General Council for Islamic Banks and Financial Institutions
CIBAFI
المجلس العام للبنوك والمؤسسات المالية الإسلامية
ISSUE 15 • December 2021

CIBAFI BRIEFING

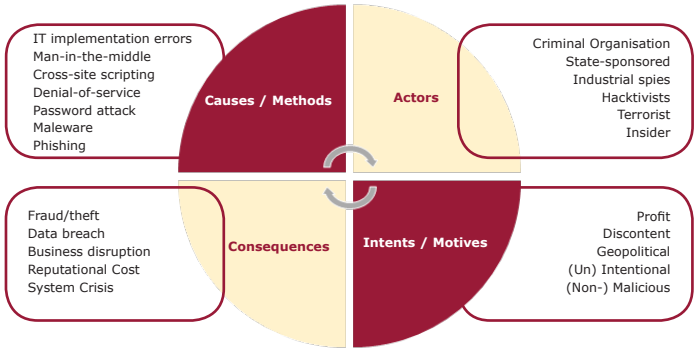
The Rising Concern of Cybersecurity in Islamic Finance: Key Risks, Current Practices, and Cyberdefense Approaches

CIBAFI is pleased to present its fifteenth "Briefing" on "The Rising Concern of Cybersecurity in Islamic Finance: Key Risks, Current Practices, and Cyberdefense Approaches". The briefing presents an overview on cyber risks and cybersecurity in the financial industry. It outlines the recent trends that have been feeding cyber risks in the industry and the effects these could have on financial stability. It also looks at the approaches for developing cyberdefense and the challenges that could be faced in the process. In addition, the briefing sheds light on cyber risks in the Islamic financial services industry and the cybersecurity practices adopted by Islamic financial institutions as well as presents policy recommendations for the strengthening and attainment of cyber resilience in the industry.

1. Introduction

The increase in digitalisation of services in recent years, accelerated by the Covid-19 pandemic, has been augmenting significantly cyber risks and particularly cyberattacks within economies, making it an increased concern across the globe. The Bank for International Settlements (BIS) defines cyber risk as 'the risk of financial loss, disruption or reputational damage to an organisation resulting from the failure of its IT systems'. Cyber risks could arise within organisations because of unintended accidental causes such as employees accidentally deleting data or intended purposes where attackers target computer/IT systems and networks to cause loss/harm for financial gain, political purposes (including 'hacktivism'[1], cyber warfare, and terrorism), or solely for curiosity and fun. These incidents could be carried out by external parties (such as criminal organisations, hacktivists, amateurs) or the employees of the organisation (known as insiders). Figure 1 below provides a taxonomy of cyber risks.

Figure 1. Taxonomy of Cyber Risks



Source: SUERF Policy Note No 206 (Bank for International Settlements (BIS) Elaboration) (SUERF, 2020)

Various methods are used today by cyber attackers to undertake their attacks, these include malware, phishing, among others (explained further in Figure 2). The sophistication of these methods has been continuously increasing over time, with technological developments such as artificial intelligence (AI) and machine learning feeding new types of risks.

Figure 2. Types of Cyberattacks

Malware
Malicious software that disrupts or damages a user's computer system or steal its data.

Distributed Denial-of-service (DDOS) attacks
Attacks to disrupt computer systems by causing huge traffic on its servers and networks.

Phishing
Using legitimate looking emails to trick users into clicking on a malicious link or downloading an attachment with malware to gain access to personal information.

Spoofing
Disguising a malicious identity to gain access to data or perform other malicious activities.

Man-in-the-middle
Cyber attacker intercepting the communication between two parties to disrupt transactions or steal data.

Structured Query Language (SQL) Injection
Controlling and stealing data from applications through the detection of vulnerabilities and inserting a malicious code (SQL statement).

Cross-site Scripting
Compromising a web security vulnerability to gain control over a user's account, actions and data in vulnerable applications.

1. Hacktivism is the combination of hacking and activism where the tools and techniques of hackers are used for political purposes.

Cyber risks can have a huge impact on organisations which can lead, in extreme cases, to systemic economic disruptions. Thus, cybersecurity[2] represents today one of the major preoccupations for policymakers and an important topic on global agendas. Due to their increased proneness to cyber threats, financial institutions need to understand the types of threats they are subject to and take concrete and continuous measures to build more secure and resilient systems.

2. Cyber Risks in the Financial Industry

It is reported that, over the last five years, the financial industry has been the most hit by cyberattacks, according to available public data[3]. It is also reported that a quarter of all cyber incidents affect the financial sector. Cyber risks in the financial industry are driven by several factors, including the availability of data and money as well as the high involvement of third-party service providers, making it highly prone to cyber attacks. In addition, the use of obsolete systems by certain institutions and the lack of awareness and cybersecurity training, as existent in other industries, drive cyber risks further.

Two important trends that have recently been feeding cyber risks in the financial industry are digitalisation and work-from-home arrangements. Strides in digitalisation, accelerated by the Covid-19 pandemic, have been fuelling these risks. Also, using personal devices and private networks due to work from home policies have been increasing institutions' vulnerabilities. The BIS reports that the financial sector was the most hit sector by Covid-19 cyber events, excluding the health sector. The emergence of open banking has also been increasing cybersecurity concerns due to the access of authorised third-party providers to banks' systems. In this case, cyberattacks targeting the third-party providers or dishonesty among these providers' staff may put banks at risk.

Amongst methods used for cyber incidents, some are used more frequently in the financial industry than others. Ransomware for example is found to be an increasingly used method for cyberattacks in the financial industry, alongside phishing and DDOS attacks. Cyber attackers are continuously revising and increasing the sophistication of their methods to suit the changes in the market; advanced technologies such as AI and machine learning are used today to be able to understand human behaviour patterns and detect vulnerabilities as soon as they arise.

While both small and large financial institutions are subject to the same risks, smaller financial institutions are seen to be more vulnerable to cyberattacks given the lower sophistication of their cybersecurity measures. Also, while most reported cyber incidents come from North America, it is observed that lower-middle-income countries are witnessing increased cyberattacks due to the rise in digitalisation for financial inclusion, e.g. through mobile banking. The rise in attacks has also been due to the lack of cybersecurity talents and skills in these countries, smaller budgets for advancing cybersecurity, and the increased cybersecurity measures by advanced economies making these

2. Cybersecurity refers to the use of processes, policies, and technologies to protect, defend and/or prevent networks, systems, devices, programs, and data from damage, unauthorised use, or exploitation.

3. It is important to note that data on cyber incidents is scarce. Most cyber-incidents are unreported and the publicly-available data comes mainly from North America, as a result of reporting obligations and freedom of information provision there. The data may therefore not be representative of the jurisdictions in which most Islamic financial institutions operate.

countries a more interesting and attainable target. In October 2020, MTN Uganda and Airtel, two telecom companies in Uganda offering mobile money transfers, were disrupted by a hack in Pegasus Technologies, halting mobile money transfers in Uganda and causing theft of at least USD 3.2 million. In the Gulf Cooperation Council, cyberattacks have also been on the rise with the increased digitalisation in the region fuelling vulnerabilities.

Cyber incidents can have important consequences such as affecting customer confidence and the institution's reputation. They can also cause material losses to financial institutions that can affect the institution's capitalisation and liquidity. Such consequences will have more implications on the financial position of small banks. In addition, the interconnectedness in the sector could make one attack affect several institutions at the same time, causing systemic damage and undermining financial stability, locally and globally. A relatively small number of institutions, but certainly including major exchanges, are so important that a significant outage at a time of high market volatility would in itself be systemically important.

3. Developing Cyberdefense: Approaches and Challenges

The rapid digital transformation, technological developments, and most recently the pandemic contributed to several developments in terms of policies, regulations, and cyber laws to encourage financial institutions to evaluate their IT systems and ensure their readiness to cyberattacks. By defining mandatory security requirements, and good practice standards, regulators and policymakers play a salient role in ensuring the security of cyberspace by enhancing security preparedness and protecting consumers. Recent regulatory initiatives include:

Globally:

- The International Organization of Securities Commissions (IOSCO) and the Committee on Payments and Market Infrastructures (CPMI) developed in 2016 the first internationally agreed guidance on cyber resilience for financial market infrastructures (FMIs).
- The BIS issued a report in 2018 presenting and comparing a set of cyber resilience practices adopted by banks and regulatory and supervisory authorities across several jurisdictions.
- The Financial Stability Board (FSB) issued in 2020 a toolkit outlining effective practices that financial institutions may adopt to respond to and recover from cyber incidents to limit related financial stability risks.

Locally and Regionally:

- The European Central Bank (ECB) in its recent guidance issued in 2020 advises banks to continuously assess the capacity of existing IT infrastructure due to the noticed increase in cyberattacks.
- The Monetary Authority of Singapore (MAS), in 2020, requested financial institutions to adopt a proactive approach in dealing with any future increase in demand for online financial services.
- The Dubai Financial Services Authority (DFSA) is encouraging banks to register to use the DFSA Cyber Threat Intelligence Platform (TIP) and exploit the cyber threat information available on TIP to enhance their cybersecurity.

Alongside regulations, cybersecurity standards play an important role in helping organisations benchmark their measures and controls against established standards. The Payment Card Industry (PCI) Security Standards for payment are one example of key standards for cybersecurity. PCI Security Standards guide institutions in maintaining payment security through a set of technical and operational requirements. Another example is the standards in the ISO/IEC 27000 family which allow organisations to manage the security of their assets such as financial information, intellectual property, employee details, or information entrusted by third parties. When it comes to reinforcing the security of the global banking system, the SWIFT Customer Security Controls Framework (CSCF) provides a set of control guidelines to mitigate specific cybersecurity risks.

In addition to complying with regulations and guidance issued by authorities, financial institutions need to deploy sophisticated and recent technologies to enhance their resilience against cyberattacks.

Although AI may be used by attackers, it is also being used to strengthen the defensive capabilities of institutions against cyber threats, helping in examining huge amounts of data efficiently to determine patterns of cyberattacks to recognise similar future attacks. The use of AI also helps in decreasing the costs of cyber incidents. According to IBM, organisations with fully deployed security AI and automation have experienced breach costs of $2.90 million, compared to $6.71 million for organisations without such measures. However, this is likely to be an approach for larger institutions who will have the volume of data necessary to train an AI.

The workforce is a double-edged sword that can either prevent or cause cyber risks. The human component represents an important part of designing, operating, and defending organisations' cyber ecosystem. The lack of sufficient cybersecurity knowledge by employees can make them an important source of cyber risks through for example system hacks and malware originating from innocent clicks on malicious links. Thus, not only should organisations employ cybersecurity specialists, but they should also equip employees with the necessary tools for mitigating cyber risks to make them a source of their cyber resilience. This involves providing continuous training and cybersecurity education to employees, in addition to periodic monitoring of the access to the organisation's systems and data to keep track of sources of cyber risks.

However, while these efforts present opportunities for enhanced cybersecurity in the industry, there still exist various challenges facing financial institutions in the protection from cyber risks. One important challenge relates to the increased sophistication in cyber criminals' methods. This poses extra complications in trying to build smarter systems that can counteract these sophisticated means, especially with the continuous development of cyberattacks. Cybersecurity measures also require huge

investment from financial institutions, possibly weighing heavily on their budgets. This could pose issues for smaller financial institutions that do not have the necessary means.

Another challenge relates to the lack of cybersecurity professionals in the market which can undermine cybersecurity measures put in place.

Thus, institutions will need to place concerted efforts in training and educating staff to achieve the required level of skills which could be time-consuming and costly.

The structure of the financial industry itself poses important challenges for financial institutions. The reliance of a financial institution on multiple service providers and multiple institutions relying on the same provider poses inherent issues of interdependence and vulnerability, undermining cybersecurity. The lack of harmonisation in regulatory approaches for cybersecurity also presents another challenge. With each jurisdiction adopting different requirements for cybersecurity, some more than others, multinational financial institutions must adopt different measures for each market fragmenting their networks into multiple segregated national systems. This can also make certain markets more prone to attacks than others and can make them a venue for cyber attackers disrupting the global financial system. Compliance laws put in place for consumer protection such as the General Data Protection Regulation (GDPR) in the EU may also complicate cybersecurity for smaller banks and financial institutions who may not be able to bear the fines relating to non-disclosure of cyber incidents.

4. Islamic Finance and Cyberattacks

It is undoubtedly clear that cybersecurity is a common challenge for both Islamic financial institutions and their conventional counterparts. Wealth and data circulating within the Islamic financial ecosystem also present a target for cyberattacks. In CIBAFI's Global Islamic Bankers' Survey (GIBS) for the years 2020 and 2021, Islamic banks cited cyber-security risk and technology risk among the top three concerning risks faced by their institutions.

From an Islamic perspective, preserving and protecting properties of individuals and organisations from any harmful act is one of the objectives of Shariah. Such properties include financial and tangible wealth, digital resources, and intangible wealth. These assets are circulating in the financial sector and are exposed to several threats affecting information systems of financial institutions and leading to theft, fraud, scams, and criminal/wrongful exploitation of public & private data. Thus, preventing such threats is aligned with the objectives of Shariah and is associated with ensuring the safety of cyberspace and the adoption of measures to reinforce Islamic finance institutions' cyber resilience.

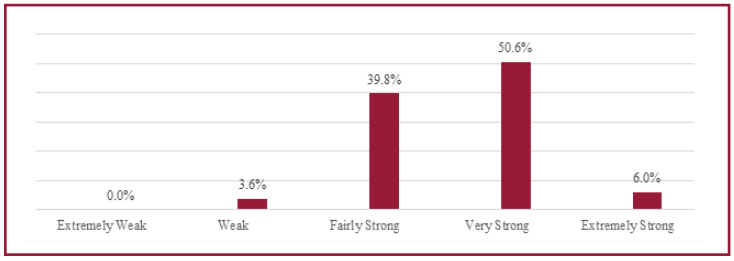
However, inherent to their size and location, Islamic banks face increased challenges in ensuring cybersecurity and resilience. Being mostly small banks, the investment in cybersecurity measures can be challenging for Islamic banks with limited resources. In addition, geopolitical tensions in regions where Islamic banks operate, for instance the Middle East, can make financial systems in these regions an increased target for cyberattacks and increase Islamic banks' proneness to cyberattacks. The weaknesses in IT infrastructures in some emerging countries also puts a further burden on small financial institutions and Islamic banks operating in these countries, especially in the case of digital financial services transactions carried out using insecure devices and over transmission lines that are not designed to protect the security of financial transactions.

5. CIBAFI Survey on Cybersecurity

CIBAFI conducted a survey in May 2021 to evaluate Islamic banks' resilience in terms of cybersecurity and examine the cyber threats faced by Islamic banks and the measures implemented to strengthen their cyberspace. A total of 100 Islamic banks from 33 countries participated in the survey.

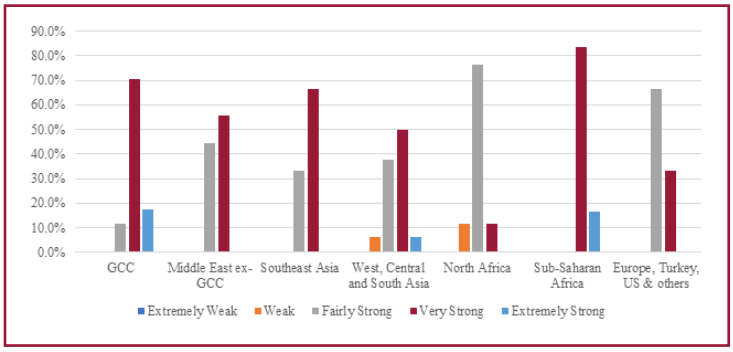
The global picture shows that Islamic banks are in general confident of their cyber resilience. Around 40% of respondents considered their cyber resilience to be fairly strong and more than half considered it to be either very strong or extremely strong.

Figure 3. Islamic Banks' Views on their Institutions' Cyber Resilience



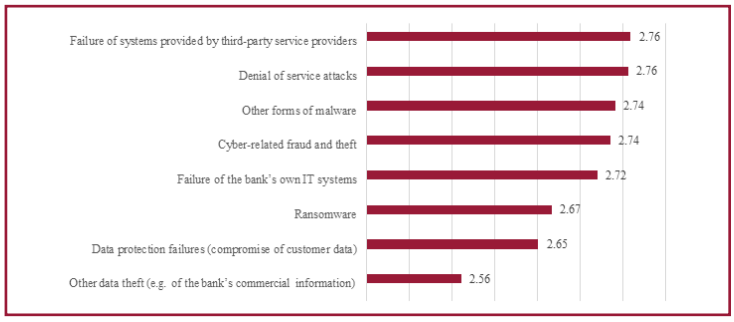
However, by region, Islamic banks in North Africa were the least confident in their cyber resilience. This could reflect the higher potential of cyber threats in the region related to weaker infrastructures or to the fact that most respondents from this region are small banks. This is followed by Islamic banks in Europe which might be less resilient due to being smaller in size as well and thus possessing less resources for enhanced cybersecurity measures.

Figure 4. Islamic Banks' Views on their Institutions' Cyber Resilience – Regional Breakdown



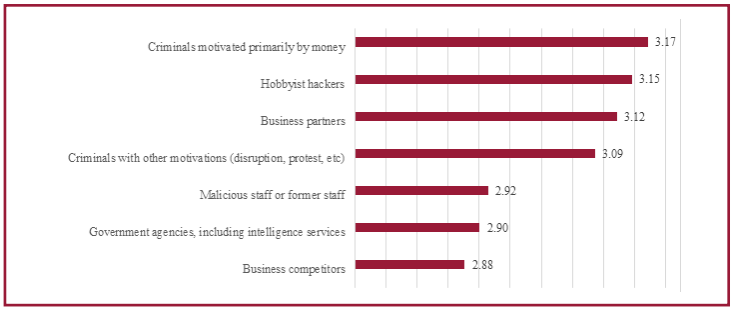
The results of the survey also showed that, from a list of potential threats, banks consider the failure of systems provided by third-party service providers and DDOS attacks as the most important cyber risks facing their institution. Cyber-related fraud, theft, and other forms of malware are found to be the second most threatening cyber risks for Islamic banks. These are followed by the failure of the bank's own IT systems. The below figure shows the overall results; it is however clear that the scores of all elements are around the same level.

Figure 5. Level of Importance of Cyber Threats Facing Islamic Banks



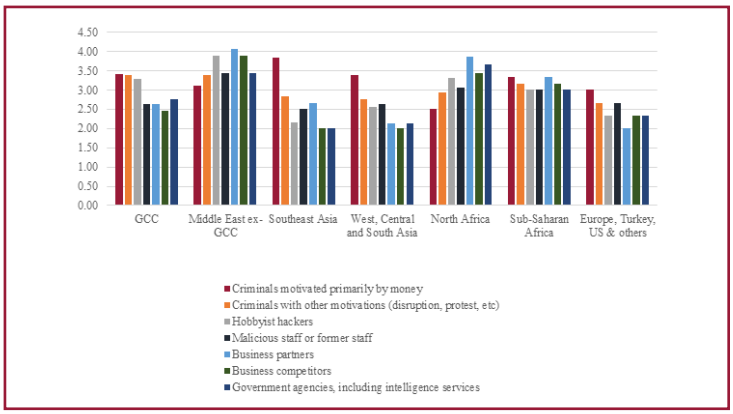
The survey also interrogated on the actors behind cyber threats targeting Islamic banks. From a list of parties, Islamic banks ranked criminals motivated primarily by money at the top, followed by hobbyist hackers and then business partners. Business competitors were considered as the least risky parties to the cyberspace of Islamic banks.

Figure 6. Actors Behind Cyber Threats Targeting Islamic Banks



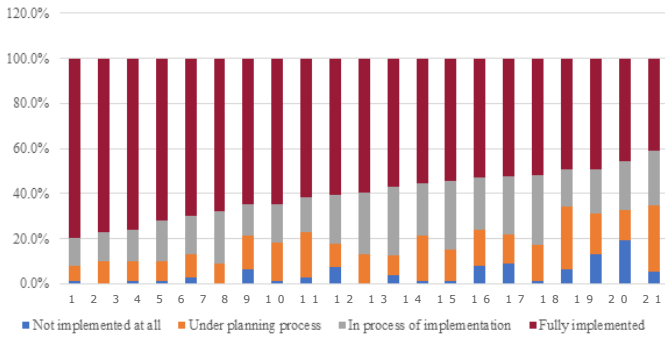
The regional picture shows that, in general, regions can be classified into two groups. One group considers parties within its business ecosystem, such as business partners and competitors, as posing cyber threats to their institutions. This is noticed in regions like Middle East Ex-GCC, North Africa and Sub-Saharan Africa. The second group consists of regions that consider external parties of the business ecosystem, such as criminals with different motives, as the parties posing more threats on the cyberspace of Islamic banks.

Figure 7. Actors Behind Cyber Threats Targeting Islamic Banks – Regional Breakdown



From a list of measures, Islamic banks were also asked to indicate the level of implementation of cybersecurity measures. The results show that most respondents are in the execution phase, either under implementation or have fully implemented all the listed measures. Employing multiple layers of security to segregate the corporate network from externally facing systems is the most implemented measure, while undertaking quarterly exercises to test the ability of institutions to respond to cybersecurity incidents is the most non-implemented measure by Islamic banks. It is observed that Islamic banks have been placing more efforts to implement measures to secure their systems and less in creating formulated strategies for cybersecurity and periodic testing to ensure the cyber resilience of their systems which should be placed as a higher priority in line with international bodies' recommendations and given the continuous sophistication of cyber threats.

Figure 8. Level of Implementation of Cybersecurity Measures by Islamic Banks



1. Formally documented cybersecurity strategy
2. Formal Chief Cyber Security Officer or similar senior executive role who is accountable for delivery of the cybersecurity framework
3. Undertaking quarterly exercises to test your ability to respond to cybersecurity incidents
4. Maintaining a current inventory of information assets with supporting systems
5. Proactively identifying hardware and software vulnerabilities and document these with their risk assessment
6. Requiring strong authentication for all remote access to the corporate network and business applications
7. Appropriate controls in place to classify information in terms of criticality and sensitivity
8. Tools and processes in place to detect and prevent sensitive data from leaving the corporate network
9. Effective processes and procedures in place to assess the security capabilities and management of cyber risk by third party providers
10. Incorporate cyber security in change management and design processes, as well as service and products development
11. Employing multiple layers of security to segregate the corporate network from externally facing systems
12. Cyber security training to your staff at least once a year
13. Monitor for and detect anomalous activities and/or events
14. Record remote access attempts, with alerts for potential malicious activity
15. Monitor personnel operating on the corporate network, including unauthorised connections or devices
16. Carry out penetration tests to identify vulnerabilities that may affect your systems, networks, people or processes
17. Use cyber threat intelligence to inform your cyber security strategy and framework
18. Undertake in-depth investigations following a cyber-security event or incident
19. Process in place to recover systems and data from an incident
20. Engage with critical third parties to understand the risks that exist between both parties, and take steps to ensure that recovery activities are clearly understood by both parties
21. Having available non-mandatory guidance on cyber security from a regulator or trade body

CIBAFI BRIEFING

The Rising Concern of Cybersecurity in Islamic Finance: Key Risks, Current Practices, and Cyberdefense Approaches

6. Conclusion and Recommendations

The benefits of technology have been driving digitalisation in the financial industry within the last years, accelerated by the Covid-19 pandemic. This helped in enhancing services, reducing costs, and increasing efficiency; however, it has also been associated with increased cyber risks. Cyber risks can have important consequences on the health of financial institutions and the financial system. The size of Islamic banks and their geographical distribution brings additional exposure to cyber risks due to lack of resources and unsophisticated IT infrastructure. It is thus crucial that efforts are put to attain cyber resilience for the stability of the financial system. This requires joint efforts from different actors and the adoption of measures at all levels and by all actors of the financial industry aiming to protect cyberspace. For Islamic financial institutions, such efforts also contribute to achieving the objectives of Shariah in preserving properties and wealth.

Therefore, it is recommended to:

- Follow a proactive approach and continuously enhance cybersecurity practices by leveraging on toolkits and best practices developed by international bodies.
- Develop clear strategies for cybersecurity within the institution including the identification of vulnerable digital assets; continuous evaluation for management of cyber threats; automation of processes to reduce human error; diversification of data storage; management of exposures to third-party risks; …etc.
- Develop clear recovery plans for quick recovery from cyberattacks.
- Promote cybersecurity and highlight its role in achieving Shariah principles.
- Establish training programs for employees on cybersecurity and educate customers on cyber criminals' methods and best practices to reduce falling a victim to cyberattacks.
- Establish platforms for information sharing between financial institutions to support cybersecurity measures.
- Develop programs to support cybersecurity in small financial institutions.
- Develop clear and harmonised definitions and categorisations of cyberattacks to ease the identification of cyber threats and the comparability of data across institutions and countries.
- Establish platforms for continuous dialogue and sharing of information on cyber incidents with infrastructural institutions and regulators to allow early detection of vulnerabilities and contribute to strengthening the national cyberspace.
- Develop flexible regulations that accommodate changes in cyber threats.
- Join forces globally to develop a universal strategy for addressing cyber threats related to the global connectivity of financial institutions and to support regions with underdeveloped IT infrastructures to enhance global cyberspace.

About CIBAFI

CIBAFI is an international non-profit organisation founded in 2001 by the Islamic Development Bank (IDB) and a number of leading Islamic financial institutions. CIBAFI is affiliated with the Organisation of Islamic Cooperation (OIC).

With over 130 members from more than 34 jurisdictions from all around the world, CIBAFI is recognised as a key piece in the international architecture of Islamic finance.

Its mission is to support the IFSI by providing specific activities and initiatives, aiming to strengthening the growth of IFSI, deepening Shariah Objectives in financial dealings and transactions, and facilitate cooperation between members and institutions of common interest.

CIBAFI is guided by its Strategic Objectives, which are 1) Advocacy of Islamic Finance Values and Related Policies & Regulations; 2) Research and Innovation; and 3) Training and Professional Empowerment.

Contact Information:

General Council for Islamic Banks and Financial Institutions (CIBAFI)
Jeera 3 Tower, Office 51, Building No. 657, Road No. 2811, Block No. 428
Manama, Kingdom of Bahrain. P.O. Box No. 24456

Email: cibafi@cibafi.org
Telephone No.: +973 1735 7300
Fax No.: +973 1732 4902
www.cibafi.org

Acknowledgements

CIBAFI would like to offer its sincere thanks to the individuals who have contributed in making the publication a success. We would like to appreciate CIBAFI Secretariat members, Mr. Peter Casey, CIBAFI Consultant and Mr. Murat Gökten, Head of Enterprise Architecture, Albarakatech Global, Turkey.

We trust that this publication will provide valuable insights to Islamic bankers around the globe on cybersecurity risks and the practices required to create a safe cyberspace.

References

For more information about the references, please access the following link:

https://www.cibafi.org/SurveyPage?ContentId=CI2137