Al-Muamalah: Jurnal Ekonomi Islam, Filantropi dan Perbankan Syariah
Vol. 01. No. 01 Mei 2024
P-ISSN: 0000-0000 | E-ISSN 0000-0000
https://journal.syamilahpublishing.com/index.php/muamalah/

Cyber Security Challenges in Syrian Bank Liquidity Management: Maintaining Stability in The Digital Age

Naila Fadilah✉, Hendri Hermawan Adinugraha
Universitas Islam Negeri K.H Abdurrahman Wahid, Indonesia
✉ naila.fadilah@mhs.uingusdur.ac.id[1]

Received: 28-04-2024	Revised: 13-06-2024	Accepted: 21-06-2024

ABSTRACT

This study explores the challenges facing cybersecurity. by financial institutions, especially the sharia bank, in the context of liquidity management to maintain financial stability in the digital age. The digital age marks the transformation of the financial landscape that gives facility but also poses a cybersecurity risk that Sharia Bank, as a financial entity that implementing the principles of Shariah, especially vulnerable to Cyber attacks that could threaten liquidity and financial stability This research covers an in-depth background on Cyber attacks and liquidity management in sharia banks. Consider the latest theories and related case studies, research This analyzes the impact of cyber attacks on liquidity and stability. Sharia bank finance. As part of the research methodology, the study In-depth literature is used to identify trends, challenges, and strategies related to cybersecurity in liquidity management. Findings This research provides a deep insight into how banks Shariah can face and respond to cybersecurity challenges, as well as strategies that can be applied to maintain stability financial in the digital age. Practical implications and recommendations for Similar financial institutions were discussed, contributing to practical understanding and policy related to liquidity management and cybersecurity. This research provides a better understanding deep on the relationship between cybersecurity and stability financial, providing the necessary framework for banks Shariah and other financial institutions to face the challenge This complex.

Keywords: cybersecurity, liquidity management, shariah banks

INTRODUCTION

In a growing digital age, the Sharia banking industry faces an increasingly complex challenge related to cyber security. Cyber security in sharia banks involves a variety of risks, including attacks on customer data, threats to day-to-day operations, and risks to financial transactions. The success of liquidity management in sharia banks will be greatly influenced by the extent to which banks can manage and address these challenges by considering the aspects of sharia.[1]

To maintain financial stability in the face of cyber security challenges, sharia banks need to adopt an integrated approach that covers technological aspects, risk management, and sharia compliance. A holistic framework will ensure that efforts to manage liquidity are not only efficient but also comply with ethical and sharia principles.[2] The importance of the link between liquidity management and cybersecurity requires further research. Good liquidity conditions require protection against cyber attacks that can affect operational and customer confidence.

Considering global trends in cybersecurity in the financial sector, it is important for sharia banks to understand and adopt best practices relevant to the sharia banking context. Analysis of this global trend provides valuable insights to address cyber security challenges effectively.[3] The cybersecurity challenges in liquidity management have a significant impact on Sharia banking practices. Successful liquidity management depends not only on the accuracy of financial strategies, but also on how banks deal with and manage cyber security threats. This study provides an in-depth overview of the literature on cybersecurity, in the context of Shariah banking. This literature review covers a deep understanding of the unique challenges of Islamic banking cyber security and how current literature suggests strategies to address these challenges.

The study identifies and analyzes various types of cyber attacks, including: Investigating the risk of ransomware and data breaches and how this affects the sustainability of liquidity management. In addition, the study will produce practical recommendations that will help sharia banks improve cybersecurity strategies and liquidity management in the face of existing challenges. In an

[1] Edy Susanto, "Manajemen Keamanan Cyber Di Era Digital," *Jurnal Bisnis Dan Kewirausahaan (Journal of Business and Entrepreneurship)* 11 No 1 (2023).

[2] Fattah, H., Riodini, I., Hasibuan, S. W., Rahmanto, D. N. A., Layli, M., Holle, M. H., ... & Marzuki, S. N. "No Title." Fintech Dalam Keuangan Islam: Teori Dan Praktik, 2022.

[3] Restika Restika and Era Sonita, "Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era Digital," *Krigan: Journal of Management and Sharia Business* 1, no. 2 (2023): 25, https://doi.org/10.30983/krigan.v1i2.7929.

increasingly sophisticated digital age, sharia banks are facing major changes in liquidity management. Effective liquidity management is crucial toining the financial stability of Sharia banks, as it is primarily aimed at ensuring that sufficient funds are available to meet financial obligations.

However, in addition to the benefits of digital technology, sharia banks also face increasingly complex and diverse cyber security threats. Therefore, an in-depth understanding of cybersecurity is a very important aspect in the management of sharia banking liquidity in the digital age. Customer Data Protection. Liquidity management in sharia banks involves the management of customer data, including financial and personal information.[4]

Cyber security is the key to protecting this data from potential attacks that could undermine its integrity and confidentiality. Inadequate security can result in the disclosure of customer data, which not only harms customers but can also damage the bank's reputation.[5] Dependency on digital transactions; Sharia Bank is increasingly adopting digital transaction to improve efficiency and provide better service to customers. However, digital transactions also open loophole for cyber attacks such as identity theft, phishing, and malware. Understanding cyber security is essential for sharia banking digital transaction to remain secure and reliable.[6] Integrity and availability of services; Liquidity management is not only about adequate funding needs, but also aboutining integrity and service availabilities. Cyber attacks that can stop or damage the bank's operating system can disrupt liquidity management processes, result in financial instability and lower customer confidence.

Compliance with Sharia principles The Sharia Bank must not only comply with the General Security Standards but also ensure compliance with the Sharia Principles.It covers aspects of cybersecurity such as transparency, integrity, and customer protection. A good understanding of how Sharia principles impact on cyber security is crucial.If Bank Shariah is subjected to a cyber security breach, the bank's reputation could be damaged and customer confidence weakened.

Sharia banks face cybersecurity risks that could threaten their liquidity, either in the form of hacking, identity theft, or malware. Although a lot of research has been done on cybersecurity in the context of conventional banking, there is still a shortage in understanding of how sharia banks in particular face

[4] Restika and Sonita.

[5] A Vebrianty, "Perlindungan Hukum Pembukaan Rekening Secara Online Dalam Layanan Perbankan Digital Pada Pt Bank Central Asia Tbk (Bachelor's Thesis)," Fakultas Syariah Dan Hukum UIN Syarif Hidayatullah Jakarta, 2021.

[6] S. SRIWULAN, "Tinjauan Yuridis Tindak Pidana Cyber Crime Di Indonesia (Doctoral Dissertation," Institut Agama Islam Negeri Palopo, 2023.

the cyber security challenges in managing their liquidity. Data security and security are very important to sharia banks, but the literature covering these aspects is still limited.

The study aims to fill these gaps by analyzing the cyber security challenges faced by sharia banks in their liquidity management. By understanding the risks involved, sharia banks can develop more effective strategies to protect their liquidity and maintain financial stability. The main motivation of this research is to provide a better understanding of how sharia banks face cybersecurity challenges in managing their liquidity in the digital age. Thus, measures needed to increase their resilience to cyber security attacks can be identified.

The aim of this research is to provide a deeper insight into the cybersecurity risks faced by sharia banks in their liquidity management, as well as identifying effective strategies to address these challenges. The aim of this study is to provide practical recommendations for sharia banks in improving their cybersecurity andining financial stability in the digital age. This research is expected to make a significant contribution to the literature on cyber security in the context of sharia banking and liquidity management.

The cyber security challenges in sharia bank liquidity management are a very important issue to consider, especially in the growing digital age. The study explores the cyber security challenges faced by sharia banks in the context of liquidity management to maintain financial stability in the digital age. Sharia banks, as financial entities implementing Sharia principles, are vulnerable to cyber attacks that could threaten their liquidity and financial stability. This research includes backgrounds on cyberattacks and liquidity management in Sharia banking, as well as an analysis of the impact of cyber-attacks on the liquidity of Sharia's banking.[7]

This research provides in-depth insight into how sharia banks can face and respond to cybersecurity challenges, as well as strategies that can be applied to maintain financial stability in the digital age. Practical implications and recommendations for similar financial institutions were discussed, contributing to practical and policy understanding related to liquidity management and cyber security. The study provides the necessary framework for sharia banks and other financial institutions to face the complex challenges faced by cyber security in liquidity management.

[7] Restika Restika and Era Sonita, "Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era Digital," Krigan: Journal of Management and Sharia Business 1, no. 2 (2023), https://doi.org/10.30983/krigan.v1i2.7929.

The cyber security challenges in sharia bank liquidity management are a very important issue to consider, especially in the growing digital age. The research shows that Sharia banks, as financial entities implementing Sharia principles, are vulnerable to cyber attacks that could threaten their liquidity and financial stability. The research includes backgrounds on cyberattacks and liquidity management in Sharia banking, as well as an analysis of the impact of cyber-attacks on the liquidity of Sharia's banks and the stability of their finances. Cyber attacks can involve the use of unwanted technology, violence, or the deletion of undesirable data, as well as violence or use of information systems.

This study provides an in-depth insight into how sharia banks can face and respond to cybersecurity challenges, as well as strategies that can be applied to maintain financial stability in the digital age. Practical implications and recommendations for similar financial institutions are discussed, contributing to the practical understanding and policies related to liquidity management and cyber security. The study provides the necessary framework for sharia banking and other finance institutions to face the complex challenges faced by cyber-security in the management of liquidity.

Applied strategies forining financial stabilities in the Digital Age include the development of effective information systems, enhancing the strength of security systems, and developing leadership that is capable of tackling cyber safety challenges. This research shows that sharia Banks and other financial institutional institutions should develop leadership capable of facing cyber Security challenges, developing efficient information systems and high-powered security systems. This study contributes to my practical security understanding in which policy management and financial liberty policies, security-related policies and practical recommendations are covered and implemented by the library security institutions.

The study provides the necessary framework for sharia banks and other financial institutions to address the complex challenges faced by cybersecurity in liquidity management. The strategies that can be applied to maintain financial stability in the digital age include the development of effective information systems, enhancing the strength of security systems, as well as developing leadership that is capable of addressing cyber security challenges, and developing efficient information systems and high security system strengths.[8]

[8] Restika and Sonita.

RESEARCH METHOD

The method of literature study is a series of activities related to the method of collecting library data, reading and recording, and managing research materials A library study is an obligatory activity in research, especially academic research whose main purpose is to develop theoretical aspects as well as practical benefits. So researchers can group, allocate, organize, and use library variations in their fields. By doing a library study, the researchers have a broader and deeper depth of the problem to be investigated.[9]

This literature study is conducted by researchers between after they have defined the research topic and established the formula of the problem, before they plunge into the field to collect the necessary data. This research uses a literary approach to explore and analyse the relationship between cyber security and financial stability, in the context of the financial sector and Shariah banking. We adopted a literature research approach to identify key findings from previous research, explain a strong conceptual framework, and build a strong knowledge base on this topic.[10]

RESULT AND DISCUSSION

Cyber Security

Research on cyber security is a response to rising threats in today's digital world. Cyber attacks are becoming increasingly complex, including data theft, malware, hacking, and DDoS attacks, all threatening computer systems and data around the world. Faced with these challenges, an in-depth understanding of the dynamics of cybercrime and effective protection strategies is essential. The study aims to investigate key aspects related to cyber security, identify the latest challenges facing organizations and individuals, and explore the most effective security strategies and measures in combating cyberattacks.[11]

Through collaborative efforts between academics, practitioners, and governments, better solutions are expected to be found in protecting computer systems and data from cyber threats. With a deeper understanding of cybersecurity, IT professionals, companies, and individual users will be expected to take appropriate action to reduce the risk of cyberattacks. This will help build

[9] M Zed, Metode Penelitian Kepustakaan (Jakarta: Yayasan Obor Indonesia, 2008).

[10] Darmadi, Pengembangan Metode Pembelajaran Dalam Dinamika Belajar Siswa (Jakarta: Rineka Cipta, 2017).

[11] Susanto, "Manajemen Keamanan Cyber Di Era Digital."

a more secure and reliable digital environment for all parties involved in the digital ecosystem.[12]

Islamic Bank

A bank is a financial institution that has the authority to collect funds from the public and channel them back to the public in the form of labour capital loans to improve the standard of living of the general public. The word "bank" comes from the Italian word "banco", which means a bench. In this sense, the bench is the place where the bankers of the past operated in serving their customers. The term "Banco" then changed and became more popular with the word "BANK".[13]

Shariah Bank is a bank that has its operational activities guided by the law and the principles of Islam and in its operating activities does not impose interest or pay interest to the customer. The remuneration obtained by the shariah bank nor that paid to the customers is incurred from the accords and also the agreement (accords) that are in the sharial banking must be subject to and obey the terms and conditions of accords as regulated in the Islamic scripture.[14]

Besides, the Sharia Bank is a bank that runs with no interest rate system. In other sense, that the Shariah banking is an institution that operates in the financial field of which its operations and even its products are developed based on the Islamic scholarship of Al-Qar'an and Al-Hadist and using the principles of fiqh. According to Said Sa'ad Marthan, he argues that the Sharia Bank is an investment institution run on Sharia principles. In its funds controlled should be in accordance with Sharia and the purpose of allocation on such investments is carried out in decommissioning the economy and social community and performing banking services according to Sharia values. Shariah Bank also aims to support the implementation of national development in support of improved justice, equality, and welfare among communities.[15]

---

[12] Edy Susanto et al., "Manajemen Keamanan Cyber Di Era Digital," Journal of Business And Entrepreneurship 11, no. 1 (2023), https://doi.org/10.46273/jobe.v11i1.365.

[13] M Prawirio, "Pengertian Bank Secara Umum, Fungsi, Tujuan, Dan Jenis-Jenis Bank," Https://Www.Maxmanroe.Com/, 2019.

[14] Hasan Sultoni and Kiki Mardiana, "Pengaruh Merger Tiga Bank Syariah BUMN Terhadap Perkembangan Ekonomi Syariah," Jurnal Eksyar : Jurnal Ekonomi Syariah 08, no. 01 (2021).

[15] Cimb Niaga, "Pengertian Tentang Bank Syariah Dan Istilah Di Dalamnya," Cimb.Co.Id, 2022.

Liquidity

Liquidity is generally defined as the ownership of sufficient funds to meet the entire requirement of an outstanding liability. Or, in other words, the ability of the company to meet its obligations at the time of charge, whether predictable or unexpected. Sharia bank liquidity management is understood as an easy-to-use liquidity control program to meet all bank obligations that are immediately payable. One of the functions of liquidity management is to give confidence to the depositors that deposits can be withdrawn at any time or at the time of expiry.

Therefore, the bank is obliged to maintain a number of liquid funds so that the bank can meet its obligations. Liquidity in financial institutions is the ability of banking institutions to liquidate funds in the short term. In general, liquidity management consists of two parts: estimating the need for funds arising from deposidalt inflows and to channel fund outflows and various financing commitments. (financial commitments). In general, the liquidity of banks is influenced by external and internal factors. External factors are uncontrollable while internal factors are generally those that can be controlled by the banks. The external factors include economic and monetary conditions. The characteristics of deposits, monetary market conditions, regulations and so on. Whereas internal factors depend heavily on the management of each liquidity instrument of the bank. Examples are the selection of asset-liabilities management implementation strategies.

Liquidity risk is the risk arising from the failure of the sharia bank to meet due obligations of the funding source must be cash and/or high-quality liquid assets that can be used, without interfering with the activity, and financial conditions of the bank. Based on this analysis, a bank should study and understand the preferences and risks of liquidity itself to reduce the likelihood of a bank leading to bankruptcy. Once a bank is in control of its liquidity, it will gain the trust of its citizens and the bank will become more advanced and prosperous.[16]

Technological Advances

Technology is the whole means of providing the goods necessary for the survival, and the comfort of human life. The use of technology by humans

[16] Wiwin Winanti, "Manajemen Risiko Likuiditas Pada Perbankan Syariah," EKSISBANK: Ekonomi Syariah Dan Bisnis Perbankan 3, no. 1 (2019), https://doi.org/10.37726/ee.v3i1.34.

begins with the transformation of natural resources into simple tools. The prehistoric discovery of the ability to control fire has increased the availability of food resources, while the creation of the wheel has helped humans on their way, and control their surroundings. The latest technological developments, including printing machines, phones, and the Internet, have reduced physical barriers to communication and enabled human beings to interact freely on a global scale. But, not all technology is used for peaceful purposes. The development of increasingly powerful weapons of destruction has been going on throughout history, from fence to nuclear weaponry .[17]

The use of the term 'technology' has changed significantly over the last 200 years. Before the 20th century, this term was not common in English, and usually refers to painting or study of applied art.[18] This term is often associated with engineering education, as at the Massachusetts Institute of Technology. (didirikan pada tahun 1861)[19] The term technology began to emerge in the twentieth century with the rise of the Second Industrial Revolution. The concept of technology changed in the early 20th century when American social scientists, starting with Thorstein Veblen, translated ideas from the German concept of Technik into technology. In German and other European languages, the differences existed between Technik and Technologie, which at the time were just none in English, because both terms are commonly translated as technology.

The evolution of human civilization was accompanied by the development of the means of delivery of information (later known as the term information technology), ranging from meaningless images on the walls of the caves, the laying of historical milestones in the form of inscriptions, to the introduction of the world of the flow of information known by the name of the Internet

Liquidity Management in The Context Of Islamic Banking

1. Principles of Liquidity Management in Sharia Banking
   Literature related to liquidity management in the context of Sharia banking emphasizes the importance of the Sharia principles that guide the

[17] B. G Gance-Clev eland, "Evaluation of Technology to Identify and Assess Overweight Children and Adolescents," Journal for Specialists in Pediatric Nursing, 2010, 15 (1): 72–83.

[18] Gance-Clev eland.

[19] M. a Julius Adams Stratton and Loretta H. Mannix, "The Birth of MIT," Cambridge: MIT Press, 2005, 190.

management of liquidity. According to,[20] These principles include operational sustainability, the availability of funds in accordance with the principles of mudharabah, and the fulfilment of Shariah obligations in ensuring that funds are managed fairly and in conformity with Islamic ethics.

2. The Relationship between Liquidity Management and Profitability.
   In research by[21] They show that effective liquidity management can make a positive contribution to the profitability of sharia banks, by creating an optimal balance between investment and fulfilment of financial obligations.
3. Special Challenges in Sharia Liquidity Management.
   Several studies, such as those carried out by[22] highlighting specific challenges in Sharia liquidity management, including the need to manage funds without using interest instruments and considering aspects of Sharia compliance in liquidity risk management.
4. Sharia Liquidity Instruments.
   The literature also covers various Islamic liquidity instruments used by Islamic banks. Study by[23] Identifying instruments such as wakalah, mudharabah, and exemption as a liquidity management tool that adheres to the principles of Shariah.
5. Regulations and Regulations in Sharia Liquidity Management.
   The regulatory and regulatory aspects of Shariah liquidity management were also emphasized. According to[24], The role of regulators in creating a framework that supports Sharia liquidity management is vital to ensuring the stability of the entire Sharia banking sector.
6. Technological Change and Digital Transformation.
   With the continued development of technology, recent literature highlights digital transformation and technological changes that influence

[20] Sundararajan, Keamanan Cyber (Cyber Security) (Penerbit Yayasan Prima Agus Teknik, 2002).

[21] A Khan, M.S. and Mirakhor, "The Financial System and Monetary Policy in an Islamic Economy," Ln Theoretical Studies in Islamic Banking and Finance., 1987.

[22] Rosly, S. A., & Sanusi, M. M. "He Application of Bay'al-'inah and Bay'al-Dayn in Malaysian Islamic Bonds–an Islamic Analysis." International Journal of Islamic Financial Services, 1999, 1 (2): 3–11.

[23] Iqbal, Z., & Mirakhor, A. "Ethical Dimensions of Islamic Finance: Theory and Practice." Springer, 2017.

[24] Beck, T., Demirgüç-Kunt, A., & Merrouche, O. "Islamic vs. Conventional Banking: Business Model, Efficiency and Stability." Journal of Banking & Finance, 2013, 37 (2): 433–47.

liquidity management in Islamic banking. Research by [25] stresses the need for adaptation to digital innovation to improve efficiency in liquidity management.

7. The Impact of the Financial Crisis on Management.
   Sharia Liquidity Study by [26] investigate the impact of the financial crisis on Sharia liquidity management. They show that effective liquidity management can be a decisive factor in responding to and addressing the challenges that arise during periods of economic uncertainty.
8. Liquidity Risk Measurement Model in Sharia Banking.
   In addition, the literature also explores liquidity risk measurement models specific to Islamic banking. Research by [27] develop a model that considers the unique characteristics of Islamic banking in identifying and measuring liquidity risk.

Cyber Security in The Financial Sector And Especially In Islamic Banks

1. Cybersecurity in the financial sector is a critical issue that continues to grow as technology progresses. According to research by [28], The financial sector has become a major target of cyberattacks because of the large volumes of sensitive data and customer funds. Operational success and public confidence in financial institutions depend heavily on the security of information systems.
2. Threats and attacks on the financial sector Study by [29]records the various types of attacks that are spying on the financial sector, including phishing, malware, and Distributed Denial of Service attacks (DDoS). Threats of this kind can damage operations, steal customer data, and cause significant financial losses. Sharia banks are no exception to this attack and need to adopt a sophisticated security strategy.
3. A special study on cybersecurity in sharia banks underscores the unique characteristics that distinguish sharia bank from conventional banks in the

[25] M. A.-T Rahman, "Ata-Driven Dynamic Clustering Framework for Mitigating the Adverse Economic Impact of Covid-19," Sustainable Cities and Society, 2020, 2: 10–23.

[26] Haque Mirakhor, "Dampak Krisis Keuangan Terhadap Manajemen Likuiditas Syariah," Manajemen, 2018.

[27] M Abduh, "Competitive Condition and Market Power of Islamic Banks in Indonesia," International Journal of Islamic and Middle Eastern Finance and Management, 2017, 20 (1): 77–91.

[28] C. C. Demchak, "China: Determined to Dominate Cyberspace and AI," Bulletin of the Atomic Scientists, 2019, 75 (3): 99–104.

[29] Ablon Libicki, "Ancaman Dan Serangan Terhadap Sektor Keuangan," Jurnal Sains dan Informatika, 2014.

face of cyber attacks. The Sharia principle governing transactions and fund management requires a security approach that takes into account ethical aspects and principles of fairness in cyber risk management [30].

4. The importance of compliance with research regulations by [31] highlighting the importance of compliance with cyber security regulations in the financial sector. Regulators and supervisory authorities play a crucial role in shaping a security framework and ensuring that sharia banks comply with the standards set to protect their data and systems.

The Relationship Between Cybersecurity And Financial Stability

1. Cyber security as the foundation of financial stability Cybersecurity has been identified as the primary foundation forining economic stability in a number of researches. According to [32] Cyber security is not just a technical issue, it is a critical element inining public confidence in financial institutions. Financial stability covers not only operational sustainability, but also the data and system integrity that underpins such operations.
2. Impact of cyber attacks on financial stability Research by [33] It describes the impact of cyber attacks on financial stability as a real threat. A successful cyber attack can result in significant disruptions to the operational functioning of financial institutions, affect the integrity of data, and ultimately undermine public confidence.
3. The relationship between financial crises and cybersecurity risks is also discussed in the literature. According to [34], Crisis conditions can increase vulnerability to cyber attacks because the focus is more on recovery than on strengthening security. Therefore, involvement of cyber security in risk mitigation planning becomes crucial.
4. Regulation and cybersecurity as a top priority Emerging regulations strengthen the link between cybersecurity and financial stability. The need for financial institutions to comply with the cyber security regulatory

[30] Susanto et al., "Manajemen Keamanan Cyber Di Era Digital."

31 I. Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, "Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources," Information & Management, 2015, 52 (3): 385–400.

[32] Yulianto, A., Utaminingsih, N. S., SE, M., Sari, M. P., & Akt, C. A. Sistem Informasi Manajemen. Cahya Ghani Recovery, 2023.

[33] T. A Gani, Pengembangan Metode Pembelajaran Dalam Dinamika Belajar Siswa (jakarta: Rineka Cipta, 2017).

[34] Bacharuddin, M. A. "The Impact of Macroeconomic Variables towards Economic Growth in Malaysia." Journal of Education Technology. 2017 (n.d.).

framework as an effort to support global financial stability. These regulations encourage financial institutions to invest sufficient resources in protecting against cyber attacks [35].

5. The role of cyber security in maintaining public trust. Public trust in the financial sector is closely related to cyber security. Study by Failure to manage cybersecurity risks can damage the reputation of financial institutions and reduce levels of public trust, which in turn can affect financial stability [36];[37].
6. In the context of financial institutions, banks, cybersecurity is also closely linked to the availability of funds. According to [38] Cyber attacks that cause operational disruption can result in massive withdrawals by concerned customers, bringing potential liquidity risks and upsetting financial stability.
7. International aspects and co-operation in cybersecurity Studies by [39] emphasized that the link between cyber security and financial stability cannot be isolated on a national basis. Cybersecurity is a global issue, and international cooperation in information exchange and training is key to mitigating the risk of attacks that can impact across borders.

Cyber Security

a. The results of the research discussion on liquidity management and cybersecurity at the sharia bank provide in-depth insight into how the results of research can be applied in the practice of liquidity and cyber security management. Here is an explanation of the discussion of the findings and their implications for the practice in both aspects:
b. Liquidity Management

   Analysis suggests that sharia banks can manage liquidity fluctuations more effectively by implementing more proactive liquidity management strategies.

[35] Ngamal, Y., & Perajaka, M. A. "Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia." Jurnal Manajemen Risiko, 2022, 2 (2): 59–75

[36] J. T Santoso, Teknologi Keamanan Siber (Cyber Security) (Penerbit Yayasan Prima Agus Teknik, 2023).

[37] T. Evi, "Transformasi Transaksi Tunai Ke Digital Di Indonesia," 2023.

[38] Saputro, E. P., Nasir, M., SE, M., Muhammad Arif, S. E., Setyaningrum, D. P., SE, M., & Febriyanto, A. "Digitalisasi Perbankan: Prospek, Tantangan & Kinerja." Muhammadiyah University Press, 2022

[39] I Rizal, M., Rukmana, A. Y., Permana, A. A., Fianty, M. I., Saputra, H., Saputri, F. R., ... & Adhicandra, "Transformasi Digital: Memahami Internet Of Things," Get Press Indonesia, 2023.

Sharia Banks may consider diversifying their liquidity sources, improving cash flow monitoring, and developing more realistic stress scenarios.Minimize the risk of bankruptcy, improve liquidity management efficiency and support operational sustainability.

c. Cyber security
Cybersecurity findings indicate that a lack of understanding of cyberspace risks among officials is a major factor that makes sharia banks vulnerable to cyberattacks. To reduce the risk of socio-technical attacks and information leaks, routine training and increased security awareness among employees must be strengthened. Increased resistance to cyber attacks, reduced risk of intruder attacks and improved rapid response to security threats.

d. Integration of liquidity management and cybersecurity.
Integration of liquidity management and cybersecurity strategies is key to ensuring financial stability and security of sharia banks. Improve operational efficiency, minimize the risk of attacks that could affect liquidity, and create a comprehensive security environment.

e. Relationship with the principle of Shariah
Sharia principles can affect liquidity management and cybersecurity strategies, especially in the context of adherence to Islamic ethical values. Maintaining the integrity of Sharia banks, enhancing customer confidence, andining a reputation as a Sharia-obedient financial institution

f. Application of technology and innovation.
The application of advanced technology and innovations in liquidity management and cybersecurity can improve the competitiveness of sharia banks. Investing in the latest technology and innovative policies can increase efficiency, minimize risk, and provide a safer customer experience. Improve market competitiveness, attract consumers who are increasingly technologically intelligent, and offer an advantage in dealing with increasingly complex cyber threats.

The outcome of the discussion on outcomes and implications for liquidity management and cybersecurity practices provides practical guidance for sharia banks to improve operational performance as well as maintain financial security and stability. Strategic integration, Sharia awareness, and the application of technology are the keys to success in these two important aspects.Through these measures, Shariah banks can ensure that they continue to operate and continue to uphold Islamic ethical principles in their business practices.

In-Depth Analysis of Research Results

a. Sharia banks, like other financial institutions, face many serious cyber security challenges in the growing digital age. A detailed analysis of these challenges gives insight into their complexity and the importance ofining fiscal stability and public confidence. Here is a detailed overview of some of the major cybersecurity challenges facing sharia banks:
b. Phishing and social engineering attacks.
   Shariah banks are vulnerable to phishing attacks.The attack uses psychological manipulation techniques to obtain sensitive information from customers and employees. .
c. Malware and Ransomware
   Malware and ransomware threats can lead to data breaches, theft of financial information and system lockdown that can interfere with banking operations, loss of control over sensitive systems and data, and potentially paying ransoms through ransumware attacks.
d. The challenge of obedience to Shariah
   Maintaining cybersecurity by adhering to Sharia principles is a unique challenge for sharia banks, which must ensure compliance with Islamic norms and ethics.
e. Legal and regulatory uncertainty
   The changing regulatory environment can make it difficult for sharia banks to comply with relevant cyber security standards. Delays in compliance can result in legal sanctions and reputational damage.
f. Lack of security awareness
   Lack of awareness of cybersecurity risks among internal and external stakeholders can increase the likelihood of security breaches. Untrained employees and customers can be the entrance to the attack, thereby increasing the risk of security breaches.
g. Ineffective identity and access management
   Invalid identity and access management can provide unauthorized access to critical systems and data. Risk of identity theft, fraud, and unauthorised access to customer funds and confidential banking information.
h. Financial technology challenges
   Fast-tech financial service providers can pose new cybersecurity challenges as sharia banks need to integrate with this technology. Data security risks and insecure integration with Fintech solutions can damage the reputation and trust of customers.

This analysis underscores the undercomplexity of the cyber security challenges faced by the sharia bank. To address these challenges requires a comprehensive approach that includes security education, strict policy, and investment in advanced technology to maintain financial stability and customer confidence, taking into account various aspects such as technology, regulation, and compliance with Islamic law.

CONCLUSION

The conclusion of this study is that the cybersecurity challenge in the management of the liquidity of the sharia bank is a crucial and complex issue that requires serious attention. Sharia bank, as a financial institution that operates according to Islamic principles, has speciality in managing the risk of cyber security because it must abide by the principles of sharia in transactions and fund management. In this context, the study highlights some important findings: The importance of a deep understanding of cyber security risks among Sharia bank officials. Lack of awareness and understanding can make banks vulnerable to cyberattacks. Therefore, routine training and increased security awareness among employees is vital. Proactive liquidity management strategies can help sharia banks manage liquidity fluctuations more effectively. Diversification of liquidity sources, better monitoring of cash flows, and the development of realistic stress scenarios are measures that can help minimize the risk of bankruptcy.

Integration between liquidity management and cybersecurity is key toining financial stability and the security of sharia banks. A close collaboration between these two areas is needed to identify, manage, and mitigate potential associated risks.Growing regulation in the field of cybersecurity strengthens the link between cyber security and financial stability. Compliance with cybersecurity regulations is becoming crucial, and regulators and supervisory authorities play a crucial role in ensuring compliance by financial institutions.

Thus, this study suggests that sharia banks need to adopt a holistic strategy in dealing with cybersecurity and liquidity management challenges. Only by understanding the risks involved and implementing appropriate measures can sharia banks increase their resilience to cyber security attacks and maintain their financial stability in a risky digital age.

REFERENCES

Abduh, M. "Competitive Condition and Market Power of Islamic Banks in Indonesia." *International Journal of Islamic and Middle Eastern Finance and Management*, 2017, 20 (1): 77–91.

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. "Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources." *Information & Management*, 2015, 52 (3): 385–400.

Cimb Niaga. "Pengertian Tentang Bank Syariah Dan Istilah Di Dalamnya." Cimb.Co.Id, 2022.

Darmadi. *Pengembangan Metode Pembelajaran Dalam Dinamika Belajar Siswa*. Jakarta: Rineka Cipta, 2017.

Demchak, C. C. "China: Determined to Dominate Cyberspace and AI." *Bulletin of the Atomic Scientists*, 2019, 75 (3): 99–104.

Evi, T. "Transformasi Transaksi Tunai Ke Digital Di Indonesia," 2023.

Fattah, H., Riodini, I., Hasibuan, S. W., Rahmanto, D. N. A., Layli, M., Holle, M. H., ... & Marzuki, S. N. "No Title." *Fintech Dalam Keuangan Islam: Teori Dan Praktik*, 2022.

Gance-Clev eland, B. G. "Evaluation of Technology to Identify and Assess Overweight Children and Adolescents." *Journal for Specialists in Pediatric Nursing*, 2010, 15 (1): 72–83.

Gani, T. A. *Pengembangan Metode Pembelajaran Dalam Dinamika Belajar Siswa*. jakarta: Rineka Cipta, 2017.

Julius Adams Stratton and Loretta H. Mannix, M. a. "The Birth of MIT." *Cambridge: MIT Press*, 2005, 190.

Khan, M.S. and Mirakhor, A. "The Financial System and Monetary Policy in an Islamic Economy." *Ln Theoretical Studies in Islamic Banking and Finance.*, 1987.

Libicki, Ablon. "Ancaman Dan Serangan Terhadap Sektor Keuangan." *Jurnal Sains Dan Informatika*, 2014.

Mirakhor, Haque. "Dampak Krisis Keuangan Terhadap Manajemen Likuiditas Syariah." *Manajemen*, 2018.

Prawirio, M. "Pengertian Bank Secara Umum, Fungsi, Tujuan, Dan Jenis-Jenis Bank." *Https://Www.Maxmanroe.Com/*, 2019.

Rahman, M. A.-T. "Ata-Driven Dynamic Clustering Framework for Mitigating the Adverse Economic Impact of Covid-19." *Sustainable Cities and Society*, 2020, 2: 10–23.

Restika, Restika, and Era Sonita. "Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era Digital." *Krigan: Journal of Management and Sharia Business* 1, no. 2 (2023): 25. https://doi.org/10.30983/krigan.v1i2.7929.

———. "Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era Digital." *Krigan: Journal of Management and Sharia Business* 1, no. 2 (2023). https://doi.org/10.30983/krigan.v1i2.7929.

Rizal, M., Rukmana, A. Y., Permana, A. A., Fianty, M. I., Saputra, H., Saputri, F. R., ... & Adhicandra, I. "Transformasi Digital: Memahami Internet Of Things." *Get Press Indonesia*, 2023.

Santoso, J. T. *Teknologi Keamanan Siber (Cyber Security)*. Penerbit Yayasan Prima Agus Teknik, 2023.

SRIWULAN, S. "Tinjauan Yuridis Tindak Pidana Cyber Crime Di Indonesia (Doctoral Dissertation." *Institut Agama Islam Negeri Palopo*, 2023.

Sultoni, Hasan, and Kiki Mardiana. "Pengaruh Merger Tiga Bank Syariah BUMN Terhadap Perkembangan Ekonomi Syariah." *Jurnal Eksyar : Jurnal Ekonomi Syariah* 08, no. 01 (2021).

Sundararajan. *Keamanan Cyber (Cyber Security)*. Penerbit Yayasan Prima Agus Teknik, 2002.

Susanto, Edy. "Manajemen Keamanan Cyber Di Era Digital." *Jurnal Bisnis Dan Kewirausahaan (Journal of Business and Entrepreneurship)* 11 No 1 (2023).

Susanto, Edy, Lady Antira, Kevin Kevin, Edo Stanzah, and Assyeh Annasrul Majid. "Manajemen Keamanan Cyber Di Era Digital." *Journal of Business And Entrepreneurship* 11, no. 1 (2023). https://doi.org/10.46273/jobe.v11i1.365.

Vebrianty, A. "Perlindungan Hukum Pembukaan Rekening Secara Online Dalam Layanan Perbankan Digital Pada Pt Bank Central Asia Tbk (Bachelor's Thesis)." *Fakultas Syariah Dan Hukum UIN Syarif Hidayatullah Jakarta*, 2021.

Winanti, Wiwin. "Manajemen Risiko Likuiditas Pada Perbankan Syariah." *EKSISBANK: Ekonomi Syariah Dan Bisnis Perbankan* 3, no. 1 (2019). https://doi.org/10.37726/ee.v3i1.34.

Zed, M. *Metode Penelitian Kepustakaan*. Jakarta: Yayasan Obor Indonesia, 2008.