مجلة الأصيل للبحوث الاقتصادية والإدارية
El - Acil Journal for Economic and Administrative Research
ISSN: 2571-9866
EISSN: 2661-7854
Volume:10 / N°2/*October 2026, PP92-113*

Cybersecurity Threats and Their Implications for the Sustainability of Innovation in the Islamic Financial System

التهديدات السيبرانية وانعكاساتها على استدامة الابتكار في النظام المالي الإسلامي

***BAALOUL Newfel**
University Of Oum El Bouaghi
newfel.baaloul@univ-oeb.dz

BOUTEMINE Wiame
University Of Oum El Bouaghi
wiame.boutemine@univ-oeb.dz

Received:16/07/2026 *Accepted:26/10/2026* *Published:31/10/2026*

Abstract :
With technological and digital acceleration, many variables have emerged in this field, and since countries strive to win the race of competition and to establish control over markets, they are always in continuous pursuit of keeping pace with digital transformation, which exposes them and their financial systems to highly dangerous threats, the most important of which are cyber security threats that have started to affect infrastructures and undermine customer trust. The subject takes on greater importance when viewed from the perspective of Islamic Sharia, which, despite its religious nature and credibility, is not immune from being exposed to internal and external security risks and threats.
The study has demonstrated, through addressing both the experience of Bank Syariah Indonesia and the Nobitex platform in Iran, that financial systems are at all times exposed to the risks of cyber threats, whether internal or external. The matter is further aggravated by the absence of competent human resources, in addition to the fact that the pace of digital innovation is faster than the ability of Islamic financial institutions to keep up with cyber risks, which increases the severity of attacks that not only result in financial losses but also extend to geopolitical losses.
Key words: Cybersecurity, Threats, Sustainability, Islamic Financial System, Innovation.
JEL classificationcodes:: G21, G32, O33, Q01f

* ***Corresponding author***

1. Introduction.

Over the past two decades, the rapid digital transformations in financial systems have reshaped the ways financial services are designed and regulated worldwide. Amid these transformations, the Islamic financial system has adopted financial innovations and FinTech solutions to ensure compliance with the principles of Shariah based on justice, transparency, and prosperity, as well as to expand access and enhance competitiveness. In the digital age, however, cyber threats have emerged as one of the most pressing challenges facing economic and financial systems globally, evolving to include the disruption of critical infrastructure and the threat to financial stability. This issue becomes even more significant in the context of the Islamic financial system, due to the growing reliance on digital infrastructure, which has exposed Islamic financial institutions to increasing levels of cybersecurity risks.

Despite the opportunities brought by innovation, the expansion of digital infrastructures has introduced a set of security vulnerabilities. Cyberattacks targeting banks, cryptocurrencies, and digital platforms have grown in both scale and complexity, posing direct threats not only to financial stability but also to undermining the confidence of clients in financial institutions. Incidents such as the ransomware attack on Bank Syariah Indonesia and the large-scale breach of the Nobitex cryptocurrency platform in Iran highlight the fragility of cybersecurity frameworks and clearly reveal the potential of such threats to erode trust in Islamic finance. The core problem lies in the widening gap between the speed of innovation and the ability of institutions to anticipate and manage cyber risks in a sustainable manner.

This research aims to examine the implications of cyber threats on the sustainability of innovation in the Islamic financial system through three dimensions: first, analyzing the nature and scope of cyber risks facing financial institutions; second, assessing the vulnerabilities specific to Islamic financial institutions in light of recent international experiences; and third, exploring strategies for integrating robust cybersecurity practices into the innovation process to ensure long-term resilience.

The significance of this study lies in its dual contribution. From a theoretical perspective, it enriches the growing literature linking cybersecurity and financial innovation, particularly within the context of Islamic finance. From a practical perspective, it provides insights for policymakers, regulatory bodies, and financial institutions on how to strengthen institutional resilience, safeguard trust, and align digital innovation with the Shariah objectives of justice and sustainability.

2. Cybersecurity Threats:

The cybersecurity framework developed by the US National Institute of Standards and Technology (NIST) following the Cybersecurity Enhancement Act of 2014 has become a key reference for managing cybersecurity risks within organizations. This framework is based on three main components: the core, which provides the guidelines and standards necessary to deal with threats; implementation levels, which determine the degree of an organization's readiness to apply these standards; and profiles, which allow an organization's needs to be aligned with the required security activities. The framework is divided into five interrelated

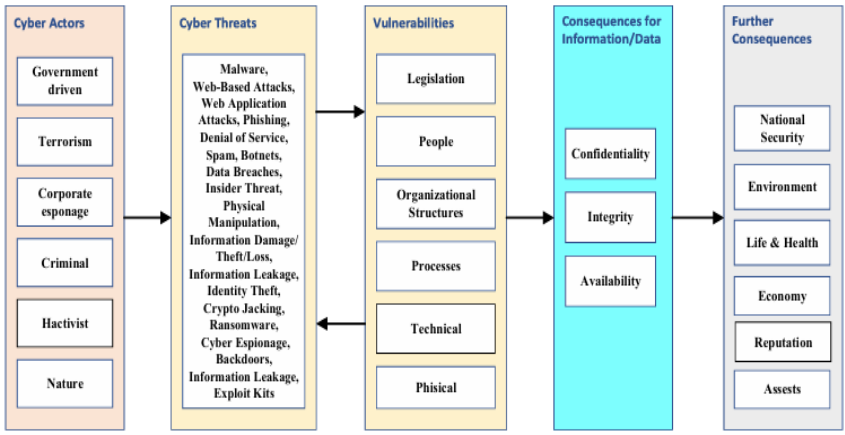
functions, starting with identifying and understanding the risks and assets at risk, then protecting by putting in place the necessary controls to secure data, quickly detecting any potential threats, followed by effective incident response, and finally recovery to ensure that systems return to safe operation (Ahsan, Nygard, Gomes, Chowdhury, & Rifat, 2022, p. 534).

Cyber security is a comprehensive system that encompasses technology, resources, organizational structure, and institutional culture, with the primary goal of securing the digital space and the interconnected systems against various threats and risks. While we benefit from the rapid and continuous advancement of technology, these changes are being integrated into the critical infrastructure, which constitutes the backbone of the overall systems, networks, and assets that are essential for national security, societal safety, and economic stability. Ensuring their uninterrupted operation becomes imperative, as they cover vital sectors without which normal life cannot continue, such as agriculture, water, energy, transportation, aviation, and nuclear systems.

A report issued by the National Institute of Standards and Technology (NIST) in the United States has warned that cyber threats exploit the high degree of complexity and interconnectivity within critical infrastructure systems, making them capable of threatening national security, the economy, and public safety. These threats are no longer limited to fraud or data theft but have expanded to include cyber terrorism, extortion, threats to national security, and even the disruption of vital resources. In this sense, the options available to attackers have multiplied in a dangerous way, which obliges societies to develop comprehensive mechanisms to address these risks, whether through legislation, governance strategies, security plans, or even tackling the associated societal dimensions (Abdulla, Mohamed, & Suriyati, 2020, p. 2).

Cybersecurity represents a complex system that goes beyond being merely a set of technical tools, as it constitutes a comprehensive framework where the technological dimension intersects with social, organizational, and cultural factors. This complexity requires analysis through various scientific theories, such as social cognitive theory, distributed cognition theory, and socio-technical theory, which explain how individuals interact within the digital space and highlight their role in either disseminating information or failing to protect it. Furthermore, data security is considered a fundamental pillar for institutional sustainability, since any data breach not only results in direct financial losses but also causes reputational damage, legal penalties, and risks related to identity theft or the criminal exploitation of data. In this regard, cybersecurity operates along three interrelated axes: prevention, through building robust systems and protecting critical infrastructure; detection, by monitoring threats and isolating them before they spread; and response, which involves containing the attack, isolating affected systems, and documenting evidence for legal proceedings(Schiliro, 2022, pp. 3-7).

Figure01: Threats and vulnerabilities affect cybersecurity.



Source: Romuald Hoffmann and all, Risk based approach in scope of cybersecurity threats and requirements,2020, Procedia Manufacturing 44 (2020) 655–662,p657.

International cooperation is considered a cornerstone in National Cybersecurity Strategies (NCSS), yet the manner in which it is addressed differs from one country to another. Some countries merely refer to international cooperation in general terms without further specification, whereas others are more explicit, stipulating regional cooperation with neighboring countries, multilateral cooperation with several states, or cooperation with specific international organizations such as the United Nations, or regional blocs such as the European Union.

The European Union issued a legislative directive (EU Directive 2016/1148) aimed at raising the level of cybersecurity in a harmonized manner across all its member states. This directive required states to adopt a national cybersecurity strategy whereby each country must set clear strategic objectives and concrete policy measures for protecting networks and information systems. It also established the Computer Security Incident Response Teams Network (CSIRT Network), a European network that brings together national teams specialized in responding to cybersecurity incidents, with the purpose of ensuring swift coordination in the event of an attack. Furthermore, the directive obliged member states to designate competent national authorities and national points of contact, so that each country would have an official body responsible for managing and overseeing cybersecurity issues.

Some researchers who conducted a comparative study of the NCSS in ten different countries observed that these strategies share common objectives such as strengthening cybersecurity culture through education, fostering international cooperation, promoting research and development, raising

societal awareness, and building trust in cyberspace so that it may serve as a safe environment for citizens, businesses, and governments.

However, alongside these shared objectives, there are country-specific differences. A notable example is Norway, whose national strategy explicitly requires private companies to digitalize their activities in a secure and reliable manner, and to assume responsibility for protecting themselves against cyber incidents (Strzępek, 2023, p. 34).

3. Financial System:

The financial system represents the backbone of any economy, as it constitutes the main driving force that is reflected in the level of economic activity within the state. It is not merely a set of institutions, but rather an integrated framework that encompasses financial institutions (such as banks and insurance companies) and financial markets (such as stock exchanges, bond markets, and sukuk) which provide the necessary mechanisms for the exchange of assets and financial instruments.

The financial system is not merely a channel for transferring funds; rather, it performs a set of strategic functions that support both economic growth and stability, which can be detailed as follows:

3.1. Full utilization of financial resources: The financial system ensures the effective use of funds available with surplus units (households or institutions holding savings) by transferring them to deficit units (households or institutions in need of financing) to be invested in productive projects, thereby preventing the underutilization of financial resources.

3.2. Monetary stability: This is achieved by maintaining a balance between the supply of and demand for money in line with the needs of the economy, thus preventing inflation or deflation and reinforcing price stability as well as the overall strength of the economic system.

3.3. Capital accumulation and productivity growth: The financial system facilitates the allocation of savings toward the most productive investments by identifying investment opportunities and channeling resources accordingly, which contributes to higher productivity levels in the long run.

3.4. Economic growth: The financial system is a rapidly growing global industry that contributes to facilitating the exchange of goods and services, mobilizing and efficiently allocating financial resources, and managing risks-thereby supporting sustainable economic growth (ATAMNIA & MEZHOUD, 2024, pp. 65-67).

4. Islamic Financial System:

The Islamic financial system is fundamentally based on the principles of Shariah as outlined in the Qur'an and the Sunnah, which define the rules governing wealth, private ownership, the means of acquisition and disposal, as well as the regulations related to public finance, including the

collection of public revenues (such as zakat and other legitimate levies) and their allocation in accordance with the objectives of Shariah.

The Islamic financial system consists of revenues and expenditures prescribed or regulated by Islamic texts, and it is also viewed as an institutional, legal, and technical framework encompassing financial institutions (such as Islamic banks), laws and regulations, and mechanisms that facilitate the creation and exchange of financial assets and the allocation of funds, but always in line with the expected return on investment and in full compliance with Shariah principles.

The Islamic financial system is founded on pillars that distinguish it from the conventional system. Chief among these is the belief that ultimate ownership belongs to God Almighty, while humans are merely trustees or stewards of wealth, managing it in a way that pleases God and serves the public interest rather than solely pursuing personal gain. It also prohibits the hoarding of wealth and discourages keeping money idle or out of circulation; instead, it must be invested and reintegrated into the economy so that its benefits are shared broadly, while fulfilling its prescribed religious obligations. Furthermore, it prohibits monopoly practices, such as withholding goods and services to raise prices and harm people, thereby ensuring fairness and equal access for all. Lastly, it emphasizes social solidarity, requiring the community to collectively assume responsibility for supporting the poor and the needy through mechanisms such as zakat, waqf, and charitable giving, thereby reinforcing mutual support among individuals and promoting social justice (Khledj & Abbou, 2024, pp. 120-122).

Since the real world is full of imperfections and deficiencies (such as taxes, asymmetric information, and transaction costs), financial innovations emerge as optimal solutions to address these problems or as responses to new opportunities. If the world were ideal-free of taxes, regulations, asymmetric information, and transaction costs-financial innovation would have no added value and would merely be considered a “neutral” change without benefit. From this perspective, some scholars view innovation as a neutral function of the financial system, while others see it as a direct outcome of financial institutions using it as a tool for competition and strengthening their position. In this context, Merton proposed a framework that identifies six fundamental functions of the financial system: transferring funds across time and space, pooling resources, managing risk, providing information to support decision-making, addressing agency problems, and facilitating payment systems. Other researchers have added functions such as enhancing liquidity and generating financing. Thus, financial innovation can be viewed either from a static perspective, which analyzes its functions without considering the timing of its emergence, or from a dynamic perspective, which interprets it as a direct response to environmental and economic changes, with the timing of innovation reflecting these changes (Tufano, 2003, pp. 313-314).

Financial innovation is not always positive, as it has carried hidden risks and costs. Financial institutions, due to competition and the declining

profitability of traditional products, constantly strive to create new and complex products that boost their profits, even if these products are poorly understood or highly risky. This has led to the emergence of "toxic" financial products that contributed to financial crises, such as collateralized debt obligations (CDOs) backed by credit default swaps (CDS).

Moreover, some reforms, such as the Dodd-Frank Act, attempted to make regulation more modern and stringent. However, there remains a common assumption that financial innovation is inherently good, while in reality, some of it is costly and dangerous. This is because it increases market complexity, making it difficult for managers, investors, and even regulators to fully grasp the real risks involved. As a result, decision-makers may reap short-term profits while society as a whole bears the costs of crises once these risks materialize (Johnson & Kwak, 2012, p. 7).

The financial sector has become increasingly vulnerable to cyber threats due to its heavy reliance on technology and digitalization. These threats are not limited to the theft of money but also include the theft, alteration, or deletion of data, which can lead to serious consequences such as:

- Damaging the reputation of banks and reducing customer trust;
- Threatening the stability of financial markets and influencing stock prices;
- Increasing complexity and security risks as a result of dependence on third parties (technology firms, digital solutions).

Moreover, fraud resulting from cyberattacks against banks and financial institutions cost end-users more than **$10.5 billion in 2016**, marking an increase of **122% compared to the previous year**. During the same period, online transactions rose by 10%. Consequently, online lenders have been under growing pressure to implement stronger and smarter authentication mechanisms in order to accelerate the approval of legitimate loans and prevent fraudulent activities.

In this context, the **NIST Cybersecurity Framework**, along with the framework of the **European Union Agency for Network and Information Security (ENISA)**, has emerged, both identifying five core functions to protect digital assets:

a. Identify: Understanding organizational risks to minimize them.
b. Protect: Designing safeguards to reduce the impact of incidents.
c. Detect: Implementing activities to identify the occurrence of cyberattacks.
d. Respond: Taking appropriate actions once a security event occurs.
e. Recover: Restoring compromised capabilities and services promptly (AL-ALAWI & AL-BASSAM, 2020, pp. 1527-1528)

The integration of financial technology (FinTech) and cybersecurity has created a new reality within the financial system. Significant

opportunities have emerged, such as decentralized finance (DeFi), digital currencies, and blockchain transactions, which offer major advantages including transparency, decentralization, and cryptographic protection. However, these innovations have not eliminated risks; instead, they have introduced new security challenges. Despite its robustness, blockchain is not entirely immune, as documented cases have revealed vulnerabilities in smart contracts, theft of cryptographic private keys, and breaches of digital trading platforms.

Artificial Intelligence (AI) and Machine Learning (ML) have become a double-edged sword. On one hand, AI has enhanced institutions' ability to analyze massive volumes of financial data to detect unusual or anomalous patterns that may indicate attacks or suspicious activities, automate fraud prevention rather than relying solely on human intervention, and improve the speed and accuracy of threat detection. On the other hand, major regulatory bodies such as the European Central Bank (ECB), the U.S. Securities and Exchange Commission (SEC), and the Financial Action Task Force (FATF) have imposed strict standards and regulations, such as the GDPR, PCI DSS, and CMMC, to ensure that financial institutions adhere to robust security measures that mitigate risks and protect financial stability. These regulations also encourage the inclusion of modern security strategies, such as continuous monitoring for real-time threat detection, multi-layered security architectures, "Zero Trust" models which assume no entity should be trusted by default without verification and Endpoint Detection and Response (EDR) systems for monitoring endpoint devices.

At the same time, cybercriminals have begun exploiting adversarial AI techniques, making it necessary to develop more advanced defensive AI-driven systems. Moreover, the human factor remains the weakest link in the financial cybersecurity chain. Many cyberattacks do not rely solely on breaching technical systems but rather exploit human behavior. Examples include phishing fraudulent emails or links that trick users into disclosing personal data social engineering, which manipulates users psychologically to reveal sensitive information, and credential theft, often facilitated through weak or accidentally disclosed passwords.

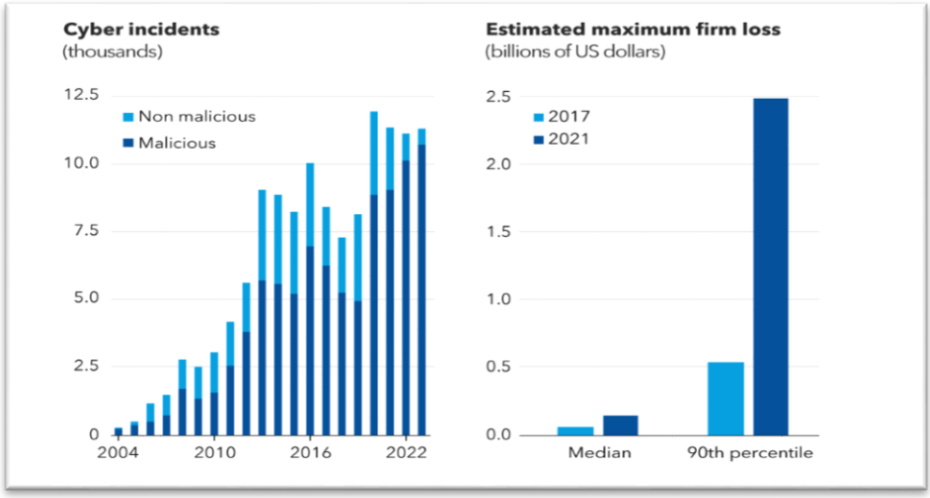
In addition, the shift toward digital financial services, such as online banking platforms, mobile payment applications, and cloud-based financial services, has improved system efficiency and accessibility but simultaneously expanded the attack surface, commonly referred to as the "Attack Surface." Cybercriminals are increasingly targeting Application Programming Interfaces (APIs), which act as bridges that enable data exchange between banks, fintech companies, and consumers. Since these interfaces are critical communication points within the financial system, any vulnerability in them provides

attackers with direct access to sensitive data, thereby escalating the severity of attacks. Similarly, the financial sector's reliance on third parties, such as cloud service providers, makes the security of these entities an inseparable part of the overall security of financial institutions.

Financial reports published by IBM Security have confirmed that misconfigured cloud environments and weak API protection were among the main causes of financial data breaches. These breaches not only led to massive direct financial losses but also resulted in heightened regulatory scrutiny. Consequently, financial institutions are now required not only to enhance their security performance but also to comply strictly with regulatory standards (Adejumo & Ogburie, 2025, pp. 1542-1546).

5. **Cyber security and financial stability:** Since the COVID-19 pandemic, the number of cyberattacks has doubled, along with the scale of losses, as demonstrated by the case of the U.S. company Equifax, which incurred fines exceeding one billion dollars after the data of nearly 150 million clients was breached in 2017. Reports confirm that the severity of such attacks is continuously increasing, with losses rising more than fourfold since 2017 to reach 2.5 billion dollars, in addition to indirect damages such as reputational harm. The financial sector, in particular, is frequently targeted due to its handling of vast amounts of sensitive data and transactions, making it a primary target for criminals seeking to steal money or disrupt economic activities. Attacks on financial institutions represent about one-fifth of all recorded incidents, with banks being the most exposed. Cyber incidents can also generate severe repercussions for economic activity by disrupting essential services such as payment systems. For instance, in December, the Central Bank of Lesotho was subjected to an attack that disrupted the national payment system and consequently halted transactions across local banks. Moreover, the growing reliance of financial firms on external technology service providers especially with the rising role of artificial intelligence although enhancing efficiency and operational resilience, can also lead to large-scale shocks if these providers are attacked. An example of this occurred in 2023, when a ransomware attack on a cloud service provider disrupted the operations of 60 credit unions in the United States simultaneously. This underscores that cyber risks are intensifying as a result of digital transformation and geopolitical tensions, thereby making it imperative to develop strong policies and governance frameworks to address them.

Figure o2: Cyber incidents and estimated maximum firm loss (2004-2022)

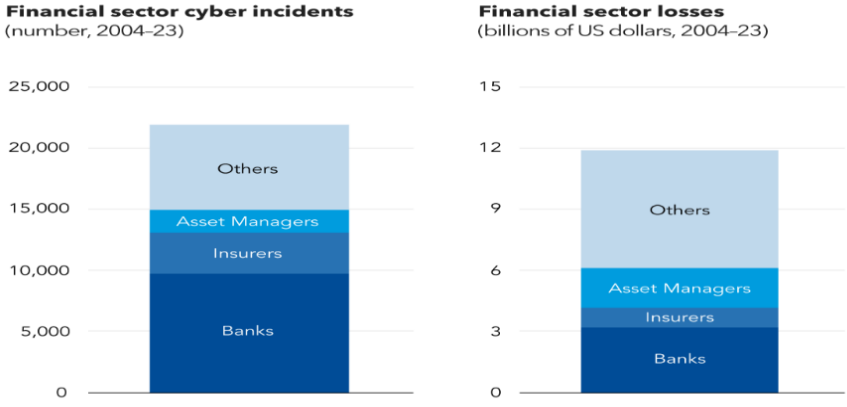


Source:[Rising Cyber Threats Pose Serious Concerns for Financial Stability]

With the aim of strengthening the resilience of the financial sector, authorities must establish adequate national strategies for safeguarding cybersecurity, accompanied by effective regulatory frameworks and supervisory capacities, including:

- The periodic assessment of the cybersecurity environment and the identification of potential systemic risks arising from interconnections and concentrations, including those associated with external service providers.

Figure 03: Financial sector cyber incidents and losses by subsector (2004-2023)



Source:[Rising Cyber Threats Pose Serious Concerns for Financial Stability]

Encouraging cyber maturity among financial sector firms, including the engagement of cybersecurity experts on boards of directors, which is supported by the analyses presented in the chapter indicating that strengthening cyber governance may help mitigate cyber risks.

- Enhancing cyber hygiene of firms, meaning the security and integrity of their online systems (including the use of anti-malware tools and multi-factor authentication), together with training and awareness.
- Giving priority to the collection and reporting of data on cybersecurity incidents and the sharing of information among financial sector participants to strengthen collective preparedness (Natalucci, Qureshi, & Suntheim, 2024).

6. Notable Cyber Incidents in the Financial Services Sector:

ION, a financial trading services group based in Dublin, Ireland suffered a ransomware attack by Lockbit. It impacted the firm's cleared derivatives platform, affecting multiple customers including banks, brokerages and hedge funds in the US and the EU. These firms were unable to process their transactions and had to find alternative means to do business. ION reportedly paid Lockbit to get their systems back online.

Latitude Financial, an Australian firm that provides loans, credit cards and insurance suffered an extortion attack by an undisclosed group. The personal and medical information of 7.9 million customers in Australia and New Zealand was reportedly compromised. Latitude believe that the attackers used the account of a third party who had privileged access into their network. Latitude did not pay the ransom.

Roughly 100 (actual number likely to be much higher) companies in the broader financial services sector worldwide were impacted by the mass exploitation of the MOVEit file transfer application by the Clop extortion group. One of the many victims was Fiserv, a global payments processing provider. They were forced to notify their customers, including Flagstar who had 830,000 customers impacted.

In November, it became apparent that threat actors were actively exploiting a severe vulnerability in Citrix Netscaler software, known as Citrix Bleed. The same month, several major organisations, including those in the financial services sector were seemingly compromised by ransomware actors. Whilst few organisations admitted it (Boeing did), researchers noted that many firms that had suffered ransomware attacks had apparently failed to patch this vulnerability, meaning it was possible that Citrix Bleed was used. Breached FSI firms in November 2023 included: November 2023

- **Industrial and Commercial Bank of China (ICBC):** The US subsidiary of the "world's largest bank" confirmed they suffered a ransomware attack at the hands of Lockbit. ICBC could not access their systems, forcing the bank to inject capital into its US Division to settle trades and repay debts.
- **TCW:** The Global Asset Management firm with $202 billion under management was compromised by Lockbit.
- **MeridianLink**: This US company provides software tools to the financial services industry. Affiliates of the ALPHV ransomware

operation took to submitting the incident to the SEC in the US themselves to add pressure to MeridianLink to pay the ransom, something not previously seen from a ransomware actor.

- **Fidelity National Financial (FNF):** Was attacked by ALPHV, and later admitted that 1.3 million customer records were compromised. The attack caused major disruption for customers trying to manage their loans and mortgages (QBE Cyber Threat Intelligence Team, 2024, p. 4).

Table01: Pros and Cons of Cyber Security in Finance.

Pros	Cons
Enhanced protection of sensitive financial data	High implementation and maintenance costs
Improved customer trust and loyalty	Potential for system slowdowns due to security measures
Compliance with regulatory requirements	Complexity in managing multiple security tools
Reduced risk of financial losses due to cyber attacks	Need for continuous updates and staff training
Improved operational resilience	Possible false positives leading to operational disruptions

Source: Cyber Security in Finance: Key Threats and Strategies.

Financial institutions remain prime targets for cyberattacks by a wide range of actors due to their potential for generating substantial financial returns. Industry sources indicate that the financial sector accounts for **15% of all cyberattacks worldwide**, the highest percentage compared to any other sector. The risks of cyberattacks are not limited to the financial institution itself but may extend to pose a threat to the **financial system as a whole**.

If a cyberattack is limited to the theft of financial data or proprietary information, this does not immediately halt the institution's financial operations; however, it does cause reputational damage, which may result in a loss of investor and customer confidence in the institution's ability to sustain itself and generate future profits. The situation becomes far more serious if the attack involves the **corruption of core data or internal systems**, as the institution would no longer be able to rely on the accuracy of its information and transactions. This creates a broader **crisis of confidence in the financial system**, potentially prompting market participants to withdraw or suspend financial dealings.

7. Response to Cyber Threats

In 2013, plans were made to allocate nearly USD 46 billion globally to cybersecurity, as it has ceased to be a secondary option and has instead become a top priority. Institutions are making substantial investments in various initiatives to strengthen their defenses, such as developing

protection technologies, monitoring threats, and building response plans to address cyberattacks. The first line of defense lies in protecting internal systems through measures such as conducting network penetration tests to identify vulnerabilities, imposing strict access control policies on system privileges, and implementing regular security updates. However, this is no longer considered an effective or sufficient solution for risk management. In Canada, efforts are underway to ensure that cybersecurity practices incorporate the necessary features to address elevated threat levels. The Office of the Superintendent of Financial Institutions (OSFI) has issued cybersecurity guidance to assist federally regulated financial institutions in assessing the adequacy of their security practices and identifying the changes required to align with industry best practices. International organizations have also been working to update their policy frameworks to keep pace with the evolving risks arising from cyber threats. The Committee on Payments and Market Infrastructures (CPMI) has published a report on current cybersecurity practices within financial market infrastructures (CPMI, 2014). The Bank of Canada has adopted the general risk-management guidance issued by this committee as the standard for designated infrastructures and fully expects to integrate any subsequent guidance related to cybersecurity (Gallagher, McMahon, & Morrow, 2014, pp. 48-51).

8. Best Practices for Securing the Financial Sector

As cyber threats grow increasingly complex, safeguarding the sensitive data and information of financial organizations becomes more difficult. To effectively protect these institutions, it is essential to adopt a set of best practices, the most notable of which include:

Implementing a Multi-Layered Security Approach: Designing a defense system that contains multiple protective barriers at the same time, such as firewalls to block unauthorized access, intrusion detection systems to monitor suspicious activities and identify malicious attempts, anti-malware programs to detect and neutralize viruses, and finally, regular security audits to ensure these measures remain up to date.

Implementing a Data-Centric Security Model: Classifying data according to its level of sensitivity, so that highly critical information—such as financial records or customer data—is handled with stricter measures. Strict access controls are then enforced, ensuring that no employee or external party can access such information beyond what is necessary.

Conducting Regular Risk Assessments: The institution regularly carries out comprehensive risk assessments to identify potential vulnerabilities that attackers might exploit, while also reviewing the effectiveness of existing security measures and their resilience against emerging threats.

Fostering a Security-Aware Culture: This includes organizing periodic training programs, conducting phishing simulation exercises, and clearly communicating security policies so that every employee understands their role in safeguarding the organization's cybersecurity.

Establishing a Vendor Risk Management Program: Monitoring vendors or external service providers with access to the organization's data or systems and subjecting them to strict security requirements, such as adhering to regular installation of security updates and undergoing periodic reviews and audits to ensure compliance with the required standards.

Cyber risks have become increasingly complex and cross-border in nature, and the figures reported (such as the U.S. economy losing between $57 and $109 billion in 2016, a 23% increase in costs within a single year, and global cybersecurity spending amounting to $124 billion in 2019) reveal that the economic impact of cyberattacks is extremely significant, particularly on the financial services sector. Although financial institutions spend enormous amounts on cybersecurity reaching approximately $124 billion globally in 2019 the scale of risks remains greater than these investments (Sentinelone, 2025).

The severity of these threats lies in the fact that they have become more organized and deliberately targeted, executed over extended periods to maximize impact, and are often difficult to detect in time, as data or backup copies may already be compromised by malicious software without the institution's knowledge. Moreover, investment in cybersecurity cannot be left solely to individual financial institutions, since cybersecurity essentially represents a *public good* that benefits society and the financial system as a whole, not just the institution making the investment.

The problem is further compounded by the fact that many financial institutions rely on shared services and infrastructures, such as payment platforms or cloud service providers, which makes them collectively vulnerable if one shared service is subject to a large-scale cyberattack. This is where *externalities* arise, as the risk from an attack does not affect just a single institution but extends to the financial system as a whole. In addition, the *free-rider problem* emerges, whereby some institutions may depend on others within the shared network to invest in strengthening security without bearing the same costs themselves. If every institution adopts this mindset, the result will be collective underinvestment in cybersecurity (Mester, 2019, pp. 2-5).

With the expansion of the digital economy, cybersecurity is no longer merely a technical safeguard but has transformed into a strategic factor for ensuring the resilience of economic and social systems, thereby becoming directly linked to sustainable development. The United Nations' Sustainable Development Goals (SDGs) have highlighted the role of technology in achieving them, and cybersecurity emerges as a key enabler that protects the digital technologies driving progress toward these goals. From ensuring access to clean energy (Goal 7) to supporting sustainable industrialization (Goal 9) and fostering innovation (Goal 17), cybersecurity stands as an essential component for achieving these objectives. The evolution of cybersecurity in the era of sustainability reflects broader shifts in economic, social, and environmental paradigms. As the world continues to face challenges and opportunities arising from digital transformation, the

role of cybersecurity in supporting sustainable development will remain pivotal.

Cybersecurity is considered a fundamental tool for safeguarding the digital infrastructure that underpins economic activities in the modern world, while the digital era also offers unique opportunities for financing mechanisms that can contribute to sustainable community development. By protecting these platforms from cyber threats, cybersecurity measures enable the effective utilization of digital financing mechanisms to support economic growth and sustainable community development (Bolatito Ige, Kupa, & Ilori, 2024, pp. 348-350).

8.1. How cybersecurity contributes to the goal 9: Industry, Innovation, and Infrastructure: Build resilient infrastructure, promote inclusive and sustainable industrialization, and foster innovation

Cybersecurity plays a pivotal role in protecting the critical systems on which the economy and society rely. It enables these systems to continue operating without complete interruption even in the event of an attack, thereby safeguarding essential services from disruption. It also ensures that these systems remain consistently available to users and function with accurate, uncompromised data. Moreover, it strengthens the trust of users and investors in digital systems, a trust that supports economic growth and contributes to sustainable development.

8.2. How cybersecurity contributes to the goal 16:

Cybersecurity contributes to protecting individuals' fundamental rights online, such as privacy and freedom of expression. The existence of robust cybersecurity systems reduces the likelihood of "cyber wars" or attacks between states and other actors. Moreover, cybersecurity has become a key instrument, comparable to military or economic security, as it enhances stability among nations and is regarded as an essential component of international cooperation and mutual trust-building.

8.3. How cybersecurity contributes to the goal 17: Partnerships For The Goals: Strengthen the means of implementation and revitalise the global partnership for sustainable development.

The existence of a strong cybersecurity framework provides a safe and reliable digital environment, which in turn encourages countries and institutions to cooperate, exchange information, and implement joint projects without fear of breaches or cyberattacks. Cybersecurity is directly linked to Goal 17 (Partnerships for the Goals), as it enhances trust among international partners and makes cooperation more effective (Odumesi & Sanusi, 2023, pp. 5-7).

9. Case Studies

9.1. Indonesia's Experience with Cybersecurity Threats

The banking industry in Indonesia recorded a new history with the presence of PT Bank Syariah Indonesia Tbk (BSI), which was

officially born on February 1, 2021 or 19 Jumadil Akhir 1442 AH. President Joko Widodo directly inaugurated the largest Islamic bank in Indonesia at the State Palace. BSI is a bank resulting from the merger between PT Bank BRIsyariah Tbk, PT Bank Syariah Mandiri and PT Bank BNI Syariah. The Financial Services Authority (OJK) officially issued a permit for the merger of the three Islamic bank businesses on January 27, 2021 through letter Number SR-3/PB.1/2021. Furthermore, on February 1, 2021, President Joko Widodo inaugurated the presence of BSI.

The composition of BSI's shareholders are: PT Bank Mandiri (Persero) Tbk 50.83%, PT Bank Negara Indonesia (Persero) Tbk 24.85%, PT Bank Rakyat Indonesia (Persero) Tbk 17.25%. The rest are shareholders with less than 5% each. This merger brings together the strengths of the three Islamic banks, providing more complete services, wider reach, and better capital capacity. Supported by the synergy with the company and the commitment of the government through the Ministry of SOEs, BSI is encouraged to compete at the global level.

BSI is an endeavor for the birth of an Islamic bank that is the pride of the people, which is expected to be a new energy for national economic development and contribute to the welfare of the wider community. The existence of BSI is also a mirror of the face of Islamic banking in Indonesia which is modern, universal, and provides goodness for all nature (Rahmatan Lil 'Aalamiin).

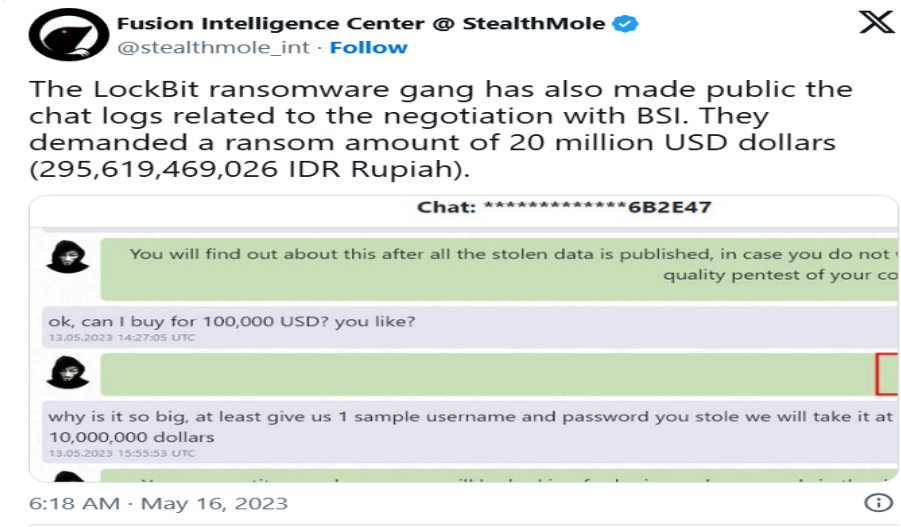
The potential for BSI to continue to grow and become part of a group of leading Islamic banks at the global level is very open. In addition to positive growth performance, the climate support that the Indonesian government has a mission to create a halal industry ecosystem and have a large and strong national Islamic bank, the fact that Indonesia is the country with the largest Muslim population in the world also opens up opportunities. It is in this context that the presence of BSI is very important. It is not only able to play an important role as a facilitator of all economic activities in the halal industry ecosystem, but also an effort to realize the hopes of the State (Bank Syariah Indonesia, 2025).

Bank Syariah Indonesia (BSI), the largest Islamic bank in Indonesia, was reportedly subjected to a ransomware attack that disrupted its services for several days. The attack involved **ransomware**, one of the most dangerous types of cyber threats, in which hackers infiltrate digital systems, disable or encrypt data, and then demand a ransom in exchange for restoring control. In the case of BSI, the hacking group **LockBit** attacked the bank's systems and paralyzed them. The breach led to the disruption of essential banking services such as the mobile banking application and ATMs, causing widespread confusion and concern among customers. Although services were gradually restored, the incident highlighted the extent to which customers and society depend on the bank's digital infrastructure, and thus its vulnerability to cyber threats.

The attack did not only disrupt systems but also involved the leakage of sensitive data. The group announced that it had stolen **1.5 terabytes of data**, including the personal information of 15 million customers and employees, such as card numbers, account details, and

transactions. This means that the damage extended to the violation of customers' privacy and the potential misuse of their data in subsequent financial crimes such as fraud or money laundering.

Figure04: Chat logs and ransom demands related to the BSI negotiation



Source: Explained: The ransomware attack on BSI, Indonesia's largest Islamic bank | Coconuts

The hacker group gave BSI 72 hours to "settle the matter." In another post, depicting a chat log between LockBit and BSI, the former demanded US$20 million to keep the stolen data from being published.Meanwhile,the bank assured its customers that their data was safe and that it would not pay the ransom. According to Darktracer,LockBit made the stolen BSI data public on the dark web today, along with a message of condemnation addressed to BSI's customers posted on the bank's own official website (Nasrie, 2023).

Despite the attack exposing customers' data, BSI corporate secretary Gunawan A Hartoyo reassured that data and funds remain secure.

"We urge customers to remain calm as we ensure the security of their data, funds, and transactions. We will also collaborate with the relevant authorities regarding this data breach issue," Gunawan said, quoted from Tekno Liputan6.com on Tuesday (16/5).

Previously, BSI president director Hery Gunardi emphasized the need of conducting further audits and digital forensics to confirm the extent of the attack.

He claimed that BSI has taken preventive measures to enhance security of its information technology, as evidenced by an increased allocation of

capital expenditure budget to strengthen the IT system, reaching IDR 580 billion compared to the previous year's approximately IDR 280 billion.

Simultaneously, the company is conducting internal investigations and maintaining coordination with relevant parties, including the National Cyber and Crypto Agency (BSSN), Financial Services Authority (OJK), Bank Indonesia (BI), and others. The BSI ransomware attack is the first hacker action to affect banking services. So far, many hacker groups have penetrated the banking system and other public institutions, but not to the extent of impairing activities.

The cyberattack that targeted Bank Syariah Indonesia (BSI) clearly reflects the extent of the fragility in Indonesia's cybersecurity infrastructure. Reports indicate that most public institutions in the country have been subjected to repeated breaches by hackers, making them an easy target compared to other nations. Studies have shown that Indonesia ranks third in Southeast Asia in terms of the number of ransomware attacks, recording nearly 14 incidents within 18 months, in addition to over 2,700 weekly attacks on the financial sector since 2022 a rate that is 252% higher than the global average highlighting the severity of the situation. In this context, the attack on BSI revealed multiple dimensions; on the technical side, the breach disrupted critical services such as mobile banking transactions and ATM operations, in addition to leaking sensitive personal data belonging to more than 15 million customers and employees, which raises the likelihood of it being exploited in financial crimes such as fraud or money laundering. Strategically, the attack inflicted significant damage on the reputation of the bank, which represents the merger of three state-owned Islamic banks, at a time when the Indonesian government is seeking to present it as a leading flagship to attract foreign investment and expand its operations globally (Indonidisia Business Post, 2023).

9.2. Iran's Experience with Cybersecurity Threats

On June 18 An anti-Iranian hacking group, which is believed to have possible ties to Israel, announced an attack on one of Iran's largest cryptocurrency exchanges on Wednesday, destroying nearly $90 million and threatening to disclose the platform's source code.

The group, known as *Gonjeshke Darande* or "Predatory Sparrow," claimed responsibility for the attack, marking its second operation in just two days. On Tuesday, the group had announced the destruction of data belonging to Iran's state-owned **Bank Sepah**, amid the escalating hostilities and missile exchanges between Israel and Iran.

The attack began in the early hours of the morning, during which the funds were transferred to wallets controlled by the hackers that carried slogans denouncing the Islamic Revolutionary Guard Corps (IRGC), according to blockchain analytics firm TRM Labs, which estimated the total losses at around USD 90 million across multiple types of cryptocurrencies.

Blockchain analytics company Elliptic explained that the wallets created by the hackers were designed in a way that prevents them from accessing the stolen funds, which means they had "effectively burned the funds" as part of a political message directed at Nobitex.

- **Details of the latest attack:**

The attack targeted **Nobitex**, one of the largest cryptocurrency exchanges in Iran. The group claimed that the platform was helping the Iranian government evade sanctions and finance illicit operations around the world, according to a message it posted on its social media channels on Wednesday morning.

Nobitex's website was unavailable on Wednesday, and messages sent to the company's support channel on the Telegram app went unanswered.

In a post on **X** (formerly Twitter), Nobitex explained that it had temporarily taken down its website and app to review "unauthorized access" to its systems (Vicens & Pearson, 2025).

The Nobitex platform, which is said to have more than 10 million users, is facing the biggest security challenge it has encountered so far. Blockchain analytics firm **Elliptic**, which studied the activity, reported that the attackers stole more than **$90 million** through multiple transactions. However, unlike most financially motivated cryptocurrency hacks, the stolen funds were not transferred to conventional private wallets. Instead, the hackers sent the money to special wallet addresses known as **"vanity addresses"** that carried anti-Iranian regime messages.

It is almost impossible to access these addresses again due to the way they were created. Simply put, the hackers had no intention of keeping or spending the money; the goal was purely retaliatory.

Elliptic noted that these vanity addresses were created with messages directed at Iran's Islamic Revolutionary Guard Corps (IRGC), and that generating such complex addresses requires **tremendous computational power**, making it highly unlikely that the hackers or anyone else could ever recover the funds (Selim, 2025).

10. Conclusion

This study reveals that the rapid digital transformations in the Islamic financial system, despite offering opportunities to enhance innovation and competitiveness, have also opened the door to increasingly complex and far-reaching cyber threats. Through the analysis of literature, international frameworks, and the cases of Bank Syariah Indonesia and the Nobitex platform in Iran, the following conclusions can be drawn:

- The study showed that the pace of financial innovation has outstripped the ability of Islamic financial institutions to absorb cyber risks, leading to notable fragility in their digital infrastructure.

- The impact of cyberattacks extended beyond direct financial losses, as they undermined customer and investor confidence, threatening one of the key pillars of sustainability in the Islamic financial system.
- Cybersecurity cannot be reduced to technical tools alone; it is an integrated system of legislation, institutional culture, and societal awareness, which requires a comprehensive approach.
  International experiences confirmed the importance of national cybersecurity strategies based on institutional coordination, international cooperation, and strengthened governance, which can serve as a foundation for effective policies in countries with Islamic financial systems.
- The case study in Indonesia demonstrated that the breach of Bank Syariah Indonesia was not merely a technical failure but a crisis affecting the country's reputation and the global standing of Islamic finance, while the Nobitex incident highlighted that cyber threats may take on geopolitical dimensions that go beyond financial motives.

Based on the above, the study recommends integrating cybersecurity as a core element in Islamic financial innovation strategies through:

- Adopting international frameworks (such as NIST and ENISA) while adapting them to the specific requirements of Sharia.
- Enhancing international and regional cooperation among Islamic financial institutions to counter cross-border attacks.
- Investing in building an institutional and societal security culture that reduces the fragility of the "human factor."

The sustainability of innovation in the Islamic financial system ultimately depends on the extent to which these institutions can make cybersecurity a strategic pillar that safeguards trust, supports growth, and ensures that digital development aligns with the objectives of Islamic law.

11.Bibliography

Abdulla, H., Mohamed, A., & Suriyati, R. (2020). A Review on Cybersecurity: Challenges & Emerging Threats. *NISS '20: Proceedings of the 3rd International Conference on Networking, Information Systems & Security* (pp. 1-7). Morocco: NISS '20.

Adejumo, A. P., & Ogburie, C. P. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews, 25*(3), pp. 1542-1556.

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., & Rifat, N. (2022). Cybersecurity Threats and Their Mitigation Approaches

Using Machine Learning—A Review. *Cybersecurity and Privacy, 2*(3), pp. 527–555.

AL-ALAWI, A. I., & AL-BASSAM, S. A. (2020). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. *Journal of Xidian University, 14*(7), pp. 1523-1536.

ATAMNIA, T., & MEZHOUD, H. (2024). The Islamic Finacial System: A Conceptual Reading. *Algerian Journal of Islamic Finance, 2*(1), pp. 63-80.

Bank Syariah Indonesia, .. (2025). *Explained: The ransomware attack on BSI, Indonesia's largest Islamic bank*. Retrieved 08 28, 2025, from Bank Syariah Indonesia: https://coconuts.co/jakarta/news/explained-the-ransomware-attack-on-bsi-indonesias-largest-islamic-bank/?utm

Bolatito Ige, A., Kupa, E., & Ilori, O. (2024). Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future. *GSC Adv. Res. Rev, 19*(3), pp. 344-360.

Gallagher, H., McMahon, W., & Morrow, R. (2014). Cyber Security: Protecting the Resilience of Canada's Financial System. *BAnk oF CAnAdA FInAnCIAL SySTEM REVIEw*, pp. 47-53.

Indonidisia Business Post, .. (2023, 05 16). *BSI's data breach: A menace to Indonesia's banking security*. Retrieved 08 28, 2025, from Indonidisia Business Post: https://indonesiabusinesspost.com/826/Politics/bsis-data-breach-a-menace-to-indonesias-banking-security#:~:text=A%20ransomware%20cybercriminal%20group%20Lockbit%203.0%20claimed%20on,million%20customers%20and%20staff%20members%20of%20the%20bank.

Johnson, S., & Kwak, J. (2012). Is Financial Innovation Good for the Economy? *Innovation Policy and the Economy, 12*(1), pp. 1-16.

Khledj, A., & Abbou, A. (2024). Highlights of the Islamic Financial System in Algeria. *Algerian Journal of Islamic Finance, 2*(1), pp. 118-134.

Mester, L. J. (2019). Cybersecurity and financial stability. *2019 Financial Stability Conference Financial Stability: Risks, Resilience, and Policy* (pp. 1-13). Cleveland: Federal Reserve Bank of Cleveland .

Nasrie, A. (2023, 05 16). *Explained: The ransomware attack on BSI, Indonesia's largest Islamic bank*. Retrieved 08 28, 2025, from Coconuts Jakarta: https://coconuts.co/jakarta/news/explained-the-ransomware-attack-on-bsi-indonesias-largest-islamic-bank/?utm

Natalucci, F., Qureshi, M., & Suntheim, F. (2024, 04 09). *Rising Cyber Threats Pose Serious Concerns for Financial Stability*. Retrieved 09 01, 2025, from IMF: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

Odumesi, J. O., & Sanusi, B. S. (2023). Achieving Sustainable Development Goals from a Cybersecurity Perspective. *Proceedings of the Cyber Secure Nigeria Conference.* Nigeria: 1-10.

QBE Cyber Threat Intelligence Team, .. (2024). *Cyber Threats to the Financial Services Industry.* QBE.

Schiliro, F. (2022). *Towards a Contemporary Definition of Cybersecurity* . arXiv:2302.02274.

Selim, n. (2025, 06 19). *Details of the hacking of Nobitex, Iran's largest cryptocurrency exchange, with losses amounting to $90 million.* Retrieved 08 28, 2025, from Youm7:

https://www.youm7.com/story/2025/6/19/%D8%AA%D9%81%D8%A7%D8%B5%D9%8A%D9%84-%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D9%85%D9%86%D8%B5%D8%A9-%D9%86%D9%88%D8%A8%D9%8A%D8%AA%D9%83%D8%B3-%D8%A3%D9%83%D8%A8%D8%B1-%D8%A8%D9%88%D8%B1%D8%B5%D8%A9-%D8%B9%D9%85%D9%84%

Sentinelone, .. (2025, 07 15). *Cyber Security in Finance: Key Threats and Strategies*. Retrieved from SentinelOne: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-in-finance/#pros-and-cons-of-cyber-security-in-finance

Strzępek, K. (2023). DEFINEDCYBERSECURITY THREATSIN UNDEFINED CYBERSPACE. *GIS Odyssey Journal*, *3*(1), pp. 31–39.

Tufano, P. (2003). Financial Innovation. In P. Tufano, *Handbook of the Economics of Finance* (pp. 307-335). Boston: ElsevierB.V.

Vicens, A., & Pearson, J. (2025, 06 18). *Iran crypto exchange hit by hackers, $90 million destroyed*. Retrieved 08 28, 2025, from Reuters: https://www.reuters.com/world/middle-east/iran-crypto-exchange-hit-by-hackers-90-million-destroyed-2025-06-18/?utm