces challenges related to national security and data protection considerations. Regulatory agencies and central banks must therefore develop clear and effective protocols for information sharing that operate within these constraints, while encouraging the adoption of global standards, shared information platforms and trust-based networks.
- **Stronger deterrence and enforcement:** Strengthening deterrence against Cyber Attacks requires making them more costly and risky for perpetrators through effective measures to confiscate the proceeds of cybercrime and prosecute offenders. Close international cooperation between law enforcement agencies and authorities responsible for critical infrastructure and Cybersecurity helps reduce risks at their source, thereby supporting global Financial Stability, especially given the cross-border nature of cyberspace.
- **Cyber capacity and culture development:** Developing human and institutional capacity in Cybersecurity and building a risk-aware culture within Financial Institutions are fundamental to enhancing Financial Stability and supporting Financial Inclusion. Developing economies and low-income countries are more vulnerable to Cyber Risks. and the COVID-19 pandemic has highlighted the vital role of digital technology in ensuring the continuity of financial services. Integrating Cybersecurity into financial development strategies is therefore a necessity, as the spread of Cyber Threats in any country has a negative impact on the security and stability of the entire global Financial System.

Given that Cyber Attacks often originate outside the financial company's home country and that financial gains can be transferred across borders, Cyber Risks must

be successfully addressed. While Cybersecurity incidents are inevitable, the Financial Sector needs the capacity to provide essential services during such disruptions. Financial firms should therefore develop and test response and Recovery procedures, and national authorities should also implement response protocols and Crisis Management frameworks and ensure their effectiveness. However, an International Monetary Fund survey of central banks and supervisory authorities indicates that cybersecurity policy frameworks remain largely inadequate, particularly in emerging market and developing economies.

For example, only about half of the countries surveyed have national Cybersecurity Strategies or Regulatory Frameworks dedicated to Cybersecurity in the Financial Sector. **(Fabio Natalucci, 2024, p. 01)**

Conclusion:

In conclusion, it can be said that Cybersecurity has become the cornerstone of ensuring Financial Stability in the face of contemporary digital challenges. It is no longer merely a technical support function, but rather an indispensable strategic component for the continuity of banking operations and the safety of the Financial System as a whole. With the rapid pace of Digital Transformation within the Banking Sector and the expansion of Electronic Banking Services, there is a growing need to adopt advanced and innovative Cybersecurity Strategies that keep pace with these transformations, while at the same time being able to anticipate future Cyber Threats and mitigate their potential impact. The study also showed that the effectiveness of cybersecurity does not stop at protecting systems and data, but extends to enhancing confidence in banking institutions, ensuring the continuity of banking services, and reducing Cyber Risks that may threaten Financial Stability at the institutional and systemic levels. Therefore, embedding Cybersecurity within Prudential Policies and Banking Governance is a prerequisite for supporting the resilience of banks and achieving Financial Soundness in the digital age, enabling the Banking Sector to respond to increasing digital shocks with efficiency and flexibility.

The findings from the study may be summarized as follows:

- The issue of Cybersecurity is of concern to the global economic arena, given the current developments in information and communications technology and the accelerating pace at which institutions, particularly banks, are adopting Digital Transformation strategies.
- Cyber Risks are a potential source of Financial Instability, given their ability to cause operational and financial disruptions that affect banks' performance.
- Raising security awareness among customers and users is a key factor in mitigating the risks associated with Cyber Threats.
- Adopting effective Cybersecurity Strategies helps reduce potential losses and enhance the Continuity of Banking Services.
- Finally, it is clear that Cybersecurity is no longer a separate technical issue, but has become a strategic component intertwined with Financial Stability, Digital Transformation and Banking Governance, as poor management can turn digital risks into Systemic Risk that affects the Financial Sector as a whole.

References:

- ABDELKADER, S. (2024, September 26). The Contribution of Data Cybersecurity to Enhancing Customer Trust in Electronic Banking Services in the Wilaya of Ghardaïa – A Field Study of a Sample of Local Development Bank (BDL) Customers. PhD Thesis, 46.
- Abdullelah Saeed Al Mohayya, A. A. (2025). The impact of social engineering on cybersecurity risks in banks in the city of Riyadh in the Kingdom of Saudi Arabia. Journal of Economic, Administrative and Legal Sciences (JEALS), 09(01), 08.
- Al-Obaidi, H. J. (2023). The Impact of Financial Stability Indicators on the Stock Value of the Banking Sector in the Iraq Stock Exchange. Journal of Management and Economics / Al-Mustansiriyah University, 48(141), 36.
- Al-Shaikh, J. S. (2023). The Role of Cybersecurity Determinants on Financial Inclusion at Islamic Banks Operating in Jordan. International Journal on Humanities and Social Sciences(52), 104.
- Amamra Yasmine, H. T. (2020). The role of the central bank in achieving financial stability by ensuring financial soundness- Algeria case study -. Journal of El-Maqrizi for Economic and Financial Studies, 04(02), 39.
- Androsova, E. V. (2016). Simulation Evaluation Of Financial Stability Of The Banking Sector Of Ukraine. International Scientific And Production Journal(30), 124.
- Azzeddine, D. (2022). Economic and Financial Effects of Cyber Attacks in the Light of Digitization: Results, Experiences and Solutions- Algeria case study -. Journal of Economic Integration, 10(02), 114.
- Benaini Rahima, S. B. (2025). Cybersecurity: An imperative necessity to enhance digital financial inclusion and financial stability. Journal of economics and management research, 06(02), 107-126.
- Boudayar, H. (2023). The Role of Central Banks in Achieving Financial Stability (From an Islamic Finance Perspective): A Case Study of the Bank of Algeria 1962-2023. Doctoral Thesis in Finance and Banking, 50.
- Crockett, A. (1997). The Theory and Practice of Financial Stability. GEI newsletter issue no6 (united kingdom : gonville and caiuscollege cambridge).
- Dalia Hussein Elsayed, T. H. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. Future Business Journal, 10(01), 1-15.
- Djeghel Djamila, Z. A. (2023). Cybersecurity and financial inclusion in the context of the digital transformation of the financial sector (threatsecurity and hedging mechanisms). Economic Development Review, 08(01), 309.
- Elbardony, N. I. (2025). The role of cybersecurity governance in enhancing disclosure of cybersecurity risk management and its impact on improving financial performance: An empirical study on banks listed on the Egyptian Stock Exchange. Alexandria Journal of Accounting Research isued by the Department of Accounting, 09(01), 15-16.
- Fabio Natalucci, M. S. (2024). Rising Cyber Threats Pose Serious Concerns for Financial Stability. International Monetary Fund BLOG, This blog is based on Chapter 3 of the April 2024 Global Financial Stability Report, Cyber Risk: A Growing Concern for Macrofinancial Stability., 01.
- Farida Mouhoub, S. L. (2022). Analysis of the role of financial soundness indicators to insure financial stability in Arab banking sector. Journal of Economic Analysis and Development Studies, 38.
- Henock Mulugeta Melaku, 2023, Context-Based and Adaptive Cybersecurity Risk Management Framework, Risks, 11 (101), P 07.
- Ibtihaj Ismail Yaqoub, Z. H. (2025). The Role of Internal Auditing in Recovering from Cybersecurity Risks in the Iraqi Islamic Banking Sector. Journal Port Science Research, 08(Special Issue), 265-280.
- ISO. (2012). Information technology – Security techniques – Guidelines for cybersecurity. ISO/IEC 27032:2012.
- Jabr, G. J. (2023). Cybersecurity Threats to Electronic Banks and Their Mitigation Mechanisms. Academic Journal of Social Sciences, 01(01), 54-55.
- Jennifer Elliot, N. J. (2020). Cyber Risks… the New Threat to Financial Stability. International Monetary Fund BLOG.
- Khamiss, S. A. (2024). The Impact of Bank's Cybersecurity Risk Disclosure Alternatives on Their Clients and Shareholders Judgments: An Empirical Study. Journal of Accounting Research, 11(03), 911.
- Md. Waliullah, a. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. American Journal of Advanced Technology and Zngineering Solutions, 01(01), 226-257.
- Senoussaoui Fatna, B. M. (2022). Strengthening financial stability in Algeria in the light of the Basel Convention 3. Creativity Journal, 12(01), 208.
- Souag Abdelkader, B. B. (2023). The impact of cyber security readiness on electronic banking services by reducing perceived risks: Case study of BDL Bank in Ghardaia. Journal of Modern Research in Economics, 06(01), 359-360.
- VIEWPOINT. (2017). Cybersecurity and Financial Stability: Risks and Resilience. Office Of Financial Research OFR, 17(01), 1-12.