Volume 6 – Issue 68
Issued on: 20 June 2025
International Journal of Research and Studies Publishing
المجلة الدولية لنشر البحوث والدراسات
ISSN: 2709-7064

Success Factors in Achieving Excellence in Cybersecurity (A Case Study of the Kingdom of Saudi Arabia)

Azizah A. Al-Zahrani
PhD Student, Department of Public Administration, King Saud University, Kingdom of Saudi Arabia
Email: azizaxmail@gmail.com

Prof. Othman I. Al-Salloum
Professor, Department of Management Information Systems, King Saud University, Kingdom of Saudi Arabia
Email: alsallom@ksu.edu.sa

Abstract:

This research aims to discover success factors which established Saudi Arabia as a cybersecurity leader. The research aims to create an extensive cybersecurity framework which promotes international knowledge sharing and improves security practices. The research employed a case study with based research design with a qualitative methodology. The research analyzed cybersecurity-related documents and reports about Saudi Arabia from the year 2017 when the National Cybersecurity Authority was founded until the nation achieved top ranking in the Global Cybersecurity Index 2024. A thematic analysis was conducted using PRISMA criteria to search for patterns in the analyzed documents. The research findings indicate that Saudi Arabia achieved cybersecurity excellence due to several important factors such as a centralized governance model that operates through decentralized operations and substantial cybersecurity investments together with international cooperation and a human capital development program that integrates gender diversity. The research also shows that cybersecurity strategies need to be connected to national objectives while creating stronger public-private sector partnerships to increase cyber threat resilience. The research findings present essential success elements which allowed Saudi Arabia to establish its position as a global cybersecurity leader. This research provides valuable insights into the critical success factors that have enabled Saudi Arabia to become a global leader in cybersecurity. The proposed framework can serve as a model for other countries seeking to enhance their cybersecurity capabilities, emphasizing the need for integrated approaches that combine governance, investment, cooperation, and human resource development.

Keywords: Cybersecurity, Saudi Arabia, Success Factors, Excellence, Qualitative Research.

1. Introduction:

Cybersecurity is a field concerned with protecting systems, networks, programs, and data from cyber-attacks. It requires basic elements such as people, authority, support from senior management, effective processes, appropriate technologies, timely communication, and budget. The primary goals of cybersecurity are to enhance the integrity and privacy of information, support business continuity, and develop the skills of specialists in this field (CST, 2023).

Many studies have shown that there is a significant risk of cyberattacks on organizations of all levels. For instance, Albuhayrii (2019) indicated that cyberterrorism attacks are increasing day by day, causing huge material and moral losses. The study highlighted that cyberterrorism has become one of the prominent topics in the world of crime, necessitating the spread of virtuous values among countries and individuals to combat these crimes. Al-Zabn (2012) explained the multiplicity of tools used in cyberterrorism, such as e-mail, websites, various means of communication, social networking sites, chat rooms, and electronic explosions, including flooding messages, planting viruses, and electronic bombs. Furthermore, Al-Harbi's study (2018) indicated that cyberterrorism harms and destroys infrastructure, damages communications, information technology, and facilities, disrupts the normal functioning of electronic control and oversight systems, and disrupts important and strategic facilities.

Recent studies have provided a broad perspective on the developments in cybersecurity. A systematic literature review on information and cyber security maturity assessment highlights significant progress in sector-specific customization and the integration of emerging technologies (Brezavšček & Baggia, 2025). Another study explores the potential of artificial intelligence as an emerging tool to enhance cybersecurity, focusing on its preventative capabilities against prevalent threats like phishing, social engineering, ransomware, and malware (Okdem & Okdem, 2024). Additionally, research on AI-driven detection methods shows that machine learning and deep learning significantly improve the detection and response to cyber threats (Salem et al., 2024). The Global Cybersecurity Outlook (2025) report provides insights into recent cyber incidents, trends, vulnerabilities, and risk predictions, emphasizing the importance of regulation and continuous updates to enhance cybersecurity resilience. Furthermore, a qualitative study investigates the effectiveness of authentic learning environments in enhancing the cybersecurity skills of in-service professionals (Karjalainen & Ojala, 2023).

Saudi Arabia stands out as a leading nation in this domain, having achieved the top position in the Global Cybersecurity Index for 2024. These achievements are the result of Saudi Arabia's continuous efforts to enhance cybersecurity through the adoption of comprehensive and integrated strategies. These strategies include the development of necessary policies, systems, and regulations, as well as building human and technical capacities and enhancing international cooperation in this field. The National Cybersecurity Authority plays a pivotal role in achieving these goals by setting policies, standards, and overseeing their implementation (Saudi Press Agency, 2024).

1.1. Research Problem:

Despite the increasing frequency and sophistication of cyber threats worldwide, Saudi Arabia has managed to establish a robust cybersecurity framework that supports its economic and social growth and It has emerged as a global leader in cybersecurity, achieving the top position in the Global Cybersecurity Index for 2024. This achievement raises a key question: what is regarding the Success Factors that have contributed to Saudi Arabia's Achieving Excellence in this domain?

1.2. Research Objectives:

This study aims to identify the key factors that have contributed to achieving excellence in cybersecurity in Saudi Arabia. Additionally, the study will leverage methodologies used in previous research to build a comprehensive framework that can contribute to enhancing cybersecurity globally. Through this study, we aim to present a model that can be emulated internationally in the field of cybersecurity, highlighting the importance of knowledge exchange to achieve a secure and reliable cyberspace that supports economic and social growth.

1.3. Significance of the Research

The significance of this research lies in its potential to provide an understanding of the success factors that have enabled Saudi Arabia to excel in cybersecurity. By identifying and analyzing these factors, the study can offer valuable insights and practical recommendations for other nations aiming to enhance their cybersecurity capabilities.

2. Research Methodology

The research methodology includes the procedures that will be followed in the research, in terms of clarifying the research design, data sources and the process of selecting them, as well as clarifying the method used in data analysis, and finally the research limits.

2.1. Research Design

This study uses a qualitative research design, using a case study approach to explore and identify the factors that have contributed to Saudi Arabia's success in achieving excellence in cybersecurity. The case study approach is particularly suitable for this research because it allows for an in-depth examination of the multifaceted processes that have led to Saudi Arabia's prominent position in the global cybersecurity arena, and by focusing the study on a single case, detailed insights and a comprehensive understanding of the influencing factors can be provided.

2.2. Data Sources

The primary data sources for this study are documents and reports related to cybersecurity in Saudi Arabia, spanning the period from the establishment of the National Cybersecurity Authority (NCA) in 2017 to 2024, when the Kingdom was ranked first in the world in cybersecurity. These documents include government reports, strategic plans, international competitive reports, and other relevant publications that provide insights into the cybersecurity landscape in Saudi Arabia. Documents were selected as a source of data to understand the strategic, political, and operational frameworks that have contributed to Saudi Arabia's cybersecurity achievements.

Documents and reports will be selected according to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) criteria, which provides a structured approach to identifying, screening, and including relevant documents in the analysis. The PRISMA framework ensures that the document selection process is transparent, replicable, and systematic, thus enhancing the reliability and validity of the study results. The document selection process includes the following steps:

- Identification: The initial step involves identifying a comprehensive list of documents and reports relevant to cybersecurity in Saudi Arabia, through a systematic search of government websites relevant to cybersecurity, academic databases, and international reports on cybersecurity in Saudi Arabia.
- Screening: The selected documents will be screened based on their relevance to the study objectives, and documents that do not focus on cybersecurity or are not directly related to Saudi Arabia, and documents published before 2017, will be excluded.
- Eligibility: Documents will be evaluated for eligibility based on specific inclusion criteria, including publication date (between 2017 and 2024), relevance to cybersecurity strategies and

outcomes in the Kingdom, availability of full text access in Arabic or English, and that the documents contain accurate, valid information from reliable sources.

- Inclusion: Finally, documents that meet all inclusion criteria will be included in the analysis and provide comprehensive coverage of cybersecurity developments in Saudi Arabia during the specified period.

2.3. Data Analysis

The selected documents will be analyzed using Braun and Clarke's (2006) thematic analysis method, which is suitable for identifying, analyzing, and reporting patterns (themes) within qualitative data. Thematic analysis allows for a flexible and detailed examination of the data, making it possible to uncover the underlying factors that have contributed to the success of cybersecurity in Saudi Arabia. The thematic analysis process involves the following steps:

- Data Familiarization: This involves immersing oneself in the data by reading and rereading documents to fully familiarize oneself with the content. This step is crucial to gaining a comprehensive understanding of the context within the data.
- Creating Initial Codes: Following familiarization, the data will be systematically coded to identify important features related to the research question, with each document reviewed to extract relevant information and insights.
- Search for Themes: Initial codes will then be examined to identify potential themes. The themes were identified based on their relevance to the research question and their ability to capture key aspects of the data.
- Reviewing Themes: The identified themes will be reviewed and refined to ensure that they accurately represent the data. This includes checking the themes and the entire dataset for relevance and coherence.
- Identifying and naming themes: Each theme will be clearly defined and named to reflect its essence and contribution to the overall research findings. This step involves writing detailed descriptions of each theme and considering how they relate to each other.
- Writing the report: The final step involves writing the analysis and integrating the themes into a coherent narrative that addresses the research question.

2.4. Research Limitations

Although document analysis enables us to understand the factors that contributed to the success of

cybersecurity efforts in Saudi Arabia, there are some limitations that we must clarify. First, our analysis is based on available documents and may not cover all important aspects in this field. Second, our study does not include interviews or questionnaires with experts, and this may limit the depth of understanding we can reach.

3. Previous Studies

The field of cybersecurity has garnered significant attention in recent years, driven by the increasing frequency and sophistication of cyber threats. This Section synthesizes research on the critical success factors influencing cybersecurity across studies. The review draws upon a diverse range of studies, each contributing unique insights into the multifaceted nature of cybersecurity success. The review will first examine studies conducted in various countries to identify key success factors in cybersecurity. Subsequently, it will focus on studies specific to Saudi Arabia, with the aim of determining the critical success factors for cybersecurity in a local context.

Yeoh et al. (2023) deliver a comprehensive study of the successful factors for implementing zero trust models of cybersecurity. The study, which is rooted at Deakin University's Centre for Cyber Resilience and Trust, uses a qualitative design in its case studies across different organizations. Yeoh et al. identify essential considerations like organizational culture, tech infrastructure, and constant monitoring as central to zero trust implementation. The study results highlight the necessity of an integrated approach that harmonizes technical and human factors in cybersecurity practices.

In another study by Yeoh et al. (2022), systematic synthesis of major success factors for cybersecurity is addressed. The study utilizes a systematic literature review method to identify and categorize success factors across different organizational contexts. The results of the study highlight the significance of governance, risk management, and employee training in improving cybersecurity practices. The authors advocate for the incorporation of dynamic capabilities to adjust to changing cyber threats, a point supported by the research findings of Noor et al. (2024) on the significance of dynamic capabilities in readiness for cybersecurity.

Hameed et al. (2023) examine the determinants of success of global cybersecurity capacity-building initiatives. Conducted at the University of Oxford, this research adopts a mixed-methods design using quantitative surveys and qualitative interviews. The study identifies collaboration, knowledge sharing, and policy alignment as determinants of successful capacity-building

activities. The emphasis on international collaboration aligns with Kazemi and Heydari (2023), who also stress cross-border cooperation as a determinative factor in cybersecurity.

Kazemi and Heydari (2023) also provide a quantitative ranking of factors that affect cybersecurity. The study applies a ranking method to rank factors in terms of relative importance. The results indicate that technological advancements, regulatory compliance, and organizational culture rank high among the factors. The quantitative ranking emphasis of this study is unique compared to other research that applies a qualitative approach, providing a new perspective on factor ranking.

Ryttare (2019) examines the change management function in achieving effective cybersecurity outcomes. Drawing on a multiple case study of Swedish organizations, the research finds that change management is a central enabler of cybersecurity success. The investigation highlights effective communication, stakeholder engagement, and flexibility measures, reinforcing the dynamic capabilities strategy advocated by Noor et al .(2024).

Noor et al. (2024) provide a thematic summary of determinants of cybersecurity readiness based on the application of dynamic capabilities theory. The research teams classify determinants into sensing, seizing, and transforming capabilities, noting that organizations need to continually evolve their security solutions. The study corroborates the evidence already established by Yeoh et al. (2022), affirming the importance of flexibility and proactive risk management in cybersecurity policies.

Alam and Ibrahim (2021) focus on the unique smart city environment, establishing success determinants for applying cybersecurity. The study, at Universitas Muhammadiyah Bengkulu and University Utara Malaysia, employs case study research to examine technological integration, cooperative stakeholders, and regulatory environments. Smart city environments' emphasis provides rich insights into the specific challenges and opportunities of cybersecurity in cities.

Aksoy (2023) explores the human factors' contribution to the management of cybersecurity, challenging the proposition that success factors are purely technical. The study employs a qualitative approach to put into the spotlight the importance of human factors such as user behavior, organizational culture, and leadership. This perspective is in line with the efforts of Yeoh et al. (2023) and Ryttare (2019), affirming the need for a harmonized strategy that considers both the technical and the human dimensions.

In a local context, Dawson (2021) delineates the mounting cybersecurity threats in Saudi Arabia as a call to strategic realignment towards cyber preparedness. Dawson refers to the recent cyberattacks on major institutions like Saudi Aramco and the Ministry of Health, drawing a parallel to the same vulnerabilities in Ukraine. The study identifies the need for new laws, robust security technology, and better public awareness against these threats. Dawson's research sets the stage to conduct research on the larger picture of the issues faced by cybersecurity in Saudi Arabia and for future research studies.

Alsemairi (2023) analyzes drivers on the compliance of Saudi Arabian employees with cybersecurity measures. In doing a survey with 245 Saudi Arabian government agency employees, it identifies ethical, legislative, technical, and administrative drivers as factors necessary. Alsemairi's research shows the importance of non-technical vulnerabilities, where ethical considerations are most important in influencing compliance. The study contributes to the body of knowledge regarding the human factor in cybersecurity, emphasizing the need for comprehensive policy structures that cover ethical and legislative elements.

Aljabri (2021) discusses cybersecurity awareness among Saudi residents through a survey of 600 participants. The study reveals a general lack of awareness and states that legal controls, though needed, can encroach on privacy. Aljabri's study establishes awareness as the solution to cybercrimes and suggests targeted training programs to ensure public awareness. This research reinforces Dawson's call for education by confirming awareness as the basis for cybersecurity policy.

Albediwi and Sadaf (2023) propose a framework for the strengthening of cybersecurity literacy in Saudi Arabia. Based on a survey related to cybersecurity assessment, negligent behavior and limited awareness among citizens are determined through their research as key findings. The proposed framework involves education sessions in schools, universities, companies, and sectors and non-governmental sectors. This comprehensive mechanism bridges the shortcomings proposed by Aljabri as an orderly way towards improving cybersecurity literacy.

Alhakami (2024) examines Saudi Arabian cybersecurity capability employing a fuzzy decision-making approach. The study underlines the value of strategic decision-making models for enhancing cybersecurity capability. Alhakami's research complements that of Albediwi and Sadaf by providing a methodological framework for the utilization of awareness programs.

The fuzzy decision-making model offers an advanced tool for the evaluation and enhancement of cybersecurity plans, consistent with the general aim of national cybersecurity readiness.

Saleh and colleagues (2025) conduct qualitative research on Saudi Arabian influencers of cybersecurity awareness. The research identifies cultural, educational, and technological influences as significant influencing factors. Saleh's research presents an overview of the socio-cultural dynamics that shape cybersecurity awareness and offers insights into the facilitators and barriers to effective cybersecurity measures. Saleh's research also complements Alsemairi's research by identifying the interplay of cultural and ethical influences in shaping cybersecurity behavior.

Similarities and Differences Among Studies

The studies in question collectively underscore the multifaceted nature of cybersecurity success and the sequence of shared threads such as organizational culture, technological infrastructure, and human factors. For instance, Yeoh et al. (2023) and Aksoy (2023) equally emphasize the central role of organizational culture and human factors in the implementation of effective cybersecurity frameworks. Similarly, the studies of Yeoh et al. (2022) and Noor et al. (2024) also stress the necessity of dynamic capabilities and flexibility in cybersecurity policies, as in the broad consensus on the significance of continuous development in security measures.

While having these similarities, the research studies vary in methodology and focus. Yeoh et al. (2023) and Kazemi and Heydari (2023) take qualitative and quantitative methods respectively, leading to different factor prioritization perspectives. While Yeoh et al. focus on the general effect encompassing technological and human factors, Kazemi and Heydari emphasize technological innovation and regulatory compliance through a ranking method. This divergence reflects the numerous varied lenses through which success in cybersecurity can be considered, each shedding light on something different that is being weighted first. In Saudi Arabia, Dawson (2021) and Alsemairi (2023) are concerned with strategic readiness and employee compliance, respectively. They differ in orientation, with Dawson referencing the broader geopolitical threats and Alsemairi emphasizing organizational drivers for compliance. Aljabri (2021) and Albediwi and Sadaf (2023) extend this argument by examining public awareness and proposing national models for cybersecurity awareness, respectively. These studies combined provide a whole picture of Saudi Arabian cybersecurity, yet simultaneously, they reveal the diversity and intricacy of the challenges ahead for the country.

Overall, while existing literature does present a good foundation for understanding the critical success factors in cybersecurity, there is more integrated and context-specific research required. The proposed study of the success factors in cybersecurity of Saudi Arabia will bridge these research gaps and offer a comprehensive framework to understand and achieve excellence within this rapidly evolving discipline. This current study will borrow methodologies from previous research to create and build upon these underlying findings.

4. Literature Review

4.1. Conceptualizing Cybersecurity

Cybersecurity is completely defined as the career with the mandate of safeguarding systems, networks, and programs against cyber-attacks. Cyber-attacks tend to target the unauthorized viewing, modification, or destruction of sensitive information, the extortion of financial resources from users, or the interference with normal business operations (Jones, 2015). Over time, the term cybersecurity has been defined in line with technological advancements, from a single focus on safeguarding individual computers to safeguarding networks and critical infrastructure. Cybersecurity is essentially concerned with the protection of information systems against unauthorized access, interference, or data compromise. It involves a broad array of protective measures that are designed to enhance the confidentiality, integrity, and availability of information (Schatz et al., 2017). Since information systems are increasingly connected via the Internet and cloud computing, cybersecurity now reaches beyond traditional IT assets to encompass critical infrastructure and industrial control systems (Asghar et al., 2019). Cybersecurity is not just a technical issue anymore; it is a complete risk management strategy involving policies, processes, and practices aimed at protecting digital assets. Academic studies emphasize the necessity of integrating cybersecurity into the culture and strategic planning of an organization to respond effectively to threats (Alnatheer, 2015; Williams, 2011). Cybersecurity has several key aspects: protection of information and systems against significant cyber threats, preservation of confidentiality, integrity, and availability, and assurance of data and transactions authenticity and accountability (Kumar, 2018). The cyber terrain is constantly changing, fueled by the rapid pace of innovation in new technologies and the rise in sophistication of cyber threats.

4.2. Importance of Cybersecurity

The importance of cybersecurity is enormous, and it has significance in countless parts of modern life as an example, protecting sensitive information is extremely important. Because many aspects

of modern life have become digital, personal information can be stored online and thus vulnerable to being accessed by a hacker. This is comparable to locking your home to ensure your valuables are safe from any break-ins. On a larger scale, cyber-attacks financially impact many sectors of the economy. The annual financial loss globally to cybercrime is expected to reach 6$ trillion dollars. This expense includes the actual theft made by cyber criminals, as well as the money spent to mitigate the damage after the breach has occurred. Cybersecurity is also important to the trust of services we use in our everyday lives. Major security incidents can erode user confidence and affect user participation in sectors relying on digital platforms like e-commerce and governmental services. Cyber threats towards critical infrastructure that sustain our electricity and healthcare systems are a cyber security concern too. Finally, when businesses invest in cyber security, they are investing in continuity and operational resiliency. Businesses also protect their bottom line by forgoing damage to their reputation and legal liabilities when they invest in cyber security. Regardless of the motive whether in the best interest of their business, reputation, or goodwill these companies are making significant investments in cybersecurity to increase their outcomes and ability to conduct business with a competitive advantage (Perwej et al., 2021; Ahmad et al., 2020).

4.3. Cybersecurity Management

Cybersecurity management involves directing cybersecurity activities to safeguard digital assets. It encompasses technical, managerial, corporate, and governance aspects (Kuusisto & Kuusisto, 2013). Employees are often the most significant source of vulnerability, but cybersecurity issues also stem from inadequate senior management guidance (Ani, He & Tiwari, 2019; Klimoski, 2016). Effective cybersecurity management requires setting strategic goals, coordinating action plans, and managing disruptions (Lehto & Limnell, 2020). The scope of cybersecurity management includes risk assessment, strategy development, policy implementation, and continuous monitoring (CISA, 2021; NIST, 2018). Businesses must adopt a holistic approach, integrating technical solutions with human factor management. Cybersecurity policies establish security goals and rules, fostering an organizational culture of security awareness (Antonakakis et al., 2017; Williams, 2019).

4.4. Cybersecurity in the Kingdom of Saudi Arabia

Some of the external developments and impacts on Saudi Arabia's cybersecurity landscape over the past decade is notable, given that, Saudi Arabia's positioning as well as natural resources

continues to make it an area of target for hackers, demonstrated by the fact that in 2020 Saudi Arabia received more than 22.5 million cyberattacks (Olech, 2021). These attacks have a colossal economic impact, spanning not only finance, but also operational, and tactical levels that could reduce citizen trust in government services (Quadri and Khan, 2019). The COVID 19 pandemic has worsened the issues already established by the above attacks, as organizations adopted remote work better positioned targets for hackers, every IT industry in the kingdom needed to pivot to prioritize data security and employees were now expected to understand more cybersecurity threats awareness (Buller, 2020; Al-Zubaidi 2021).

4.4.1. Cybersecurity strategic initiatives in Saudi Arabia

against the backdrop of growing cybersecurity threats, Saudi Arabia has taken a number of strategic steps to enhance a sound cybersecurity infrastructure, Perhaps the most public of these initiatives was the establishment of the National Cybersecurity Authority (NCA) in 2017 was a huge step toward centralizing and consolidating the country's cybersecurity push. The role of the NCA is to have regulatory and operational roles coupled with liaison with public and private bodies in safeguarding critical infrastructure and supplementing the Vision 2030 strategy. The strategic priority goals under the NCA vision 2030 are cybersecurity alignment, management of risks, optimal cyberspace performance, dynamic defense, international partnership, and development of cyberspace. These objectives reflect Saudi Arabia's commitment to establishing a secure and resilient digital environment, among the most important factors in Saudi Arabia's cybersecurity excellence is a pattern of centralized governance combined with decentralized operation, Centralizing cybersecurity administration falls within the responsibility of the National Cybersecurity Authority (NCA), such as setting standards, policies, and incident response guidelines at the national level. This centralized approach ensures consistency and unification of cybersecurity practice across the Kingdom. At the same time, operational responsibilities are decentralized so that national entities can be responsible for their on-premises activities. This dual approach ensures a robust cybersecurity environment where entities can tailor their security to specific needs while adhering to national guidelines.

In addition, the Kingdom has also created Saudi CERT to encourage cybersecurity awareness and mitigate possible security weaknesses. The Saudi CERT publishes alerts about cyber vulnerabilities and runs educational campaigns to increase cybersecurity awareness.

One key initiative is the Saudi Federation for Cybersecurity Programming and Drones, developed in conjunction with the Saudi Olympic Committee. The aim of the federation is to develop national talent aligned with the expansion of software and drone technology. The federation strives to develop programs and activities to increase public awareness around programming, cybersecurity, and advanced technologies as well as support young Saudis in becoming specialists in these core areas. The National Cybersecurity Academy powered by collaboration between the Ministry of Communications and Information Technology and the Human Resources Development Fund (HRDF), will improve national digital capability in the technology solutions area. Education and training programs including those on artificial intelligence data analysis, cloud computing, web and application development, gaming development and design, and executive development programs will be delivered by the Academy. These channels are designed to provide citizens and the nation with the ability to keep pace with digital transformation. The Haseen National Portal is another prominent nationwide effort designed to enhance cybersecurity across the Kingdom of Saudi Arabia, it offers a wide range of advanced cybersecurity solutions to national entities and contributes to enhancing local content related to cybersecurity, thereby enhancing local awareness and capabilities in this vital field. The platform also enables national entities to effectively carry out their tasks and operational responsibilities, which contributes to enhancing their performance and achieving their goals. The platform also seeks to improve the efficiency of government spending in the field of cybersecurity, ensuring optimal and effective use of resources. Finally, the platform works to enhance cybersecurity at the national level, which contributes to protecting the information infrastructure and reducing cyber risks. (Saudi Government, 2025).

4.4.2. Cybersecurity strategies and frameworks in the Kingdom of Saudi Arabia

The cybersecurity ecosystem in Saudi Arabia is defined by the implementation of several strategies and frameworks, all of which are naturally aligned with the goals of the Vision 2030 plan. The most prominent among these is the National Cybersecurity Strategy, which forms the foundation on which the security of the nation's digital ecosystem is based. This strategy emphasizes alignment with Vision 2030 by embedding cybersecurity into economic and societal transformation initiatives. The strategy emphasizes governance, capacity building, partnership, and innovation in technology to establish a solid platform for managing cybersecurity risk through centralized governance and decentralized operations by allocating roles and responsibilities, enabling efficient risk management.

Human capital development and innovation have been prioritized to surmount emerging cybersecurity threats, with private sector involvement and performance metrics as a must for ongoing improvement (NCA,2020).

Saudi Arabia's Critical Systems Cybersecurity Controls (CSCC – 1: 2019) prioritize alignment with national objectives, establishing governance structures for effective risk management. The controls promote the integration of cybersecurity into project management disciplines, such that the security requirements are embedded from the very first stage. The importance of human resource management is also highlighted, requiring skilled professionals for technical roles. Key aspects include improved network defense mechanisms such as multi-factor authentication and intrusion detection systems complemented by continuous monitoring and collaboration with cloud security providers for system integrity.

Operational Technology Cybersecurity Controls (OTCC -1: 2022) offer a bespoke answer to the specific needs of industrial and infrastructure environments. The controls emphasize governance, general risk management, and the development of human capital. Technological change is prioritized, with the focus on the implementation of state-of-the-art protection and automated tools. Sustained improvement and compliance are ensured through review and periodic updates in the framework, while information sharing within and across sectors is deemed a requirement for collective security enhancement.

Data Cybersecurity Controls (DCC -1:2022) focus on implementing governance frameworks and defense mechanisms for safeguarding sensitive information. The controls are focused on policy adherence to national laws and utilizing advanced technological means for threat detection and response. Vendor compliance and cloud architecture management are key to managing third-party cybersecurity. Regular updates and assessments are conducted to ensure continuous enhancement and adherence, facilitating a comprehensive data protection strategy.

The unique requirements of securing remote workplaces are outlined in Telework Cybersecurity Controls (TCC -1: 2021). The controls are based on overarching governance and policy frameworks in alignment with national law and emphasize cybersecurity awareness and training. Robust defense controls, such as asset management and identity access controls, are required. Continuous monitoring and flexibility in technology are achieved through regular updates, ensuring alignment with national standards.

For social media account management in organizations, Cybersecurity Controls (OSMACC - 1:2021) emphasize governance structure, risk management, and compliance. Awareness raising is at the center of which human resource participation is involved, supported by training programs. Technological controls, including asset inventory management and access controls, are imperative. Incident response and threat management approaches, addressing third-party and cloud computing concerns as necessary, are included in the controls.

The Saudi Cybersecurity Workforce Framework (SCyWF - 1: 2020) stresses the need for a structured approach in defining cybersecurity skills and roles, benchmarked to international standards. The framework is focused on lifelong learning and upgrading of skills, with allowances made for organizational adjustments as needed. Consistency is ensured through alignment with national frameworks by embedding, with risk management and regulatory adherence being top priorities.

The National Cryptographic Standards (NCS – 1: 2020) aim at developing adaptive standards for cryptographic practice with flexibility based on data sensitivity. Successful deployment of cryptographic mechanisms requires effective implementation and adherence, with strong emphasis on key lifecycle management and emerging threats like post-quantum cryptography. Interoperability across sectors is assured through good governance and oversight.

The Saudi Cybersecurity Higher Education Framework (SCyber-Edu – 1: 2020) is determined to align education programs with national and global standards. Comprehensive curriculum development addresses a wide range of cybersecurity topics, allowing for specialization and practical competencies development through hands-on practice. The framework supports stakeholder coordination, aiming to develop a qualified cybersecurity workforce in alignment with national objectives.

Essential Cybersecurity Controls (ECC – 2: 2024) are a critical element of Saudi Arabia's cybersecurity approach. The controls emphasize strategic alignment, governance, comprehensive risk management, and ongoing monitoring. Employee training programs are required for building a cybersecurity-aware culture, while compliance and regulatory demands guarantee alignment with legislation and technological advancement.

Cybersecurity Best Practices for E-commerce Consumers and Service Providers (CGEC – 1: 2019) address the cybersecurity concerns specific to e-commerce. These best practices cover a

comprehensive, multifaceted approach to online security that includes consumer awareness, cutting-edge security technologies, and adherence to regulatory compliance requirements. Continual monitoring and incident response are paramount, offering periodic review and information-sharing among stakeholders to ensure continued protection against threats.

A recurring theme across these different controls and strategies is strategic alignment with national objectives. This alignment supports Vision 2030's broader aspirations, fostering a consistent method of cybersecurity through governance and regulatory frameworks. The emphasis on human capital development and ongoing improvement through workforce innovation and evolution reflects the evolving nature of cybersecurity threats. Technology development and cross-sector collaboration are recurring themes, mirroring Saudi Arabia's dedication to a robust cybersecurity stance. Despite these similarities, each strategy has distinctive emphases and implementation details, responding to specific technology requirements and compliance issues within various cybersecurity spheres.

4.4.3. The Role of Cybersecurity in Saudi Arabia's Economic and National Security

The cybersecurity sector adds considerably to the economy of Saudi Arabia, accounting for 15.6 billion SAR of GDP According to the comprehensive report on the main economic indicators in this sector for the year 2024. This represents the enormous economic impact of spending on cybersecurity and is part of the strategic justification for investment in cybersecurity both for national security and economic growth. The level of investment of significant amounts of money by government and private sector organizations particularly in the case of critical national infrastructure responsibilities, emphasizes a strong commitment to protecting physical and digital assets. Moreover, the focus on growth and innovation and investment in the cybersecurity sector reinforces the economic contribution of this sector and reinforces its importance for national success. The success of the cybersecurity field is strengthened by extensive market analysis and data-supported knowledge using advanced analytical models and a rigorous methodology that provide a high level of statistical confidence and dependability of results. The information space looks at market size, patterns of spending, the geographic distribution of supply and demand, enabling the sector to develop a full pattern of the cybersecurity landscape. This systematic, data-supported approach supports action-oriented decision making and tactical decision-making implementing decision making, both critical in responding to current cyber challenges and anticipating emerging issues in cybersecurity.

Working with each of our international partners (for example, Boston Consulting Group or the International Data Corporation) and local participants in the sector is an essential part of Saudi Arabia's cybersecurity strategy. This is one of the biggest strengths; by bringing global knowledge and best practices (formal and informal) together with local strategies and solutions to enable the Kingdom to effectively address complex and dynamic cybersecurity issues. The opportunity to work with a spectrum of stakeholders (government organizations, private sector companies, educational institutions, and cybersecurity vendors) to support the development of the sector (to ensure the development and interactions are inclusive) offers various lines of development, and more importantly, presents avenues for innovation and capacity building that are critical for a high standard of excellence. With 19,600 cybersecurity professionals working in the Kingdom (32% women) the development of a professional cybersecurity workforce is critical for sustaining excellence in cybersecurity because there needs to be a workforce with expertise available to deal with the ever-evolving new threats. Encouraging women to participate is particularly important since it enhances diversity increase the talent pool for cybersecurity. The Kingdom is developing a sustainable and resilient cybersecurity workforce to support its strategic objectives through investments in education and training. With its emphasis on cloud security, network security, and managed security operations centers, Saudi Arabia is embracing new technologies wholeheartedly. By fostering a culture where countries can innovate and develop and implement advanced cybersecurity solutions to solve existing problems, I believe Saudi Arabia is positioned to do so. Research and development and technology transfer will only further this innovation agenda and make it likely that the Kingdom will be one of the leading players in cybersecurity going forward.

5. Results

The results of this study on the success factors contributing to Saudi Arabia's excellence in cybersecurity are informed by a comprehensive review of documents. The documents, selected based on the PRISMA criteria, are data-rich documents that have been systematically analyzed through thematic analysis. The findings reveal a sophisticated model of cybersecurity by means of the conjoining of centralized regulation with decentralized operations, substantial expenditure on cybersecurity, strategic collaborations, and focus on the creation of human capital. This part outlines the prominent themes and trends that have appeared from the findings, with a focus on the factors that have raised Saudi Arabia's status within global cybersecurity:

5.1. Decentralized Operations and Centralized Government

One of the most powerful conclusions of the analysis is the centralized governance-decentralized operations model that has been crucial to Saudi Arabia's cybersecurity success. The National Cybersecurity Authority (NCA) is the focal point of this model and sets national standards, policies, and incident response procedures. Centralized governance ensures consistency and unity in cybersecurity practices across the Kingdom and provides a strong foundation for cybersecurity measures. However, operational tasks are decentralized so that every entity may design its security arrangements based on individual requirements while remaining in conformity with national standards. This two-pronged measure promotes a robust cybersecurity ecosystem so that flexibility and responsiveness may emerge in the presence of emerging threats. This two-pronged measure aligns with the findings of Yeoh et al. (2023), who emphasize organizational culture and governance in zero trust framework implementation.

5.2. Strategic Investment in Cybersecurity

Heavy investment in cybersecurity is one of the major successful drivers. It was estimated the contributions of the cybersecurity industry to the Kingdom's GDP is 15.6 SAR billion, which helps reinforce the importance of cybersecurity nationally in terms of both security and economic development. This is seen through significant investment in cybersecurity from both the government sector and private sector. The focus on driving growth, innovation, and investment in cybersecurity drives this economic contribution to be at the center of a country's wealth. This finding aligns with the technological innovation focus identified by Kazemi and Heydari (2023) and Alam and Ibrahim (2021) when they examined smart cities and regulatory regimes. Data-driven insights and market analysis utilizing sophisticated analytical models had assisted strategic, operational, and tactical planning and decision-making. Given the challenges it faced amid emerging trends in cybersecurity, the insights helped it address current security issues and manage decisions and develop and deploy responses. This aligns with Yeoh et al.'s (2022) integrated approach to cybersecurity strategy, or dual-mode ventures highlighting the need to account for the technical and human aspects of security strategy.

5.3. Strategic Collaborations and International Partnerships

The security strategy of Saudi Arabia also relies on collaboration with international parties and local stakeholders. The Kingdom's collaboration with international partners like Boston

Consulting Group (BCG) and the International Data Corporation (IDC), in addition to local partners, improves its ability to address certain complex issues about cybersecurity. Such collaboration addresses cybersecurity issues using globally established practices, grounded in contextual concerns of the local parties, in particular the government and local stakeholders. This relates to innovation, capacity building, and co-design of solutions for common challenges. Hameed et al. (2023) and Kazemi and Heydari (2023), have demonstrated how government, based partners, regional cooperation can address these factors and facilitate cross-border knowledge transfer. Saudi Arabia's development includes a bigger set of stakeholders which could consist of: Governmental Entities, Private industry, Educational Institutions, plus a young startup sector, including entrepreneurs and cybersecurity vendors. The nature of the stakeholders indicates that the country's development of the cybersecurity sector will be comprehensive, rather than exclusive. This level of collaboration is critical to achieving excellence in cybersecurity, while addressing the multifaceted nature of cyber threats.

5.4. Human Capital Development and Gender Inclusion

The research makes a clear case that human capital development is essential to Saudi Arabia's success in cybersecurity. Out of 19,600 cybersecurity professionals in the Kingdom, some 32% are women. Developing talent is paramount to continuing its level of excellence in cybersecurity. Gender inclusion also warrants attention because it helps uphold diversity and increase the talent pool. With investment in education and training, the Kingdom is building a resilient cybersecurity workforce to utilize in the interest of its strategic objectives. The National Cybersecurity Academy and the Saudi Cybersecurity Workforce Framework clearly outline the need for workforce development and skills enhancement to keep the Kingdom's cybersecurity competitiveness up to date. Within those working relationships have an emphasis on diversity and education that parallels the recent work authored by Aksoy (2023) which construes that human factors have importance in cybersecurity management.

5.5. Technological Advancements and Innovation

The Kingdom's focus on technology and innovation is evident from its interest in cloud security, network security, and managed security operation centers. This renders Saudi Arabia an excellent setting for innovation and creating sophisticated cybersecurity solutions for addressing modern-day problems.

This technology-led strategy is underpinned by promoting research and development and technology transfer to keep the Kingdom at the forefront of cybersecurity advancements since Kazemi and Heydari (2023) identify technological advancement as one of the highest-ranked success factors. The embedding of emerging technologies in critical cybersecurity controls and the emphasis on advanced network and data protection mechanisms demonstrate the proactive role of the Kingdom in leveraging technology to counteract emerging cyber threats.

5.6. Strategic Alignment and Integrated Risk Management

Detailed risk management, combined with strategic alignment with national visions such as Vision 2030, is another common thread among the documents that were examined. The charter either for the National Cybersecurity Strategy or specific cybersecurity controls is the alignment of specific cybersecurity activities to both national goals and regulatory processes i.e. an assurance that everything undertaken will be a contribution to the broader goal of Vision 2030 so that all groups can start working together safely at the operational level to a collective purpose on something as complicated as cybersecurity. Again, the focus on strategic alignment and governance reflects the stance of Noor et al. (2024), who advocate for administering such alignment through dynamic capabilities to counter the ongoing evolution of threats. The focus on strategic alignment and governance matters when sustaining an efficient and effective cybersecurity posture that enables the Kingdom to empower itself in the disorienting and chaotic cybersecurity environment.

5.7. Engagement between Public and Private Sector

Public-private sector engagement, which is determined to be a necessary part of Saudi Arabia's cybersecurity strategy, entails close collaboration between a government entity and the private sector to foster cybersecurity resilience and innovation. Engagement will ensure that designed cybersecurity measures have an inclusive and holistic impact in the pursuit of sectorial needs and challenges. Stakeholder engagement as emphasis aligns with Saleh et al. (2023) data that recognizes different factors such as cultural, educational and technological influences, which collectively shape awareness of cybersecurity. The data emphasize relevant stakeholders in the broader frame of stakeholder engagement models for the Saudi Cybersecurity Higher Education Framework, and National Policy for Managed Security Operations Centers as a necessity towards collaborative efforts that drive better awareness of cybersecurity and growth in the sector.

5.8. Commitment to Gender Inclusion and Workforce Development

The Kingdom's commitment to gender inclusion and workforce development is a key success factor in its cyberspace strategy. Saudi Arabia's move to publicize the growth of women in cybersecurity as a percentage of the workforce it will increase diversity and bolsters the alternative talent pool. This commitment is visible through initiatives like the National Cybersecurity Academy and the Saudi Cybersecurity Workforce Framework, which seek to sustain and advance a skilled workforce that is diversified to keep pace with the growing emergence of threats. The emphasis on education and training will allow the Kingdom to compete with its peers in the cyberspace landscape while creating a culture of adaptability and continuous learning. This follows up on Aksoy's (2023) research findings regarding the human elements in cybersecurity (management) strategy.

5.9. Cloud Security and Managed Security Operations Centers

The focus on cloud security and managed security operations centers showcases Saudi Arabia's commitment to leveraging advanced technologies to better its cybersecurity posture. The Kingdom recognizes that increased cloud users mean an increased demand for secure cloud services, and the need for security operations to continue to efficiently operate is more important now than in the past. Coupled with the Kingdom's greater agenda of expanding innovation while maintaining technological advantage, the kingdom will continue to use enablers to innovative while ensuring they can deal with impactful advances in cybersecurity today and in years ahead. Therefore, both cloud security and managed security operations centers allow the kingdom to proactively manage today's cybersecurity issues.

6. Cybersecurity Enhancement Framework

To develop a comprehensive framework that can enhance cybersecurity, based on the success factors identified in Saudi Arabia's cybersecurity Case, we can create a structured model that incorporates these key themes. The framework will focus on centralized governance, strategic investments, international collaborations, human capital development, technological advancements, comprehensive risk management, public-private sector engagement, gender inclusion, and a focus on cloud security and managed security operations.

1. Centralized Governance with Decentralized Operations:

- Build a National Cybersecurity Authority (NCA): A centralized body that will create national cybersecurity standards, and national cybersecurity policies and protocols for incident response.
- Decentralized Implementation: Allow organizations to move toward security measures that are based on their needs, and follow established national standards, while becoming more flexible and responsive.

2. Investment in Cybersecurity

- Fund a Substantial Budget: Ensure a significant budget for cybersecurity to advance national security and economic development.
- Encourage Investment from Public-Private investors: Funding from the public and private sector, particularly for critical infrastructure, will foster national growth and innovation.

3. International Partnerships and Collaborative

- Engage Global participants. International consulting firms, volunteers from the cybersecurity sector deployment in relation to local need are important parts of partnering to develop solutions for large cybersecurity challenges.
- Support knowledge sharing and collaboration across borders: Cross-border cooperation and knowledge-sharing can contribute to capacity development and innovation.

4. Skill and Human Capital Development and Gender Inclusion

- Developing Cyber Security Workforce: Support education and training to develop a skilled Cyber Security workforce.
- Gender Diversity: Enabling gender inclusion in Cyber Security roles helps to expand the talent pool and diversify the pool.

5. Technology and Innovation

- Advanced Technologies: Invest in cloud security, network security, managed security operations to respond to present-day challenges.
- Promote Research and Development: Support innovation-oriented approaches by establishing conditions that support research, development, and technology transfer.

6. Risk Management and Alignment

- Aligning strategies with national goals: Cyber Security strategies must be aligned with the national objectives and regulatory frameworks (such as Vision 2030).

- Risk Management Frameworks: Put risk management plans in place to respond to evolving risks.

7. Public and Private Sector Engagement

- Promote Collaboration: Collaboration between the public sector and private sector is key for developing resilience and innovation.
- Stakeholder Participation: Engage communities with direct stakeholder involvement from institutions of learning and Cyber Security vendors to develop holistic Cyber Security.

8. Commitment to Gender Inclusion and Workforce Development

- Encourage Diverse Workforce: Continue to commit to inclusion of women and underrepresented classes of staff to take to Cyber Security workforce.
- Continuous Learning: Create / continue initiatives to ensure ongoing learning and development, and competency to remain competitive.

9. Emphasizing Cloud Security and Managed Security Operations Centers

- Invest in Cloud Security Solutions: Place emphasis on securely developing and deploying cloud services.
- Security Operations: Increase managed security operations to improve all aspects of effective and efficient security management.

Implementation Steps

- Conduct a National Cybersecurity Assessment: Performance assessment in cyber security.
- Develop a National Cybersecurity Strategy: Develop a cybersecurity strategy incorporating all elements of the framework, addressing the country context
- Develop Regulations and Policy Frameworks: Develop appropriate regulations and policies to promote the implementation of the cybersecurity strategy.
- Conduct Public Awareness Campaigns: Conduct public awareness campaigns targeting people and the public and private sectors about best practices for cybersecurity and the critical importance of cybersecurity.
- Monitor and Evaluate Implementation: Monitor and evaluate the effectiveness of the initiatives to improve cybersecurity and change in strategies where necessary.

7. Recommendations:

- Encourage and enhance the ability of central agencies to develop cybersecurity policies and standards.

- Increase budgets designated for cybersecurity to achieve national security and improve economic growth.
- Promote and provide opportunities to consult a network of international experts to address cyber issues.
- Increase funding for education and training programs to further develop the cybersecurity workforce.
- Increase initiatives related to cyber awareness for the public and private and public sectors.
- Focus on cybersecurity infrastructure to improve the security of information and networks.
- Facilitate work between the public and private sector to promote innovation and resilience to cyber threats.
- Conduct a comprehensive assessment of cybersecurity services , consider their strengths and weaknesses.
- Consider the components of the components of the proposed framework and develop a national cybersecurity strategy.
- Conduct awareness campaigns to improve the public and private sector knowledge of the best practices in cybersecurity.

8. Future Research:

- Expert opinion surveys on the success factors identified in this research.
- A comparative study of the success factors identified compared to those of other countries that have achieved leadership in cybersecurity.
- An analysis study of the challenges and obstacles facing Saudi Arabia in achieving excellence in cybersecurity.

9. Conclusion:

The Kingdom of Saudi Arabia has worked to establish its position among countries as a global leader in cybersecurity, as evidenced by its top spot in the Global Cybersecurity Index 2024.
This is attributed to the Kingdom's adoption of a robust framework with several important factors of success. This study pinpoints the key factors that have made this possible and enabled it, including centralized decision-making based on decentralized processes, massive investment in

cybersecurity, measured international cooperation, high priority on building human capital, and, of course, gender inclusion. Saudi Arabia also prioritizes staying ahead of new technologies and all that relates to end-to-end risk management, mapping them to national objectives. The cooperation between the private and public sectors cannot be ignored. Placing these actions at the top of the agenda has enabled the Kingdom to achieve a leading position in the field of cybersecurity and become an example for other countries, as one can easily see in the framework suggested to increase cybersecurity.

10. References:

A. Alzubaidi, *Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia*, Heliyon, Vol. 7, 1st edition, 2021

Aksoy, C. (2023). Are critical success factors for cybersecurity just technical issues? Cybersecurity management and the human factor. *Research Journal of Business and Management*, 10(2), 51-57. https://doi.org/10.17261/Pressacademia.2023.1735

Alam, R. G., & Ibrahim, H. (2021). Cybersecurity implementation success factors in smart city. *Journal of Theoretical and Applied Information Technology*, 99(13), 3353-3362.

Albediwi, M. R., & Sadaf, K. (2023). A framework for cybersecurity awareness in Saudi Arabia. *Journal of Engineering and Applied Sciences, 10*(1).

Albuhayri, W. (2019). *The future of electronic terrorism: challenges and methods of confrontation.* International Center for Future and Strategic Studies: Cairo.

Alhakami, W. (2024). Enhancing cybersecurity competency in the Kingdom of Saudi Arabia: A fuzzy decision-making approach. *Uncertain Supply Chain Management*.

Al-Harbi, F. E. (2018). *Cyber terrorism.* Riyadh.

Aljabri, S. (2021). Cybersecurity awareness in Saudi Arabia. *International Journal of Research Publication and Reviews, 2*(2), 320-330.

Alsemairi, S. S. (2023). Factors influencing employees on compliance with cybersecurity policies and their implications for protection of information and technology assets in Saudi Arabia. *Intelligent Information Management, 15*, 259-283. https://doi.org/10.4236/iim.2023.154013

Al-Zabn, Badra Huimel. (2012). *Terrorism in cyberspace.* Jordan: Amman University.

Ani, U.D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *J. Sys. Info. Technol., 21*, 2–35.

Antonakakis, N., et al. (2017). Understanding the Mirai botnet. In *Proceedings of the 26th USENIX Security Symposium* (pp. 1093-1110).

Brezavšček, A., & Baggia, A. (2025). Recent trends in information and cyber security maturity assessment: A systematic literature review. *Systems, 13*(1), 52. https://doi.org/10.3390/systems13010052

Buller, A. (2020). Saudi Arabia sees cyber security boom as coronavirus bites. Computer Weekly. Retrieved from https://www.computerweekly.com

CISA. (2021). *Cybersecurity and Infrastructure Security Agency Strategic Plan 2021-2025*. CISA.

CST. (2023). *What is Cybersecurity?* Retrieved from Communications, Space & Technology Commission: https://www.cst.gov.sa/en/Digitalknowledge/Pages/cyber-security.aspx

Dawson, M. (2021). An argument for cybersecurity in Saudi Arabia. *International Journal of Cyber Criminology, 17*(1), 40.

Global Cybersecurity Outlook 2025: Insight Report. (2025). World Economic Forum.

Hameed, F., Agrafiotis, I., Weisser, C., Goldsmith, M., & Creese, S. (2023). Analysing trends and success factors of international cybersecurity capacity-building initiatives. *International Journal of Reliability, Risk, and Safety: Theory and Application*, 6(1), 63-69. https://doi.org/10.22034/IJRRS.2023.6.1.7

Karjalainen, M., & Ojala, A. L. (2023). Authentic learning environment for in-service trainings of cyber security: a qualitative study. *International Journal of Continuing Engineering Education and Life-Long Learning, 1*(1), 1. https://doi.org/10.1504/ijceell.2023.10041126

Kazemi, A., Heydari, S. (2023). Ranking of factors affecting cybersecurity. *International Journal of Reliability, Risk, and Safety: Theory and Application*, 6(1), 63-69. https://doi.org/10.22034/IJRRS.2023.6.1.7

Klimoski, R. (2016). Critical success factors for cyber security leaders: Not just technical competence. *People Strategy, 39*, 14–18.

Kuusisto, R., & Kuusisto, T. (2013). Strategic Communication for Cyber-security Leadership. *Journal of Information Warfare, 12*(3), 41–48. Retrieved from: https://www.jstor.org/stable/26486840

Lehto, M., & Limnell, J. (2020). Strategic Leadership in Cyber Security, Case Finland. *Information Security Journal: A Global Perspective, 30*, 1-10. https://doi.org/10.1080/19393555.2020.1813851.

National Cybersecurity Authority (NCA). (2025). National Cybersecurity Strategy (Overview). Kingdom of Saudi Arabia.

National Institute of Standards and Technology (NIST) (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. NIST. Retrieved from https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

NCA. (2019). Critical Systems Cybersecurity Controls (CSCC - 1: 2019). National Cybersecurity Authority, Kingdom of Saudi Arabia.

NCA. (2019). Cybersecurity Guidelines for e-Commerce (CGEC – 1: 2019). National Cybersecurity Authority, Kingdom of Saudi Arabia.

NCA. (2020). The National Cryptographic Standards (NCS – 1: 2020). National Cybersecurity Authority, Kingdom of Saudi Arabia.

NCA. (2020). The Saudi Cybersecurity Higher Education Framework (SCyber-Edu – 1: 2020). National Cybersecurity Authority, Kingdom of Saudi Arabia.

NCA. (2020). The Saudi Cybersecurity Workforce Framework (SCyWF - 1: 2020). National Cybersecurity Authority, Kingdom of Saudi Arabia.

NCA. (2020). National Cybersecurity Strategy. Kingdom of Saudi Arabia.

NCA. (2021). Organizations' Social Media Accounts Cybersecurity Controls (OSMACC - 1:2021). National Cybersecurity Authority, Kingdom of Saudi Arabia.

NCA. (2021). Telework Cybersecurity Controls (TCC -1: 2021). National Cybersecurity Authority, Kingdom of Saudi Arabia.

NCA. (2022). Data Cybersecurity Controls (DCC -1:2022). National Cybersecurity Authority, Kingdom of Saudi Arabia.

NCA. (2022). Operational Technology Cybersecurity Controls (OTCC -1: 2022). National Cybersecurity Authority, Kingdom of Saudi Arabia.

NCA. (2024). Essential Systems Cybersecurity Controls (ECC – 2: 2024). National Cybersecurity Authority, Kingdom of Saudi Arabia.

NCA. (2024). Report on key economic indicators in the cybersecurity sector of 2024. National Cybersecurity Authority, Kingdom of Saudi Arabia.

Noor, A. F. M., Moghavvemi, S., & Tajudeen, F. P. (2024). Factors affecting cybersecurity readiness from dynamic capabilities perspective: A thematic review. *Journal of Theoretical and Applied Information Technology*, 14(4), 23970. https://doi.org/10.6007/IJARAFMS/v14-i4/23970

Okdem, S., & Okdem, S. (2024). Artificial Intelligence in Cybersecurity: A Review and a Case Study. *Applied Sciences*, 14(22), 10487. https://doi.org/10.3390/app142210487

Olech, A. (2021). Cybersecurity in Saudi Arabia. Institute of New Europe.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management, 9(12), 669-710. DOI: 10.18535/ijsrm/v9i12.ec04

Quadri, A., & Khan, M. K. (2019). Cybersecurity challenges of the Kingdom of Saudi Arabia: Past, Present and Future. Global Foundation for Cyber Studies and Research.

Ryttare, E. (2019). Change management: A key in achieving successful cybersecurity. A multiple case study of organizations in Sweden. Luleå University of Technology.

Saleh, T., Kanaan, R., Alzubaidi, R., Kanaand, G. G., & Nino, M. (2025). Factors affecting cybersecurity awareness: A qualitative study in Saudi Arabia. Uncertain Supply Chain Management, 13(2025), 751–762. https://doi.org/10.5267/j.uscm.2024.12.005

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data, 11*, Article 105.

Saudi Government. (2025). Cybersecurity in the Kingdom. Retrieved from Saudi Government website https://my.gov.sa/en/content/cybersecurity

Saudi Press Agency. (2024). Saudi Arabia Tops Global Cybersecurity Rankings. Retrieved from https://www.spa.gov.sa/en/N2125487

Saudi Press Agency. (2024, October 15). Saudi Arabia affirms commitment to global economic stability. Saudi Press Agency. https://www.spa.gov.sa/en/N2125487

Williams, P. A. (2019). *Cybersecurity: A comprehensive overview for directors and executives*. Wiley.

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. Deakin University, Centre for Cyber Resilience and Trust.

Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). A systematic synthesis of critical success factors for cybersecurity. *Computers and Security*, 118(July), 1-17. https://doi.org/10.1016/j.cose.2022.102724

Jones, A. (2015). Cybersecurity: Protecting critical infrastructures from cyber-attacks. International *Journal of Critical Infrastructure Protection*, 9, 1-2.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cybersecurity. *Journal of Digital Forensics, Security and Law, 12*(2), 53-74.

Asghar, M. R., Habib, M. A., & Khan, M. K. (2019). Cybersecurity challenges in cloud computing. *Future Generation Computer Systems, 100*, 544-561.

Alnatheer, M. (2015). Understanding and measuring information security culture in developing countries: Case of Saudi Arabia. *Journal of Information Security and Applications, 20*, 1-8.

Williams, P. (2011). The role of information security in protecting organizations from cyber threats. *Information Security Journal*: A Global Perspective, 20(1), 1-2.

Kumar, A. (2018). Cybersecurity: Protecting the future. *Information Security Journal: A Global Perspective, 27*(4), 1-8.

Doi: doi.org/10.52133/ijrsp.v6.68.3