Educational Administration: Theory and Practice
2024, 30(9) 549-562
ISSN: 2148-2403
https://kuey.net/

Research Article

Cybersecurity from Islamic Economics perspective: Concepts, Characteristics and Challenges in Saudi Arabia

Al-Siddig Talha M. Rahma[1*], Mohamed Sharif Bashir Elsharif[2]

[1*]Imam Mohammad Ibn Saud Islamic University, Saudi Arabia Email: etrahma@imamu.edu.sa
[2]Imam Mohammad Ibn Saud Islamic University, Saudi Arabia Email: mbelsharif@imamu.edu.sa

Citation: Al-Siddig Talha M. Rahma and Mohamed Sharif Bashir Elsharif (2024) Cybersecurity from Islamic Economics perspective: Concepts, Characteristics and Challenges in Saudi Arabia, *Educational Administration: Theory and Practice*, *30(9)* 549-562
Doi: 10.53555/kuey.v30i9.7823

ARTICLE INFO

ABSTRACT

This paper examines the concept and practice of cybersecurity from an Islamic economic perspective. It also addresses the risks of data breaches and the emergence of various crimes based on the perception of selected Saudi experts. This paper answers the central question of whether Islamic economics is capable of achieving cybersecurity through effective regulatory frameworks. Data was collected through survey questionnaires, employing a descriptive analytical approach to analyse the opinions of Saudi experts' perspective on cybersecurity challenges in Saudi Arabia. The findings underscore the important role of Islamic economic principles in formulating regulations to mitigate cyber risks. This paper recommends urgent action to develop and activate a comprehensive system for the security and protection of cyberspace as well as enhancing the legal environment for the prevention of cybercrime. It also suggested the need to develop a strategy to raise awareness among the various segments of society.

Keywords: Islamic economics, cybercrime, cybersecurity, cyberattacks, cyberspace, Saudi Arabia.

1. Introduction

Cybersecurity is the practice of protecting important systems and sensitive information from digital attacks, also known as information technology security. Cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from within or outside the organisation. There have been many cyberattacks and continuous thefts of information from inside and outside the devices, further deepening the challenges of cybercrimes. In response, these challenges require effective legislation and policy measures. Therefore, the Islamic economics model emerged, considering that it stems from the orientations of the Islamic religion. Thus, the concept should paint Islamic economics in rich strokes of comprehensive and effective frameworks to achieve cybersecurity and protection. This paper seeks to answer the central question of whether Islamic economics is capable of achieving cybersecurity through effective laws and regulations that address growing issues and challenges.

In this era of technology, ensuring the security and protection of information is critical to repelling any electronic attack against state agencies and institutions. Consequently, cybersecurity has become an essential part of state security. God instructs mankind to pursue justice and reject injustice and oppression, and this is evident in Therefore the preservation of the five necessities from Shari'ah (Islamic law): religion, soul, mind, money, and offspring., this study is based on spreading the culture of cybersecurity in line with Shari'ah's objectives, clarifying its role in societal stability. This includes defining cybersecurity, its importance, objectives, types, and components to establish a comprehensive system through a package of legislative and institutional mechanisms to adapt to the information revolution and stay abreast of developments in the cyber world. Which made cybersecurity one of the most prominent trends of this era, and cybersecurity is related to the security, political, economic and social aspects.

1.1 Purpose and Objectives

The main objective of this study is to define the concept of cybersecurity from the perspective of Islamic economics. The specific objectives include:

1. Clarifying the concept of cybersecurity, its types and components.
2. Identifying the role of the Islamic economics in achieving cybersecurity.
3. Determining the obstacles to cybersecurity, and explaining the extent of the cyber threat to citizens and the state.
4. Addressing the risks of data breaches and the emergence of various crimes based on the perception of selected Saudi experts.

1.2 Research Questions

The study seeks answers to the following questions:

1. What is the concept of cybersecurity, its types and components?
2. What is the role of Islamic economics in achieving cybersecurity?
3. What are the most important obstacles to cybersecurity, and the statement and to what extent the cyber threat to citizens and the state.?
4. What is the perception of Saudi experts about addressing the risks of data breaches and the emergence of various crimes?

1.3 Significance of the Study

This study is significant because of its focus on information security, one of the most vital fields protecting various information from potential threats. cybersecurity protects data from malicious software and various viruses. The significance of this research can be formulated as follows:

1. This research aims to provide an analytical study that attempts to understand the importance of cybersecurity, the challenges of global espionage, and electronic penetrations of countries, by addressing various related concepts such as the concept of cyberspace.
2. The study contributes to the practical application of cybersecurity principles by providing information to stakeholders and decision makers to benefit from it in developing programs and setting plans, policies and mechanisms that are effective in developing cybersecurity.
3. The study monitors the cybersecurity centres that were established in some Muslim states. The unit initiated the development of governance frameworks, policies, and instructions necessary to strengthen the cybersecurity system for financial and banking sector institutions and to enhance the readiness and ability of this sector to confront and respond to cyber risks, leading to the development and implementation of security programs and standards. Additionally, the study assesses the efficiency and effectiveness of cybersecurity controls, and to measure the maturity level of each organisation.

2. The Role of Islamic Economy in Cybersecurity

2.1 The Purpose of Islamic Legitimacy

Shari'ah and principles call for justice and the rejection of injustice and oppression. The term 'objectives of the Shari'ahh' is applied to both the general and specific goals that Shari'ah seeks to achieve. These goals prioritise the interests of the people into three categories: Necessities, Needs, and Improvements)[1]. The status of cybersecurity is found in the rank of necessities, and it is therefore one of the vital elements of life. The objectives of the Shari'ah include both general and specific objectives. The general objectives serve national and social interests and are achieved through legal rulings, whilst special objectives pertain to specific goals that Shari'ah seeks to achieve in various areas of life, including the economic or political system. If they are disrupted, it can lead to insecurity, instability and chaos and the emergence of corruption.

Many verses of the Holy Qur'an underscore the significance of cybersecurity. For instance, {God sets forth an example of a village that was safe and secure, its sustenance coming to it in abundance from everywhere, but it denied the blessings of God, so God made it taste hunger and fear with what they were making}(16:112). These verses tackle the concepts of tranquility, and the absence of fear, and that is why God Almighty made security one of the greatest blessings under which many countless blessings fall.Surat Quraish also reinforces the concept of security through global trade at that time.· The verse states, "For the protection of the Quraysh (1) The protection of the winter and summer journey (2) Let them worship the Lord of this House (3) Who fed them from hunger and made it safe from fear" (4). According to the above, the concept of cybersecurity represents one of the necessities upon which people's lives are based, as exemplified by the texts mentioned in the Holy Qur'an and the Sunnah of the Prophet.

[1] - Ashour, Muhammad Taher, purposes of Islamic law 2004 AD, part 3, p. 2022

2.2 Islamic Economic and Innovative New Products

Islamic finance institutions worked mainly to clarify the role of financial technology as a modern experience in the banking sector. It plays a crucial role in enabling this sector to achieve economic and social development by enabling various Islamic finance institutions to acquire electronic services[2]. On the other hand, the Secretary-General of the Council of Islamic Banks stated that 50% of Islamic banks have a cybersecurity strategy (2021), and many Islamic finance institutions, led by Emirates Islamic Bank, have used blockchain technology in achieving complex financing conditions and transactions that are compatible with Islamic law. Experience is also important. Bahraini Alco Bahrain Financial Technology aims to restore the growth of the Islamic banking industry and prepare it for a quantum leap (Shawi 2020). On the other hand, the Islamic Financial Services Board (IFSB), headquartered in Kuala Lumpur, acts as an international organisation in setting standards for the work of regulatory and supervisory bodies, which have a direct interest in ensuring the strength and stability of the Islamic financial services industry, which generally includes banking, capital markets, and takaful (Islamic insurance) sectors. In carrying out its mission, the IFSB works to develop a robust and transparent Islamic financial services industry, by introducing new standards or adapting existing international standards in a manner consistent with the principles of Islamic Shari'ah[3].
The IFSB is an international standard-setting body that aims to develop and enhance the strength and stability of the Islamic financial services industry by issuing prudential standards and guidelines for this industry, which generally includes the sectors of Islamic banking, capital markets, and takaful. The IFSB also conducts research activities, coordinates initiatives on issues related to the industry, as well as organises panel discussions, seminars and scientific conferences for regulatory authorities and stakeholders interested in these industries.

The IFSB is the main interface for displaying and reflecting Islamic financial activities and an interface that expresses the concepts of the Islamic economy and its institutions. This institution held the its15th summit of the Council where ways to combat cyber risks were discussed[4]. Discussions at the summit revolved around emerging risks and the regulatory and supervisory steps taken by the concerned authorities to combat cyber risks and support its effective response to these attacks. During the summit, the Governor of the Bank of Bangladesh emphasised: "*We are facing several challenges and we have lost a lot due to piracy operations. Given this, we are working on developing many legislations and guidelines related to cybersecurity. We have also strengthened control efforts and the use of financial technologies, including blockchains"*.[5] Regarding the effects of cyber risks, he stressed the need to realise how cyber risks can negatively affect Islamic financial servicesSimilarly, on December 11, 2022, in Amman, Umniah Company, a subsidiary of the Batelco Bahrain [6]. Group, organised a workshop aimed at strengthening its leadership in cybersecurity. The workshop focused on the most prominent services and solutions provided by Umniah in the field of cybersecurity to its clients from the financial and banking sector institutions. In cooperation with several global solution providers, the workshop shed light on the services and solutions provided by Umniah in line with the needs of the market in general and the needs of this sector in particular[7].

3. Conceptual Review

3.1 The Concept, Importance and Benefits of Cybersecurity

The word "cyber" is an adjective within computer culture, information technology, or cyber reality.[8] Specifically, cybersecurity is the practice of protecting systems, networks, and programs from digital attacks, which usually aim to access, change, or destroy sensitive information, extort money from users, or interrupt business operations.The term cybersecurity encompasses the security of various elements, such as networks, systems, informatics, data, information and devices connected to the internet (Samara, 2023). It is a field related to procedures, measures and standards of protection that must be taken or adhered to in order to confront threats, prevent infringements and limit their effects in the harshest and worst cases.[9] Edward Amoroso also defines it as "a group of means that reduce the risk of attack on software, computer hardware, and networks."[10] These include the means and tools used to confront piracy, detect and stop digital viruses, and provide encrypted communications.

---

[2] Ayman El-Segini, CEO of the Islamic Corporation for the Development of the Private Sector 2021
[3] Reports/Islamic Financial Services Board 2020
[4] The Islamic Financial Services Board Conference, Summit No. 15, Jeddah 2021
[5] Abu Farah Muhammad Nasir, Deputy Governor of the Bank of Bangladesh 2021
[6]- Omar Al-Ansari - Secretary General of the Accounting and Auditing Organization for Islamic Financial Institutions 2020
[7] - The Arab Banking Forum for Cybersecurity - in its new session, - March 2022 «Cybersecurity, financial stability challenges and the readiness of digital criminal investigation
[8] - Al-Rabiah, Salih Bin Ali, digital security and user protection from the dangers of the Internet
[9] - Mona Al-Ashqar - Cyber is the Obsession of the Age, The Arab Center for Legal and Space Research, p. 26
[10] - Edward Amorso, author of the book "Cybersecurity", which was published in 2007

Cybersecurity is technical, organisational and administrative means that protect against harm and vulnerability to various threats, including extortion, penetration, disruption, modification, unauthorized access, and illegal exploitation. Cybersecurity has worked to protect data and data privacy, and it serves as one of the important strategies used by governments and considered part of its modern warfare. It is even called the "fourth arm of the modern army."[11]The importance of cybersecurity is highlighted in finding programs and technologies that protect against harm, prevent vulnerability to extortion, penetration, disruption, modification, entry, use or illegal exploitation. The concept of cybersecurity includes information security, electronic security, digital security, as well as the security of communications, space and technology (CST).
Cybersecurity is one of the techniques designed to take the necessary technologies and measures for many systems, networks, programs, devices, and electronic data to protect from attacks, penetration, and exploitation of the information on them. The primary goal of cybersecurity is mitigating the electronic risks that users, companies and others may be exposed to. It is continuously developing to to keep pace with all the electronic developments that have spread in the world, and it also seeks to achieve its goals, including the availability of data, confidentiality and integrity.Cybersecurity is considered one of the most prominent and important modern technical sciences that have emerged in recent times. This modern science has various benefits and features that make it an indispensable science in our world today.

As a result of the proliferation of internet networks and the numerous services it provides, new terms have emerged in the world of crimes and attacks related to stealing information or data of various types of companies. Therefore, the need to preserve the security of the information and data of these companies called for the establishment of a new science that works to secure this data. Among the most prominent of these benefits include:

1. Protecting networks and data from unauthorised access.
2. Improving the level of information protection and ensuring business continuity.
3. Enhancing the confidence of shareholders in the company.
4. Retrieving the leaked data in a real time in the event of a breach of the cybersecurity system[12]
5. Protecting personal information and getting rid of spyware[13] and improving cybersecurity in general.

The process of protecting various networks, systems, and data is one of the most prominent benefits offered by modern cybersecurity science. The specialists in this field apply various means and methods that mainly aim to improve the level of protection and security of data, networks and resources of companies. This is done through the periodic maintenance of the protection systems and programs that these companies follow[14]

3.2 Types of Cybersecurity and Ways of Protecting Information &insurance

The concept of cybersecurity follows a unified approach that usually consists of several layers of protection installed in computers, networks, programs or data that the user intends to protect in cyberspace. Cyberspace is a digital interactive environment that includes physical and non-physical elements consisting of a group of digital devices, check systems, software, and users, whether operators or users.
Accordingly, many types were known in cybersecurity, and each type has a special mission to protect modern devices and computers from electronic attacks and viruses and ensure the preservation of data and information without exploitation and penetration. Some of these types are network security, application security, cloud security and operating security.Several methods can be used to prevent the occurrence of any attacks or fraud through computers or mobile phone application, including:

1. Using artificial intelligence to prevent threats to the public.
2. secure protocols to protect computers from hacking.
3. Preserving the principle of privacy, in addition to confidentiality and integrity of private information and data.
4. Protecting national information and services from espionage.
5. Using modern technological information systems in order to reduce potential risks when using the Internet.

3.3 Electronic Terrorism and Security Risks in Cyberspace

Electronic terrorism employs modern technologies to serve terrorist operations, including recruitment, communication, training, and espionage, often via the Internet or wired and wireless networks, including satellite communications. Confronting the phenomenon of electronic terrorism and its danger has become one of the most important problems facing contemporary governments, thus necessitating the creation of modern

[11]- - Chairman of the Board of Directors of the Association of Banks in the name of Salem - Jordan 2021 AD
[12] 1 - Harvard Business Review, administrative concepts 2021
[13]- The benefits of cybersecurity and what are its most important goals Abdulsalam Basaheh Last updated: March 22, 2022
[14] - The benefits of cybersecurity and what are its most important objectives
Abdul Salam Basahir Updated: March 22, 2022

information technologies and means aimed at limiting the movement of terrorism and making its virtual movements more rigorous. Electronic terrorism manifests in various forms, including:

1. Attacking private or public databases that exist in computers, or any other electronic devices and digital networks.
2. Attacking economic and banking institutions by violating the confidentiality of digital and non-digital financial data, transactions and exchanges.
3. Facilitating money laundering and transnational cybercrime, in addition to the illegal exploitation of women and children and the infringement of the sanctity, dignity and prestige of people's private lives through crimes of defamation and electronic defamation.
4. Engaging in undeclared wars in cyberspace between states, which include espionage, hacking, and cyber threats to the defense and security systems of states (Dali 2021).

Cyber risk is the possibility of a threat and vulnerability within the country's cyberspace that harms the security and safety of information systems and basic information infrastructure structures. Moreover, the threats can exploit existing vulnerabilities in a way that affects the integrity and security of the information system, information networks or network infrastructures[15].

Cybersecurity is one of the important areas used to protect information from electronic attacks, but there are many cybersecurity risks facing individuals, companies, and organisations with increasing reliance on technology.

Some of these risks include:

1. **Malware:** This is the most prevalent form of cybersecurity risk, and it refers to malicious programs or viruses that automatically install themselves on a target system, which leads to unusual behavior by the system, such as file deletion, information theft and the inability to log in or gain access to some of the programs installed on the device.

2. **Threat to Financial Stability:** Electronic financial services are the industries that are most exposed to risks related to cybersecurity. These risks target major financial institutions, and frequently used financial systems and services, which makes them suffer from instability and loss of confidence among customers, leading to accounts cancellation or discontinuation of electronic financial services usage.

3. **Password Theft:** Electronic accounts may be hacked by an unknown person by stealing the password, either by guessing it or using hacking programs, such as brute force programs.

4. **Congestion Cutting and Interception:** Also known as eavesdropping, congestion cutting involves an unwanted third party intercepting information shared between parties, leading to theft of information and passwords.

5. **Social Engineering:** This is a comprehensive method aimed at deceiving users disclose sensitive information through tactics such as sending friend requests from unknown people, sending messages, or e-mails. Attackers use information about the target user that he obtains from his social media to craft convincing schemes.

6. **The water hole attack**. This is an attack strategy targeting websites that are frequently used by institutions or organisations, as the attack loads viruses and malware on the target sites.[16]

3.4 Threats to the Financial Sector

The world is witnessing a significant increase in the size and complexity of cyber-attacks that have targeted various countries, especially in the Arab region, and the financial sector is considered the most vulnerable to the danger of these cyber-attacks, as financial and banking institutions are an attractive target due to their vital role in financial intermediation. Many organisations are still using outdated systems that may not provide the required protection from cyberattacks. If successful, there could be significant direct consequences for the organisation, including financial losses and reputational damage.As for the security of financial institutions, it is much greater than the individual level, as it includes securing the bank's network from intrusions, securing its devices from malicious programs and their spread, securing the powers for each user and device, distributing devices on levels to limit risks, using secure protocols in communication processes, training and qualifying employees on how to respond if they suspect something and other means[17]

[15] -Secretariat of the Higher Technical Committee for Communications and Information Security - Iraq - 2021 AD

[16] - previous source

[17]2020/4/13)-) Khartoum: Cybersecurity and combating piracy in banks - workshop

Al-Sharkas (2015) pointed out that:
The most prominent reasons for cyber-attacks that may threaten the stability of the financial system are the risk of concentration and the lack of alternatives to several financial institutions of systemic importance and the infrastructure of financial markets, as well as the loss of confidence that results from the occurrence of a cyber event, in addition to the increase in interdependence between the components of The financial system that expands the risk of contagion, which leads to the spread of contagion through the entire financial system. This requires increased coordination between local and international authorities and the development of ways of cooperation in the field of cybersecurity.

Al-Sharkas explained further:
The World Bank estimates also indicate that the financial services sector is witnessing cyberattacks that exceed other sectors by 65%, which requires the regulatory and supervisory authorities and financial institutions to work in a participatory approach and unite efforts to build a comprehensive system for managing cybersecurity at the sector level, to provide A safe and reliable cyber environment to protect information and business, raise the level of readiness to respond to cyber incidents and reduce the effects resulting from them, without neglecting the importance of preparing the technical environment in advance to support digital forensic investigations when any of the cyber incidents occur[18].
This is in addition to strengthening local and international efforts as an effective means
Of reducing cybercrime and manage cybersecurity risks efficiently.

3.5 Models of Cyber Attacks
Cyber-attack is the deliberate exploitation of computer systems, networks, and entities that rely on information technology and digital communications to cause damage. Therefore, cyber risks represent a source of concern for any government agency or private institution, as well as individuals. In the event of the occurrence of these technical risks, it could cause devastating and costly damages that may reach billions of riyals. The number of cyber-attacks has multiplied alarmingly during the past years. A report in 2020 identified multiple sectors vulnerable to cyber risks, including the banking, manufacturing, energy, retail, professional services, government, health, media, transportation, and education sector.

Models of Cyber Attacks can be explained as follows:
1. One of the most famous cyber breaches involved the influence on the 2016 US elections, which garnered significant attention on social networks and in American streets.
2. Researchers at the IBM Institute have observed that the losses incurred by the United States due to this issue amounted to more than 35 million US dollars. Despite some pointing fingers at Russia for carrying out these hacks, IT engineers are well aware that this accusation lacks technical merit and cannot be substantiated with concrete evidence. The hacked person, regardless of their technical proficiency, would not likely leave a visible digital IP trace. They can electronically hide their location under the guise of any country, whether through Russia or South Korea, while he is staying in an apartment in Miami or Los Angeles.
3. As for the other most famous case in the field of cybercrime worldwide, it was the Pay Ransom and Cyber Extortion cases, where many cybercriminals “Hackers” hacked the devices of people and organisations and obtained sensitive information or confidential documents. Subsequently, they copied that data to their devices and blackmailed their owners with demands for payment until the information was returned or threatened to be publicly disclosed on the internet.

3.6 The Consequences of Cyber-Attacks
Cyber-attacks lead to serious consequences, resulting in substantial financial losses, the compromise of important and sensitive information, business interruption, impersonation and exploitation of personal data. In 2020, the average cost of a data breach was $3.86 million globally and $8.64 million in the United States. These costs include the expense of detecting and responding to the breach, the cost of downtime and lost revenue, and long-term damage to the company’s reputation and brand. Cybercriminals target customers’ Personally Identifiable Information (PII), such as names, addresses, national identification numbers (such as Social Security numbers in the US and financial codes in Italy) and credit card information, which they then sell those records on underground digital marketplaces. A breach of PII often results in loss of customer trust, regulatory fines, and even legal action[19]
Research has revealed that 88% of security breaches are caused by human errors. Therefore, priority must be given to investing in raising awareness of cybersecurity, strengthening educational and training programs for users and specialists, and improving the culture of security within institutions and companies. Emphasis should be placed on enhancing youth capabilities in electronic security as one of the basic ingredients for business development in light of the increasing reliance on digital technologiesOn the other hand, observers of the challenges and losses caused by the hacking and piracy operations that many banks were subjected to,

[18] - Governor of the Central Bank of Jordan, Dr. Adel Al-Sharkas
[19] - Melih Monday, July 26, 2021

especially in the Arab Gulf region, notes the size of the amount, which is estimated at $800 million during the previous years. At the global level, financial and banking institutions and some economic sectors exceed their annual losses, reaching approximately $600 billion. As communication and information technology develop, cyberspace hackers develop their skills dramatically and rapidly. The losses that will be caused by the global economy by the end of 2025 are estimated at about 3 trillion dollars. This is a large number which negatively affects the global economy, leading to a huge financial burden for financial institutions and banking in the world and the target countries. If Islamic financial institutions do not take preventive measures in time, they will also be targeted by these electronic attacks. It is important to undertake all necessary precautions to mitigate cyber risks, leveraging existing expertise and capabilities to protect their programs and data, thereby enhancing their competitivenessOn the other hand, Bassem Al-Salem affirmed that, "Banks are among the institutions that pay special attention to cybersecurity issues. Because the potential effects of cyber penetration involve exposing financial institutions to direct and indirect financial losses resulting from cyber-attacks, business disruption, reputational damage, and others." He underscored "the need to intensify preventive procedures and measures that enhance the cybersecurity of banks and increase their ability to address any threats," stressing "the importance of creating unified frameworks in the Arab banking sectors for exchanging and sharing information related to cyberthreats, and the need for more joint activities that discuss cybersecurity issues."

3.7 The Progress of Cybersecurity in Saudi Arabia

Currently leading the Arab world and ranking 13th globally in the United Nations Cybersecurity Index out of 175 countries, Saudi Arabia demonstrates a strong commitment to building a secure and adaptable cyberspace. This reflects the great importance given by the authorities in charge in the Kingdom to build a safe and flexible cyberspace to protect the priorities of the country and the citizen, work to strengthen the Saudi economy against electronic threats, respond to electronic incidents, activate security awareness operations for the electronic situation in line with the Kingdom's Vision 2030, and protecting national interests, critical infrastructure and government services and activities[20].

In alignment with Vision 2030, Saudi Arabia has made substantial efforts to provide a secure environment for data and digital operations through a solid security system, and to develop, implement and supervise a national cybersecurity strategy. An explanation of the basic controls and policies described in the Basic Cybersecurity Controls Guide, and national programs and initiatives, including the Saudi Federation for Cybersecurity and the launch of the National Academy for Cybersecurity launched by the Ministry of Communications and Information Technology is provided. It also covers the great acceleration in digital transformation processes. The rates of cyber-attacks and the risks of data breaches increased, which made the Kingdom keener in providing a secure environment for data and digital operations through a solid security system. Here comes the role of the National Cybersecurity Authority in developing, implementing and supervising strategies. The National Cybersecurity Strategy has been developed to reflect the strategic ambition of the Kingdom in a balanced manner between safety, trust and growth, and to achieve a safe and reliable Saudi cyberspace that enables growth and prosperity.

[21].

Despite the significant progress of cybersecurity in the Kingdom of Saudi Arabia, the country has experienced cyber-attacks that have severely damaged the infrastructure of some major organisations. The year 2012 witnessed one of the most prominent major incidents in Saudi Arabia, as the cyber-attack targeted the state-owned Saudi Aramco. This malware caused a malfunction and disrupted the company's activity for a month, marking one of the largest breaches in history. The Over Security Advisory Council report issued in 2016 indicated that the attack on Saudi Aramco cost it to change 5,000 hard disks for its computers, and it was unable to use the internet for about five months. This is considered a record time for repair, especially taking into consideration Aramco's financial and technical capabilities. In July 2017, another Mamba Ransomware attacked the corporate networks within the Kingdom of Saudi Arabia.

4. Empirical Review

Alzubaidi (2021) examined the level of cybersecurity awareness of cyber-crime in Saudi Arabia during the period between August to October 2019. He used a combination of purposive and snowball techniques from 1230 respondents. There was found to be a moderate correlation between online extortion and identity theft which means that these activities contribute significantly to cybercrime in Saudi Arabia.

Alhalafi & Veeraghavan (2023) explored the challenges and issues in adopting smart Saudi cities and validated a newly developed cybersecurity practices in Saudi Arabia. Based on question survey data collected from 108 IT professionals, 554 common public, and applying the theory of acceptance and use of technology, the measurement and structural model have been used to assess the relationship between studied factors. They

[20] - Shaqran Al-Rashidi, Administrative Development Journal, Issue 195 - 20 Rajab 1444

[21]- - Chairman of the Board of Directors of the Association of Banks in the name of Salem - Jordan 2021 AD

identified some factors influencing the adoption of cybersecurity measures in smart Saudi cities. These cybersecurity factors including safety, resilience, secrecy, integrity and availability items. The study emphasized the importance of economic and social factors in shaping behavioural intention and actual use of smart city technology.

Distinct from previous studies, current research uses the Islamic economic perspective to identify challenges and responses to achieve and implement cybersecurity. This way of addressing issues arising from cybersecurity challenges is a unique approach that has not been widely explored. Hence, this research would fill the research gap in this field, and can provide some practical implications to address and manage cybersecurity risks and challenges.

4. Results and Discussion

4.1 Method and Data Analysis

The study employed the descriptive analytical approach. The research population consists of selected by using Likert scale to measure the expert perception on cybersecurity challenges and responses. The study employed convenient sampling technique to select fifty (50) employees and specialists in cybersecurity in government institutions in Saudi Arabia. This selection of sample size and collection technique was made as a result of the difficulty in accessing experts in cybersecurity in government institutions. Furthermore, it is believed that the sample size is appropriate for this reason as it meets the purpose of the study. Questionnaires were used as a tool to collect primary data. We analysed the questionnaire data using the statistical analysis program (SPSS) The analysis of data was conducted using two measures: descriptive statistics presented and the chi-squared as shown in Tables 1-6.The field study data was analysed using the Statistical Package for Social Sciences (SPSS) program, employing the descriptive statistical analysis method represented in the frequency tables to describe the study sample. In addition, the study hypotheses were tested using nonparametric- Chi-Square test for one variable. The level of significance or probability value (p-value) was compared to the error rate ($\alpha = 0.05$). If the p-value exceeded 0.05, the hypothesis was rejected; if it was less than 0.05, the hypothesis was accepted. Secondly, hypothesis testing was conducted using the Chi-Square Test.

Table 1. Protecting the Organisation's Network

Requirement	Responses	Frequency	Percentage	Chi-squared value
Organisations work to protect their network from hacking.	Yes	43	86.0	25.920
	Neutral	7	14.0	
	No	0	0	
There is a strengthening of international, regional and national partnerships, including partnerships with the private sector and academic institutions, to prevent cybercrime.	Yes	32	64.0	25.920
	Neutral	12	24.0	
	No	6	12.0	
The data is protected by using modern specialised applications to monitor and analyse the transmitted and received data to discover any breach and alert the specialists	Yes	43	86.0	25.920
	Neutral	7	14.0	
	No	0	0	
Complex protocols are used to encrypt and protect data from hacking.	Yes	42	84.0	25.920
	Neutral	8	16.0	
	No	0	0	

From Table1, it is clear that most of the respondents' answers tend to agree with the statements, as 86% of the respondents agreed that the institutions work to protect their network from penetration, and 64% agreed that there is a strengthening of international, regional and national partnerships, including partnerships with the private sector and academic institutions to prevent Cybercrime. 68% agreed that data is protected by using

specialised modern applications to monitor and analyse sent and received data to discover any breach and alert specialists. 84% agreed that complex protocols are used for encryption and data protection from penetration, and the frequency differences of phrases are statistically significant. This is because the probability value of error is less than 05. This means that the latest applications are used to protect the organisation's network from penetration.

Table 2. Obstacles to the Application of Cybersecurity

Requirement	Responses	Frequency	Percentage	Chi-squared value
There are no obstacles to the application of cybersecurity	Yes	13	26.0	6.280
	Neutral	12	24.0	
	No	25	50.0	
The lack of specialised expertise is an obstacle to applying cybersecurity	Yes	42	84.0	58.840
	neutral	7	14.0	
	No	1	2.0	
The cyber obstacles are identical to the obstacles to electronic information.	Yes	37	74.0	40.840
	Neutral	12	24.0	
	No	1	2.0	
The inability to keep pace with the rapid developments of communication and technology and the evolution of information hackers and cyberspace stands as an obstacle to achieving effective cybersecurity.	Yes	36	72.0	33.640
	Neutral	7	14.0	
	No	7	14.0	

From Table 2, it is observed that 50% of the respondents do not agree that there are no obstacles to the application of cybersecurity. Additionally, 84% agreed that the lack of specialised expertise constitutes an obstacle to the application of cybersecurity, whilst 74% agreed that cyber obstacles coincide with obstacles to electronic information. Furthermore, 72% agreed that the inability to keep pace with the rapid developments of communication and technology and the development of information and cyberspace hackers stands as an obstacle to achieving the effectiveness of cybersecurity. The frequency differences of these phrases are statistically significant because the probability value of error is less than 0.05. This means that there are indeed obstacles to the application of cybersecurity.

Table 3. Islamic Legislation Limits New Cybercrimes

Requirement	Responses	Frequency	Percentage	Chi-squared value
Islamic law stipulates the controls for achieving cybersecurity	Yes	44	88.0	28.880
	Neutral	6	12.0	
	No	0	0	
Many Quranic verses and prophetic sayings stipulate achieving cybersecurity	Yes	43	86.0	25.920
	neutral	7	14.0	
	No	0	0	
Spreading the culture of cybersecurity in the light of the Islamic law objectives	Yes	38	76.0	13.520
	Neutral	12	24.0	
	No	0	0	
Developing appropriate Islamic legislation for cybersecurity that works to deter cybercrimes and enhance the protection of citizens and the state	Yes	43	86.0	25.920[a]
	Neutral	7	14.0	
	No	0	0	

From Table 3, it is clear that there are recurring differences, as most of the respondents' answers tend to agree with the statements. 88% agreed with the Islamic Shari'ah stipulating controls for achieving cybersecurity, and 86% agreed with many Quranic verses and sayings of the Prophet that stipulate achieving cybersecurity. Again, 76% agreed that spreading the culture of cybersecurity is considered in the light of the purposes of Islamic law, while 86% agreed that the development of appropriate Islamic legislation for cybersecurity works to deter cybercrime and enhance the protection of the citizen and the state. This means that Islamic legislation limits new cyber crimes

Table 4. Cybersecurity is One of the Purposes of Islamic Law

Requirement	Responses	Frequency	Percentage	Chi-squared value
Cybersecurity in Islamic law is considered a necessity and one of the essentials of life. If it is lost, life is lost	Yes	32	64.0	13.520
	Neutral	18	36.0	
	No	0	0	
The necessities in Islamic law, which are intended to ward off corruption from religion, soul, mind, lineage, honour and money	Yes	44	88.0	28.880
	neutral	6	12.0	
	No	0	0	
Cybercrimes committed against individuals, such as defrauding the money of others are considered crimes against preserving the five necessities according to the purposes of Islamic law.	Yes	32	64	22.240
	Neutral	12	24	
	No	6	12.	
Cybersecurity is related to the jurisprudence of Shari'ah politics. Therefore, Islam has established controls that direct the state's policy in the face of security threats	Yes	38	76.0	13.520
	Neutral	12	24.0	
	No	0	0	

It is clear from Table 4 that there are statistically significant frequency differences, as most of the respondents' answers tend to agree with the statements. Specifically, 64% agreed that cybersecurity in Islamic Shari'ah is considered a necessity and an integral aspect of life. Moreover, 88% acknowledged the importance of necessities according to Shari'ah principles. Moreover, 64% agreed that cybercrimes committed against individuals, such as defrauding others' money, are considered crimes against preserving the five necessities for Islamic law. Additionally, 76% of respondents agreed that cybersecurity is related to the jurisprudence of Shari'ah politics. Therefore, Islam has established controls that direct the state's policy in the face of security threats, and the frequency differences of the phrases are statistically significant because the probability value of error is less than 0.05. This means that cybersecurity is considered one of the purposes of Islamic law.

Table 5. Innovations for Protection and Cybersecurity

Requirement	Verification	Frequency	Percentage	Chi-squared value
The more the means of communication and information technology develop, the more cyberspace hackers develop their skills dramatically and rapidly	Yes	37	74.0	11.520
	Neutral	13	26.0	
	No	0	0	
The losses caused by the electronic invasion of the global economy are increasing annually	Yes	44	88.0	28.880
	neutral	6	12.0	
	No	0	0	
Countries are working to take all	Yes	24	48.0	4.960
	Neutral	12	24.0	

necessary precautions to face these risks and work to enhance their ability to face all cyber risks and potential cyber-attacks.	No	14	28.0	
The innovations of the employees of the institutions in the field of cybersecurity do not correspond to the needs of the departments in those institutions.	Yes	48	96.0	42.320
	Neutral	2	4.0	
	No	0	0	
The state encourages innovators, allocates competitions and prizes, and sponsors innovators in the field of cybersecurity.	Yes	28	56.0	.720[b]
	Neutral	0	0	
	No	22	44.0	

It is clear from Table 5 that there are statistically significant frequency differences, as most of the respondents' answers tend to agree with the statements. Specifically, 74% agreed that the more the means of communication and information technology develop, the more cyberspace hackers develop their skills significantly and rapidly. Moreover, 88% acknowledged the losses they suffer due to electronic invasion of the global economy, which is increasing annually. Additionally, 48% agreed that countries are working to take all necessary precautions to confront these risks and enhance their ability to address cyber risks effectively. Also, 96% agreed that the innovations of institutional workers in the field of cybersecurity do not correspond to the needs of their respective departments. Moreover, 56% of respondents agreed that the state encourages innovators, organises competitions and award prizes, and provide sponsorship to individuals in the field of cybersecurity.

Table 6. Approval of Cybersecurity Laws in Islamic Countries

Requirement	Responses	Frequency	Percentage	Chi-squared value
Many Islamic countries have issued cybersecurity laws.	Yes	27	54.0	9.640
	Neutral	12	24.0	
	No	11	22.0	
The Arab and Islamic region is considered to be a consumer of electronic services and not a producer of them.	Yes	29	22.0	14.440
	Neutral	13	58.0	
	No	8	26.0	
Islamic banks are among the financial institutions targeted for electronic attacks.	Yes	46	92.0	35.280
	Neutral	4	8.0	
	No	0	0	
Islamicfinancial institutions work to acquire the expertise and capabilities to allow them to protect their programs and data and enhance their competitiveness.	Yes	48	96.0	42.320
	Neutral	2	4.0	
	No	0	0	

From Table 6, it is evident that statistically significant frequency differences exist, with a majority of respondents expressing agreement with the statements. Specifically, 54% of the respondents agreed that many Islamic countries have issued laws for cybersecurity, while 58% agreed that the Arab and Islamic region is considered a consumer of electronic services and not a producer. Moreover, 92% agreed that Islamic banks are

considered among the financial institutions targeted for electronic attacks Also, 96% agreed that Islamic financial institutions work to possess expertise and capabilities to allow them to protect their programs and data, thereby enhancing their competitiveness.

4.2 Findings

4.2.1 Using Advanced Applications for Network Protection

1. 86% of respondents acknowledged that institutions are actively engaged in safeguarding their networks from penetration.
2. 64% recognised the importance of bolstering international, regional, and national partnerships, including collaboration with the private sector and academic institutions, to combat cybercrime.
3. 84% affirmed the use of complex protocols for encryption and data protection.

4.2.2 There Are Obstacles to the Application of Cybersecurity

Regarding obstacles to implementing cybersecurity measures, approximately 50% of the respondents disagreed that there are no obstacles to the application of cybersecurity. About 84% agreed that the lack of specialised expertise constitutes an obstacle to applying cybersecurity. Moreover, 72% agreed that the inability to keep pace with the rapid developments of the means of communication and technology and the evolution of information hackers and cyberspace stands as an obstacle to achieving effective cybersecurity Islamic legislation limits the new cybercrimes:

The influence of Islamic legislation on cybersecurity was also explored. Approximately 88% of respondents concurred with Islamic Shari'ah, which prescribes regulations for achieving cybersecurity. Around 86% supported various Quranic verses and teachings of the Prophet that underscore the importance of cybersecurity. Moreover, around 76% affirmed that promoting a culture of cybersecurity aligns with the objectives of Islamic law. Additionally, approximately 86% expressed support for the development of Islamic legislation tailored to cybersecurity, aiming to deter cybercrimes and bolster the protection of both citizens and the state.

4.2.3 Cybersecurity Holds a Significant Place within the Framework of Islamic Law

About 64% agreed that cybersecurity in Islamic law is considered a necessity and one of the essentials of life. If it is lost, life is lost. About 88% of the respondents agreed with the necessities in Islamic law, which are intended to prevent corruption in various aspects, such as religion, the soul, the mind, lineage, honor and money. Furthermore, around 64% of participants recognised cybercrimes as offenses against individuals, such as financial fraud, which directly violate the sanctity of life and the preservation of the aforementioned essentials. Additionally, approximately 76% acknowledged that cybersecurity is related to the jurisprudence of Shari'ah politics. Therefore, Islam has established controls that direct state policy in the face of security threats.

4.2.4 Innovations for Cybersecurity

About 74% agreed that the more the means of communication and information technology develop, the more cyberspace hackers will develop their skills significantly and rapidly. Moreover, 88% recognised the escalating economic losses caused by electronic invasions annually, which underscores the urgency for robust cybersecurity measures. While 48% acknowledged that countries are working to take all necessary precautions to face these risks, 96% agreed that the innovations of employees in institutions in the field of cybersecurity do not correspond to the needs of the departments in those institutions. However, 56% noted governmental initiatives foster innovation in cybersecurity, including incentives such as competitions, prizes, and sponsorship programs.

4.2.5 Adoption of the Cybersecurity Law in Islamic Countries

About 54% of the respondents agreed that many Islamic countries have issued cybersecurity laws. Moreover, around 58% agreed that the Arab and Islamic region is considered a consumer of electronic services and not a producer of them. Around 92% agreed that Islamic banks are among the financial institutions targeted for electronic attacks. Furthermore, around 96% agreed that Islamic financial institutions work to possess the expertise and capabilities to allow them to protect their programs and data and enhance their competitiveness.

The legal foundation of cybersecurity and its relationship to the objectives of Shari'ah

The sections of objectives in Islamic law include:

1 -The general purpose: It is what is for the benefit of the entire nation or the public, and this is achieved through the totality of the provisions of Shari'ah.

2 -Special objectives: These are the goals that Shari'ah seeks to achieve in a special area of life, such as the economic, family, political system, etc.

The Shari'ah's purpose for people is three things: necessities, needs, and improvements. Given the status of cybersecurity in Islam, we find it in the rank of necessities, and it is intended to ward off corruption from the religion, the soul, the mind, honor, and money (Al-Shanqeeti 1410). In the Prophetic hadiths, there is an

indication that security is an important goal, as in the words of the Prophet Muhammad, the Messenger of God, may God bless him and grant him peace: (Whoever among you wakes up safe in his flock, healthy in his body, has the sustenance for his day, it is as if the entire world has been possessed for him). (Al-Tirmidhi 4/167)

5. Conclusion and Recommendations

This study examined the concept and practice of cybersecurity from an Islamic economic perspective. The paper answers the central question of whether Islamic economies are capable of achieving cybersecurity through effective laws and regulations that address growing issues and challenges. This study used descriptive analytical approach and data was collected using survey questionnaires to analyse the opinions of Saudi experts on important issues such as the risks and challenges posed by cyberspace in Saudi Arabia. The study revealed the importance of the role of Islamic economy framework in achieving cybersecurity by developing regulations and laws to eliminate various risks. In conclusion, the study has shed light on the position of the various Islamic economies on cybersecurity. It touched on key features of cybersecurity such as safety, secure solutions, confidentiality, availability, identification and authentication.

Some recommendations and policy implication can be provided as follows:

1. Cybersecurity is considered an independent goal within the confines of public law related to the nation-building Shari'ah rulings. and Developing community awareness of the seriousness of cybercrimes and methods of prevention is important.
2. Activating the disciplinary punishments legislated by Islamic economics is crucial so that people in their countries, societies and different countries can live in safety and peace. Spreading the culture of cybersecurity in the light of Islamic economics through its various fields is paramount. It is important to create awareness and explain to the state and society about cybercrime and the resulting difficulties. The Islamic economy should explain the importance of its role in treating cybersecurity through its various applications to develop a national strategy for cybersecurity and supervise its implementation. Follow up on compliance in updating policies, controls and instructions related to cybersecurity, along with the establishment of specialised centers and platforms, are essential for effective cybersecurity management.
3. Encryption protocols should be integrated into national policies and standards. Building national capacities in the field of cybersecurity, preparing training courses, specific activities and national campaigns related to warning of the dangers of cybercrimes are also necessary. Standardisation and control mechanisms should be implemented in the clearance and licensing processes for importing or exporting high-sensitivity hardware and software imports. National cadres specialised in the field of cybersecurity should be recognised. The government should also support the competent authorities during the inference and investigation of crimes related to cybersecurity while establishing special courts to protect cyberspace and prosecute perpetrators of information crime
4. Adopt the concept of cybersecurity in accordance with the rule of legal necessity. Cybersecurity achieves a flexible digital economy, stimulating innovations, effective participation, development, and the flow of direct foreign investment. There is a need for development of cybersecurity in parallel with the development of methods and forms of cybercrime. This will help open new ways to enhance measures to confront risks and work to strengthen the infrastructure of countries including its private sector
5. The study calls for formulation of strategies for cybersecurity, including identifying the main methods for designing and implementing public policy in the field of cybersecurity. Promoting international cooperation in the field of cybersecurity is very important to achieve higher levels of security effectiveness. Creating an environment for the development of education and training will help in the process of dissemination of Islamic and legal legislation to reduce cybercrimes across the country and the whole region of the Arab world.

Funding Statement

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research through the project number IFP-IMSIU-2023044. The authors also appreciate the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) for supporting and supervising this project.

References:

1. Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI) (2017). *Legal standards*. Bahrain.
2. Achieving cybersecurity for administrative information systems - Mona Al-Samhan, King Saud University, 2000 AD
3. Afifi and Abdel Ghaffar (2016) The Cyber Threat, Makkah Al-Mukarramah *Journal* (921), pp. 20-36.
4. Ahmed Abees Nima Al-Fatali, Cyber Attacks: Their Concept and International Responsibility in Light of Contemporary International Regulation, Al-Mohaqqiq Al-Hali. *Journal of Legal and Political Sciences,* University of Babylon - College of Law, Fourth Issue, Eighth Year, 2019
5. Ahmed Mukhtar Omar, *A Dictionary of Contemporary Arabic Language* 2008, Volume 1.
6. Al-Azadi, Aws Majid Ghaleb (2016) *Cyber Information Security,* Al-Bayan Center for Studies and Planning, Baghdad.

7. aldarir, Al-Siddiq Muhammad Al-Amin (1996). alsalm and its contemporary applications. *International Islamic Fiqh Academy Journal, 9*(1) Organization of the Islamic Conference.
8. Alhalafi, N., & Veeraraghavan, P. (2023). Exploring the challenges and issues in adopting cybersecurity in Saudi smart cities: Conceptualization of the cybersecurity-based UTAUT model. *Smart Cities, 6,* 1523-1544. https://doi.org/10.3390/smartcities6030072
9. Al-Imam Al-Mawardi, investigated by Ahmed Gad, Al-Ahkam Al-Sultaniyya, Dar Al-Hadith, Cair.
10. Al-Sharari, Khaled Al-Warda and cyberspace arenas of future wars 2017
11. Alzubaidi, A. (2021). Cybercrime awareness among Saudi nationals: Dataset. *Data in brief, 36,* 106965. https://doi.org/10.1016/j.dib.2021.106965
12. Arab Planning Institute (2019) Risks of electronic (cyber) attacks and their economic effects: a case study of the Gulf Cooperation Council countries
13. Bakhrudin, Bakhrudin & Margolang, Fahmi & Sudarmanto, Eko & Sugiono, Sugiono. (2023). Islamic Perspectives on Cybersecurity and Data Privacy: Legal and Ethical Implications. West Science Law and Human Rights. 1. 166-172. 10.58812/wslhr.v1i04.323.
14. Basamh, Saeed & Qudaih, Hani & Ibrahim, Jamaludin. (2014). An overview on cybersecurity awareness in Muslim countries. *International Journal of Information and Communication Technology Research, 4*. 21-24.
15. Bhagwati, Jagdihln. Defence of Globalization. New York: Oxford University Press ،/ gov.fbi.www://https
16. Bin Zaidan, Fatima Al-Zahraa 2019 "Analysis of the Islamic finance sector using SWAT. Research submitted to the International Conference and Institutional Integration of the Islamic Financial Industry Algeria Al-Masry, Rafiq Younis.(1988)
17. Chairman of the Board of Directors of the Association of Banks in the name of Salem - Jordan 2021.
18. Communication, Space & Technology Commission (June 2020). Cybersecurity Regulatory Framework (CRF) for Service Providers in the Information and Communications Technology Sector. Version 10. https://www.cst.gov.sa/en/RulesandSystems/CyberSecurity/Documents/CRF-en.pdf
19. Cybersecurity, reference curriculum, national defense, Canadian Defense Academy Office 2016.
20. David, E. L. (2000) ،Electronic Crime Scene Investigation. New York.
21. Denning, D. E. (Aug 2000) Cyber terrorism", Global Dialogue.https://citra.gov.kw/sites/ar/Pages/Sectors/CompetenciesInformation TechnologySector.aspx
22. K. A. Meerangani, A. F. Ibrahim, M. Y. Omar, M. H. M. J. Mukhtar, A. Badhrulhisham, and M. A. A. Termimi, "Cybercrime and its Violation of Digital Platform Security: An Islamic Law Perspective," 2022
23. K. K. Panigrahi, Information Security and Cyber Law, published by tutorials point,2015.
24. Kandour, Abdul Karim: I(2007). Islamic Financial Engineering, King Abdulaziz University, *Journal of Islamic Economics, 20,* Issue 02, 2007, pp. 20-34.
25. 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*(04), 166–172. https://doi.org/10.58812/wslhr.v1i04.323
26. Michael N. Schmitt, Computer network attack and the use of force in international law: Thoughts on a normative framework, Columbia *Journal of Transnational Law,* 1998– 1999, Vol. 37.
27. National University Blog. (2024). What is cybersecurity and its importance to business. Lightwave Ave, San Diego, CA 92123. https://www.nu.edu/blog/what-is-cybersecurity/
28. Omar Muhammedjih, Objectives of Islamic Shari'ah, PhD dissertation in the principles of jurisprudence and objectives of Shari'ah, 2005, p. 343-357.
29. Qusai Abu Shama / November 29, 2021 / Audited by: Islam Sammour / Cybersecurity Objectives.
30. Samara, N. K. (2023) Cybersecurity Requirements for Management Information Systems. *Journal of Information Security, 14*, (3): 212-226. doi: 10.4236/jis.2023.143013.
31. Shafiq, Nouran (2015) Electronic space and patterns of international interactions: a study in the dimensions of electronic security, Al-Nahda Magazine, Egypt 16/ p. 136