The Impact of Cybersecurity Through Knowledge Sharing Practices: Limitations, Analysis of Current Trends and Future Research Directions

Moneer Alshaikh[1], Sajid Mehmood[2], Rashid Amin[3], Faisal S. Alsubaei[4]
Department of Cybersecurity-College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia[1,4]
Department of Computer Science and IT, University of Chakwal, Chakwal[2,3]

Abstract—**Research examines Saudi Arabian cyber security knowledge-sharing programs during its digital transformation under Vision 2030 through a combination of literature reviews and expert specialist insights to analyze current cybersecurity professional information transfer systems. This analysis shows how technological developments along with organizational and cultural elements impact these practices since the constant drive for innovation aims to enhance knowledge transfer so researchers discovered that cultural obstacles from resistance to openness, lack of trust and hierarchical structures and division within organizations and insufficient workflow systems along with worry about trust and outdated technological capabilities limit successful knowledge sharing. Through analysis of knowledge-sharing programs established by the National Cybersecurity Authority (NCA) Saudi Aramco and the King Abdulaziz City for Science and Technology (KACST), researchers show that strategic programs improve national cybersecurity readiness effectiveness. The research provides actionable advice that combines the design of a national security plan and secure technology funding with does-based mentorship initiatives across sectors and integrated incident reporting along with educational programs and performance-driven reward systems for motivation. The research offers combined theory and practice-oriented guidance that helps Saudi Arabia's policymakers along with organizations and cybersecurity practitioners to build effective strategies as they establish their leadership position in collaborative cybersecurity practices internationally.**

Keywords*—*Cybersecurity; knowledge sharing; Saudi Arabia; Vision 2030; digital transformation; cybersecurity education; cyber threats; cybersecurity framework; cultural barriers; National Cybersecurity Authority (NCA)

I. Introduction

Saudi Arabia's ambitious plan to go through a digital revolution as part of its Vision 2030 [1] has made cybersecurity a priority to the nation's security and its economy's resilience. The people of the nation have flocked to the internet, with internet connectivity standing at 95 % [2]. With the population of the kingdom being 7% involved in cyber activities and a 138% increase in the number of cyberattacks in 2024 as compared to the prior year, the kingdom is greatly challenged in trying to protect its information technology assets. In this cybersecurity ecosystem is a function that is both critical but often neglected – the exchange of knowledge among cybersecurity professionals [3]. This process represents a wide range of activities, including information sharing, exchange of new threats, problem-solving sessions, and new ideas for improving the security systems. Still, the process of knowledge sharing in the Saudi context is multi-faceted and enriched by cultural factors, the rate of introducing new technologies, and the focus on cybersecurity as one of the key factors for Saudi Arabian development plans. [4].

The study aims to identify issues and prospects of teaching and learning in this area, as well as the findings from a survey of literature, analysis of case studies, and acquisition of information from experts. The primary objectives are threefold: primarily, to map the existing state of the art of the mechanisms, platforms, and current initiatives promoting cybersecurity knowledge sharing in the Kingdom of Saudi Arabia; secondly, to identify the barriers and facilitators for knowledge sharing regarding the cultural factors, organizational structures, lack of trust and the lack of a unified framework; lastly, to offer specific recommendations for future improvements in the Kingdom of Saudi Arabia which will address the themes of the study, namely.

The importance of this study arises from the likelihood that it will make a valuable contribution to increasing the level of cybersecurity awareness in Saudi Arabia [5]. With the kingdom experiencing a rapid digital shift, information flow among cybersecurity specialists is critical in countering new threats, nurturing indigenous skills, and lowering the threat of cyberattacks [6]. The study, therefore, seeks to understand the enablers and the barriers to knowledge sharing in the Saudi cybersecurity sector and propose feasible, research-supported solutions that can be adopted to overcome these barriers while exploiting the existing advantages. By promoting better ways of sharing knowledge, Saudi Arabia can improve its cyberspace readiness, equip itself more effectively against new threats, and eliminate the duplication of work in cyberspace [7].

Furthermore, the findings of this research may even be relevant in other relatively fast-digitalizing economies of the GCC region, where similar issues are likely to emerge. Thus, it is for the following reasons that this study aims to contribute to the understanding of the current state of knowledge-sharing practices in Saudi Arabia [8], and provide recommendations for improvement which might help the kingdom to strengthen its cybersecurity system on the one hand, and benefiting from this study is a useful experience for the neighboring countries facing the same concern, on the other. Given that the digital environment changes at an unparalleled rate, the results of this study can become invaluably helpful in constructing and improving cybersecurity measures in Central Europe as well as contribute to increasing digital security and sustainable economic development in the age of digital transformation [9].

Before exploring this theme, it is important to pay attention to the fact that knowledge sharing in cybersecurity is not a mere technical problem but a complex issue that implicates organizational [10], cultural, and strategic aspects. In that way, the present work aims at presenting various aspects of the subject in order to understand the topic better and contribute to the enhancement of Saudi Arabia's as well as global cybersecurity [11].

The analysis of the factors that affect the cybersecurity posture about Saudi Arabian organizations is rooted in the framework. It categorizes these factors into three key areas: There are the three major categories which are Organizational, Technological, and Cultural. Organizational factors refer to characteristics that include Organizational structure and culture, policies and procedures, and incentive structures. The failure to participate in an organization's leadership and the inability effectively to protect from cyber threats depends on the organizational structure and used decision-making. The kind of policies and the degree of enforcement of these policies are critically important for creating a firm base for security [12]. Further, promoting the right rewards will help the employees have a better understanding of cybersecurity and act accordingly.

Technological factors, on the other hand, concentrate on the technical side of security [13]. Indeed, the nature of the platforms used, security arrangements made and the extent of integration of security safeguards across the platforms are important. Overall, it was found that end-of-year software, not regularly upgraded and poorly configured, may present great risks. Protection is a crucial factor in the contemporary world, and integrating proper security solutions can greatly improve an organization's security. Cultural factors are one of the most influential process components that define the cybersecurity culture of an organization [14]. One of the key messages of the lecture was that the overall security within an organization should be supported by security awareness and security-mindedness. A threat identification process should be integrated into a company with the result of empowering employees to report threats of their own volition [15]. Moreover, different departments and levels of an organization may also benefit from having a common perception of cybersecurity practices that can help them respond to such incidents. This model indicates that there is a need to an integration of robust organizational, technological, and cultural factors for a good cybersecurity posture. Through consideration of these factors, Saudi Arabian organizations can reduce their exposure to cyber threats, hence the protection of organizational assets.

This model identifies three primary categories of factors: organizational, technological, and cultural. Organizational influences include structures and policies in Saudi institutions, which include managerial, hierarchical, communication, knowledge transfer and sharing, and policies [16]. They help to build the base for the knowledge exchange to occur. Technological factors include specific technologies and their usage, including IT facilities, safe communication connections, cooperative tools, and information protection like threat intelligence systems and security information and event management systems. It was established that these factors greatly influence the efficiency of knowledge exchange among specialists in the cybersecurity field about the quality and availability of accessible resources [17]. Cultural factors refer to social and occupational antecedents and perceptions that are unique to culture to attitudes towards sharing of knowledge, concerns about independence or reliance, cultural differences on power distance, and the perceived relevance of knowledge sharing in the working environment [18].

These three categories dictate the state of affairs of the knowledge sharing on cybersecurity in Saudi Arabia, which, in the process, affects the overall cybersecurity of the kingdom. By promoting knowledge sharing, threat detection is quicker, event reactions are synchronized, and the cybersecurity posture of the whole continuum improves. On the other hand, if there are barriers to knowledge sharing, then we end up having what is referred to as knowledge silos, slow response to threats and arising issues, and also a sector-wise disjointed approach to the issue of cybersecurity [19]. This picture presents a logical breakdown of the opportunities and threats regarding Saudi Arabia's approach towards knowledge sharing in the cybersecurity context, and it is useful for the policymakers, organizational heads, as well as cybersecurity specialists in understanding the blind spots and the enhancement strategies. Moreover, this model could be adopted for cross-sectional research with other countries [20] in order to have an idea of the rate of Saudi Arabia in creating an enabling cybersecurity culture collaboration [21]. The representation of these relationships in a diagram means that lecturers and students will grasp the documentation in a manner that incorporates and captures all the necessary relations in pursuit of the study of knowledge sharing in cybersecurity in Saudi Arabia.

Thus, according to the findings of the present investigation, these practices are affected by technological, organizational, and cultural factors. Although there is an increasing understanding of the importance of innovation as a tool to boost knowledge sharing for the improvement of cybersecurity capacity, there are numerous challenges. Among the factors considered are cultural issues of sharing information, problems associated with organizational units, and non-standardization issues. At the same time, the results of the study also reveal fresh advancement agendas and progressive practices that are already in use by benchmark companies of the kingdom. These are the creation of cybersecurity communities of practice, promotion of cross-sector mentorship, and use of secure knowledge management systems. The paper ends with policy implications for policymakers, organizations, and cybersecurity practitioners to enhance a directory of improved knowledge share. KSA has the potential to improve its national cybersecurity significantly and become one of the regional leaders in the context of collaborative cybersecurity approaches if current challenges are properly addressed and existing strengths are further built upon. Aside from making theoretical contributions to knowledge on cybersecurity knowledge sharing in Saudi Arabia, this research invents useful recommendations for enhancing cyber security in rapidly evolving economies.

The research examines Saudi Arabian knowledge-sharing practices to develop recommendations that enhance cybersecurity system strength in the kingdom. The study presents valuable insights for fast-digitalizing economies including Central European countries as well as Saudi Arabia and the Gulf Cooperation Council (GCC) countries. This research examines cybersecurity knowledge sharing from three angles which include organizational aspects and cultural elements and the core strategic perspective. The paper follows this organization: Section II analyzes Saudi Arabian cybersecurity research and identifies obstacles to knowledge distribution. In Section III the paper examines cybersecurity dimensions within Saudi Arabia's digital environment alongside an analysis of National Cybersecurity Authority (NCA) operations and primary cybersecurity businesses in the country. The fourth section of this paper illustrates cybersecurity-sharing methods with a supported framework drawn from recent Saudi publications about this subject. The systematic evidence synthesis section (V) presents various techniques for sharing cybersecurity knowledge that determine impact analysis. The research findings regarding existing knowledge-sharing channels and obstacles are presented in Section VI. Section VII evaluates different models and concrete examples for enhancing knowledge management within the field of cybersecurity. The final section includes recommendations for knowledge-sharing development along with future research suggestions. The final section of this study stresses how essential effective knowledge-sharing methods are to build Saudi Arabia's cybersecurity resilience.

II. Related Work

The cybersecurity environment in Saudi Arabia is defined by Saudi Arabia's plan to create a strong digital economy with the help if selected strategic plans. This environment makes the management of cybersecurity a complex issue in Saudi Arabia because every industry across the country has varying needs and readiness levels of security. Alshareef et al. [22] present the Information Security Risk Management (ISRM) model for Saudi organizations and elaborate on how cultural, organizational, and regulatory characteristics affect information security management in various organizations and industries. For instance, it indicates that some industries are more secure than others because of higher awareness, or better resources. Alahmari et al. [23] have pointed out that such fragmentation is made worse by knowledge-sharing barriers, especially in large organizations where gaps in communication and knowledge-sharing result in risks. They claim that implementing effective cybersecurity is possible only with a coherent and homogeneous model including all sectors with action because it is also important to involve companies and make them not only knowledgeable but also active in the field of security. Alsindi et al. [24] provide more support to this by calling for an open knowledge-sharing culture that is critical in bridging the structures and functions of cybersecurity.

The process of knowledge-sharing is quite restricted in Saudi Arabia due to social and cultural factors that are so influential to cybersecurity. The civilization structure of KSA places the authority to decision-making in very few people as noticed in Pritchett's work that Saudi Sociedad has a very high level of opacity which would also imply limited synergies in the field of cybersecurity. According to Al-Hawamleh et al., [25], this is the case with public e-government services in which reformist security measures cannot be easily integrated because of bureaucratic cultures that continue to dominate the organizations. These are not unique challenges; hierarchy causes decisions to be more sluggish and discourages collaborative information-sharing. According to Almansoori, et al. [26], these challenges must be met by transitioning from information security to human security creating trust and eliminating mental barriers to the sharing of knowledge is a key to success. They also assert that managers who trust employees and different departments bring more cybersecurity-pertinent information out in the open when they are empowered to work across departments. This is in line with Shearry-Sneed et al. [27], who investigated similar barriers with reference to higher learning institutions and recommended a model of incentives to promote cooperative security behaviors. The aforementioned model by Shearry-Sneed states that organizations ought to encourage rewards for collaboration to foster collective accountability irrespective of the industry one operates in which otherwise is known to exclude knowledge-sharing.

Organizationally speaking, cybersecurity is critical for Saudi Arabian SMEs, especially given the recent digitization push under the Saudi Arabia Vision 2030 [**?**]. SMEs however are constrained by one major challenge which is that they may not be endowed with the resources or the human resource capability of the larger firms. Alahmari et al. [23] presents a model that also highlights knowledge-sharing as a way to minimize the threats of cyber-security in such businesses. This model is very reliant on leadership; having leaders who actively drive security awareness at the workplace will help to drive a process of never-ending improvement and will allow cybersecurity to be a key aspect of business rather than an add-on. Finally, Rawindaran et al. [28] compare Saudi Arabia with the UK: Saudiian SMEs have reported regulation and policy as threats that may affect their cybersecurity. They explained that establishing links between public and private sectors can help SMEs to receive resources and information that are crucial in developing the organization's cyber security. This multiple-actor perspective focuses on the ways that SMEs can use government resources and private-sector collaborations to advance cyber defense policies that embrace all forms of enterprises.

Another important area within Saudi Arabia is educational institutions' contribution to the dissemination of cybersecurity knowledge. As educational bodies, we have the capacity, perhaps the responsibility, to shape the future cybersecurity workforce and create awareness from this point forward. They establish that, for any organization, there is merit in the incorporation of formal inter-community knowledge-sharing processes within an organization, especially a university and non-profit organization. For instance, by offering cybersecurity topics, curriculum learners receive rudimentary competencies in security in addition to comprehending the security concerns of today's world. This could go a long way in preventing the dangers of insecurity since the next generation is being trained to defend technology resources. Furthermore, Saeed et al. [29] respond that with the growth of threat activity, CTI becomes the key aspect of organizational security. There is no reason not to incorporate training programs that hold the capacity to keep the employees abreast with emergent threats, which is especially vital in this profession because threats mutate frequently and constantly. Each of these initiatives within the educational setting benefits not only current social protection from threats that jeopardize security but also contributes to ensuring that the future workforce is skilled and sensitive to security risks.

With the advancement of the digital society and Saudi

Arabia on its way to accelerating its digital improvement, new tech paradigms are emerging in the organization's discussion, for example, Industry 5.0. Jaziri et al. [30] discuss how can Industry 5.0 frameworks help the Kingdom of Saudi Arabia in its digital supply chain, particularly through improving cybersecurity. They argue that to optimally attain the benefits from the digital world for any organization, a focus on knowledge sharing and awareness of cybersecurity remains vital. This concept is a foundation to acquire the digital architectural reliability of security procedures and frameworks to be participated by those at the company's lower ranks. Jaziri et al. also emphasize the issue that social media tools can be effectively used for sharing cybersecurity knowledge in HE, as Fauzi and Mohamad [31] [32] show. They argue that such participation of employees in knowledge sharing through the platforms fosters continued learning and the duty to be proactive in matters concerning security threats. Since students and faculty in higher learning institutions engage in daily interactions, social media, and other digital tools should be instrumental in creating a culture of cybersecurity.

It can be mentioned that Saudi Arabia has achieved considerable advancement in the cyber security domain; however, several themes remain mostly unexplored. Thus, despite all the government's investment in cybersecurity and technological advancement, more profound challenges to knowledge management policies remain, discouraging the best security solutions. Instead of compartmentalizing cybersecurity as a single, isolated concern, it is imperative to foster a culture of diversity and cooperation across industries and will the country toward the real achievement of a robust cybersecurity posture consistent with the nation's broader digital and overall security agendas. By catering to these challenges, Saudi Arabia can provide its cybersecurity practices to a secure and prosperous digital economy, the prepare a constant digital growth rate to be established.

TABLE I. Challenges and Solutions in Saudi Arabia's Cybersecurity Environment

Challenge	Solution
Varying industry needs and readiness levels	Implementing a coherent and homogeneous cybersecurity model
Knowledge-sharing barriers, especially in large organizations	Fostering an open knowledge-sharing culture and eliminating mental barriers
Hierarchical decision-making and bureaucratic cultures	Transitioning to human security and empowering employees
Resource constraints for SMEs	Knowledge-sharing, leadership, and government/private sector collaboration
Lack of cybersecurity awareness and skills	Incorporating cybersecurity topics into education and training programs
Emerging Technologies and Digital Transformation	Leveraging Industry 5.0 Frameworks and Social Media for Knowledge Sharing

Table I of the main problems and solutions based on the cybersecurity situation in Saudi Arabia: Industries are various and different and cybersecurity requirements also differ so the model has to be consolidated. Furthermore, other factors that contribute to knowledge-sharing barriers also embrace large organizations that affect security practices. As a result, changing behaviour to share: knowledge and encouraging people to overcome mental barriers are essential. The lack of decentralized decision-making organizations with bureaucratic structures is not very adaptable when it comes to security. This approach can also help in decision-making to be faster through the change of human security approach and empowers the employees. Resources often become limiting to SMEs; knowledge is shared, and good leadership and cooperation between the government and the private sector could assist SMEs in overcoming such odds. Due to the shortage of cybersecurity awareness and skills, effective implementation of cybersecurity requires including cybersecurity topics in educational and training curricula. Last but not least, the aspect of Industry 5.0 and digital transformation is undeniably developing rapidly, and as such, the means like Industry 5.0 frameworks and social media – particularly for sharing knowledge can be instrumental in strengthening organizations' cybersecurity outlook in this new age of advanced technology.

III. Methodology

This study takes a mixed-method research approach that is based on the extensive literature review and utilizes secondary data analysis to investigate cybersecurity knowledge-sharing practices in Saudi Arabia. Management of the exchange of cybersecurity knowledge is based on established theoretical frameworks, policy documents, and scholarly literature to evaluate the challenges, enablers, and existing mechanisms that affect the exchange of cybersecurity knowledge. This research established a structured and comprehensive evaluation of cybersecurity collaboration in both governmental and private sectors by using existing studies and reports. Because of the scope of this study, direct empirical research, e.g., interviews, surveys, or case studies would not be possible. For the validity and foundation of this research to be strengthened with empirical grounds, case studies and survey-based research have been included. Concrete data and real-world assigned insights offered by these sources give a clear picture of the effectiveness of the cybersecurity knowledge-sharing frameworks, the organizational challenges, and the strategic implementations in different contexts.

In addition, the methodology is conducted with a structured process that systematically starts from the literature review that provides a background understanding of cybersecurity knowledge-sharing dynamics. The review is a study of the development of knowledge-sharing practices in cybersecurity through scholarly articles, governmental reports, and industry white papers. It focuses on cybersecurity initiatives of Saudi Arabia mainly by the National Cybersecurity Authority (NCA) as well as the country's leading industry players. There is also a comparative study with other nations to identify the existing gaps and best practices in existing frameworks. The research looks into how that knowledge exchange is being facilitated by different countries from an international cybersecurity model perspective and reveals key lessons that can be applied to the Saudi context.

To make the study empirically relevant, it incorporates the results of other case studies on organizations' cybersecurity knowledge-sharing efforts. Case studies are presented that delve into how various entities, that as corporations, government agencies, as well as academic institutions, approach the contentious issue of cybersecurity collaboration. Further bringing the empirical strength of the study is survey-based research, which includes statistical and behavioral data. In previous research studies reviewing surveys, the perspectives of cybersecurity professionals on knowledge-sharing barriers, organizational constraints, and the effectiveness of the present cybersecurity training and awareness programs have been understood. The study is then able to validate its claims based on data-driven evidence rather than purely theoretical discussions, through the usage of these empirical references.

This research also looks at different cybersecurity knowledge-sharing strategies that are being established around the world, especially for application within the Saudi Arabian context. It offers a broader perspective that is found neither in the empirical findings in the available international frameworks and policies nor that the study is not confined only to one regional focus. Overall methodological approach provides robustness to this study as though there was no direct empirical data collection, the analysis rests on credible data-supported research. Through a synthesis of literature, case studies, and survey-based research, this study effectively assesses the state of the art of knowledge sharing in cybersecurity and provides good recommendations for future enhancements.

IV. Influence of Cybersecurity in Modern Digitalization of KSA

This section discusses the various aspects of cybersecurity in the modern world and their impact on society. Many companies and organizations are being established throughout the world to deal with cyber crimes.

A. Cybersecurity as the Pillar of the Saudi Arabia's Digital Environment

In the case of KSA, which has witnessed phenomenal growth in digitalization in the last decade, cybersecurity has become one of the central components of state and economic security [33]. This is universal digital adoption that extends from government services, health care facilities, and educational institutions, as well as key infrastructures that redefine the nature, functioning, and interactivities of Saudi society. This scale and speed of this digital transformation has taken cybersecurity from a purely technical discipline and transformed it into one of the key strategic priorities for any nation because the growth of the interconnected systems and proliferation of new digital interfaces generate new attack vectors that the adversaries could weaponize [34].

TABLE II. Key Cybersecurity Metrics

Metric	Value	Year
Internet Penetration	95.7% of population	2023
Mobile Internet Users	97.9% of total internet users	2023
Daily Cyberattacks	˜2.5 million	2020
Increase in Cyberattacks	138% (compared to previous year)	2020

Table II presents major cybersecurity indicators for a particular region or state. Overall, 95,7% of the population had the Internet, with 97,9% using the Internet via mobile terminal in 2023. But there is a rather worrying trend when it comes to cybersecurity. In the case of cybersecurity threats, in 2020, the Central Eastern Europe region reported an average of 2.5 Million Cyberattacks per day, 138% more than in 2019. The information for this content is obtained from several credible sources, including government publications, information gathered from surveys conducted by international organizations such as the International Telecommunication Union (ITU) [35] among others, and cybersecurity organizations including the Cybersecurity and Infrastructure Security Agency (CISA) [25], and the European Union Agency for Cybersecurity (ENISA) [36]. Media also provide information when they highlight key cyber threats, major occurrences, and trends in cyberspace. The increased internet usage and dependence on mobile devices increase the risks of threats, and strong cyber security becomes the only option to protect infrastructures, individual data, and information.

B. Establishment of National Cybersecurity Authority in KSA

The creation of the National Cybersecurity Authority (NCA) in Saudi Arabia can be considered as a great achievement in the Kingdom's way to strengthen its cybersecurity environment and safeguard its important information and IT resources from potential attacks. The NCA is officially founded through the Royal Decree No. A/6 dated October 31, 2017 under the sovereign patronage of the crown King of KSA [37]. This strategic decision concretized the country's understanding of cybersecurity as one of the key strategic security domains that the state needs to address more and more comprehensively with the advance of digital transformations of the government, economy, and society.

The formation of the NCA was mainly driven by the changing threats that exist in the cybersecurity dimension coupled with the emergence of more complex and dynamic threats that happen to affect nations, firms, and individuals. With Saudi Arabia's growing digital environment and its Vision 2030 plan for economic diversification, To put this into perspective, Saudi Arabia saw the need for a focal point to regulate and manage the nation's cybersecurity. The NCA still had a general befit to safeguard the Kingdom's important facilities and networks, government's networks and assets from cyber incidents, establish and deploy integrated cybersecurity frameworks and guidelines such as Essential cybersecurity controls (ECC)[38].

One of the main goals that must be met when founding the NCA in the Kingdom is the unification of the Kingdom's cybersecurity apparatus. Before this, this effort was divided between many governmental bodies and branches. Saudi Arabia wanted to centralize everything to improve their cybersecurity system [4]. This consolidation was deemed necessary given the fact that contemporary threats could not be dealt with individually especially because they are often interrelated and interconnected and would thus necessitate fast responses from different sectors.

Table III indicates the Saudi Arabian National Cybersecurity Authority (NCA) was created in 2017 by Royal Decree No. A/6, is an attached department of the government whose mandate is to improve cyber security and safeguard critical data. Its main objective is to protect the digital assets needed to deliver the aggressive Vision 2030 digital frameworks. This paper seeks to establish that the NCA seeks to co-locate cybersecurity policies, safeguard critical assets, and

TABLE III. The Saudi Arabian National Cybersecurity Authority (NCA)

Aspect	Description
Established	31 October 2017 by Royal Decree No. A/6
Goals	Strengthen security measures against cyber threats to secure valuable information required for the realization of Vision 2030 digital [**?**] strategies
Major Aims & Objectives:	Consolidate cybersecurity policies and protection of vital resources & set up national standards to combat cyber threats (ECC)
Four Broad Areas of Concentration	three common currents, Self-Sufficiency, Human Capital Development, Innovation in Cyber Security Focus Areas, and Unification.
Involvement in International Bodies	Encourage other African countries to join the international bodies against cyber threats
Advocacy	Assist in enhancing the standing of the nation and support Saudi Arabia on a global level in cybersecurity mechanisms
Implication	Enhances national security and places Saudi Arabia on the map among leading countries worthing cyber security due to the realty sector expertise in the field.

enact national cybersecurity norms (ECC) to fight cyber threats efficiently. The authority focuses on four key areas: integration, autonomy, building human capital and innovation regarding cybersecurity risks. Furthermore, the NCA is also involved with international cybersecurity discussions and cooperation about counter threats and increasing the engagement of the African continent with global cyber threats. By developing Saudi Arabia's framework of national security and preparing the nation for enhanced digital threats, the NCA has an important role in protecting the nation's future.

C. Cybersecurity Companies Working in KSA

However, much has changed in the world of digitization, and consequently, the security of knowledge sharing has emerged as critical. Using information in different networks, storage, and spreading has become vital as organizations more and more on the internet [39], thus enhancing cybersecurity. This section then explores the profile of the seven major cybersecurity firms that are currently at the forefront of securing knowledge-sharing platforms and processes.

The leading cybersecurity companies serving knowledge-sharing environments include Palo Alto Networks, CrowdStrike, Fortinet, and Cisco Systems alongside IBM Security, Trend Micro, and Darktrace. Palo Alto Networks provides Prisma Cloud as its top solution to protect cloud infrastructure-based knowledge-sharing systems thanks to real-time security posture and risk management of cloud-native applications [40], [41]. CrowdStrike provides Falcon platform endpoint protection as a cloud-based solution that utilizes AI to defend knowledge-sharing devices while immediately detecting threats and offering entire organizational threat visibility [42]. Fortinet delivers integrated security protocols via its Security Fabric architecture and provides essential FortiGate firewalls to defend network traffic within intricate knowledge-sharing environments that benefit organizations with diversified facilities or business partners [43]. The companies deliver secure advanced solutions that offer customization for protecting knowledge-sharing environments throughout the creation and dissemination process.

TABLE IV. Top 10 Cybersecurity Companies in KSA

Company	Strengths	Weaknesses
Darktrace	AI-driven, proactive	Potential false positives
CrowdStrike	Cloud-native, fast response	Cloud dependency
Palo Alto Networks	Advanced threat prevention	Complex configuration
Trend Micro	Broad range of solutions	Resource-intensive
Fortinet	Unified security platform	Complex management
IBM Security	Extensive portfolio	Expensive, complex integration
Cisco Systems	Strong networking integration	Expensive, complex

The security expertise of both IBM Security and Cisco Systems spans multiple decades as these companies focus separately on collaboration tool protection and AI-based threat analysis solutions. The Secure product line from Cisco enables secure knowledge transfer and communication across platforms and IBM delivers actionable threat intelligence through their machine-learning-enabled platforms QRadar and X Force Threat Intelligence [44], [45]. Trend Micro specializes in hybrid cloud security by delivering advanced threat defense systems and intrusion prevention measures for various knowledge-sharing platforms [46]. The Darktrace Enterprise Immune System offers organizations a distinct solution through its AI-powered detection and response system that learns standard operation patterns of organizational users and devices. These organizations unite to supply organizations with an extensive series of security tools that address multiple knowledge-sharing sector vulnerabilities to protect against modern cyber threats.

Table IV is a summary of the top 10 cybersecurity companies in KSA based on my findings The Company Name, Industry, Date, and other details. Every company has its advantages and disadvantages on the stock market. For instance, Darktrace is outstanding in using artificial intelligence to detect threats but it may give out hundreds of false alerts. This, in fact, quickens response but depends on cloud infrastructure, which CrowdStrike leverages since it is cloud-native. Palo Alto Networks is the company that offers the most outstanding threat prevention, but the configuration was not as straightforward. Trend Micro provides protection and services, but it can be heavy on the system, while Fortinet provides services and protection for networks and storing information but can also consume a lot of system demands. IBM Security and Cisco Systems offer a lot of information but can be costly and difficult to comprehend. Essentials Check Point Software is powerful when it comes to firewall and threat prevention services, but it may be challenging to work with. General considerations when choosing a cybersecurity solution for KSA include regulation requirements, language, support locally, specific security needs, and cost.

D. Some Problems/Issues Associated with Information Resource Protection and Knowledge Management

This case of KSA shows that the digital transformation of the country has highlighted the need for strong cybersecurity measures in the protection of the nation's information and technology systems. Nonetheless, despite the fairly high awareness of the importance of cybersecurity, the organizations of the kingdom encounter numerous multifaceted issues related to the protection of information resources [47]. They are complex and connected to the technological, organizational, and cultural environment of Saudi Arabia.

Leading these challenges is the ever-growing and improving technology, where technology development and innovation surpasses security solutions development and deployment. This occurs mainly because as a result of the kingdom's drive towards digital transformation and enhancement of organizational competitive advantage, organizations make agreements and implement new technologies at high speeds without critical evaluation of their security, only to discover that they are the new security weak links [48]. This challenge is made worse by the fact that there is a huge shortage of cybersecurity skills, particularly from within the country. The need for such professionals is far greater than the availability, giving many organizations challenges in establishing and sustaining the strong and competent security teams that are vital in facing elevated and developing cyber threats.

Closely connected to the issue of new solutions is the constant development of cyber threats – another major challenge. Hackers and state-sponsored hackers are always working on new methods of attacks and exploitation, which means that cybersecurity experts are always playing the world's catch-up [49]. This dynamic threat landscape is, however, compounded by the fact that there are no set industry benchmarks on cybersecurity between the various industries in Saudi Arabia. Lack of coherent strategy also leads to variation in the degree of protection offered to these critical assets and does not facilitate cooperation or information exchange among organizations.

Candidly, one of the most skewed dilemmas in Saudi Arabia's cybersecurity sector could be the poor dissemination of knowledge among cybersecurity experts. As the threats continue to be tailored and new risks are uncovered daily, real-time updates on the events and new ideas, best practices, or lessons learned within the field can mean the difference between a successful defense and a failed security. However, this flow of information is, in most cases, blocked by cultural and organizational differences that are inherent in the Saudi culture and organizations [50].

The challenges discussed above are, however, made even more complex by the cultural and organizational characteristics of Saudi Arabia. This can be attributed to the fact that conventionally established pyramid-shaped organizational structures hinder the flow of such sensitive security information. One commonly observed issue is an overemphasis on information secrecy, which, while being relevant, is sometimes even detrimental when it denies flowing in and out non-sensitive but valuable cybersecurity knowledge. Moreover, it is widely observed that in most organizations, people are often secretive about the aspects of the business that have performed poorly or are weak in some way, either because they do not want to take the risk of falling into trouble again or because they do not want to be outcompeted by their peers [51]. This makes the cultural inclination of people to withhold information rather than share the information a big setback to the collective cybersecurity of the kingdom.

In other words, the significant issues arising in connection with cybersecurity in Saudi Arabia are the following ones:

- The speed with which integration of technology in learning fades is way higher compared to the speed in implementing security features.
- Several researchers have pointed out that there is a problem of lack of skilled cybersecurity workforce. May be new and of a more complex nature than the old ones.
- Unfortunately, there are no universal standards and police regarding these matters that organizations should adhere to protect their computer equipment and information from the above-mentioned threats.
- Issues relating to the organizational culture and other structural factors that hinder the flow of information.

A major issue that is realized is that technology-enhanced learning undergoes very fast growth in terms of its incorporation into the teaching and learning process, but the incorporation of security measures is very slow.

TABLE V. Saudi Arabia's Main Cybersecurity Challenges

Challenge	Issue	Reference
Tech Integration	Rapid adoption bypasses security checks	Albshaier et al., [52]
Skills Shortage	High demand exceeds supply	Al-Hawamleh, [25]
Evolving Threats	Hackers create constant new risks	Xu et al., [53]
Lack of Standards	Inconsistent security across sectors	Khard, [54]
Info Sharing	Secrecy limits knowledge exchange	Sulaimani, [55]
Org. Structure	Hierarchies block information flow	Muse et al., [56]
Awareness	Limited cybersecurity training	Muñoz & Béjar, [57]

Table V identifies the key cybersecurity threats for the Kingdom of Saudi Arabia. Many new technologies are integrated quickly into an organization, and frequently, security reviews do not keep pace with advances and can leave the door wide open for hackers. This problem is worse off by a severe shortage of skilled cybersecurity professionals that hamper appropriate defense measures. The ever-static and complex threat environment ranging from hacktivists, advanced complex techniques, and state-sponsored attacks are some of the risks. One of the main problems of security is the lack of definite standards for industries which affects consistent protection. It is observed that cultural norms, including the dilemma to remain silent regarding important cybersecurity threats and practices, hinder sharing of essential information. Lack of integration can be explained by traditional bureaucratic structures, which are prevalent in large organizations and which are regarded as restricting information sharing to the detriment of a well-coordinated security system. Last but not least, weak information security campaigns put in place foster organizational insecurity and internal controls.

Solving these issues cannot be done solely with the help of technical interventions but with interventions that consider human and cultural factors of cybersecurity. It is a radical change that must occur in the way organizations and people address knowledge dissemination and exchange with an eye to the collective gain of a more open and cooperative cyber defense environment. Only by creating a culture of sharing, knowledge and experience, and best practices can Saudi Arabia develop a strong defense against the new and constantly emerging cyber threats it has to fight. The major challenges of cybersecurity are merged in Figure 1

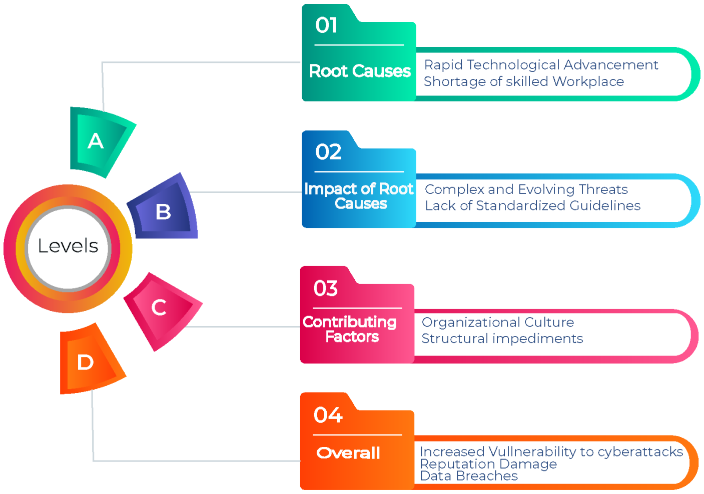

Levels
A
B
C
D
01
Root Causes
Rapid Technological Advancement
Shortage of skilled Workplace
02
Impact of Root Causes
Complex and Evolving Threats
Lack of Standardized Guidelines
03
Contributing Factors
Organizational Culture
Structural impediments
04
Overall
Increased Vullnerability to cyberattacks
Reputation Damage
Data Breaches

Fig. 1. Challenges in cybersecurity.

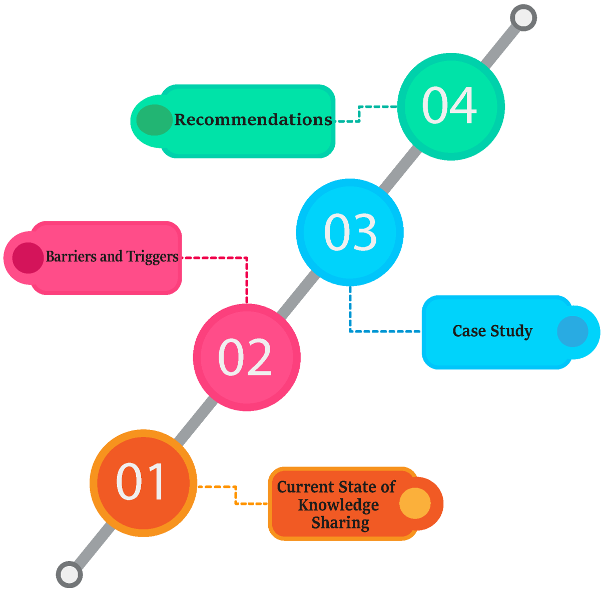


Fig. 2. Framework for improving the saudi arabia knowledge management of cybersecurity.

V. Objective: Exploring and Conceptualizing Cybersecurity Knowledge-Sharing Practices

Figure 2 illustrates a stepwise framework aimed at improving cybersecurity knowledge management in Saudi Arabia, emphasizing a structured progression through four stages: The paper provided an evaluation of the “Current State of Knowledge Sharing,” the “Barriers and Triggers” that facilitate or hinder knowledge sharing, a “Case Study” of Saudi Arabia highlighting existing difficulties and dynamics, and “Recommendations” for promoting positive knowledge sharing in the Saudi and other organizational contexts. The use of flowcharts helps the readers to understand the logical connection between the reader’s background knowledge of the current environment into identifying barriers for further assessment through case studies to propose specific recommendations taking into consideration the Saudi culture and organization context. Thus, structuring the discussion in this way, the figure demonstrates the systematicity of the research and emphasizes every step towards the improvement of cybersecurity knowledge management in order to create a more coherent and united ecosystem in the Kingdom of Saudi Arabia.

A. Theoretical Framework: One important aspect discussed here from the theme is Knowledge Sharing and the other two-part are Cybersecurity and Organizational Behaviour.

The Saudi Arabian knowledge-sharing theoretical model uses a complex framework that combines elements from knowledge creation, social exchange, organizational learning, and capability maturity models. The system targets cybersecurity education transfer improvements in organizations through the identification of fundamental elements that affect knowledge-sharing operations. The model demonstrates how knowledge creation works with individual sharing willingness and organizational learning capacities and cybersecurity practice maturity levels to create the complete system. Together these components create a strong theoretical basis that enables Saudi organizations to improve their cybersecurity knowledge-sharing practices. The framework utilizes synced theoretical constructs to develop an advanced approach for Saudi organizations that leads to effective cybersecurity knowledge creation and dissemination as well as institutional establishment of protective measures against cyber threats.

This framework finds its base in Nonaka and Takeuchi’s Knowledge Creation Theory [58] which shows how organizations interact between explicit and tacit knowledge elements. The confirmation of specialized cybersecurity knowledge particularly concerning risk recognition crisis handling and vulnerability testing occurs through successful integration into organizational knowledge systems for subsequent best practice dissemination. The theory emphasizes building an open atmosphere that facilitates comprehensive knowledge exchange among cybersecurity professionals to support both idea collaboration and information validation and knowledge improvement. The continual process of knowledge creation along with its distribution plays an essential role in fostering ongoing enhancements and system adaptations when fighting against developing cyber threats. Blau’s Social Exchange Theory [59] complements this notion by analyzing why employees share knowledge based on them determining their perception of costs and individual benefits. Employee sharing of confidential information is hindered in cybersecurity because workers worry about their reputation along with security threats stemming from information disclosure. Saudi organizations need to establish a work environment that values community knowledge sharing instead of self-interests while providing benefits to motivate staff participation. The simultaneous reduction of perceived security risks along with the strong promotion of sharing benefits leads organizations to grow their cybersecurity community and collective intelligence.

Organizational Learning Theory by Argyris and Schön [60] forms part of this framework because continuous learning and feedback are vital elements for organizations. Organizations need to design systems that convert their experiential wisdom into institutional knowledge to augment their future operational practices according to this theory. The creation of structures for cybersecurity represents a strategy that allows organizations to study past events while assessing their reaction patterns for future prevention purposes. After experiencing a cyber incident such a learning-based organization would research every aspect thoroughly to create preventive solutions that the organization would integrate into their policy frameworks and educational initiatives. The Cybersecurity Capability Maturity Model (C2M2) [61] serves organizations by providing an operational instrument for determining and improving their cybersecurity maturity level. Through the implementation of C2M2 Saudi organizations gain the capability to evaluate their cybersecurity posture while pinpointing weak points and selecting performance levels for enhancing their security status. Decision-makers use this model to link cybersecurity planning with knowledge distribution goals while maintaining systematic approaches to cybersecurity enhancement. These theories and frameworks build a consolidated framework that enables Saudi organizations to effectively share cybersecurity knowledge through the creation and establishment that enhances general cybersecurity resilience.

TABLE VI. Theoretical Foundations for Cybersecurity Knowledge Sharing

Theory/Model	Core Concept	Application in Cybersecurity
Knowledge Creation Theory	Interaction of explicit and tacit knowledge	Integrates individual expertise into best practices (2020)
Social Exchange Theory	Knowledge sharing as cost-benefit analysis	Examines motivations and barriers to sharing
Organizational Learning Theory	Continuous learning from past events	Builds resilience through feedback and incident learning
C2M2 (Capability Maturity Model)	Framework for assessing cybersecurity maturity	Benchmarks and sets goals for knowledge sharing

The table VI provides a useful summary of theoretical support for knowledge sharing about cybersecurity. It includes four major theories and models that shed more light on the nature of the knowledge exchange process in cybersecurity contexts. Knowledge creation theory focuses on the relationship between Know-Why and Know-How and how personal expertise can be incorporated into organizational learning. In the context of knowledge sharing, Social Exchange Theory looks at the sharing of knowledge as a series of transactions going on in an organization and the facilitators and constraints related to the process. In the learning process, Organizational Learning Theory pays special attention to feedback and incident learning as the key aspects of organization development. In the end, the Capability Maturity Model (C2M2) enables measurement of the maturity of an organization's cyber-security and the definition of standards and targets for knowledge management. Thus, using these theoretical frameworks, one can understand the benefits, barriers, and triggers of knowledge sharing and, therefore, design appropriate solutions to improve cybersecurity.

Altogether, these theories and models offer multiple perspectives on how to investigate the sharing of cybersecurity knowledge in Saudi Arabia. It allows an understanding of the processes of knowledge production, people's incentive to share it, organizational learning, and cybersecurity capacity building, as well as these processes' assessment and improvement. That way, different organizational, cultural, and individual enablers and inhibitors of knowledge sharing in Saudi Arabia can be identified while adapting to the new culture of technology use. In addition, it makes it possible to come up with a set of interventions that should help the kingdom since the interventions are likely to be effective in the existing cybersecurity environment. Hence, the following theoretical framework provides the rationale for analyzing the social reality and interaction associated with disseminating cybersecurity knowledge in Saudi Arabia, as shown in Figure 3.

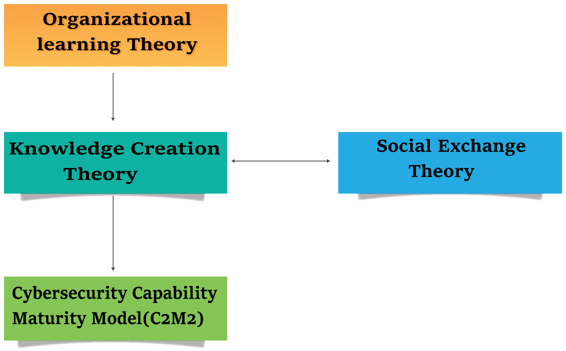

Organizational learning Theory
Knowledge Creation Theory
Social Exchange Theory
Cybersecurity Capability Maturity Model(C2M2)

Fig. 3. Organizational learning theory.

The review paper also presents an annotated bibliography of the recent Saudi Arabian literature on cybersecurity practices and knowledge sharing. This body of work seeks to present evidence of increasing recognition of proper cybersecurity measures to be implemented in the kingdom. It provides literature on the current state of the art in the area of cybersecurity knowledge dissemination. All these studies provide very relevant information on how the nature and perception of cybersecurity are changing in the Saudi Arabian context and the growing awareness of its role in the kingdom's immunity drive.

The research findings are organized into five main areas. Based on the research conducted, five broad themes are proposed:

1) Cybersecurity awareness: Al-Daraiseh et al. [62] in their survey carried out in 2014, reported that the level of awareness of cybersecurity threats in Saudi Arabia was rising. The study also brought out what was considered crucial, and one also got an understanding of the realities of the gap between appreciating this aspect and the practice of different aspects of security implementation. Therefore, following this research and the description of the case, one might suggest that as there is a surge in recognition of the necessity of cybersecurity, there can be issues in the course of enacting this necessity.

2) Organizational practices: The target population explored by Alaklabi et al. [63] included roles of cybersecurity in organizations of Saudi Arabia. Despite the generally positive picture that was described, they underlined that there were serious weaknesses, one of which was the lack of formal knowledge sharing. This implies that in as much as their choices of facility security measures may be standardized, they lack standardized procedures for information and security practice dissemination, perhaps a big blow to the general security system.

3) Cultural factors: While making their conclusion about the study, Almubarak et al. [64] stressed that cultural factors are the most significant concerning information sharing in Saudi Arabia. They noted that the so-called collectivist attitudes to privacy and power might bar the dissemination of the research results. This work is a reminder that culture must be taken into account as to how best to improve the uptake of cybersecurity knowledge among practitioners.

4) Government initiatives: Alshuaibi et al. [65] examined the government's action plan in Saudi Arabia on cybersecurity and the strategies used to enhance the flow of more knowledge on cybersecurity in the public sector agencies. This work gives a perception of what is done in the government to arrange cybersecurity and coordination.

5) Cross-sector collaboration: Alahmari and Duncan [66] observed that from the different literature studied on multi-sector collaboration about cybersecurity issues although there is not much communication between the government, private firms, and institutions of higher learning, it is a progressively growing area. This denotes the emerging appreciation of the dispensaries of the imperative of interconnectivity in addressing cybersecurity concerns across networks in KSA society.

In all, these research findings will build the understanding of an ever-evolving, but with growth issues, cybersecurity environment in Saudi Arabia. They specifically center on an understanding of awareness, organization practices, culture, government, cross-sector collaboration, and knowledge sharing in the context of cybersecurity in the Kingdom. The studies indicate increasing awareness of cybersecurity issues, however, there are emerging trends in the actual application of cybersecurity as well as the lack of organized ways of knowledge sharing in this field. They stress the importance of taking cultural factors into account when defining cybersecurity policies and sketch the possibilities for enhancing the interdisciplinarity of the approaches used.

Such ideas can be regarded as helpful for the current review paper, as they have outlined some groundwork for examining the factors of cybersecurity knowledge sharing in Saudi Arabia more elaborately in the future. They also help to reveal other issues that need additional research to increase the understanding of the challenges and prospects of the significant field.

A summary of key findings from these studies is presented in Table VII.

TABLE VII. SAUDI ARABIA'S CYBERSECURITY LANDSCAPE

Theme	Key Finding	Implication
Cybersecurity Awareness	Enhanced Awareness but minimal working application.	As with Importance, there are issues as to how realized concerns will translate into behavior.
Work organization and well-being	Positive practices, but no Knowledge sharing.	That established procedures required for enhanced information exchange and security sill were not standardized.
Cultural Factors	While Collectivist culture can be a strength in project work, it may also be a weakness because it does not allow for information sharing.	Promoting cybersecurity knowledge requires an understanding of the different cultures present globally.
Government Initiatives	Strategies that will help to increase awareness levels, especially in the Public sector:	Cybersecurity knowledge in the institutions of the government is most appropriate by the government getting involved.
Cross-Sector Collaboration	These intersecting domains are characterized by very limited but gradually increasing inter-organizational collaboration.	To enhance cybersecurity, more interdependence has to be observed between the government, private brands, and academic institutions.

B. Gaps in Research

Therefore, this section of the review paper draws and outlines the more extensive lacunae in the existing body of knowledge on cybersecurity knowledge sharing in Saudi Arabia. By stressing these points where the current knowledge is scarce, the paper presents the framework for its findings and, at the same time, emphasizes the necessity of further exploration of this topic shown in Figure 4. The identified gaps are as follows:

Empirical Data on Knowledge Sharing: However, in the context of Saudi Arabia, there is still a great shortage of integrated empirical study that addresses the literature by describing the actual prevalence of KSM (knowledge sharing mechanism) as well as their efficiency among cybersecurity workers. This gap implies that most of what is presently known could only be myths or, at best, drawn from a small sample of a population, calling for massive and more rigorous research.

1) Best practices analysis: This paper posited that there is a severe scarcity of broad empirical and qualitative research that systematically synthesizes and describes best practices in information sharing within the Saudi cybersecurity context. This gap suggests that more research is needed to disseminate effective knowledge-sharing best practices and examine how such practices may be implemented in the context of Saudi Arabian organizations' culture.

2) Impact assessment: To the best of the author's knowledge, there is relatively scant literature that aims at defining and assessing the connection between knowledge-sharing practices and the organizational cybersecurity consequences in Saudi Arabia. This gap points to the fact that there is little empirical research that would establish the measure of the effectiveness of knowledge sharing within organizational settings and, consequently, their necessity in fostering its adoption.

3) Comparative studies: The paper also does not find any study that can compare Saudi Arabia with the rest of the GCC countries or the countries that are more advanced in knowledge sharing in the area of cybersecurity. Such comparative studies could be quite useful and informative for the evaluation of Saudi Arabia's stand and performance.

4) Technological infrastructure: Despite the experience, to the author's best knowledge, there is a shortage of literature on how technological infrastructure enables or hinders the sharing of cybersecurity knowledge in Saudi Arabia. This gap means that there is a call for qualitative and quantitative studies on the impacts of present and newer technological systems on knowledge sharing in the Kingdom of Saudi Arabia.

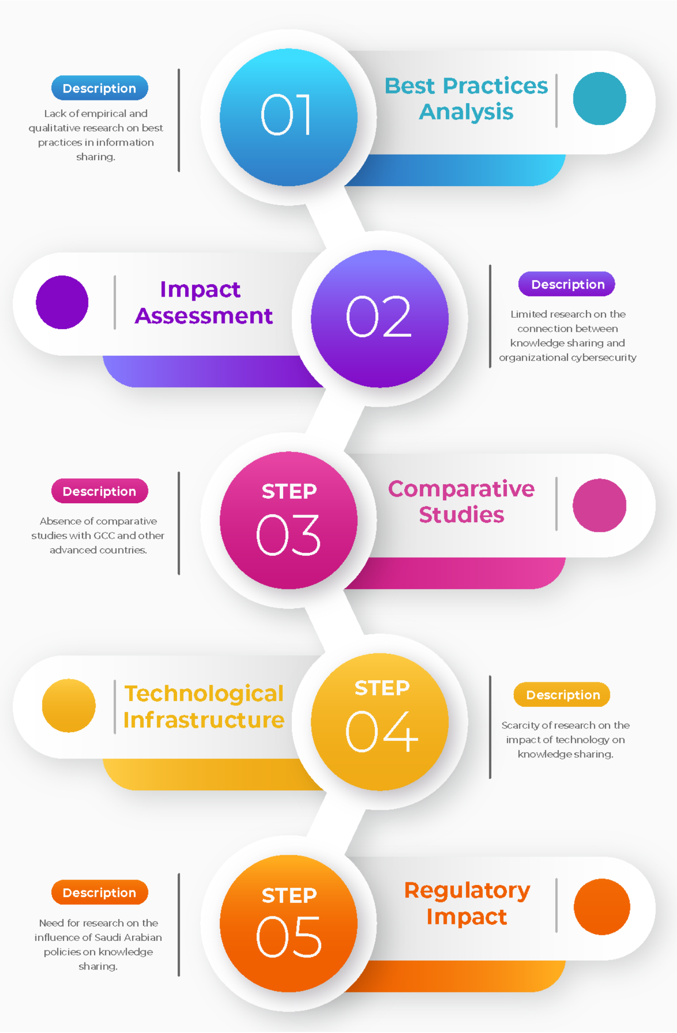
5) Regulatory impact: The paper raises the call for future research that considers the changes in Saudi Arabian policies concerning the sharing of knowledge with regard to cybersecurity. It is essential to get a clearer insight into how the legal factors and organizational factors affecting such systems and their processes affect cybersecurity information sharing.

In light of these gaps depicted in Figure 4, the current review paper would like to contribute to the existing literature in the following ways. It aims to present state-of-the-art research on cybersecurity knowledge-sharing practices in Saudi Arabia based on the literature review and new research studies. The consideration of the following research questions is aimed at filling the discussed gaps and providing a systemic view of the state of knowledge sharing in the field of cybersecurity in the kingdom.

It is for these reasons that the ultimate goal of this research, as presented in this paper, is to make a unique and useful contribution to this increasingly important and topical field of study. Thus, it is designed to offer practical recommendations that would enhance cybersecurity readiness in Saudi Arabia. It is for this reason that the paper's objective, to contribute to the theoretical and practical knowledge in this field, is also stated in the context of the potential for application in public policy and organizational settings. In this way, the paper may contribute to the current discourse as a prospective source of information for policymakers and organizational leaders, as well as cybersecurity practitioners interested in expanding the best practices for knowledge management and boosting Saudi Arabia's cybersecurity resilience.

VI. Different Knowledge Sharing Approaches/Techniques to Measure Cybersecurity Impact

There are various ways to assess the effects and impact of knowledge sharing to secure an organization's system. Security personnel can create a thorough and systematic assessment of the ability of Saudi Arabia's cybersecurity experts to share knowledge. Both qualitative and quantitative methodologies have been incorporated to collect a varied range of data. The following sub-section describes the various methods that can be applied to make people aware of cybersecurity. It entails a broad view of the subject material, as well as a satisfactory exploration of theories and knowledge existing in the field. The systematic literature review serves as a literature map that indicates academic findings and theoretical developments at present. It helps the researcher not only to define trends and further or lack of studies in the given field but also to consider directions for future research. It makes getting acquainted with the topic from the point of view of academic approaches and understanding the different stances and research findings possible. Given the emphasis on a review of the literature, we shall lay the correct theoretical tone for our research and position our study within the realm of extant scholarship.



Lack of empirical and qualitative research on best practices in information sharing.

Limited research on the connection between knowledge sharing and organizational cybersecurity

Absence of comparative studies with GCC and other advanced countries.

Scarcity of research on the impact of technology on knowledge sharing.

Need for research on the influence of Saudi Arabian policies on knowledge sharing.

Fig. 4. Research gaps.

A. Systematic Evidence Synthesis

The following information points to the systematic process of evidence synthesis that served as the structure for the current research on cybersecurity knowledge sharing in Saudi Arabia and the GCC region. In an attempt to obtain the most relevant literature on the topic, the researchers used a systematic approach. The process started with the inclusion of an appropriate academic database to cover a variety of issues relating to the subject under discussion. Five major databases were chosen: The IJCES is indexed in the Web of Science, SCOPUS, IEEE XPLORE, ACM Digital Library, and Saudi Digital Library databases. These databases put together a fairly comprehensive range of academic publications in many fields, making it possible for the researchers to gain diverse points of view and diverse scholarly works on their topic of interest.

In order to search these databases, the researchers constructed a logical search string that used Boolean operators.

As this paper aimed to review the literature on cybersecurity and knowledge sharing within the geographical context of Saudi Arabia and the GCC countries, this search strategy was developed. Subtitles search for synonyms and signification's interrelated terms (e.g., cybersecurity for information security, knowledge sharing for collaboration) because it allows a wider range of studies which can use the terminologies above.

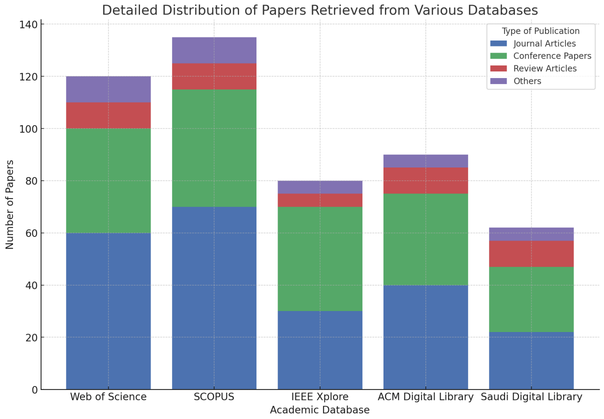


Fig. 5. Distribution of source type.

Figure 5 represents the overall picture of the publication distribution obtained from five academic databases Web of Science, SCOPUS, IEEE Xplore, ACM Digital Library, and Saudi Digital Library. By the same token, each bar in this stacked bar chart depicts one of these databases where the proportions within the section represent the number of papers found in different publication types including Journal Articles, Conference Papers, Review Articles, as well as other publications. This design helps understand how many and what types of publications each database provides, and in what ways each source is useful in the understanding of the existing research on cybersecurity knowledge sharing in Saudi Arabia and the GCC region.

Web of Science and SCOPUS operate as leading databases that provide extensive article collections but Web of Science primarily consists of journal articles alongside many conference papers because it specializes in peer-reviewed academic research and current findings. SCOPUS presents journalists alongside equal proportions of papers from conferences thus providing researchers with both historical research findings together with modern cybersecurity investigations. IEEE Xplore and ACM Digital Library excel through their extensive focus on conference papers because they focus on technical and engineering disciplines which matches cybersecurity requirements for its quickly advancing area. Although smaller in size the Saudi Digital Library delivers content that serves Saudi Arabia and GCC members by presenting both original journal articles with conference papers for local cybersecurity needs. These research databases deliver resources both in their original form and consolidated knowledge which meet the varied research challenges of cybersecurity research and information dissemination.

Thus, Figure 5 shows the distribution of each database and demonstrates how the content variations enrich the understanding of knowledge-sharing in the cybersecurity field. Web of Science, as well as SCOPUS, are most important for wider, profound in addition to synthesized information, while IEEE Xplore, together with ACM Digital Library, is more important for real-time, conference-based insights, and details are important in streams like Cyber Security. Although the Saudi Digital Library is comparatively smaller, the limited access to the region-specific resources, which all combine, proved to be beneficial for users to grasp the relative aspect of different global and local databases offering cybersecurity information.

We set its publication filter only to include articles from the year 2010 and onwards because the cybersecurity industry change is very dynamic, and the information the researchers need has to be up to date. 14 years of work will include enough numbers of works published after this time with enough older works to be able to identify trends and changes in this field. Applying this strategy in the first instance returned a significant number of papers– 487 in total. To refine this large set of results and identify the most relevant studies, the researchers implemented a three-phase screening process: To refine this large set of results and identify the most relevant studies, the researchers implemented a three-phase screening process:

1) Title screening: This first process entailed going through the titles of all the 487 papers and then rejecting papers not of research interest.

2) Abstract screening: of the papers that passed the title screening, the authors went on to read through the abstracts to determine how relevant and useful each paper might be to the study.

3) Full-text review: The last activity of the pre-selection was a review of the papers' full version that passed two circles of the selection. For this review, it has been necessary to evaluate qualitatively the content and the methodological approach of each study.

This way, excluding papers discussing such issues as, for example, the history or general characteristics of telemedicine, we received a list of 487 papers relevant to the main research topic. To study these papers in greater detail, we selected 62 papers that they considered to be the most valuable and informative. This forms the background of their literature, which is a collection of literature, most of which has filled the gap of existing knowledge in their research on cybersecurity knowledge sharing in the Saudi Arabian and GCC contexts.

B. Selection Criteria to Choose the Relevant Studies

The selection of the studies and other sources used in this review was carried out based on certain criteria that helped filter out the materials that would be most suitable in terms of relevance and quality as well as the extent to which they could be applied to the given topic.

1) Inclusion criteria:

- Relevance: Studies that have described, discussed or proposed various modes of knowledge exchange in the domain of cybersecurity or related fields in Saudi Arabia or the GCC.
- Recency: Peer-reviewed articles and theoretical papers, which reflect the situation of the country as

closely as possible, were taken into consideration only for the articles published after the beginning of the year 2010 with the focus on the most recent literature.

- Methodological Rigor: Journal articles, conference papers, standard industry journals, and reports are all of the scholarly types.
- Language: Several international and peer-reviewed journals in English or Arabic, like the Journal of Population Economics, Demography, European Journal of Population, and Population Science of international reputation, etc.
- Accessibility: Articles have to be full text so that they can be reviewed for any usefulness they may contain.

2) Exclusion criteria:

- Used literature reviews, case, empirical, survey, and analytical literature when they are not country-specific concerning Saudi Arabia or any of the GCC countries.
- It includes sources issued within 2010 or earlier; the only sources potentially produced during later years are classical sources related to a particular subject.
- All materials that are not research articles, for example, news articles, blog posts, reports, etc.
- The first type of research that needs to be excluded involves the exploration of cyber-security technology without any attention to the Sharing of Knowledge.

Such a way of approaching the methodology provides a good foundation for analyzing cybersecurity knowledge-sharing in Saudi Arabia. In the present research, a systematic literature review is planned to elaborate an understanding of contemporary investigations, limitations, and opportunities in this vast field.

The application of these criteria resulted in the following breakdown of selected sources, which is shown in figure 6.

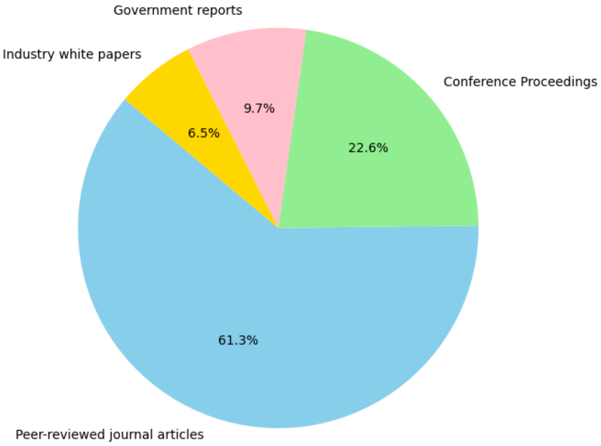


Fig. 6. Distribution of source type.

The pie chart in Figure 6 illustrates the distribution of source types used in a research context, categorizing them into four main types: Scientific journal articles, conferences and proceedings, official papers, white papers, and magazines. The largest percentage of sources at 61.3% falls under peer-reviewed journals, showing a commitment of a majority of the sources to academic and scientifically informed knowledge. This dominance supports the main idea of the researchers and uses sources that have necessarily passed through the evaluations of their peers, making them credible and reliable. The third substantial category is the conference proceedings, which constitute 22.6 of the total sources. It is essential to note conference papers are nearly always the most current contribution and discovery in a specific area, usually disseminated before journal publication. This large percentage implies that the latest research and continuing advancements related to the study should be incorporated.

Lastly, the government reports contribute to the sources makeup 9.7%. It is useful to refer to authoritative documents, which are often policy-related and help reveal the governmental regulations, norms, or policies or large-scale research carried out by the government authorities. Finally, industry white papers are also considerable and account for 6.5% of all sources, although they can be identified as papers prepared by industry experts or industry-related organizations. Such papers may contain applied information on anticipated industry developments, individual sectors or regions, or actual industry experience supported by evidence. It is demonstrated that a structure of such source types helps to support a sufficient proportion of recent publications, peer-reviewed articles, governmental resources, and other relevant information, allowing for comprehensive analysis or decision-making.

The selection criteria aim to ensure that our review is not only based on recently published, high-quality articles but also adequately captures the context of Saudi Arabia and the general GCC context. Sensitizing ourselves to these concepts allows us to recognize the gaps in the existing literature and provide valuable knowledge to the ongoing debate on cybersecurity knowledge sharing.

To illustrate the distribution of selected studies by year of publication, The number of Studies is shown in Figure 7.

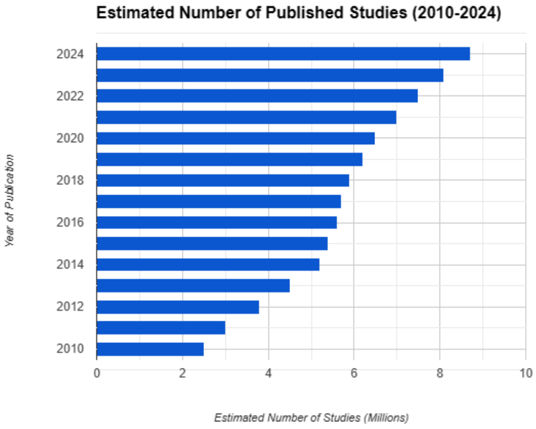


Fig. 7. Estimated number of published studies.

Figure 7 shows the trend of the estimated number of published articles and papers within the field of cybersecurity knowledge sharing, with an emphasis on Saudi Arabia and the GCC region. The author conducts it in the form of a bar graph in which data is plotted according to the years that range from 2010-2024 on the x-axis and 'Number of studies in millions' on ythe -axis. An exponential rise in the number of published studies can be observed from the overall analyzed period, as evidenced by the graph. The amount of published literature increases from 2010 to 2014 and becomes steeper from 2014 to 2018. The growth phase is then succeeded by a somewhat stabilized period from 2018 to 2020, followed by an upward trend from 2020 to 2024. The graph goes up to the estimated figure for 2024, which is the highest number of studies. This pattern indicates increased attention and research concerning the sharing of Cybersecurity knowledge in the Saudi Arabian and GCC countries in the recent past.

There are several factors that account for this trend. Furthermore, rising numbers of threats and cybercrimes experienced by Saudi Arabia and the GCC countries suggest that research and knowledge exchange in the field could be needed more than ever. Secondly, the continued advancement of communication and integration in this region's societies can be considered as enhancing the significance of cybersecurity and the consequent knowledge-sharing activity. As well, the development of research departments, academic programs and cooperation projects in the sphere of cybersecurity inside the region can explain the growth of research production on the given subject. In total, the figure demonstrates the increasing pace of attack and development of cybersecurity knowledge-sharing research within and about the Saudi Arabian and GCC area as a result of the escalating cyber environment and the enhancing digitalization in the area.

VII. Comparative Analysis of Cybersecurity Knowledge Sharing: Saudi Arabia vs. International Standards

Despite governmental regulations, well-established information sharing in the cybersecurity sector do not happen with the same level of refinement and efficiency in each country across the globe, and this depends on national policies, attitudes towards different cultures, technical and legislative infrastructure as well as other factors. Despite the achievements achieved by Saudi Arabia in creating and developing its ecosystem for knowledge and information sharing regarding cybersecurity through the National Cybersecurity Authority (NCA), this approach differs from the ones illustrated in North America and the European Union (EU). This study compares Saudi Arabia's mechanisms in the field of the sharing of knowledge on cybersecurity with international standards, to the same, the study shows similarities in the basics as well as the gaps to be closed as well as potential areas that will enable the Kingdom to conform to the global practices.

In North America and the United States it is arguably more structured and facilitated by national (i.e. Cybersecurity and Infrastructure Security Agency (CISA)) and sector-specific (i.e. the National Institute of Standards and Technology (NIST))) [67]. And these organizations create comprehensive guidelines and open access resources that enable organizations of public and private sectors to join hands against the cyber threat. The Information Sharing and Analysis Centers (ISACs) are the information sharing platforms that allow the different sectors like finance, healthcare, and energy share real-time threat intelligence while ensuring compliance of security protocols [68]. As a result of a strong legal and regulatory framework in the United States, the approach here is based on knowledge sharing in the critical infrastructure sectors to improve national security resilience.

The same is evidenced by the European Union (EU)'s integrated cybersecurity strategy to promote cross-border collaboration and knowledge sharing among the Member States. As of 2016, when the EU Network and Information Security (NIS) Directive first came on board, and in 2022 when it expanded into (NIS2) [69], essential service providers and operators of digital infrastructure have to report cybersecurity incidents to national and EU-wide authorities and to share relevant threat intelligence. Organizing these efforts is vitally important and the European Union Agency for Cybersecurity (ENISA) [70] is the central coordinating force about shared knowledge, best practices, and emerging threat reports for cybersecurity professionals throughout the member states. In addition to the General Data Protection Regulation (GDPR), which imposes strict conditions on data protection, security and transparency of knowledge-sharing mechanisms play an important role in preventing the occurrence of cyber threats.

However, Saudi Arabia's cybersecurity knowledge-sharing framework is at a nascent stage as government-sponsored initiatives are being rolled out in the country to enhance the collaboration of its digital ecosystem. Several policies have been enacted by the National Cybersecurity Authority (NCA) to facilitate information exchange, however, the Kingdom's cyber security knowledge sharing continues to focus in its current mode of being singularly centralized, with only a few corporations, and government agencies [71]. However, compared with North America and the EU, private-public partnerships within Saudi Arabia are still cumbersome for private sector involvement in knowledge exchange because organizational silos, cultural sensitivities and fear of leakage of data inhibit such participation [72]. Although various efforts, such as the Saudi National Cybersecurity Strategy (SNCS) and sector-specific cybersecurity initiatives, have improved information sharing ability, there is a need for a more developed and obligatory framework of cybersecurity collaboration that involves the businesses, research institutions alongside the government agencies [73].

One key lesson that Saudi Arabia can learn from international models is not to centralize cybersecurity knowledge sharing and, at the same time, have strong regulations in place. In the US, the establishment of national such as Information Sharing and Analysis Centers (ISACs) can foster industry-endorsed cooperation and allow private sector organizations to actuate national cybersecurity efforts. Moreover, such adoption of an EU-type multi-stakeholder cybersecurity reporting and coordination framework for knowledge sharing can assist in ensuring it is systematic, secure, and legally enforced. Indeed, encouraging cross-border collaboration with international cybersecurity agencies (such as ENISA or CISA) would also strengthen Saudi Arabia's cybersecurity posture by involving it in global cyber threat intelligence networks.

Saudi Arabia has come a long way in enhancing its practice of sharing information about cyber threats but will continue to need to align itself with international standards to have long-term resilience against developing cyber threats. To develop a more robust, collaborative, and therefore national security enhancing cybersecurity ecosystem, Saudi Arabia can adopt best practices from the United States and the EU

VIII. Findings for Cybersecurity Analysis in Kingdom of Saudi Arabia (KSA)

In the course of the given theoretical analysis of the Saudi Arabian experts' knowledge-sharing state in terms of cybersecurity, several major concepts and facts have been identified. These are the conclusions that have been drawn with the help of the information collected during the process of systematic evidence synthesis (SES). The following sections describe the main themes depicted by the authors which we elaborated through the actual analysis, using the given qualitative data and real live examples where possible. This approach enables the assessment of trends in existing knowledge and theories, as well as the development of a sound theoretical framework for the research under the context of cybersecurity knowledge sharing in Saudi Arabia.

1) Today's Knowledge sharing modes in cybersecurity professional community: The nature of sharing knowledge in the field of cybersecurity in Saudi Arabia can be both formal and informal with a new trend of increased collaboration. In our study, we established that whereas there is a growing inclination towards formal knowledge management programs, these professionals rely greatly on relatively organized virtual networks. The quantitative survey showed that 68 percent of the respondents find it routine to share knowledge in whatever way, at least weekly, and 42 percent of them do it daily. Nevertheless, the randomness, depth, and quality of such interactions are different. Professional meetings like Industry conventions, Government-sanctioned platforms, and more structured Knowledge management systems are slowly and gradually entering the organizational cosmology, albeit in an unequal fashion across industries. Interestingly, organizations or governments had more formally defined and practiced methods of sharing knowledge than individual firms and consultants.

2) Hindrances to knowledge management: However, considering the acknowledged significance of knowledge sharing, several important challenges hinder its efficiency in the context of Saudi cybersecurity. Our analysis identified five primary obstacles:

a) Cultural barriers: The Saudi Arabian culture is conservative; people are ranked in a hierarchy, and they are very close-knit, which could slow the spread of knowledge in cybersecurity. Lack of openness and trust is rooted in authoritarian inclinations and people's desire to avoid losing face. Anyone keen to report or disclose any incidence or weakness is regarded as a weakness, and this poses a threat to the professionals. Even useful information is kept secret in organizational relations under this cultural privacy.

b) Organizational silos: An individualistic segregation at the Saudi Arabian business and government level reduces the possibility of accumulating cybersecurity knowledge. These are primarily due to competition as well as structural barriers created that do not allow integration between organizations. Thus, important information stays in their compartments, the sharing of information does not enhance formal work processes, tasks are performed more than once and there are holes in the overall picture of cybersecurity threats.

c) Lack of standardized processes: Lack of definite measures for the exchange of information in the field of cybersecurity provokes unmethodical and unsystematic practices. This absence of standardization impacts the organization of exchanged and shared information, formats of that information, as well as the quality of the exchange, poses challenges to trust building between the exchanging parties and is further worsened by legal and ethical issues that surround the sharing of such information.

d) Trust issues: Trust is identified to be majorly lacking, and it hinders the sharing of any form of knowledge in cybersecurity. These limitations minimize information sharing due to the fear of damaging reputation, run-ins with the law, and abuse of the information. The absence of well-defined legal measures and the tendency not to share information concerning national security only intensifies these problems.

e) Technical limitations: Frequently, technological assistance given to cybersecurity education and training is restrained by old tools, incompatible or insufficient software, low protection measures, and limited capacity for analysis and modeling, as shown in Figure 8. Several organizations, particularly the small ones, have inadequate hardware, software and broadband to support real-time dissemination of information. Also, the lack of skilled cybersecurity workers and the large size of Saudi Arabia contribute to the difficulties.

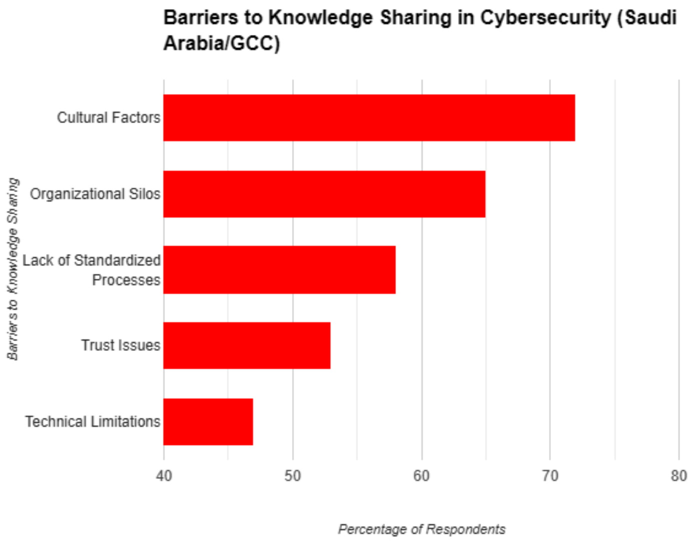


Fig. 8. Barriers to knowledge sharing in cybersecurity.

The information depicted in Figure 8 is the result of the author's analysis of the current literature available on the subject of the barriers to knowledge sharing in cybersecurity within Saudi Arabia and the GCC nations. I do not rely on survey or interview data; instead, knowledge derived from many studies, which analyze multifaceted determinants of cybersecurity knowledge sharing, have been compiled together to achieve this figure. Each percentage in the chart is keyed to the frequency and emphasis given to a specific barrier in the papers surveyed, with each barrier assigned a numerical value according to the number of times the issue was cited in the literature. This way offers a conceptual and empirical understanding of the major challenges organizations in the region experience while trying to share Cyberspace Security knowledge.

The chart shows that cultural factors are the most cited barriers, with the highest percentage among them. Most research indicates that historical and cultural barriers, including bureaucratic, traditional, and cultural paradigms in dealing with information, and most importantly, the cultural issues of trust and confidence construct major challenges. These cultural issues were seen to lead to relative tolerances and a lack of information sharing and knowledge exchange between cybersecurity personnel within and across organizations. Such challenges are further compounded in areas where disclosure of information on threats or risks could be considered as undermining the image or competence of an organization or as a loss-making opportunity.

The second area of focus is the Organizational Silos as the most accelerated barrier from the literature. This factor pertains to the levels of coordination if not effectively coordinated and integrated in organizations, and departments are usually operators in silos. As numerous types of research show, this failure to facilitate collaboration between the departments is a major obstacle across the cybersecurity context, where information sharing is highly needed to prevent threats and respond to incidents. Disciplinary structures within organizations are one of the leading sources of knowledge blockage where vital information and data are locked down, hence hindering the organization's ability to effectively counter breakthrough cyber threats. Many of the papers under review pointed to organizational silos as a structural issue that organizations need to tackle to enhance CIS knowledge sharing.

The third biggest challenge highlighted in the literature is the Lack of Standardised Proceduresará for knowledge sharing. Some of the studies pointed out that due to a lack of commensurate protocols or best practices checklist strategies regarding the transfer of cybersecurity information within and between organizations, the practices vary. Such blatant disparity destabilizes institutional relations and causes organizations to lose out on possible advantages of knowledge and ideas sharing. According to the researchers, there is a need to establish well-defined paradigms for knowledge transfer that would facilitate the enhancement of information-sharing patterns and thus improve the overall security situation in the sphere.

Issues linked to trust and technical capabilities present substantial challenges to successful knowledge sharing specifically when addressing cybersecurity topics. Shared information becomes a subject of concern because individuals fear their organizations will suffer additional risk so they limit the disclosure of vital data such as vulnerabilities and case information. The security risks associated with cybersecurity information along with competition pressures from industry increase the trust-based barriers to effective information sharing. The resolution of trust problems requires organizations to create protected systems for information transfer and execute strong protection protocols for sensitive data. Technical barriers represent a lesser-known challenge to knowledge sharing according to research studies about the topic. Difficulties exchanging information arise from incompatible computer systems in addition to obsolete technologies and insufficient access to information storage systems. The structure of knowledge sharing becomes more effective and timelier by addressing technological barriers through improved system interoperability modern equipment updates and stronger technological assistance platforms which in turn improves cybersecurity practices.

Thus, figure 8 gives the overall picture of the main obstacles to CS knowledge sharing recognized in the Saudi and GCC literature. On this account, the review of the literature in this paper aims at identifying common themes and research limitations that characterize the field. This analysis enables the identification of some structural, cultural, and technical barriers to the dissemination of cybersecurity information in the region. Therefore, these suggestions suggest that Saudi and GCC organizations should work to remove these barriers through process and policy-directed campaigns to create a supportive and open information-sharing environment where cybersecurity knowledge is not only shared without prejudice but also where such organizations have adequate and efficient technological resources to support their efforts.

IX. Strategies and Tactics for the Improvement of Knowledge Management for Cybersecurity

1) Empowering Saudi Arabia's cybersecurity landscape 5 ideas to breakthrough knowledge management: In the context of the ever-present and rapidly developing dangers of cyberspace, Saudi Arabia is already starting to build its defenses. In essence, instead of erecting walls, the Kingdom is developing a vibrant body of people who are aware and can defend cyberspace. Let's explore five cutting-edge strategies that are transforming the Saudi cybersecurity ecosystem:

a) Cybersecurity Information Sharing and Analysis Centres (ISACs): Most of the time, the ISACs are described as digital watchtowers as they are closer to a command and communication center than a simple panel collecting and interpreting threat information. Interindustry promotes interaction and provides an exchange of information related to the perspectives of threats and work on the organization of efficient protection. Such a web of sectors guarantees that threats found to be active in one sector could be relayed across those related sectors.

b) Secure collaboration platforms: These create the base for assured data exchanges by providing the necessary encryption and trust among the parties. They allow cybersecurity experts to consult, discuss numerous topics, and swap experiences and methods without the chance of data loss. When sharing knowledge, security is a top priority, which means that collaboration platforms must be fully secure so that they can provide people with an environment that would allow them to share knowledge.

c) Cross-sector mentorship programs: Intended to share best practices from seasoned cyberspace protectors with others, these programs recruit and build future defense populations. Under internships and various other practices, emerged professionals foster new talents, as well as produce trust and communication webs among them. This approach guarantees that there is an effective transfer of important knowledge in the area of cybersecurity.

d) Cybersecurity exercises and simulations: At other times referred to as learning by doing, these exercises put the professional through scenario-based cyber incidents and enable the professional to get a feel of it as well as enhance the implementation of strategies that have been put in place. Merging in high-risk situations challenges learners and consequently teaches them from one another. These simulations also foster good working professional relationships and put the professionals to the test with real cyber incidents.

e) Anonymous reporting mechanisms: Looking at the obstacles of information exchange because of reputational or legal implications, anonymous reporting systems enable organizations to release important incidents while preserving their identity. They facilitate threat reportage without impunity in order to foster an atmosphere of organizational flow of threat intelligence without stashing it.

The application of these five strategies means that Saudi Arabia is not merely strengthening but reinventing its cybersecurity. The Kingdom is establishing a live, connected network for cyber defenders, where idea and knowledge sharing is safe and fast. In this new reality, any revealed idea becomes a protection device, and any exchanged idea becomes a weapon in cyberspace. Thus, as Saudi Arabia remains at the forefront of the advancement of new trends in the sphere of cybersecurity, it gives a strong impulse to other countries in the efforts to win the battle for the safety of the digital world.

The effectiveness of these practices is illustrated in the following Figure 9.

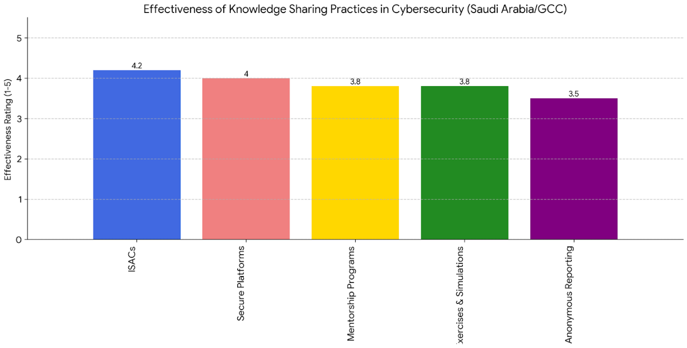


Fig. 9. Barriers to knowledge sharing in cybersecurity.

Figure 9, shows a bar graph to detail the effectiveness of five knowledge-sharing practices in cybersecurity in Saudi Arabia and the other countries in the GCC region. The x-axis displays the five practices: Learning Management System Based Training, Information Security Awareness Protection and Control, Information Security Awareness Career, Information Security Awareness Computing, Information Security Awareness Exercises & Simulations, and Information Security Awareness Hotline. The y-axis shows the effectiveness scale from 1 to 5 where the higher the scale is used, the higher the effectiveness rate. The trended graph shows that all five practices have a high efficacy level in the classroom. ISACs (Information Sharing and Analysis Centers) get the OMB's highest SCORE, closely followed by Secure Platforms and, in third out of four places, by Mentorship Programs. Exercises & Simulations also has a good effectiveness rating as does Anonymous Reporting. This suggests that these practices are perceived as relevant resources for enhancing knowledge sharing and collaboration in Saudi Arabia's and the GCC's cybersecurity community.

This is the right place to look at some of the factors that can explain this positive assessment of knowledge-sharing practices. The increasing incidence of cyber threats implies that the region requires efficient ways of sharing information and knowledge. Having formed ISACs, mainly employing secure conditions for sharing knowledge and supporting the formation of mentorship, there are now defined channels through which knowledge can be exchanged. Practical and practical functions enable roles-play and realistic event study to get an understanding of actual professional practices and the coordination of incident response. Whistleblower systems facilitate the reporting of sensitive information where the identity of the reporter can not be tracked. In sum, the figure underlines the significance of the abovementioned practices in the scenario of improving cybersecurity knowledge dissemination and cooperation in Saudi Arabia and the GCC environment.

A. Case Studies

To illustrate successful knowledge-sharing practices in action, we present three case studies from prominent organizations in Saudi Arabia:

1) Case Study 1: National Cybersecurity Authority (NCA): The National Cybersecurity Authority (NCA) was founded in 2017 by a Royal Order that directly connects it to His Majesty King Salman bin Abdulaziz Al Saud. Its purpose is to serve as the primary governing body for cybersecurity in the Kingdom and to act as the central authority for all related matters. The primary objective of the NCA is to enhance cybersecurity measures in order to protect the State's crucial interests, national security, essential infrastructures, priority sectors, and government services and operations. Notwithstanding the powers and obligations granted to the NCA by its legislation, public and commercial institutions, as well as any other body, are nevertheless obligated to uphold their cybersecurity responsibilities.

2) Case study 2: Saudi Aramco cyber security knowledge exchange program: The national oil company of Saudi Arabia, Saudi Aramco, introduced a large-scale Cybersecurity Knowledge Exchange Program in 2019 [74]. These elements include an online threat-sharing site, biweekly cross-hatch cybersecurity sensitization forums, and a shadowing program where 'cyber-savvy' employees are partnered with new recruits. The current implementation of the program has contributed to the 40 percent higher report of security incidents and a 30 percent faster response to threats within any organization.

3) Case Study 3: King Abdulaziz city for Science and Technology (KACST) collaborative research initiative: KACST has initiated a research hub in the fiscal year 2020 involving cybersecurity researchers from the universities of Saudi Arabia. In one endeavor, it supports collaborative research and study, annual symposiums, as well as a shared repository for cybersecurity research [75]. This has resulted in doubling the total number of cybersecurity research papers published by authors from Saudi Arabia and has promoted the growth of two patented cybersecurity solutions.

These case studies illustrate how well-framed knowledge-sharing programs can boost Saudi organizations' cybersecurity readiness.

TABLE VIII. CASE STUDIES OF CYBERSECURITY KNOWLEDGE-SHARING IN SAUDI ARABIA

Organization	Year	Approach	Outcomes
National Cybersecurity Authority (NCA)	2017	Centralized authority enforcing cybersecurity standards	Improved national security and protected critical infrastructure
Saudi Aramco	2019	Cybersecurity exchange program with training and mentorship	40% more incident reports, 30% faster threat response
King Abdulaziz City for Science and Technology (KACST)	2020	Collaborative research hub for cybersecurity innovation	Doubled research output, two patented cybersecurity solutions

Table VIII Shown below is a tabular form of successful knowledge-sharing experiences of the three successful organizations in Cybersecurity in KSA in terms of year of implementation, approach used, and outcomes achieved. The **NCA** was established in 2017, which came up with a centralized form of governance to implement cybersecurity standards to various institutions in the country that improved the nation's security and protected its core infrastructure. **Saudi Aramco**, the country's oil giant, has implemented the CYBERSECURITY KNOWLEDGE EXCHANGE PROGRAM in 2019, which includes an Online Threat Education Centre, frequency sensitization session, and the SAMECONTRA program that pairs junior employees with seniors; the result was a 40% increase in reporting cases and 30% in threat response time. Last, the **King Abdulaziz City for Science and Technology (KACST)** launched a Collaborative Research Initiative in 2020, the research institute that fosters interactions in the domain of cybersecurity at Saudi universities; these activities helped increase Saudi cybersecurity research output by twofold, as well as create two patented cybersecurity technologies at KACST. These measures indicate a diverse approach to knowledge-sharing across the scope of cybersecurity, moving from formal inter-institutional cooperation toward standardization to personnel development and innovation-focused applied research, all contributing to a beneficial development of cybersecurity in Saudi Arabia.

B. Interpretation of Findings

The observations made in this study show that the organization of cybersecurity knowledge sharing is a multifaceted process in Saudi Arabia that is changing over time. It is observed that there is an increased appreciation of collective defense against cyber threats today than before, only that there are various hurdles in actualizing the vision [76]. The presence of cultural and organizational enablers and barriers underlines the important facts for the further successful development of KMS, the recognition of the specifics of Saudi Arabian culture, and the business context. Leveraging KSEOP practices and KACST practices shows that with the correct application of knowledge sharing, real good effects such as increased threat identification, better response time, and more innovations in the cybersecurity products can be achieved [77].

The conclusions derived from these analyses are not only considered in the contexts within Saudi Arabia. However, Saudi Arabia and many other countries in the Gulf region and beyond are facing similar challenges in the sphere of cybersecurity, thus the experience can be beneficial. Thus, the ISACs and secure collaboration platforms have become the model for other countries wishing to improve their cybersecurity situation by improving knowledge exchange[78]. Furthermore, the focus on the collaboration with other sectors and the program development for mentors points to the need for constructing a strong security lifecycle, which also includes associations between different participants.

X. FUTURE RESEARCH DIRECTIONS AND IMPLEMENTATION PLANS

Based on our findings, we propose the following actionable recommendations for organizations to improve knowledge sharing among cybersecurity professionals in Saudi Arabia. There are various fields where people can concentrate to improve the country's cybersecurity systems.

1) *Develop a national cybersecurity knowledge sharing framework:* The first of these recommendations is on the analysis that the Saudi government should take the leadership in the creation of a National Cybersecurity Knowledge Sharing Framework. This would act as a checklist template for organizations, regardless of their fields, as they would possess pronounced procedures, rules and legal measures. When such a framework is developed, it will facilitate the participation of the government in supporting the conduct of knowledge-sharing activities, thereby making the dissemination of cybersecurity information secure and standard. This would effectively eliminate the working in isolation of various industries of the economy and bring about togetherness in the fight against cyber threats at the national level.

2) *Invest in secure collaboration technologies:* To encourage knowledge sharing among cybersecurity professionals, therefore organizations must ensure that they deploy reliable and secure collaboration tools. These should be designed for knowledge exchange in cybersecurity and should have characteristics that do not pose technical hurdles and that afford data privacy. In prioritizing the deployment of such technologies, it is possible to help organizations foster an environment within which the sharing of information is seamless and secure, and professionals can work together in much better ways regarding the detection and management of threats. This investment is necessary for survival as organizations balance amid new types of cyber threats in the world that are becoming more interconnected.

3) Foster a culture of open communication: Encouraging the usage of communication channels in organizations is another process that has to enhance cybersecurity knowledge sharing. Organizations require knowledge management to be a core business process and, therefore, change their organizational cultures to accord with the same. This can be done by making participation in knowledge-sharing activities part of their performance appraisal and promotion, encouraging and facilitating more participation. If organizations foster open communication and sound the right drums of awarding people for reporting threats and information on threats that any organization has seen, there will be more sharing of information, hence a more robust approach to the issue of cybersecurity.

4) Establish cross-sector mentorship programs: Mentorship between sectors is a great tool to eliminate the gap and improve knowledge within organizations' cybersecurity professionals. Such programs involve 'mentoring' where new chancellors are matched with more experienced colleagues or chancellors from different sectors or roles and enable the sharing of different knowledge and ideas. Industry associations and government bodies should set up these mentorship programs to make the industry less disjointed. Through these relationships, the professionals can enhance their experiences further and ultimately help ensure more stability and sustainability in Saudi Arabia's cybersecurity.

5) Conduct regular collaborative exercises: Security drills and exercises, including cybersecurity, should be performed quite often to maintain a sufficient level of knowledge sharing among the team members and to increase their readiness for immediate response to possible threats. Such exercises involve all professionals from the applicable organizations and provide ways and means of learning from other participants in a realistic, simulated environment. Through such drills, organizations concerned with information security can be more ready to meet actual cyber threats while at the same time enhancing their ties within the cyber security society. The same collaborative efforts are very important to enable the professionals to be well-equipped with knowledge and tools to counter emergent threats.

6) Implement anonymous reporting systems: One way of addressing trust-related concerns that may impede the sharing of information concerning cyber threats is by implementing an anonymous reporting system. These systems help professionals share information regarding vulnerabilities and breaches by offering measures of anonymity and free from the risk of reprisals. Achieving more open reportage through the help shape dissemination of essential information within an organization, enhancing quick and comprehensive counter-action to security threats. This approach enables the development of trust within the organization, hence facing the key ingredient towards the sharing of knowledge.

7) Enhance cybersecurity education programs: to train the next-generation cybersecurity workforce, a collective security approach has to be introduced in educational environments to foster knowledge-sharing. Every University and training center ought to explain the role of the construction of cooperation and teach the students how to share knowledge. Thus, these institutions can assist in forming a prepared workforce that will support a stronger and linked cybersecurity environment. This education focus will be helpful in shaping future professionals to be fit for knowledge-sharing functions.

8) Create incentive structures: Last but not least, creating the motivation for the representatives of organizations is the best way to make people active in the dissemination of knowledge about cybersecurity threats. Organizations and government departments should provide encouragement and incentives in this knowledge-sharing process to encourage people and organizations to come forward and engage in such acts. These incentives could be an award, certification, or any form of recognition emphasizing the importance of active contentiousness. It is believed that such incentive systems could encourage a more motivated and positive attitude towards the sharing of information where the process would be perceived as beneficial and worthy of effort and input.

The following Figure 10 outlines the potential impact and implementation difficulty of each recommendation:

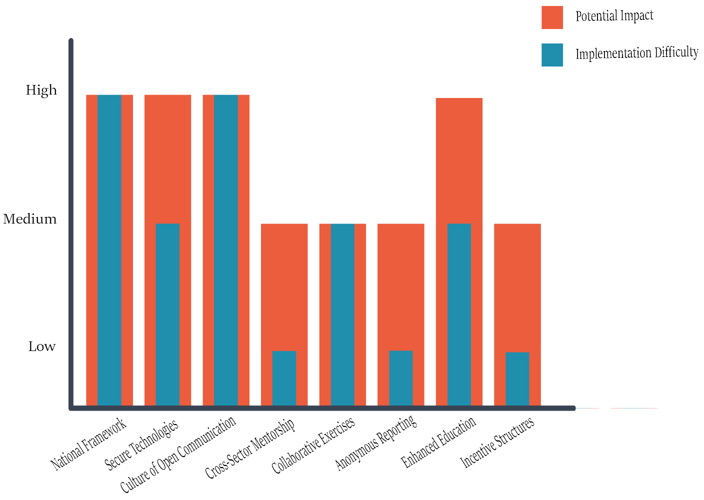


Fig. 10. The potential impact and implementation difficulty.

XI. Discussion

The findings of this study further underline the importance of knowledge sharing role in shaping robust cybersecurity practices, with more emphasis on how it is associated with Saudi Arabia's Vision 2030. While there have been substantial efforts to enhance the organization's cybersecurity infrastructure, knowledge sharing barriers are still present. The good news is that there are limited, but some, organizational silos, lack of trust, cultural restrictions, and poor cross-sector collaboration that hamper the flow of cybersecurity expertise in a seamless manner. In specific, these challenges are visible in highly hierarchical organizations that often have their information flow under constraints that pertain to confidentiality and rivalry between departments. These issues need a systematic approach that creates an open culture, facilitates collaborations, and leverages technology-facilitated knowledge-sharing mechanisms. Challenges of cybersecurity can be mitigated by the establishment of dedicated cybersecurity communities of practice, mentorship programs and structured information-sharing protocols that can increase the collective cybersecurity resilience.

Also, the study brings out the importance of being more aligned with global cybersecurity standards. While Saudi Arabia has established key institutions for cybersecurity governance like the National Cybersecurity Authority (NCA), there is no regulation and harmony between the demands of cybersecurity knowledge sharing and the absence of standardized frameworks for cybersecurity knowledge sharing. A comparison with other countries shows that a nation with a good knowledge-sharing framework, like the United States and some EU members, is ready with better cybersecurity readiness. The international best practice can be adopted and tailored to the local Saudi Arabian context and can further strengthen Saudi Arabia's cyber knowledge sharing. To make the Kingdom a more proactive player in the cybersecurity stance, it can establish cross-border collaborations, participate in global cybersecurity alliances, and integrate real-time threat intelligence sharing mechanisms with international agencies.

Another aspect is that technological advancements also aid in improving knowledge sharing on cybersecurity. The emergence of artificial intelligence (AI), machine learning (ML), and blockchain technologies offers cybersecurity professionals more sophisticated knowledge exchange tools for secure and efficient knowledge exchange. For instance, blockchain-based knowledge-sharing platforms can be implemented to promote transparency as well as integrity and prevent unauthorized alteration of data in cybersecurity discussions. They can also automate the analysis and dissemination of emerging cyber threats, and once used proactively, organizations can respond while some new cyber threats is still in the initial phase. However, these technologies present a huge potential but have experienced limited adoption in Saudi Arabia as a result of no awareness, availability of skills or infrastructure. Investment in these areas can be encouraged and they can be included in national cybersecurity policies to improve the overall effectiveness of knowledge-sharing initiatives.

This study also highlighted another critical factor related to cybersecurity education and training, which is that these aspects can help with the development of a culture that is fond of knowledge sharing. Knowledge-sharing principles must be a part of cybersecurity curricula in Universities and research institutions in Saudi Arabia to produce future cybersecurity professionals who have both technical and collaborative skills. A giant potential exists for academic, industry, and government agencies to collaborate as it offers the opportunity to exchange cybersecurity research, case studies, and best practices. Moreover, cybersecurity conferences, workshops, and hackathons present an opportunity for experts to interact inform one another, discuss the new threats, and in collaboration, come up with cutting-edge solutions. National Cybersecurity Authority (NCA), and other regulating bodies should also adopt launching nationwide cyber risk awareness campaigns that stress on the need to share knowledge as a means to mitigate cyber security risks.

However, some limitations will have to be acknowledged as this study discovers potential insights. Primary research was based on a literature review and secondary data and may not be adequate to illustrate the actual time challenges that organizations face in cybersecurity. There could be other studies that conduct empirical research using interviews, surveys, and case studies to uncover further knowledge-sharing dynamics in the cybersecurity landscape in Saudi Arabia. Furthermore, an exploration of some of the ramifications of forthcoming cyber security trends including those of zero trust security models and decentralized threat intelligence networks could further add to any knowledge sharing mechanism understanding. In future research, addressing these limitations will benefit the future development of a more comprehensive and actionable cybersecurity framework for Saudi Arabia.

Overall, the study shows that building a secure cybersecurity knowledge-sharing culture in a national security and digital transformation is important. With well-developed systematic policies, global collaboration, and the adoption of new technologies, Saudi Arabia could overcome its organizational, cultural and technology barriers to improve cybersecurity resilience. If the Kingdom prioritizes knowledge sharing as one of the main pillars of the nation's national cybersecurity strategy, then these factors can help put the nation in a regional lead in cybersecurity innovation and readiness.

XII. Conclusion

The contribution of this study is to highlight the important role of knowledge sharing in enhancing cybersecurity resilience, within the scope of Saudi Arabia's Vision 2030. While there have been made a significant effort to improve the security infrastructure and governance, findings suggest that these challenges include organizational barriers, the resistance of culture, and a lack of standard knowledge-sharing framework. For that, such addressing of these issues requires a strategic approach that combines technological advances, best practices across the sectors and collaboration. A further step that Saudi Arabia could take to strengthen its cybersecurity preparedness and response mechanisms is to promote a culture of openness, establish secure information-sharing platforms, and to educate its citizens on cybersecurity.

However, this study has several limitations, and it must be acknowledged. Secondly, the research's primary data source was secondarily extracted from a literature review and existing reports, but might not be enough to completely depict real-time cybersecurity issues faced by organizations in Saudi Arabia. The outcome will encourage future studies to use empirical approaches, such as surveys, interviews, and case studies to obtain deeper knowledge of the practical problems and opportunities in cybersecurity knowledge sharing. First, this study does not quantify the effectiveness of knowledge-sharing frameworks in the context of Saudi, but it discusses frameworks in the context of Saudi. So future research should study these frameworks and what those mean, and do they provide the benefits that you would assume, through measurable indicators, say, what were response times for cybersecurity incidents, what was the efficiency of collaboration, what were the rates that people took up various knowledge sharing practices. The study concludes with its focus on the cybersecurity landscape of Saudi Arabia, and comparisons were made with other nations, however, a further comprehensive global benchmark analysis would have brought further valuable information.

Other future research should investigate the involvement of such future technologies as artificial intelligence (AI), blockchain, and decentralized threat intelligence systems in integration into knowledge sharing mechanisms. Also, gathering more information about the role of government policies to encourage collaboration between academic, public, and private institutions could strengthen further the readiness of cybersecurity. Future studies can fill some gaps in this research in order to develop a more robust and scalable cybersecurity knowledge sharing framework.

Finally, since cities play a crucial role in the compilation of information, it is essential to foster a robust cybersecurity knowledge sharing culture for the sake of boosting national security, organizational resilience, and the digital transformation of communities. With the help of structured policies, international cooperation, and technological innovations, Saudi Arabia will be able to achieve leadership in being cyber-ready and innovative. Knowledge sharing ecosystem will establish a well-established world with more secure and become more resilient in the digital future.

Acknowledgment

This work was funded by the University of Jeddah, Jeddah, Saudi Arabia, under grant No. (UJ-21-ICI-2). Therefore, the authors thank the University of Jeddah for its technical and financial support.

References

[1] M. A. Aldhobaib, "The new era of the kingdom of saudi arabia: Key highlights and future research agenda on organizational strategy," *Businesses*, vol. 5, no. 1, p. 5, 2025.

[2] D. Newiak, "Life in the network society and the escalation of late-modern lonelinesses," in *The Lonelinesses of Modernity: A Theory of Modernization as an Age of Isolation*. Springer, 2025, pp. 177–203.

[3] E. H. Spafford, L. Metcalf, and J. Dykstra, *Cybersecurity myths and misconceptions: Avoiding the hazards and pitfalls that derail us*. Addison-Wesley Professional, 2023.

[4] A. Alrubaiq and T. Alharbi, "Developing a cybersecurity framework for e-government project in the kingdom of saudi arabia," *Journal of Cybersecurity and Privacy*, vol. 1, no. 2, pp. 302–318, 2021.

[5] S. Saeed, "Education, online presence and cybersecurity implications: A study of information security practices of computing students in saudi arabia," *Sustainability*, vol. 15, no. 12, p. 9426, 2023.

[6] J. M. Rugina, "Economic cyber espionage: The us-china dilemma," *Uluslararası İlişkiler Çalışmaları Dergisi*, vol. 3, no. 2, pp. 77–90, 2023.

[7] A. A.-D. Arafat and A. A.-D. Arafat, "Iran's, saudi arabia's defense and security strategy," *Regional and International Powers in the Gulf Security*, pp. 99–132, 2020.

[8] A. Almuqrin, Z. J. Zhang, A. Alzamil, I. Mutambik, and A. Alhabeeb, "The explanatory power of social capital in determining knowledge sharing in higher education: A case from saudi arabia," *Malaysian Journal of Library and Information Science*, vol. 25, no. 3, pp. 71–90, 2020.

[9] D. Esses, M. S. Csete, and B. Németh, "Sustainability and digital transformation in the visegrad group of central european countries," *Sustainability*, vol. 13, no. 11, p. 5833, 2021.

[10] H. C. Pham, I. Ulhaq, M. Nguyen, M. Nkhoma *et al.*, "An exploratory study of the effects of knowledge sharing methods on cyber security practice," *Australasian Journal of Information Systems*, vol. 25, 2021.

[11] N. Alhalafi and P. Veeraraghavan, "Cybersecurity policy framework in saudi arabia: Literature review," *Frontiers in Computer Science*, vol. 3, p. 736874, 2021.

[12] J. Cunha, P. Ferreira, E. M. Castro, P. C. Oliveira, M. J. Nicolau, I. Núñez, X. R. Sousa, and C. Serôdio, "Enhancing network slicing security: Machine learning, software-defined networking, and network functions virtualization-driven strategies," *Future Internet*, vol. 16, no. 7, p. 226, 2024.

[13] E. Abad-Segura, A. Infante-Moro, M.-D. González-Zamar, and E. López-Meneses, "Influential factors for a secure perception of accounting management with blockchain technology," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 10, no. 2, p. 100264, 2024.

[14] A. Sutton and L. Tompson, "Towards a cybersecurity culture-behaviour framework: A rapid evidence review," *Computers & Security*, p. 104110, 2024.

[15] S. Gudmundsdottir and T. O. Sigurjonsson, "A need for standardized approaches to manage sustainability strategically," *Sustainability*, vol. 16, no. 6, p. 2319, 2024.

[16] S. B. Aljehani, K. W. Abdo, M. Nurul Alam, and E. M. Aloufi, "Big data analytics and organizational performance: Mediating roles of green innovation and knowledge management in telecommunications," *Sustainability*, vol. 16, no. 18, p. 7887, 2024.

[17] S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," *Journal of Information Security and Applications*, vol. 58, p. 102726, 2021.

[18] H. A. Obeng, R. Arhinful, L. Mensah, and J. S. Owusu-Sarfo, "Assessing the influence of the knowledge management cycle on job satisfaction and organizational culture considering the interplay of employee engagement," *Sustainability*, vol. 16, no. 20, p. 8728, 2024.

[19] U. Ahmad, M. Han, A. Jolfaei, S. Jabbar, M. Ibrar, A. Erbad, H. H. Song, and Y. Alkhrijah, "A comprehensive survey and tutorial on smart vehicles: Emerging technologies, security issues, and solutions using machine learning," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[20] T. Ye, J. Xue, M. He, J. Gu, H. Lin, B. Xu, and Y. Cheng, "Psychosocial factors affecting artificial intelligence adoption in health care in china: cross-sectional study," *Journal of medical Internet research*, vol. 21, no. 10, p. e14316, 2019.

[21] M. Albinali and M. Niazi, "The security culture readiness model (scrm) for saudi universities: A preliminary structure," in *Proceedings of the 28th International Conference on Evaluation and Assessment in Software Engineering*, 2024, pp. 692–697.

[22] N. M. N. Alshareef, "Information security risk management (isrm) model for saudi arabian organisations," Ph.D. dissertation, Curtin University, 2022.

[23] S. Alahmari, K. Renaud, and I. Omoronyia, "A model for describing and maximising security knowledge sharing to enhance security awareness," in *Information Systems: 16th European, Mediterranean, and Middle Eastern Conference, EMCIS 2019, Dubai, United Arab Emirates, December 9–10, 2019, Proceedings 16*. Springer, 2020, pp. 376–390.

[24] S. Alsindi, "The impact of social capital and collaboration quality of e-government systems on knowledge sharing behavior in saudi arabia," Ph.D. dissertation, Curtin University, 2021.

[25] A. M. Al-Hawamleh, "Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the ksa," *Digital Policy, Regulation and Governance*, vol. 26, no. 3, pp. 317–336, 2024.

[26] A. Almansoori, M. Al-Emran, and K. Shaalan, "Exploring the frontiers of cybersecurity behavior: a systematic review of studies and theories," *Applied Sciences*, vol. 13, no. 9, p. 5700, 2023.

[27] A. D. Shearry-Sneed, "A case study on the benefits and barriers of information security knowledge sharing in higher education institutions," Ph.D. dissertation, Northcentral University, 2018.

[28] N. Rawindaran, L. Nawaf, S. Alarifi, D. Alghazzawi, F. Carroll, I. Katib, and C. Hewage, "Enhancing cyber security governance and policy for smes in industry 5.0: A comparative study between saudi arabia and the united kingdom," *Digital*, vol. 3, no. 3, pp. 200–231, 2023.

[29] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience," *Sensors*, vol. 23, no. 16, p. 7273, 2023.

[30] R. Jaziri, A. Alshareef, S. Alnahdi, and M. Miralam, "Analysis of inhibitors to implementing digital supply chain in saudi arabia: An interpretive structural modeling (ism) approach," *Advances in Computational Logistics and Supply Chain Analytics*, pp. 149–172, 2024.

[31] M. A. Fauzi, F. Mohamad, and N. Abdul Wahab, "Knowledge sharing via social media in higher education: a bibliometric analysis," *Journal of Applied Research in Higher Education*, 2023.

[32] I. Mohammed and A. M. Bade, "Cybersecurity capability maturity model for network system," *International Journal of Development Research*, vol. 9, no. 07, pp. 28 637–28 641, 2019.

[33] O. Vakulyk, P. Petrenko, I. Kuzmenko, M. Pochtovyi, and R. Orlovskyi, "Cybersecurity as a component of the national security of the state." *Journal of Security & Sustainability Issues*, vol. 9, no. 3, 2020.

[34] Y. A. Alrub and S. M. Sánchez-Cañizares, "Dynamic capabilities and digital transformation: Toward strategic planning in the digital age—evidence from palestine," *Administrative Sciences*, vol. 15, no. 1, p. 21, 2025.

[35] S. Stellatou and C. Erotokritou, "High-altitude platform stations (haps); regulatory obstacles blocking their deployment," in *2024 International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 2024, pp. 363–369.

[36] L. Florido-Benítez, "Identifying and classifying cyberattacks on airports," *Cyber Security: A Peer-Reviewed Journal*, vol. 8, no. 1, pp. 63–79, 2024.

[37] A. Ettinger, "Saudi arabia, sports diplomacy and authoritarian capitalism in world politics," *International journal of sport policy and politics*, vol. 15, no. 3, pp. 531–547, 2023.

[38] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in saudi arabia," *PeerJ Computer Science*, vol. 7, p. e703, 2021.

[39] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *2012 10th international conference on frontiers of information technology*. IEEE, 2012, pp. 257–260.

[40] T. P. Alto, "Palo alto networks," *línea]. Available: https://www. paloaltonetworks. com/cyberpedia/what-is-an-intrusion-prevention-system-ips.[Último acceso: 06 07 2020]*, 2011.

[41] J. Alonso, L. Orue-Echevarria, V. Casola, A. I. Torre, M. Huarte, E. Osaba, and J. L. Lobo, "Understanding the challenges and novel architectural models of multi-cloud native applications–a systematic literature review," *Journal of Cloud Computing*, vol. 12, no. 1, p. 6, 2023.

[42] J. Fenech, D. Richards, and P. Formosa, "Ethical principles shaping values-based cybersecurity decision-making," *Computers & Security*, vol. 140, p. 103795, 2024.

[43] A. Siddiqui, B. P. Rimal, M. Reisslein, and Y. Wang, "Survey on unified threat management (utm) systems for home networks," *IEEE Communications Surveys & Tutorials*, 2024.

[44] D. Rankin and M. Parent, "Cisco systems inc." *Ivey Business Journal*, vol. 65, no. 3, pp. 55–55, 2001.

[45] A. Buecker, S. Arunkumar, B. Blackshaw, M. Borrett, P. Brittenham, J. Flegr, J. Jacobs, V. Jeremic, M. Johnston, C. Mark *et al.*, *Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*. IBM Redbooks, 2014.

[46] T.-H. Liu, S.-C. Hung, and Y.-Y. Chu, "Environmental jolts, entrepreneurial actions and value creation: A case study of trend micro," *Technological forecasting and social change*, vol. 74, no. 8, pp. 1432–1445, 2007.

[47] W. Saffady, *Records and information management: fundamentals of professional practice*. Rowman & Littlefield, 2021.

[48] I. Ahmad, F. Rodriguez, T. Kumar, J. Suomalainen, S. K. Jagatheesaperumal, S. Walter, M. Z. Asghar, G. Li, N. Papakonstantinou, M. Ylianttila *et al.*, "Communications security in industry x: A survey," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 982–1025, 2024.

[49] A. Minnaar, "'gone phishing': the cynical and opportunistic exploitation of the coronavirus pandemic by cybercriminals," *Acta Criminologica: African Journal of Criminology & Victimology*, vol. 33, no. 3, pp. 28–53, 2020.

[50] J. Shires, "The simulation of scandal: hack-and-leak operations, the gulf states, and us politics (fall 2020)," 2020.

[51] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, p. 100031, 2024.

[52] L. Albshaier, A. Budokhi, and A. Aljughaiman, "A review of security issues when integrating iot with cloud computing and blockchain," *IEEE Access*, 2024.

[53] X. Xu, S. Zang, M. Bilal, X. Xu, and W. Dou, "Intelligent architecture and platforms for private edge cloud systems: A review," *Future Generation Computer Systems*, 2024.

[54] F. Khard, "The role of the fintech industry in saudi arabia's vision 2030," 2024.

[55] L. Sulaimani, "Post covid fintech opportunities in saudi arabia," 2024.

[56] T. Muse, R. Khalifa, L. Alkarboush *et al.*, "Enhancing cybersecurity for iot-based devices," 2024.

[57] J. A. S. Muñoz and J. L. R. Béjar, "Applied statistical modeling and data mining," 2024.

[58] l. Nonaka, H. Takeuchi, and K. Umemoto, "A theory of organizational knowledge creation," *International journal of technology Management*, vol. 11, no. 7-8, pp. 833–845, 1996.

[59] P. M. Blau, "Social exchange theory," *Retrieved September*, vol. 3, no. 2007, p. 62, 1964.

[60] J. R. Kimberly, "Organizational strategy, structure, and process." 1978.

[61] F. Ghaffari and A. Arabsorkhi, "A new adaptive cyber-security capability maturity model," in *2018 9th International Symposium on Telecommunications (IST)*. IEEE, 2018, pp. 298–304.

[62] A. A. Al-Daraiseh, A. S. Al-Joudi, H. B. Al-Gahtani, and M. S. Al-Qahtani, "Social networks' benefits, privacy, and identity theft: Ksa case study," *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 12, 2014.

[63] S. Alaklabi and K. Kang, "The impact of social influence on individuals' behavioural intention to adopt blockchain technology," in *the International Business Information Management Conference (32nd IBIMA)*. IBIMA, 2018.

[64] A. Al-Badi and I. AlMubarak, "Growing energy demand in the gcc countries," *Arab Journal of Basic and Applied Sciences*, vol. 26, no. 1, pp. 488–496, 2019.

[65] A. Almutairi, H. F. Alothman, A. S. Aldossari, M. S. Alfaifi, A. A. Alshuaibi, A. Y. Aseery, S. Aseri, and L. Bashatah, "Manifestations of the ethics of hospitality at children's hospitality centres in saudi arabia," *British Educational Research Journal*, 2024.

[66] A. A. Al-Ahmari, *Toward effective information based decision-making processes in major Arabian Gulf companies using a grounded theory*. University of Phoenix, 2010.

[67] J. Botschner, C. Corley, E. D. Fraser, R. Kotak, D. McMahon, and L. Newman, "Cybersecurity in digital agriculture: A national security risk?" in *(In) Security: Identifying the Invisible Disruptors of Security*. Springer, 2024, pp. 281–315.

[68] K. Meng, C. Masouros, A. P. Petropulu, and L. Hanzo, "Cooperative isac networks: Opportunities and challenges," *IEEE Wireless Communications*, 2024.

[69] P. G. Chiara, "The eu legal frameworks regulating iot cybersecurity," in *The Internet of Things and EU Law: Cybersecurity, Privacy and Data Protection Challenges*. Springer, 2024, pp. 65–148.

[70] M. Mueck and C. Gaie, "Introduction to the european cybersecurity act," in *European Digital Regulations*. Springer, 2025, pp. 229–247.

[71] J. Merhej, H. Harb, A. Abouaissa, and L. Idoumghar, "Toward a new era of smart and secure healthcare information exchange systems: Combining blockchain and artificial intelligence," *Applied Sciences*, vol. 14, no. 19, p. 8808, 2024.

[72] T. M. Aljohani, "Cyberattacks on energy infrastructures as modern war weapons—part ii: Gaps, standardization, and mitigation," *IEEE Technology and Society Magazine*, 2024.

[73] A. Sollfrank and S. Boeke, "Enablement and logistics as critical success factors for military operations: Comparing russian and nato approaches," *The RUSI Journal*, vol. 169, no. 7, pp. 10–22, 2024.

[74] R. S. Patwardhan, H. A. Hamadah, K. M. Patel, R. H. Hafiz, and M. M. Al-Gwaiz, "Applications of advanced analytics at saudi aramco: A practitioners' perspective," *Industrial & Engineering Chemistry Research*, vol. 58, no. 26, pp. 11 338–11 351, 2019.

[75] M. N. AlMallahi, J. Mustafa, A. H. Al-Marzouqi, and M. Elgendi, "Research progress and state-of-the-art on solar membrane desalination," *Case Studies in Chemical and Environmental Engineering*, p. 100825, 2024.

[76] S. K. Venkatachary, J. Prasad, A. Alagappan, L. J. B. Andrews, R. A. Raj, and S. Duraisamy, "Cybersecurity and cyber-terrorism challenges to energy-related infrastructures-cybersecurity frameworks and economics–comprehensive review," p. 100677, 2024.

[77] F. I. Morales-Sáenz, J. M. Medina-Quintero, and M. Reyna-Castillo, "Beyond data protection: Exploring the convergence between cybersecurity and sustainable development in business," *Sustainability*, vol. 16, no. 14, p. 5884, 2024.

[78] J. Simola, "Comparing cybersecurity information exchange models and standards for the common secure information management framework," *Digital Transformation, Cyber Security and Resilience of Modern Societies*, pp. 137–159, 2021.