

E-ISBN: 978- 605-74046-3-3

5. ULUSLARARASI İSLAMİ FİNANS VE EKONOMİ KONFERANSI BİLDİRİ KİTABI

5 TH INTERNATIONAL CONFERENCES ON ISLAMIC FİNANCE AND ECONOMICS PROCEEDING BOOK

22-23 EKİM 2024
22-23 OCTOBER 2024

HKÜ KAMPÜSÜ, KONGRE VE KÜLTÜR MERKEZİ / GAZİANTEP
HKU, CONGRESS AND CULTURAL CENTER / GAZIANTEP

5. ULUSLARARASI İSLAMİ FİNANS VE EKONOMİ KONFERANSI

5 TH INTERNATIONAL CONFERENCE ON ISLAMIC FINANCE AND ECONOMICS

(22 - 23 Ekim 2024)

Editörler

Doç. Dr. Yıldız ÖZKÖK

Doç. Dr. Zeynep KÖSE

Dr. Öğr. Üyesi Bilal ÇAYIR

İktisadi, İdari ve Sosyal Bilimler Fakültesi

Faculty of Economics, Administrative and Social Sciences

Gaziantep 2024

TAKDİM

Değerli Katılımcılar,

Geleneksel bankacılık ve finans sistemlerine alternatif olan ve faiz duyarlılığı nedeniyle yatırımlarını değerlendirme ve güvence altına alma ihtiyacını karşılama konularında farkındalığı artırmak ve çözümler bulmak amacıyla 5. Uluslararası İslami Finans ve Ekonomi Konferansı'nı (22-23 Ekim 2024) tamamlamış olmanın gururunu hep birlikte yaşadık. Gaziantep'te konferans ve İstanbul'da workshop olmak üzere iki aşamalı olarak etkinliklerimizi tamamladık. Bu yılki konferansımızda İslami Finansın Geleceğini Dijital ekonomi ve sürdürülebilir kalkınma bağlamında tartıştık.

Konferansın planlanma aşamasından sonuçlandırılmasına kadarki bütün süreçlerinde, her türlü desteği ve katkıyı esirgemeyen başta Hasan Kalyoncu Üniversitesi Mütevelli heyet başkanımız Sayın Haluk Kalyoncu'ya, Rektörümüz Sayın Profesör Doktor Türkay Dereli'ye ve geçen yılki düzenleme kurulu başkanımız Prof. Dr. Mazlum Çelik'e teşekkürlerimi sunuyorum. Kitabın hazırlanmasında emeklerini esirgemeyen Doç. Dr. Zeynep Köse, Dr. Öğr. Üyesi Bilal Çayır ve Arş. Gör. Muhammed Talha Şen ile Üniversitenin her kademesindeki çalışanlarına konferansın gerçekleştirilmesi için gösterdikleri gayret ve çabaları için teşekkür ediyorum.

Hasan Kalyoncu Üniversitesi tarafından hibrid olarak düzenlenen 5. Uluslararası İslami Finans ve Ekonomi Konferansı'na (22-23 Ekim 2025) bildiri sunumlarıyla veya dinleyici sıfatıyla destek veren tüm katılımcılara, konferans düzenleme kurulu adına teşekkür ederim. 2016'da başladığımız konferansımıza bu yıl 5 farklı ülkeden 90'a yakın değerli bilim insanı katkı sağlamıştır. Durham Üniversitesi, Sakarya Üniversitesi, Uludağ Üniversitesi, Endonezya Uluslararası İslam Üniversitesi ve Ankara Sosyal Bilimler Üniversitesi'ne paydaş olarak konferansımıza katkılarından dolayı teşekkür ediyorum. Durham Üniversitesi öğretim üyesi Prof. Dr. Mehmet Asutay hocama konferansın başından sonuna kadar planlarken her bir detayında verdiği destek ve emek için çok teşekkür etmek istiyorum. Son olarak, konferansımıza davetimizi kabul ederek gelen ve çok değerli katkı sağlayan Prof. Dr. Murat Çizakça, Dr. Umar A. Oseni, Dr. Farrukh Raza, Dr. Seyfullah Demirlek, Adnan Ünverdi, Dr. Kamran Sherwani ve Dr. Moutaz Abajeib'e katılımları ve destekleri için teşekkür ediyorum.

Etkinliklerimize sponsor olarak destek sağlayan Albaraka Türk, İstanbul Finans Merkezi, Ziraat Katılım ve resmi havayolu olan Türk Hava Yolları'na özel olarak teşekkürlerimi sunuyorum.

ICIFE'24 Düzenleme Kurulu Başkanı

Doç. Dr. Yıldız ÖZKÖK


5th INTERNATIONAL CONFERENCE ON ISLAMIC FINANCE AND ECONOMICS
22-23 October 2024 | 09:00-19:00
Hasan Kalyoncu University
Congress and Culture Center
Keynote Speakers Panel
Moderator: Prof Dr. Ahmet KESER
Hasan Kalyoncu University, Political Science and International Relations
Prof. Dr. Murat Çizakça
İslam İktisadı ve Finans, KTO Karatay Üniversitesi
Prof. Dr. Mehmet ASUTAY
Director, Durham Centre for Islamic Economics and Finance, Durham University, UK
Dr Umar A. Oseni
Secretary-General, OIC (Organization of Islamic Cooperation) Arbitration Centre;
Dr. Farrukh Raza
Group CEO, IFAAS; Chairman, Governance and Ethics Board, AAOIFI
Moderator: Assoc. Prof. Dr. Yıldız ÖZKÖK
Hasan Kalyoncu University, Economics
Dr. Seyfullah Demirlek
Investor Relations and Sustainability Manager, Albaraka Türk
Adnan Ünverdi
Chairman of the Board, Gaziantep Chamber of Industry
Kamran Sherwani
Head of Internal Shariah Control and the Secretary to the Internal Shariah Supervision Committee, SDG Academy
Dr. Moutaz Abajeib
Leading position in Islamic fintech projects at ISRA Research Centre, INCEIF, AAOIFI Fintech Working Group.
For detailed information: https://icife2024.hku.edu.tr
Gold Sponsor
alBaraka
Silver Sponsor
ISTANBUL FINANCIAL CENTER
Resmi Havayolu Official Airlines
TURKISH AIRLINES
Strategic Partners
HASAN KALYONCU ÜNİVERSİTESİ


WORKSHOP ON ISLAMIC FINANCE
"International Training Programme"
21 October 2024, 09:00-18:00 | Ziraat Towers, Istanbul Financial Center
For registration link: https://icife2024.hku.edu.tr/workshop/
Participants will be given a "Certificate of Participation"
Guest of Honor
Prof. Dr. Mehmet Asutay
Director, Durham Centre for Islamic Economics and Finance, Durham University
Guest of Honor
Workshop 1
Liquidity Management in Islamic Financial Institutions
Dr Umar A. Oseni
Secretary-General, OIC (Organization of Islamic Cooperation) Arbitration Centre;
Workshop 2
Product Development; Sukuk Structuring and Pricing
Dr. Kamran Sherwani
Head of Internal Shariah Control and the Secretary to the Internal Shariah Supervision Committee,SGD Academy
Workshop 3
Corporate & Shariah Governance in Islamic Financial Institutions
Dr. Farrukh Raza
Group CEO, IFAAS; Chairman, Governance and Ethics Board, AAOIFI
Workshop 4
Islamic FinTech and Cryptocurrency
Dr. Moutaz Abajeib
Leading position in Islamic fintech projects at ISRA Research Centre, INCEIF, AAOIFI Fintech Working Group.
For detailed information: https://icife2024.hku.edu.tr
Main Sponsor
Ziraat Katılım
Silver Sponsor
ISTANBUL FINANCIAL CENTER
Resmi Havayolu Official Airlines
TURKISH AIRLINES
ÇAĞRI MERKEZİ 0342 211 80 80
HASAN KALYONCU ÜNİVERSİTESİ

İÇİNDEKİLER / CONTENTS

KONFERANS KURULLARI (CONFERENCE COMMITTEES) **6**
ONUR KURULU (HONARY COMMITTEE) **6**
DÜZENLEME KURULU (ORGANIZATION COMMITTEE) **6**
BİLİM KURULU (SCIENTIFIC COMMITTEE) **6**
BİLDİRİLER **9**
KATILIM SİGORTACILIĞININ EKONOMİK ETKİLERİ: TÜRKİYE ÖRNEĞİ 10
DİJİTAL ÇAĞ'DA İSLAMİ FİNANS 20
TÜRKİYE'DEKİ GELENEKSEL VE KATILIM BANKACILIĞININ ÇALIŞMA YÖNTEMLERİ ARASINDAKİ FARKLAR 26
COMPARATIVE DEVELOPMENT ANALYSIS OF ISLAMIC BANKING SYSTEMS: INSIGHTS FROM THAILAND AND SOUTHEAST ASIA 31
SÜRDÜRÜLEBİLİR KALKINMA İÇİN İSLAM EKONOMİSİ 43
İSLAMİ FİNANS VE BLOKZİNCİR: ETKİSİ VE GELECEĞİ 51
THE FUTURE OF INTERNATIONAL ENVIRONMENTAL LAW: A REVIEW 58
DİJİTALLEŞMENİN İSLAM EKONOMİSİNE ETKİSİ: ANALİTİK ÇIKARIMLAR VE GELECEK PERSPEKTİFLERİ 65
İSLAMİ FİNANS OKURYAZARLIK DÜZEYLERİN BELİRLENMESİ VE İNCELENMESİ: HASAN KALYONCU ÜNİVERSİTESİ ÜZERİNE BİR ALAN ARAŞTIRMASI 72
KATILIM ENDEKSLERİ ve ARINDIRMA İŞLEMİNİN FAİZ HASSASİYETİNE SAHİP YATIRIMCILAR NEZDİNDE BİLİNİRLİĞİ 83
KATILIM BANKALARININ FİNANSAL PERFORMANSLARININ CRITIC-ROV YÖNTEMİ İLE DEĞERLENDİRİLMESİ 90
İSLAMİ FİNANS YAKLAŞIMIYLA KATILIM BANKALARININ FON KULLANDIRMA YÖNTEMLERİ 100
İSLAM EKONOMİSİ VE FİNANSAL SİSTEMİN YÖNETİMİNE TEORİK YAKLAŞIMLAR 105
FİNTECH VE İSLAMİ FİNANS KURUMLARINDA KULLANILAN GÜNCEL FİNTECH UYGULAMALARI 120
KATILIM BANKALARININ ENTROPİ TEMELLİ COCOSO YÖNTEMİ İLE FİNANSAL PERFORMANSLARININ SIRALANMASI 127
CYBERSECURITY RISKS FOR ISLAMIC FINANCE – A HONG KONG REGULATORY ANALYSIS 147

DİYANET PERSONELİNİN İSLAMİ FİNANS ALGISI (SAKARYA ÖRNEĞİ) ... 160
KATILIM 50'DE YER ALAN ŞİRKETLERİN KATILIM ENDEKSİNE BAKIŞ AÇILARI 170

KONFERANS KURULLARI (CONFERENCE COMMITTEES)

ONUR KURULU (HONARY COMMITTEE)

Prof. Dr. Türkay DERELİ
Hasan Kalyoncu Üniversitesi Rektörü

DÜZENLEME KURULU (ORGANIZATION COMMITTEE)

Düzenleme Kurulu Başkanı (Honorary Board)
Doç. Dr. Yıldız ÖZKÖK, Hasan Kalyoncu Üniversitesi

Düzenleme Kurulu Üyeler (Organizing Committee)
Prof. Dr. Mazlum ÇELİK, Hasan Kalyoncu Üniversitesi
Prof. Dr. Filiz GÖLPEK, Hasan Kalyoncu Üniversitesi
Prof. Dr. İbrahim Halil EKŞİ, Gaziantep Üniversitesi
Prof. Dr. Metin TOPRAK, İstanbul Sabahattin Zaim Üniversitesi
Prof. Dr. Osman OKKA, Karatay Üniversitesi
Prof. Dr. Tuba BÜYÜKBEŞE, Hasan Kalyoncu Üniversitesi
Doç. Dr. Eda DİNERİ, Hasan Kalyoncu Üniversitesi
Doç. Dr. Erhan AKKAŞ, Sakarya Üniversitesi
Doç. Dr. Fatma Gül BİLGİNER ÖZSAATCI, Hasan Kalyoncu Üniversitesi
Doç. Dr. Zeynep KÖSE, Hasan Kalyoncu Üniversitesi
Doç. Dr. Zeynep ÖZGÜNER, Hasan Kalyoncu Üniversitesi

Düzenleme Kurulu Sekretaryası (Organizing Sekretary)
Arş. Gör. Bilal ÇAYIR, Hasan Kalyoncu Üniversitesi
Arş. Gör. M. Talha ŞEN, Hasan Kalyoncu Üniversitesi
Arş. Gör. C. Gökçe ÖZMEN, Hasan Kalyoncu Üniversitesi
Arş. Gör. Sinem KÜÇÜKYILMAZ, Hasan Kalyoncu Üniversitesi

BİLİM KURULU (SCIENTIFIC COMMITTEE)

Prof. Dr. Mehmet ASUTAY / Durham University
Prof. Dr. M. Hanifi ASLAN / Hasan Kalyoncu University
Prof. Dr. Almir ALIHODZIC / Zenica University
Prof. Dr. Ahmet F. AYSAN / Hamad Bİn Khalİfa University
Prof. Dr. İsmail BEKÇİ / Süleyman Demİrel University
Prof. Dr. Abdulkadir BİLEN / Dİcle University
Prof. Dr. Tuba BÜYÜKBEŞE / Hasan Kalyoncu University
Prof. Dr. Filiz GÖLPEK / Hasan Kalyoncu University
Prof. Dr. Ahmet Vecdi CAN / Sakarya University
Prof. Dr. İlhan EGE / Mersİn University
Prof. Dr. Yücel EĞRİÇAY / Sütçü İmam University

Prof. Dr. Halil İbrahim EKŞİ / Gazİantep University
Prof. Dr. Seyfettin ERDOĞAN / Medenİyet University
Prof. Dr. Hakan ERKUŞ / İnönü University
Prof. Dr. Mehmet ERSOY / Artvin Çoruh University
Prof. Dr. H Mohammad HUDAİB / University of Glasgow
Prof. Dr. Yoshiaki JINNAI / Keizai University
Prof. Dr. Reşat KARCIOĞLU / Atatürk University
Prof. Dr. Saim KAYADİBİ / Karabük University
Prof. Turalay KENC / International Centre For Education In Islamic Finance
Prof. Dr. Mustafa KISAKÜREK / Kahramanmaraş Sütçü İmam University
Prof. Dr. Osman OKKA / Konya Karatay University
Prof. Dr. Yıldırım Beyazıt ÖNAL / Çukurova University
Prof. Dr. Mehmet Akif ÖNCÜ / Düzce University
Prof. Dr. Turan ÖNDEŞ / Atatürk University
Prof. Dr. Mehmet ÖZBİRECİKLİ / Mustafa Kemal University
Prof. Dr. Salih ÖZTÜRK / Namik Kemal University
Prof. Dr. Raif PARLAKKAYA / Necmettin Erbakan University
Prof. Dr. Şakir SAKARYA / Balikesir University
Prof. Dr. Mehmet Kutluğhan SAVAŞ ÖKTE / İstanbul University
Prof. Dr. Fatih SAVAŞAN / Sakarya University
Prof. Dr. Necdet ŞENSOY / İstanbul Ticaret University
Prof. Dr. Murat ŞİMŞEK / Karabük University
Prof. Dr. Ahmet TABAKOĞLU / Sabahattin Zaim University
Prof. Dr. Cengiz TORAMAN / İnönü University
Prof. Dr. Kemal Burç ÜLENGİN / İstanbul TekniK University
Prof. Dr. Mahmut YARDIMCIOĞLU / Kahraman Maraş Sütçü İmam University
Prof. Dr. İbrahim Güran YUMUŞAK / SabahattİN Zaim University
Doç. Dr. Haşim BAĞCI / Aksaray University
Doç. Dr. M. Fatih BUGAN / Gaziantep University
Doç. Dr. Figen BÜYÜKAKIN / Kocaeli University
Doç. Dr. Cuma ERCAN / Gaziantep University
Doç. Dr. Ayfer GEDİKLİ / Medeniyet University
Assoc. Prof. Bojan GEORGIEVSKI / Wittenborg University of Applied Sciences
Doç. Dr. Gülsün İŞSEVEROĞLU / Uludağ University
Doç. Dr. Ali KABLAN / Trakya University
Doç. Dr. Yunus KILIÇ / Akdeniz University
Doç. Dr. Metin KILIÇ / Bandırma University
Doç. Dr. Emrah KOÇAK / Erciyes University
Doç. Dr. Ahmet ÖZ / Kahramanmaraş Sütçü İmam University
Doç. Dr. Fatma ŞENSOY / İstanbul Sağlik ve Teknoloji University
Doç. Dr. Yıldız ÖZKÖK / Hasan Kalyoncu University
Assoc. Prof. Mosab TABASH / Al Ain University
Doç. Dr. Osman ULUYOL / ADIYAMAN University

Dr. Öğr. Üyesi Hakan ASLAN / Sakarya University
Asst. Prof. MUHAMMAD ALI / Ucsi University Graduate Business School
Asst. Prof. Ahmed BOUTESKA / Tunis El Manar University
Dr. Öğr. Üyesi İbrahim ÇEMBERLİTAŞ / Van Yüzüncü Yıl University
Dr. Abdurrahman ÇETİN / BDDK
Dr. Öğr. Üyesi Suna Akten ÇÜRÜK / Necmettin Erbakan UniversitySİ
Dr. Öğr. Üyesi Yavuz DEMİRDÖĞEN / Süleyman Demirel UniversitySİ
Dr. Öğr. Üyesi İsmail DURAK / Düzce University
Dr. Öğr. Üyesi Fatih GÜÇLÜ / Karabük University
Dr. Arif GÜMÜŞ / Turgut Özal University
Asst. Prof. Samed GÜNAY / American University of The Middle East
Dr. Hasan KAZAK / Necmettin Erbakan University
Dr. Öğr. Üyesi Tolga ORAL / İnönü University
Dr. Mücahit ÖZDEMİR / Sakarya University
Dr. Öğr. Üyesi Pınar PEHLİVAN / Celal Bayar University
Dr. Öğr. Üyesi Ömer Nasuhi ŞAHİN / Dumlupınar University
Dr. Öğr. Üyesi Yavuz TÜRKAN / Bingöl UniversitySİ
Dr. Öğr. Üyesi Salih ÜLEV / Sakarya University
Asst. Prof. M. Hersi WARSAME / University of Sharjah
Dr. Ayhan YATBAZ

BİLDİRİLER

PROCEEDINGS

CYBERSECURITY RISKS FOR ISLAMIC FINANCE – A HONG KONG REGULATORY ANALYSIS

Klemens KATTERBAUER
Prof., Department of Earth Science and Global Management, Euclid University
ORCID: 0000-0001-5513-4418

Rahmi Deniz ÖZBAY
Prof., Istanbul Ticaret University, Faculty of Business, Department of Economics
rdozbay@ticaret.edu.tr
ORCID: 0000-0002-3927-8216

Hassan SYED
Dr., BPP University, Islamic Finance Law
h.syed2@my.bpp.com
ORCID: 0000-0003-2114-2473

Sema YILMAZ
Prof., Yildiz Technical University, Faculty of Economics and Administrative Sciences, Department of Economics
sygenc@yildiz.edu.tr
ORCID: 0000-0002-3138-1622

Abstract

The finance sector will be one of the most vulnerable to cybersecurity threats. Along with healthcare and professional services, the financial sector has significant cybersecurity challenges, with emails containing ransomware and other malware among the most common threat incident types. Concerns about cyber risks have grown significantly due to the COVID-19 outbreak and the acceleration in service digitization. Cyberattacks within economies have become more common. The Bank for International Settlements (BIS) defines cyber risk as the risk of financial loss, interruption, or reputational damage to a corporation caused by an IT system failure. One of the goals of Shariah, according to Islam, is to protect and defend the property of individuals and organizations from any detrimental acts. Such properties include digital resources, ethereal riches, and actual and financial wealth. These assets are used in the financial industry. They are vulnerable to a wide range of risks that could compromise financial institutions' information systems, resulting in fraud, theft, scams, and the improper or unlawful use of personal and public information. As a result, preventing such attacks is consistent with Shariah's objectives and is linked to maintaining cyberspace security and implementing measures to strengthen Islamic financial institutions' cyber resilience. Due to their size and location, Islamic banks confront unique problems in guaranteeing cybersecurity and resilience. For Islamic banks intending to list in Hong Kong and maybe be dual-listed on the stock link, ensuring cybersecurity and following Islamic values are vital.

Keywords: Islamic finance, cybersecurity regulations, Hong Kong

Jel Codes: G1, G15

İSLAMİ FİNANS İÇİN SİBER GÜVENLİK RİSKLERİ - HONG KONG MEVZUAT ANALİZİ

Özet

Finans sektörü siber güvenlik tehditlerine karşı en savunmasız sektörlerden biri olacaktır. Sağlık hizmetleri ve profesyonel hizmetlerle birlikte finans sektörü, fidye yazılımı ve diğer kötü amaçlı yazılımları içeren e-postaların en

yaygın tehdit olayı türleri arasında yer aldığı önemli siber güvenlik zorluklarına sahiptir. COVID-19 salgını ve hizmet dijitalleşmesindeki mevcut hızlanma nedeniyle siber risklerle ilgili endişeler önemli ölçüde artmıştır. Ekonomiler içinde siber saldırılar daha yaygın hale gelmiştir. Uluslararası Ödemeler Bankası (BIS) siber riski, bir BT sistemi arızasının neden olduğu finansal kayıp, kesinti veya bir kurumun itibarına zarar verme riski olarak tanımlamaktadır. İslam'a göre Şeriat'ın amaçlarından biri, bireylerin ve kuruluşların mülklerini her türlü zararlı eylemden korumak ve savunmaktır. Bu tür mülkler dijital kaynakları, manevi zenginlikleri ve gerçek ve finansal serveti içerir. Bu varlıklar finans sektöründe kullanılmaktadır. Finansal kurumların bilgi sistemlerini tehlikeye atabilecek, dolandırıcılık, hırsızlık, dolandırıcılık ve kişisel ve kamusal bilgilerin uygunsuz veya yasadışı kullanımıyla sonuçlanabilecek çok çeşitli risklere karşı savunmasızdırlar. Sonuç olarak, bu tür saldırıların önlenmesi Şeriat'ın hedefleriyle tutarlıdır ve siber alan güvenliğinin sürdürülmesi ve İslami finans kuruluşlarının siber dayanıklılığını güçlendirecek tedbirlerin uygulanmasıyla bağlantılıdır. Büyüklükleri ve konumları nedeniyle İslami bankalar siber güvenlik ve dayanıklılığı garanti altına alma konusunda benzersiz sorunlarla karşı karşıyadır. Hong Kong'da listelenmeyi ve belki de borsada çift kote olmayı amaçlayan İslami bankalar için siber güvenliğin sağlanması hayati önem taşımakta ve İslami değerleri takip etmektedir.

Anahtar Kelimeler: İslami finans, siber güvenlik düzenlemeleri, Hong Kong

Jel Kodları: G1, G15

Introduction

The finance sector will be at the forefront of cybersecurity challenges and be amongst the most attacked industry sectors. Along with healthcare and professional services, financial sectors exhibit significant cybersecurity challenges, with emails spreading ransomware and other malware among the most common threat incident types. Concern over cyber dangers has grown globally due to the COVID-19 epidemic and the recent acceleration of service digitization. Cyberattacks within economies have become increasingly common. Cyber risk is the risk of financial loss, disruption, or reputational damage to an organization resulting from the failure of its IT systems, based on the definition of the Bank for International Settlements. Cyber risks can occur in an organization for intentional or unintentional reasons, such as employees erasing data by accident or because hackers target computer systems and networks to cause harm or loss for monetary gain or political reasons. This implies "hacktivism," cyber warfare, terrorism, or just plain curiosity (Uddin, Ali, & Hassan, 2020).

These acts may have been committed by insiders, members of the organization's staff, or by outside parties like amateurs, hacktivists, or criminal organizations. Cybercriminals employ various techniques to carry out their attacks, such as phishing and malware. Over time, these techniques have become more sophisticated as new hazards have been created by technological advancements like machine learning and artificial intelligence (AI). Cyber hazards can significantly affect organizations, and in the worst situations, they can cause systemic economic disruptions. As a result, cybersecurity is currently a top concern for decision-makers and a significant issue on international agendas worldwide.

Financial institutions are generally vulnerable to cyberattacks due to the challenges arising from money transfers. This requires these financial institutions to recognize the risks they face and take proactive steps to create more robust and secure systems. Based on publicly accessible statistics, the banking sector has been the most targeted by cyberattacks during the past five years. Additionally, a quarter of all cyber events impact the financial industry. The financial sector is generally prone to cyberattacks due to several circumstances, including the availability of data and funds and the significant engagement of third-party service providers.

In addition, the usage of antiquated technology by specific organizations and the lack of knowledge and cybersecurity training, as prevalent in other industries, raise cyber threats further. This is especially prevalent given the awareness challenges of professionals and the prevalence of people falling for social and other related cybersecurity scams (Gutiérrez Ponce, Chamizo González, & Al-Mohareb, 2023).

The banking industry has been facing cyber dangers due to two significant trends. There is growing flexibility in terms of work location arrangements and increasing digitalization. The COVID-19 epidemic has fueled these concerns and advances in digitalization. Additionally, using private networks and personal devices due to work-from-home rules has increased organizations' vulnerabilities. Except for the health sector, the BIS states that the financial sector was most affected by the COVID-19 cyber events. Because open banking allows permitted third-party providers to access bank systems, there is also a growing worry regarding cybersecurity. In this instance, banks may be in danger from cyberattacks directed toward third-party providers or employee dishonesty at these companies (Pendley, 2018).

Specific approaches to cyber events are employed in the financial sector more frequently than in others. For instance, ransomware is being utilized increasingly in the banking sector for cyberattacks, phishing, and denial-of-service attacks. Cybercriminals are continually updating and improving the complexity of their techniques to adapt to market shifts. Modern technologies like artificial intelligence (AI) and machine learning are utilized to recognize patterns in human behavior and identify weaknesses as soon as they appear. Large and small financial institutions face the same threats, but because their cybersecurity defences are less sophisticated, smaller financial institutions are thought to be more susceptible to cyberattacks (Ng & Kwok, 2017).

Additionally, even though North America accounts for the majority of recorded cyber incidents, lower middle-income nations are reporting an increase in cyberattacks due to the growing trend of digitalization for financial inclusion, such as through mobile banking. Less funding for cybersecurity advancement, a lack of cybersecurity expertise in these nations, and more stringent cybersecurity policies by developed economies have all contributed to the surge in attacks by making these nations more appealing and reachable targets. A Pegasus Technologies attack in October 2020 caused disruptions to MTN Uganda and Airtel, two Ugandan telecom firms that offered mobile money transfers. The intrusion prevented mobile money transfers in Uganda and resulted in at least USD 3.2 million stolen. Cyberattacks have also escalated in the Gulf Cooperation Council due to the region's growing digitalization, creating more vulnerabilities (Smith, 2020).

Cyber events may have significant repercussions, harming the institution's brand and client confidence. They may also result in significant losses for financial institutions, impacting the organization's capitalization and liquidity. These outcomes will have a greater impact on small banks' financial standing. Furthermore, because of the sector's interdependence, a single attack may have simultaneous effects on multiple institutions, resulting in systemic harm and jeopardizing financial stability both locally and internationally. The importance of a relatively limited number of institutions, including major exchanges, is such that even a minor outage during extreme market volatility would have systemic implications. Financial institutions are being encouraged to assess their IT systems and make sure they are prepared for cyberattacks based on several policy, legislation, and cyber law developments brought forth by the rapid digital transition, technological advancements, and, most recently, the pandemic. Regulators and legislators are key players in guaranteeing the security of cyberspace by improving security readiness and safeguarding consumers through the establishment of mandated security requirements and good practice standards. On the regulatory side, there have been major initiatives across the world (Cheng, Li, Luo, & Zhu, 2024).

In 2016, the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) created the first globally recognized guidelines for cyber resilience for financial market infrastructures (FMIs). This was followed in 2018 when the BIS published a report outlining and contrasting several cyber resilience measures that banks and regulatory and supervisory bodies throughout the world had used. To reduce associated risks to financial stability, the Financial Stability Board (FSB) released a toolkit in 2020 that outlines best practices that financial institutions may use to respond to and

recover from cyber disasters. Locally and regionally, the European Central Bank (ECB) has advised banks to regularly evaluate the capability of their current IT infrastructure in light of the observed rise in cyberattacks. This advice was included in a recent guideline document released in 2020. Additionally, in 2020, the Monetary Authority of Singapore (MAS) asked financial institutions to deal with any potential spike in demand for online financial services by taking a proactive stance. To improve their cybersecurity, banks are being urged by the Dubai Financial Services Authority (DFSA) to register on the DFSA Cyber Threat Intelligence Platform (TIP) and take advantage of the cyber threat data that is accessible there. The article discusses cybersecurity and the associated regulatory challenges of Islamic financial institutions operating in Hong Kong and mainland China, as well as being listed on the Hong Kong Stock Exchange (Florackis, Louca, Michaely, & Weber, 2023).

1. Financial cybersecurity requirements in Hong Kong

The Securities and Futures Ordinance and the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (the "Code of Conduct") make no specific mention of cybersecurity events or data breach reporting requirements. Rather, the Code of Conduct requires SFC-licensed corporations ("LCs") to notify the SFC immediately of any material breach, infringement, or non-compliance with the requirements of any regulatory authority, as well as any material failure or error and defect that may occur during the trading, accounting, clearing, or settlement systems or equipment, and to comply with a variety of additional requirements when conducting electronic trading. The SFC published a circular in 2017 advising LCs to notify the SFC immediately of any material cybersecurity event, including ransomware attacks. According to the SFC, 12 LCs reported 27 cybersecurity incidents in the 18 months ending March 31, 2017, with the majority involving hackers gaining access to customers' internet-based trading accounts with securities brokers, resulting in unauthorized trades totalling more than HK$110 million, and some others involving distributed denial-of-service ("DDoS") attacks targeting their websites accompanied by extortion threats (Ng & Kwok, 2017).

However, neither these Code of Conduct responsibilities nor later SFC circulars provide additional information on what the SFC regards to be a serious cybersecurity event. For example, there is the question of whether all DDoS or ransomware assaults should be reported. Instead, the emphasis is on materiality and how it affects the "operation or functioning" of certain systems. LCs must consequently make a judgment call on whether a cybersecurity event is material and so notifiable to the SFC. An attack that results in a prolonged outage of a financial institution's trading system or client internet trading accounts is likely to be regarded as significant. Similarly, a ransomware assault that encrypts all of an asset manager's systems, blocking the collecting of client instructions or the transmission of trading orders, is likely to be substantial and reportable to the SFC.

The SFC has not released any particular guidelines or regulations regarding client data leaks. Under the existing standards, an email hack that extracts personal data but permits the continuation of routine operations might not be deemed relevant to the SFC. The SFC recommends "minimum standards" expected of the LC in cases where it engages in internet trading (i.e., order instructions are sent through "an internet-based trading facility"). These standards include establishing written policies and procedures outlining how a suspected or actual cybersecurity incident should be reported both internally (to the responsible officers in charge of internet trading, for example) and externally. Hence, rather than defining the circumstances in which the LC must report to the SFC, the SFC mandates that the LC establish the policies and procedures it must adhere to. Similarly, the Banking Ordinance does not mention cybersecurity or cyber events, even though the HKMA is quite worried about cybersecurity in banking services (Carter & Crumpler, 2022).

In its Supervisory Policy Manual for Technology Risk Management and its circular on Incident Response Management Procedures, the HKMA emphasizes that an authorized institution authorized by the HKMA under the Banking Ordinance ("AI") must "notify the HKMA immediately and provide [the HKMA] with whatever information is available at the time" upon becoming aware of a significant incident, IT-related fraud, or a major security breach. The HKMA is very explicit that AIs must report incidents to the HKMA as soon as they occur, regardless of whether they have fixed the issue. This is more explicit than the SFC's obligations.

A specific duty to proactively notify the customers affected or likely to be affected and advise them of the steps or precautionary measures that they need to take, as well as whether the bank would reimburse any losses, is also provided by the HKMA's Incident Response and Management Procedures circular. In the case of a "cyber threat," AIs should also strive to provide warning messages to all relevant consumers as soon as practical. AIs must also consider going public when the circumstances call for it, such as when a significant incident has occurred or when a significant number of consumers have been impacted (Cheng, Li, Luo, & Zhu, 2024).

The HKMA emphasizes that these are merely general guidelines and that other considerations might be necessary for AIs. The HKMA has not released lists of occurrences that it believes need to be reported to it and those that don't. An AI must promptly notify the HKMA upon becoming aware of a severe event. Therefore, AIs are responsible for weighing the impact and severity of cyber incidents and how they may affect customers and AI operations when determining whether to notify customers or the HKMA. AIs should also issue a second statement to the public if an incident affects a larger portion of the population. The HKMA has gone above and beyond the SFC in offering detailed instructions on consumer data protection and when reporting data privacy incidents. The HKMA's circular on Customer Data Protection outlines the protocols that AIs must follow to handle, respond to, and report an incident involving stealing, losing, or leaking customer data (Lee, 2022).

First, appropriate incident handling and reporting protocols must be in place (before the occurrence of an incident). Second, it is necessary to appoint a suitably senior officer or a designated management committee chaired by senior management to oversee the handling and reporting of privacy violations. Third, it requires reporting the occurrence to the HKMA and "relevant regulatory authorities," including the PCPD, "where appropriate." Finally, it demands that affected customers be notified "as appropriate" or explain why they were not notified. AIs should also follow any applicable codes of practice issued or approved by the Privacy Commissioner for Personal Data (the "PCPD"), which provide practical guidance on complying with the Personal Data (Privacy) Ordinance (the "PDPO"). The HKMA makes it clear that a data privacy incident is significant. For example, if the incident is likely to have a significant impact on the AI's reputation, the number of customers affected is large, or the stolen customer data is sensitive, the affected AI is expected to report the incident to the HKMA and the PCPD, as well as notify affected customers as soon as possible after becoming aware of or being notified of it. The HKMA's Customer Data Protection circular retains some discretion for AIs but provides clearer advice on when AIs are expected to notify a customer data breach. The PCPD has produced the industry-specific advice notes listed below (Arner, Gibson, & Barberis, 2020).

The first is the guidance on the Proper Handling of Customers' Personal Data for the Banking Industry, which helps banks and other financial institutions (including LCs) understand and comply with the PDPO's relevant requirements while also promoting good practices in the collection, accuracy, retention, use, security, and access to customers' data. Furthermore, there are Tips for Using Fintech, which include recommended (but not required) good practices for FinTech providers and operators, such as developing protocols for dealing with data breach situations (Huang, Cheung, & Wang, 2020).

The HKMA's guideline, therefore, goes beyond both the PCPD and the SFC in demanding cyber incident reporting to regulators and affected data subjects. For SFC-licensed companies,

there is greater discretion in determining if the incident requires a notification to the SFC provided there is sufficient justification, and there is no mandatory obligation to disclose to the PCPD or impacted data subjects. However, if an LC fails to notify a data breach, the SFC would most likely question why when assessing the necessary reaction to the occurrence.

When dealing with and responding to any cybersecurity event, time is of the essence. A rapid, pre-planned response can be important in minimizing the consequences of the occurrence. As financial services and data privacy regulators tighten regulations and impose more stringent cyber incident reporting requirements, financial services companies would benefit from implementing a comprehensive cyber-risk prevention and control system to ensure effective and timely responses to such incidents. This should include the designation of accountable personnel for reporting cybersecurity issues to regulatory organizations (Huang & Li, 2018).

The regulatory reporting duties in Hong Kong remain ambiguous regarding when a cyber incident is material enough to necessitate notification to financial services regulators, despite the HKMA's guidelines becoming clearer. We have not seen any enforcement proceedings taken by the SFC, HKMA, or PCPD for failing to notify or late reporting a material cybersecurity issue. Under Hong Kong's personal data protection law, there is still no legislative duty to notify the PCPD of a data breach. When deciding whether a cybersecurity event should be reported to regulators, customers, or the public, LCs, and AIs should assess the possible impact on the company and its reputation, the gravity of the occurrence, and the extent of the damage to customers. If they are unsure, they should get legal guidance right away. If there is any doubt about whether an incident should be reported, LCs and AIs may wish to file a voluntary report with the SFC / HKMA 'out of an abundance of caution' to demonstrate to regulators that the company is taking a responsible approach to being the victim of an illegal attack. Finally, this article focuses solely on the duties of reporting under Hong Kong law and regulations. Laws and regulations governing data privacy and cybersecurity are growing throughout Asia. In addition to the rising extraterritorial reach of data privacy legislation, the worldwide nature of financial services implies that corporations may be required to report in multiple jurisdictions (Tsuchiya, 2016).

In contrast to Hong Kong, financial institutions subject to Singapore reporting duties must notify a personal data breach to Singapore's Personal Data under Hong Kong's data protection law. Protection Commission within three calendar days, or report a system breakdown or IT security event to the Monetary Authority of Singapore within one hour. Therefore, LCs and AIs operating in Asia should evaluate the legal and regulatory reporting duties in all relevant jurisdictions. This may include locations with clients but no operations (Didenko, 2020).

2. New changes in Hong Kong cybersecurity regulations

On June 25, 2024, a new cybersecurity law was suggested to protect Hong Kong's critical infrastructure (CI) computer systems. The proposed new law is tentatively titled the "Protection of Critical Infrastructure (Computer System) Bill" (Proposed Legislation), and the proposed legislative framework was laid out in a paper (Paper) submitted by the Hong Kong Government to the Legislative Council (LegCo) for consideration on July 2, 2024. The government intends to present the draft bill to LegCo before the end of 2024. Once adopted, the proposed legislation will most likely be implemented in stages, with complete adoption expected by 2026. The Proposed Legislation aims to increase the security of CIs' computer systems and reduce the likelihood of important services being disrupted or compromised due to cyberattacks. The developments in Hong Kong are part of a global trend of increased cybersecurity legislation, bringing Hong Kong in line with other key jurisdictions with similar cybersecurity laws regulating CI operators, such as Mainland China, Macao, Australia, Singapore, Malaysia, and Thailand in the Asia-Pacific region, as well as globally in the UK, EU, US, and Canada. The proposed legislation is an

important step toward aligning Hong Kong with other countries to improve the protection of CIs and overall computer system security in Hong Kong. Businesses should actively follow developments related to the Proposed Legislation and examine existing cybersecurity safeguards.

The proposed legislation applies exclusively to identified critical infrastructure operators (CIOs) and critical computer systems (CCSs). The list of CIOs will not be made publicly available. CCSs based outside of Hong Kong may also be regulated. CIOs will be subject to three sorts of statutory requirements. These are organizational, preventive, and incident responses for any cybersecurity incident. CIOs must disclose significant computer system security issues within two hours and other security incidents within 24 hours. A new Commissioner's Office will be established under the Security Bureau. Specific sector regulators (such as the Hong Kong Monetary Authority (HKMA)) would be designated as authorities to oversee compliance with the respective CIOs' organizational and preventive duties. The Commissioner's Office will have broad investigative powers, including compel a CIO to produce information (even if it is situated outside of Hong Kong) or access their premises. The proposed legislation will create offences and fines for non-compliance may be levied on CIOs but not individuals. The proposed framework will only regulate officially appointed CIOs and CCSs.

A new Commissioner's Office will designate CIOs and CCSs, and the CIO list will not be made public. This approach is consistent with that of other jurisdictions, like China and Singapore. CIOs: An organization will be designated as a CIO if it operates an infrastructure that the Commissioner's Office considers a CI, considering the organization's level of control over the infrastructure. The proposed legislation is intended to target huge corporations rather than small and medium-sized businesses. The proposed legislation will only compel CIOs to be responsible for safeguarding their CCSs; it will not affect the personal data or commercial information stored in those systems. CIs: The government recommended two key categories: Infrastructures for providing essential services in Hong Kong in eight selected sectors, namely, energy, information technology, banking and financial services, land transport, air transport, maritime, healthcare services, and communications and broadcasting. Furthermore, other infrastructures for the maintenance of key societal and economic activities include, among other things, large sports and performance venues, research and development parks, and so on. CCSs: Computer systems will be designated as CCSs if they are relevant to the provision of critical services or computer system core functions, and if they are disrupted or damaged, they will significantly impact the normal operation of the CI. This means that the Proposed Legislation will not apply to other computer systems that have not been recognized as CCS.

CCSs outside of Hong Kong may also be subject to regulation under the Proposed Legislation, as is the case with Singapore cybersecurity regulations. The Commissioner's Office will consult with the organization that will be identified as a CIO, and any designated CIO will have the ability to object to the designation and appeal to an independent board. An organization-based approach will be taken, which means that the organization in charge of operating a CI must fulfil its commitment to protecting the security of its computer systems. An organization that has been designated as a CIO must meet three types of obligations. This includes the organizational obligations of maintaining a Hong Kong address and office, reporting changes in ownership and operatorship of CIs, and establishing a computer system security management unit with professional knowledge, which may be outsourced and supervised by the CIO.

Another crucial part is the preventive obligations. This includes informing the Commissioner's Office of material changes to their CCSs. For example, this includes design, configuration, security, and operation. Furthermore, formulating and implementing a computer system security management plan and submit the plan to the Commissioner's Office. Finally, a computer system security risk assessment (at least once every year) will be conducted, and the assessment report will be submitted to the Commissioner's Office.

Additionally, they have to conduct an independent computer system security audit (at least once every two years) and submit the audit report to the Commissioner's Office. Finally, the objective is to adopt measures to ensure their CCSs' compliance with the relevant statutory obligations even when third-party service providers are employed. To comply with incident reporting and response duties, individuals must engage in a computer system security drill organized by the Commissioner's Office every two years. The Mandatory Incident Notification duty requires CIOs to report computer system security issues to the Commissioner's Office so that the Commissioner can direct a timely response as necessary. Computer system security incidents are actions taken without lawful authority on or through a computer system that jeopardizes or negatively impacts its computer system security (Cheng, Li, Luo, & Zhu, 2024).

The severity of the incident determines the time frame for Mandatory Incident Notification. Within two hours of becoming aware of the incident, report serious computer system security incidents, which refer to incidents that have or are about to have a significant impact on the continuity of essential services and normal operation of CIs or lead to a large-scale leakage of personal information and other data, and within 24 hours after becoming aware of the occurrence, report any other computer system security incidents. If the initial report is made over the phone or via text message, the CIO must present a written record within 48 hours. The Proposed Legislation further calls for filing a follow-up written report within 14 days of becoming aware of an incident, which would provide additional facts about the occurrence (including the cause(s), impact, and corrective steps). A Commissioner's Office will be established inside the Security Bureau to carry out the proposed legislation. The office will identify CIOs and CCSs, create a Code of Practice, and monitor security threats. Furthermore, it shall assist with incident response, investigate non-compliance, collaborate with other government departments, and provide written instructions to CIOs to address potential security gaps.

The Commissioner's Office will have broad authority to examine computer system security events and crimes under the Proposed Legislation. This is compatible with other cybersecurity legislation, such as those in Singapore and Malaysia. Specifically, the Commissioner's Office will be able to request information from CIOs (even if it is based outside of Hong Kong), take corrective action, and enter relevant premises for inquiry with a magistrate's warrant. In more serious circumstances (i.e., when a CIO refuses or cannot respond to a cyber event), the Commissioner's Office may connect equipment to or install programs in the CCS with a magistrate's warrant. Since some CIs are already thoroughly regulated by statutory sector regulators, specific sector regulators will be designated as authorities to monitor the relevant sectors' compliance with organizational and preventative requirements. The Commissioner's Office will monitor compliance with incident reporting and response requirements. This method enables the designated authorities to develop standards and requirements within their existing regulatory regimes that are most appropriate for the needs of the sectors. CIOs in these areas will not face double regulation, which means they will not be required to meet additional requirements imposed by the Commissioner's Office regarding organizational and preventive measures. At this stage, two sector regulators have been proposed. The first is the HKMA for banking and financial services and the Communications Authority for communications and broadcasting. Designated authorities may offer applicable guidelines for the entities they regulate. It is uncertain whether all financial institutions in Hong Kong will be protected. However, it is proposed that the HKMA regulate "some" service providers in the banking and financial services sector. We also observe that the majority of the CIOs to be regulated will be from large enterprises. The Proposed Legislation proposes several offences, such as non-compliance with statutory obligations, written directions from the Commissioner's Office, investigation requests, and providing relevant information about a CI are all examples of CIOs' failure to comply (Carter & Crumpler, 2022).

The proposed legislation solely specifies fines established by courts as potential penalties. Offences and sanctions will only apply to organizations. Therefore, individual officials or staff members will not be fined.

It is proposed that failure by CIOs to comply with any of the requirements result in sanctions ranging from HK$500,000 to HK$5 million. If non-compliance continues, additional daily fines may be issued. If a CIO's failure to comply with statutory responsibilities is caused by a third-party service provider's ineffective activity, the CIO will still be held accountable. Non-compliance with current criminal legislation, such as making false claims or committing fraud-related offences, may result in personal criminal liability for the personnel concerned. In contrast, non-compliance can result in criminal penalties in Singapore and Malaysia, including imprisonment. By the end of 2024, the government intends to bring the proposed legislation before LegCo. It also hopes to establish the Commissioner's Office within a year after the proposed Bill's passing, with the Bill being enacted six months later. It is envisaged that the Secretary for Security will have the right to specify or alter specific features through subsidiary law, including the critical services sectors designated as a CI and the scope of security management plans and security audits. As this reform moves forward, we'll keep an eye on its progress and bring you more updates after the legislation is finalized. If you would like to talk more, please get in touch with your regular HSF contact.

3. Cybersecurity risks for Islamic banking

Cybersecurity standards are crucial in assisting organizations to compare their controls and measures to defined benchmarks in addition to requirements. One example of important cybersecurity standards is the Payment Card Industry (PCI) Security Standards for payments. With operational and technical criteria, PCI Security Standards help institutions maintain payment security. Another illustration would be the ISO/IEC 27000 family of standards, which enable organizations to control the security of their assets, including personnel information, financial data, and information given to them by third parties. The SWIFT Customer Security Controls Framework (CSCF) offers a collection of control principles to prevent specific cybersecurity threats, thereby strengthening the security of the global financial system. While AI can be a tool for attackers, it is also being used to assist institutions in becoming more resilient to cyberattacks by analyzing vast volumes of data effectively and identifying patterns that can be used to identify similar attempts in the future. The application of AI also reduces the costs associated with cyber incidents. IBM reports that breach costs for organizations with fully implemented security AI and automation have been $2.90 million, whereas breach costs for organizations without such safeguards have been $6.71 million (Al-Alawi & Al-Bassam, 2020).

This is probably a strategy for larger organizations, though, as they will have the amount of data required to train an AI. The workforce has two potential effects, which are the opposite. It can either reduce or increase cyber threats. The human component is a significant part of planning, managing, and defending organizations' cyber ecology. Employees who do not know enough about cybersecurity can be a major source of cyber dangers, such as malware that enters systems through innocent clicks on harmful links and system hacks. To turn people into a source of cyber resilience, organizations should not only hire cybersecurity specialists but also provide them with the tools they need to mitigate cyber risks. Identifying potential sources of cyber risk entails regularly monitoring employee access to the organization's systems and data and offering ongoing cybersecurity education and training.

Even though these initiatives offer prospects for improved cybersecurity within the sector, financial institutions face several obstacles when it comes to safeguarding themselves from cyber threats. A significant obstacle is the growing complexity of cybercriminals' techniques. This offers further problems in building smarter systems that can fight these sophisticated ways,

especially with the ongoing growth of cyberattacks. Financial institutions must also invest significantly in cybersecurity measures, which may strain their finances. Smaller financial institutions that lack the requisite resources may find this problematic. The dearth of cybersecurity experts in the industry is another issue that could compromise the security precautions taken. For financial institutions, the structure of the financial sector itself presents significant obstacles. Cybersecurity is compromised when a financial institution depends on several service providers, and when numerous institutions depend on the same supplier, interdependence and vulnerability are inherent problems. Another issue is the absence of uniformity in cybersecurity regulatory frameworks. Multinational financial companies must implement distinct cybersecurity protocols for every market that divides their networks into many national systems, as different jurisdictions have varying cybersecurity needs (Komaruddin, Utama, Sudarmanto, & Sugiono, 2023).

Additionally, this may render some markets more vulnerable to cyberattacks than others and provide a platform for hackers to destabilize the whole financial system. Compliance requirements for consumer protection, such as the General Data Protection Regulation (GDPR) in the EU, may also complicate cybersecurity for smaller banks and financial institutions, which may not be able to withstand the fines connected to non-disclosure of cyber incidents. It is evident that cybersecurity poses a similar issue to mainstream financial organizations and Islamic ones. Cyberattacks can also target the wealth and data moving through the Islamic banking ecosystem. The top three risks that Islamic banks were concerned about for their institutions were technological and cyber-security risks, according to CIBAFI's Global Islamic Bankers' Survey (GIBS) for 2020 and 2021.

From an Islamic standpoint, one of Shariah's goals is to preserve and defend people's and organizations' property against any damaging acts. Examples of such properties are digital resources, intangible riches, and tangible and financial wealth. These assets are in use in the financial industry and are vulnerable to several risks that could compromise financial institutions' information systems and result in fraud, theft, scams, and improper or unlawful use of personal and public data. As a result, stopping such attacks is consistent with Shariah's goals and is linked to maintaining cyberspace security and implementing steps to strengthen the cyber resilience of Islamic financial institutions. However, Islamic banks confront greater hurdles in guaranteeing cybersecurity and resilience due to their size and location. Islamic banks with low resources may find it difficult to invest in cybersecurity measures because they are primarily tiny. In addition, geopolitical tensions in places where Islamic banks operate, for instance, the Middle East, might make financial systems in these regions an enhanced target for cyberattacks and raise Islamic banks' proneness to cyberattacks (Qudah, et al., 2023).

The weaknesses in their IT infrastructures further burden small financial institutions and Islamic banks operating in some emerging nations. This is particularly true regarding digital financial services transactions conducted over transmission lines that are not intended to protect financial transactions' security and use insecure devices. To assess Islamic banks' cybersecurity resilience, CIBAFI was surveyed in May 2021. The study looked at the cyber threats that Islamic banks faced as well as the steps taken to fortify their cyberspace. 100 Islamic banks from 33 different countries participated in the poll.

Global data indicates that Islamic banks have a generally high level of confidence in their cyber resilience. Forty per cent of the participants rated their cyber resilience fairly high, while over fifty per cent classified it as very strong or extremely strong. North African Islamic banks, however, had the lowest level of confidence in their cyber resilience across all regions. This might result from the region's heightened risk of cyberattacks due to shoddy infrastructures or the fact that small banks account for most responders from this area. Next in line are Islamic banks in Europe, which may also be less robust because they are smaller and have fewer resources available for more advanced cybersecurity safeguards (Ahmad, et al., 2023).

The survey's findings also revealed that banks rank denial-of-service (DDOS) assaults and system failures from third-party service providers as the two biggest cyber threats that could affect their organization. The second most dangerous cyber threats for Islamic banks are determined to be fraud, theft, and other malware-related issues. The breakdown of the bank's internal IT systems comes next. The overall findings are displayed in the figure below, and it is evident that all element scores are approximately equal. The actors responsible for cyberattacks against Islamic banks were also questioned in the study. Islamic banks rated criminals driven mostly by financial gain at the top of a list of parties, followed by hobby hackers and business partners. The parties deemed least hazardous in Islamic banks' cyberspace were their business rivals. The regional map demonstrates that regions can be broadly divided into two categories. A certain group regards entities that are part of their business network, such as rivals and partners, as potential cyber risks to their establishments. This is observed in North Africa, Sub-Saharan Africa, and the Middle East Ex-GCC. Regions that view outside actors in the business ecosystem, such as lawbreakers with varying agendas, as greater threats to Islamic banks' online make up the second group (Joveda, Khan, Pathak, & Chattogram, 2019).

Islamic banks were also requested to indicate the degree of cybersecurity measure execution from a list of measures. The findings indicate that most participants either execute the suggested measures or have finished doing so. Islamic banks' most commonly implemented security measures include multiple layers of protection to isolate the corporate network from externally facing systems. The least common implementation is holding quarterly exercises to evaluate the institutions' preparedness for responding to cybersecurity incidents. It has been noted that Islamic banks have concentrated more of their efforts on putting cybersecurity measures into place and less on developing cybersecurity strategies and conducting routine testing to ensure their systems are cyber-resilient. These tasks ought to be given higher priority following international bodies' recommendations and considering the ongoing sophistication of cyber threats (Vedral, 2021).

The benefits of technology have been driving digitalization in the banking business throughout the previous years, boosted by the COVID-19 pandemic. This has been linked to higher cyber dangers even if it has improved services, decreased costs, and enhanced efficiency. Cyber hazards may significantly impact the financial system's and financial institutions' stability. Due to their small size and dispersed geographical locations, Islamic banks are particularly vulnerable to cyber threats because of their inadequate resources and antiquated IT infrastructure. For the financial system to remain stable, efforts must be made to achieve cyber resilience. This needs cooperative efforts from different actors and the adoption of measures at all levels by all actors in the financial industry intending to secure cyberspace. Such initiatives help Islamic financial institutions achieve Shariah's wealth and property preservation goals. As a result, there is advice to adopt a proactive stance and consistently improve cybersecurity procedures by utilizing toolkits and best practices created by global organizations. Furthermore, it requires the development of clear strategies for cybersecurity within the institution, including identifying vulnerable digital assets, and there is continuous evaluation for the management of cyber threats. Additionally, there are initiatives to achieve automation of processes to reduce human error (Cheng, Li, Luo, & Zhu, 2024).

Finally, data storage diversification and managing exposures to third-party risks play a critical role. Furthermore, it creates a precise recovery plan to ensure a speedy recovery from cyberattacks, raises cybersecurity awareness, and emphasizes how it helps implement Shariah principles. Furthermore, cybersecurity training programs are created for staff members to inform clients about the strategies used by cybercriminals and safe measures to lessen their vulnerability to cyberattacks. Additionally, the request is to create channels for financial institutions to exchange information to help cybersecurity efforts and should foster initiatives to help small financial institutions with cybersecurity.

Another challenging area is the facilitation of the detection of cyber threats and the comparability of data across institutions and nations, establishing precise and uniform definitions and classifications of cyberattacks. Additionally, it should create channels for ongoing communication and information exchange about cyber incidents with regulators and infrastructure organizations to enable early vulnerability discovery and help fortify the country's cyberspace. Finally, adaptable regulations should be developed that handle changes in cyber risks. Finally, there are united efforts to create a common approach to countering cyber threats associated with financial institutions' global connectivity and to assist areas lacking an adequate IT infrastructure in developing their cyberspace (Arner, Gibson, & Barberis, 2020).

Conclusion

The finance sector will be at the forefront of cybersecurity concerns and one of the most targeted industries. Along with healthcare and professional services, the financial sector has substantial cybersecurity issues, with emails containing ransomware and other malware being among the most common threat incident types. Concerns about cyber threats have developed widely as a result of the COVID-19 pandemic and the current acceleration of service digitization. Cyberattacks within economies have become more widespread. According to the Bank for International Settlements (BIS), cyber risk is the risk of financial loss, interruption, or reputational damage to a company as a result of an IT system failure.

One of the aims of Shariah, from an Islamic perspective, is to protect and defend people's and organizations' property from any harmful activities. Examples of such properties include digital resources, ethereal riches, and tangible and financial wealth. These assets are used in the financial industry and are susceptible to a variety of threats that could undermine financial institutions' information systems, resulting in fraud, theft, scams, and the improper or illegal use of personal and public data. As a result, preventing such assaults aligns with Shariah's purposes and is linked to preserving cyberspace security and implementing measures to increase Islamic financial institutions' cyber resilience. However, Islamic banks face more challenges in ensuring cybersecurity and resilience due to their size and location. For Islamic banks looking to list in Hong Kong as well as be potentially considered to be dual listed on the stock connect, ensuring cybersecurity plays a critical role that is in line with Islamic principles.

References

Ahmad, R. A., Tarshany, Y. M., Ayasrah, F. T., Mohamad, F. S., Saany, S. I., & Pandey, B. (2023). The Role of Cybersecurity in E-Commerce to Achieve the Maqasid of Money. 2023 *International Conference on Computer Science and Emerging Technologies (CSET)* , 1-8.

Al-Alawi, A. I., & Al-Bassam, M. S. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University,* 14(7): 1523-1536.

Arner, D. W., Gibson, E., & Barberis, J. (2020). FinTech and its regulation in Hong Kong. Research Handbook on Asian Financial Law, 431-453.

Carter, W. A., & Crumpler, W. D. (2022). Financial Sector Cybersecurity Requirements in the Asia-Pacific Region. Center for Strategic and International Studies (CSIS).

Cheng, S., Li, J., Luo, L., & Zhu, Y. (2024). Cybersecurity governance and digital finance: Evidence from sovereign states. *Finance Research Letters,* 63, 105533.

Didenko, A. N. (2020). Cybersecurity regulation in singapore's financial sector: protecting FinTech 'Ants' in a jungle full of 'Elephants'. *UNSW Law Research Paper,* 20-45.

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies,* 36(1), 351-407.

Gutiérrez Ponce, H., Chamizo González, J., & Al-Mohareb, M. (2023). Sustainable finance in cybersecurity investment for future profitability under uncertainty. *Journal of Sustainable Finance & Investment,* 13(1): 614-633.

Huang, H., & Li, T. S. (2018). A centralised cybersecurity strategy for Taiwan. *Journal of Cyber Policy,* 344-362.

Huang, R. H., Cheung, C. S., & Wang, C. M. (2020). The risks of mobile payment and regulatory responses: A Hong Kong perspective. *Asian Journal of Law and Society,* 7(2): 325-343.

Joveda, N., Khan, M. T., Pathak, A., & Chattogram, B. (2019). Cyber laundering: a threat to banking industries in bangladesh: in quest of effective legal framework and cyber security of financial information. *International Journal of Economics and Finance,* 11(10): 54-65.

Komaruddin, K., Utama, A. S., Sudarmanto, E., & Sugiono, S. (2023). Islamic Perspectives on Cybersecurity and Data Privacy: Legal and Ethical Implications. *West Science Law and Human Rights,* 1(4): 166-172.

Lee, E. (2022). Technology-driven solutions to banks' de-risking practices in Hong Kong: FinTech and blockchain-based smart contracts for financial inclusion. *Common Law World Review,* 51(1-2): 83-108.

Ng, A. W., & Kwok, B. K. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance,* 25(4): 422-434.

Pendley, J. A. (2018). Finance and accounting professionals and cybersecurity awareness. *Journal of Corporate Accounting & Finance,* 29(1): 53-58.

Qudah, H., Malahim, S., Airout, R., Alomari, M., Hamour, A. A., & Alqudah, M. (2023). Islamic finance in the era of financial technology: A bibliometric review of future trends. *International Journal of Financial Studies,* 11(2): 76.

Smith, S. S. (2020). Emerging technologies and implications for financial cybersecurity. *International Journal of Economics and Financial Issues,* 10(1), 27.

Tsuchiya, M. (2016). Cyber security of financial sectors in Japan, South Korea and China. Managing Cyber Risk in the Financial Sector, 96-111.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management,* 22(4): 239-309.

Vedral, B. (2021). The vulnerability of the financial system to a systemic cyberattack. 2021 13th International Conference on Cyber Conflict (CyCon), 95-110.