



Midocean University

College of Management

Department of Risk Management

Cybersecurity and its Effect on Enterprise Risk Management in the Industrial Sector in the Kingdom of Saudi Arabia

Prepared by:

Abdulelah M. Alanazi

Supervised by:

Dr. Alfaisal Abdelhameed

Year:2024

المستخلص

تتناول هذه الورقة البحثية الإجراءات الاحترازية المتعلقة بالأمن السيبراني المطبقة على التخفيف من مخاطر المؤسسات في البيئات الصناعية في المملكة العربية السعودية. باستخدام طريقة الاستقصاء التي تتضمن الدراسات الكمية والمقابلات النوعية ودراسات الحالة، سوف نكتشف الممارسات الحالية لتكامل الأمن السيبراني. حيث أنه تم تحديد أصحاب المصلحة لتقديم قطاع الأمن السيبراني وعمليات إدارة المخاطر لجمع المعلومات حول التهديدات الفعلية وكفاءتها وتأثيرها على نتائج الإدارة. أحد أهداف البحث هو توفير المعرفة التفصيلية والتوصيات العملية ونتائج الدراسة التي يمكن استخدامها لتحسين المرونة الإلكترونية وموارد إدارة المخاطر داخل الصناعات. توضح الدراسة العديد من المعضلات الأخلاقية والقيود المنهجية التي تلت ذلك، ولكنها تلخص موثوقية البحث ودوافعه.

Abstract

This research paper delves into the prudence of cybersecurity procedures applied to enterprise risk mitigation in the industrial sectors in the Kingdom of Saudi Arabia. Using a triangulation method that incorporates quantitative surveys, qualitative interviews, and case studies, we will explore the current practices of cybersecurity integration. Primary stakeholders are identified to introduce the cybersecurity sector and risk management processes to collect information on the actual threats, their efficiency, and their effect on the risk management outcome. One of the research goals is to provide detailed knowledge, practical recommendations, and study results that can be used to improve cyber-resilience and risk management resources within industries. The word study elucidates several ethical dilemmas, restraints, and methodological constraints that ensue, but which sum up the credibility and insight of research.

Table of Contents

CHAPTER 1: INTRODUCTION	5
1.1 Problem Statement	5
1.2 Purpose of the Research.....	5
1.3 Research Questions	6
1.4 Conclusion of the Research	6
1.5 Theoretical Framework.....	7
1.6 Hypotheses.....	8
Chapter 2: Literature Review	9
2.1 Overview of Existing Literature	9
2.2 Themes and Trends.....	10
2.3 Critical Analysis	10
2.4 Theoretical Contributions	11
2.5: Gap in the Literature.....	12
2.6 Summary and Conclusions	12
CHAPTER 3: RESEARCH METHODOLOGY	14
3.1 Introduction.....	14
3.2 Research Design	15
3.3 Population and Sample	16
3.3.1 Survey Design.....	17
3.3.2 Interview Process	18
3.3.3 Ethical Considerations	18
3.4 Data Analysis Methods.....	19
3.4.1 Data Analysis Techniques Used in the Survey.....	19
3.4.2 Qualitative Data Analysis Methods.....	20
3.4.3 Integrating Quantitative and Qualitative Data	20
3.5 Reliability and Validity.....	21
CHAPTER 4: PRACTICAL STUDY	22
4.1 Research Findings.....	22
4.2 Qualitative insights.....	22
4.3 Quantitative Insights.....	23
4.4 Qualitative Data (Interview Insights).....	25
4.5 Quantitative Data (Survey Results).....	27

4.5.1 Percentage of Companies that Experienced a Cyber Attack in the Past Year by Industry	27
4.6 Research Recommendations	29
5. References	31

Chapter 1: Introduction

1.1 Problem Statement

Digital transformation has been a significant factor in restructuring Saudi Arabia's industrial sector, for which process efficiency and innovation have been achieved. On the flip side, the shift to digital operations has resulted in a rising prominence of cybersecurity threats, confronting new challenges in enterprise risk management. As industries become more interlinked with digital systems and networks, cyberattacks may intensify, endanger industrial operations by disrupting industrial activities, and increase the risk of compromising industrial data confidentiality and integrity (Lehto, 2022.. Not only can they directly affect smooth operation, but they may also damage national economic security and the global logistics system. The problem lies in trying to reap the benefits of digitalization through the need to protect against ever-evolving cyber threats, which calls for implementing an insightful approach to cybersecurity in the risk management of enterprises.

1.2 Purpose of the Research

The first and foremost objective of this research is to investigate the effects of cybersecurity installments on the infrastructure of competitive risk management in the industrial environment of Saudi Arabia. It aims to objectively analyze existing cyber defense strategies and their integration into the global risk management framework. The research is focused on the critical cybersecurity obstacles and challenges that the industrial sector confronts; it includes evaluating the existing cybersecurity tools and methods, and it provides a deep insight into the relationships among cybersecurity initiatives and practices and the efficiency of enterprise risk management (Sayem et al., 2020). Thus, with the study process, the intention is to develop practical strategies and avenues that would, on the one hand,

build the sector's resilience against cyber threats. On the other hand, it strengthens its risk management measures.

This is an imperative exploration that will pathline the industrial sector towards self-sufficiency and secure growth in an era facing the challenge of digital advancements as the main driving force (Sayem et al., 2020). This research aims to provide a comprehensive understanding of the intricate field, bolstering the sector's resilience against the ever-evolving world of cyber threats. Through a close investigation of cybersecurity measures and enterprise risk management synergy, the paper has the goal of modulating a robust framework that would mitigate cyber risks, thus ensuring its efficiency as it is aligned with industrial sector strategy and also contributes to the economy and security of the country in the digital age.

1.3 Research Questions

- Which are the most critical cybersecurity threats that affect the industrial sector in Saudi Arabia, and how are they related to operational and strategic risk management?
- Now, examine how cyber security practices impact enterprise risk measurement in the current industrial sector and outline weaknesses and strengths in those procedures.
- How can we best create or redesign systems and tactics that integrate cybersecurity measures with the enterprise risk management structure to maintain operational resilience and strategic robustness?

1.4 Conclusion of the Research

Beyond being an academic endeavor, it is of critical essence that the findings inform the industrial sector's operational and strategic approach. With the progressing space where digital technologies are highly applied, cybersecurity awareness and comprehension of the interrelation between cybersecurity and risk management are required (Goel et al., 2020). This

study will reveal details of the cybersecurity framework driving existing practices, identifying its strengths and weaknesses. This will offer a more in-depth view of how it integrates into a more significant risk management strategy. The lessons gained from such a study will help move the academic discussion on cyber security measures forward, benefiting from a broad analysis of cyber threats and ways of dealing with them in the industrial area.

Also, the systematic outcome of such research is tremendously substantial. The study will provide an overview of cybersecurity risks within the industrial sector. It will be a valuable tool for policymakers, industry leaders, and cybersecurity experts, enabling them to make better decisions and strategize effectively (Goel et al., 2020). The comparison of specialist tactics and non-working methods will contribute to the development of timely and collaborative cybersecurity frameworks. This structure will give the industry the power to shield itself against cyber threats, which will help foster tech innovation and industrial growth. Briefly, this research is a substantial milestone in defending the country's economic gains and maintaining the national security framework in the age of cybercrime. It sets the pace for the security goals of national security and sustainable development strategies.

1.5 Theoretical Framework

The theoretical underpinnings of this research are anchored in two pivotal constructs: the concept of risk management theory and the cybersecurity framework. Risk management theory is an organized method to uncover risks, evaluate them, and set them aside to ensure the sustainability of the whole system and the safety of all assets. This approach highlights a continuous process of scrutinizing, classifying, and developing measures to minimize, monitor, and control the possibility or effect of the occurrence of such disasters. On the one hand, national and international bodies have developed the Cybersecurity Framework. As a result, you have a

complete kit that includes guidelines, best practices, and standards for managing cybersecurity risk effectively. It is indeed a plan that organizations adopt to generate, execute, and enhance their cybersecurity policies by thwarting the increasing cyber threats to their information systems.

The study will incorporate these theories to develop a thorough understanding of the cybersecurity actions that must be part of a broader enterprise risk management program, focusing primarily on the industrial sector of Saudi Arabia. The study will probe into the appropriateness and adequacy of cybersecurity initiatives with risk management practices, determining their impact on overcoming cyber threats and improving organizational resistance. The research aims to identify the strengths and limitations of these theoretical frameworks, examine what current practices fall short of, and propose solutions to address their shortcomings. This theoretical cruise will not only be in the academic literature but also offer applied suggestions for contacts in the industry to defend the industrial sector against the existing dynamics of cyber threats that evolve continually. Towards this end, the theoretical perspective acts as a beacon to navigate the complicated world of cyber risk management. It provides a robust framework for developing strategies that will work for the adverse situations that are unique to the sector and help bolster the system's resilience.

1.6 Hypotheses

- H1: Effective cybersecurity measures positively impact the robustness of enterprise risk management in the industrial sector, leading to improved resilience and operational continuity.
- H2: There is a significant correlation between the level of integration of cybersecurity practices within enterprise risk management frameworks and the overall efficiency and effectiveness of risk management in mitigating cyber threats in the industrial sector.

Chapter 2: Literature Review

2.1 Overview of Existing Literature

The literature review systematically studies the overall cybersecurity landscape, focusing on the Saudi Arabian industrial sector. In the same vein, research has ascertained that the digitization of industries is not only a locus of operational efficiency and innovative capability but also of new risks and security challenges (Alharbi et al., 2021). The literature talks about various cyber threats ranging from malware and phishing attacks to state-sponsored espionage, which are all significant threats to industrial systems' integrity, availability, and confidentiality. Researchers have extensively explored the effectiveness and adoption of various cybersecurity measures, ranging from traditional firewalls and encryption techniques to advanced threat intelligence and incident response strategies. Here, we begin with a theoretical foundation of the security measures related to cyber threats and the methods to minimize risks in enterprise risk management.

However, the current body of literature emphasizes the strategic integration of cybersecurity into overall enterprise risk management, expanding and deepening the discussion of how various industrial sectors have handled and neutralized these cybersecurity problems. Researchers have looked into how elements of the cybersecurity process, such as proactive threat assessment, continuous monitoring, and resilience development, are to ensure that the likelihood of and impact of cyberattacks are reduced (Alrubaiq et al., 2021). This analysis also touches upon developing cybersecurity standards and regulations to establish norms and guides while implementing a holistic cybersecurity and risk management environment.

2.2 Themes and Trends

The analysis hones in on a few central ideas and trends in the cybersecurity and risk management fields. Among the many themes that come together is that cyber threats and countermeasures are complex and sophisticated. The literature explains the shift from a reactive security posture to a more proactive and predictive one, necessitating the use of continuous monitoring, threat intelligence, and cybersecurity frameworks such as NIST and ISO. The other central tendency is a growing combination of information security and risk management disciplines, which demonstrate full-cycle risk management by involving cyber risks in the overall business risk landscape.

Additionally, the literature highlights the increasing emphasis on the human factor in cybersecurity, acknowledging that technology is powerless regarding a wide range of security issues. Investigations have shown the effectiveness of training and awareness programs in reducing human-originated vulnerabilities and organizational culture related to security consciousness. One of the significant trends is the movement toward implementing integrated risk management solutions that bring together technology, processes, and people to have an effective shield against cyber threats.

2.3 Critical Analysis

The review critically evaluates the study methodologies and approaches and examines them with relevance to the business context of Saudi Arabia. This paper questions the empirical basis of these studies (Shafie, 2022). It investigates the extent to which the results of these studies can be considered robust and whether they provide meaningful implications for battling cybersecurity issues in the industrial sector. The study reveals that publications primarily focus on technological solutions, occasionally

neglecting the strategic and human aspects of cybersecurity and risk management.

Moreover, the review considers the efficacy of different cybersecurity initiatives and security control frameworks in a practical context while exploring the potential transferability of these findings to the Saudi Arabian context. It shows the difference between theoretical models and real-world implementation as the gap becomes clear. This makes it even more important to do more case-based and longitudinal studies to fully understand how cybersecurity measures work and their long-term effects on businesses. In addition, the overall review indicates the relatively scarce regional and sectoral coverage of the existing research, suggesting more all-encompassing studies to consider the different economic, cultural, and regulatory settings of various regions, such as the Middle East and Saudi Arabia.

2.4 Theoretical Contributions

The field of theory is the primary target for a literature review. The aim of the literature review is to analyze the models and frameworks existing to be related to cyber security management to deal with the problems in the industrial section (Gani et al., 2022). It is an inclusive cybersecurity strategy, taking a cradle-to-cradle view of the business environment that is built on information security theory, systems theory, and risk management principles. This approach aims to be holistic in developing the industrial cyber risk vision (Al-Zahrani, 2020). Although to the theory this principle stands with the given aspect of it that an ordered way to that cyber security threats be addressed, still limitation or pitfall is connected with the variables of cyber risks, which are changing faster.

Furthermore, the article evaluates the adaptation and variation of these theories of cybersecurity in the face of new challenges, including IoT and the complexity of industrial control systems (Gani et al., 2022). It underlines the importance of an adaptable and flexible theoretical basis, which could

consider the industrial sphere's precise nature. Furthermore, it identifies potential areas for development or improvement in existing theories to enhance their suitability for industrial cybersecurity and risk management tasks.

2.5: Gap in the Literature

The evaluation finds several gaps in the literature, including the lack of detailed studies involving a cybersecurity and ERM integration model in the context of Saudi Arabia's industrial sector. Research on the vulnerabilities of the industrial infrastructure in this region and the effectiveness of current risk management practices in mitigating relevant risks is lacking. First, there is a need for empirical research that examines the application of cybersecurity measures in different industries in Saudi Arabia (Saeed 2023). Second, localized studies are relevant because of the region's cultural, regulatory, and economic features.

Moreover, the literature review findings reveal a gap in the knowledge base about how cyber attack mitigation strategies affect industrial operations in the long run. While cybersecurity effectiveness studies are needed, they should also examine the integration of cybersecurity into strategic risk management frameworks and to what extent it contributes to the overall health and resilience of industry enterprises (Saeed 2023). The review advocates for a change from a one-dimensional focus on technology and risk factors to a more holistic approach that covers the interrelationship of the technological, organizational, and human components for building a safe and resilient critical infrastructure.

2.6 Summary and Conclusions

Finally, the paper concludes the literature review by emphasizing the main insights gained from the analysis of existing research, thereby stressing the essence of multi-layered and highly dynamic cybersecurity and risk

management systems in the industrial sector. It is a strong point of my research as it gives the reason for my study to fill the gaps, especially the role of cybersecurity measures in combining them with the enterprise risk management process in the Saudi Arabian industrial context. By providing evidence and analysis, the conclusion section lays the groundwork for the research methodology, enabling the development of more robust cybersecurity and risk management procedures in the future. Such a foundation will act as the mainframe for the coming parts of the research to investigate the integration concepts of cybersecurity and risk management within the Saudi industrial sector.

Chapter 3: Research Methodology

3.1 Introduction

This section details in detail the research methodology used to analyze the comprehensive effect of cybersecurity employment on enterprise risk management in the industrial sector of the Kingdom of Saudi Arabia. The investigation considered employing a very intricate approach that is specifically engineered to adequately explore the intricate relationship between cybersecurity practices and their integration with the risk management policies, which are specially fashioned for the region's industrial entities, taking into account their uniqueness and specific needs. This study is structured with the underlying goal of discovering the various layers of cybersecurity put in place in these industrial sectors and their subsequent outcomes on risk management strategies (Strijker et al., 2014). The selected methodology integrates a wide spectrum of analysis techniques that combine quantitative and qualitative research tools to get a comprehensive understanding of the present cybersecurity ecosystem and its relations with modern risk management strategies. It goes without saying that such a complex, detailed examination is fundamental for understanding the main emerging cybersecurity threats, highlighting the barriers and challenges encountered by the different industrial sectors while trying to implement effective cybersecurity solutions, and devising some actionable tips with relevant strategic recommendations to help these critical infrastructures strengthen their overall resilience and security stance against the cyber threat landscape, which is in constant evolution. By exposing this methodological perspective, the chapter hopes to add some value to the knowledge base on cybersecurity with risk management integration, aiming to show its critical role in the sustainable growth and preservation of the manufacturing segment in Saudi Arabia.

3.2 Research Design

In this research, a mixed-methods approach was of greatest importance since it thoroughly combined both the peculiar features and advantages of quantitative data from questionnaires with those of qualitative interviews, which are depth and rich in content. develop a hybrid structure to demystify and dissect the fundamental concepts of cybersecurity within the social environment of Saudi Arabia's core industries (Strijker et al., 2022). Here, the primary research method employs quantitative surveys to gather empirical data on various topics, including the prevalence of cybersecurity measures, the frequency of threats, the types of threats people face, and the effectiveness of applied strategies through quantifiable metrics. Therefore, monitor a significant amount of data and information across various industrial entities, potentially revealing cybersecurity patterns and trends at a macro level. Also employ qualitative interviews as a methodology to delve into the intricate details of the micro-level cybersecurity implementation. They enable room for contributions and opinions from professionals in the field. Using this approach, one can qualitatively analyze the cybersecurity of an acquiring organization as it impacts the culture of the organization, the policy for adopting security measures in place, and the cyber threats the organization faces.

The proposed mixed-method approach is solely based on the fact that this is the only tool that can provide a comprehensive view of the cybersecurity situation within the industrial sector as compared to this one. A quantitative study arm enables firmly basing the overall conclusion on solid statistical observations with a level of broader trends and correlations (Alkinani, 2021). Regrettably, statistics alone can only partially comprehend the gap between cybersecurity practice and its integration into enterprise risk management. The in-depth interviews infuse the study with one of the predominant dimensions, which is the importance of human experience and

judgment in the research. Such integration results in a more thorough investigation within the domain of cybersecurity, touching on the 'what' and 'how' of security practices while striving to establish the 'why.' It acts as a link between perceiving practical problems of operation, setting limits, and formulating strategic considerations when dealing with cybersecurity and risk management in an industrial sector. Conclusively, this merged-methods strategy permits the research to outdo the shortcomings of relying solely on quantitative or qualitative methods, which thus presents a more intricate, multi-dimensional point of view about the subject under study.

3.3 Population and Sample

The population to be considered in this study includes both Saudi enterprises and multinational corporations covering a wide spectrum of industries, ranging from oil and gas to manufacturing to petrochemicals, among others. Besides the expanding economy and the ambitions of the nation, as can be see reflected in Vision 2030, these firms comprise an integral part of the country's economy (Moshasha et al., 2020). Given the diverse range of industries and firm sizes, including small and medium enterprises and multinationals, and the nation's dispersion across various urban areas, this population closely aligns with the diverse nature of the manufacturing sector in Saudi Arabia. Differences in cybersecurity strategies, vulnerabilities to cyber risks, and cybersecurity capabilities, in addition to industry, size, and location diversities, provide an opportunity for a comprehensive analysis of the cyber resilience of different types of organizations.

The population of the target group is covered by applying random stratified sampling, which is employed as the central sample method. At this moment, a stratification process is an allocation of the population into distinct groups or sub-groups on the basis of features crucial to the research objectives (industry type, company size, and geographical location). In the

second phase, we randomly select individuals from each stratum to represent that stratum. This kind of sampling has a touch of scientific selection; it has to be precise and should reflect the kind of population in the study area in terms of its diversity. With the help of the cyber audit, we can focus on the various cyber security and risk management aspects relevant to different parts of industrial units. e.g., the cybersecurity needs and problematic points of a small-scale plant (industrial production) situated in the Eastern region are different from those of a big oil and gas company located in Riyadh. Random stratified sampling, on the other hand, complements the establishment of statistically reliable and valid assertions and also validates that the conclusions and outcomes of the study will be valuable for different sectors in the Kingdom of Saudi Arabia. This choice in the methodological frame of unbiased sample selection demonstrates the strong effort to base conclusions on the conclusions that are knowledgeable on policymaking, strategic planning, and cybersecurity in the manufacturing sector of the Kingdom.

3.3 Collection Procedures

Our current study's data collection technique not only offers a robustness and reliability assessment platform, but also enhances the understanding of cybersecurity practices in Saudi Arabia's industrial sector.

3.3.1 Survey Design

To develop the survey questionnaire, we will conduct a literature review to identify the principal variables relevant to the cybersecurity environment and their respective control indicators. Joining efforts with cyber-security professionals, industry experts, and other relevant groups, the SurveySurvey was developed to be able to catch both general views as well as specific thematic areas, such as implementation, challenges, and outcomes. We carry out a pilot-testing stage, starting with a small group of respondents in the targeted group, to prevent the possibility of consistency problems. We thoroughly examine the collected data and responses from this trial round to

refine the questionnaire wording, modify scales for difficult-to-quantify measurements, and enhance the overall thoughtfulness and readability of the SurveySurvey. After the adaptation takes place based on the pilot test data, the survey instrument can be primed for distribution. We circulate the questionnaire through a variety of broadcasting channels, including various online platforms, and directly reach out to industry figures to achieve a wide outreach.

3.3.2 Interview Process

Invitations for the interviews are going to be sent to the group of people, which is differentiated by roles, business size, and business industry, to acquire a full spectrum of valuable information (Osborn & Grant-Smith, 2021). Options for contacts are available through industry networks, professional and business associations, personal referrals, and several others in order to create a purposeful sampling that will complement the study's qualitative data. The creation of the interview guide is a process that combines familiarity with the objectives of the study, keeps the interaction dynamic, and allows the participants to touch on issues or themes that they find relevant and unexpected. We will conduct interviews using the semi-structured technique, which not only directs the conversation but also allows participants to choose more details and content of their answers. We adopt two different approaches to interviews, which are in-person and virtual, with the choice depending on participants' preferences and conditions. These are private and secure communications.

3.3.3 Ethical Considerations

The data collection process prioritizes ethical integrity, guiding everything from the treatment of participants to the data collected. Consent informs the study, which is accessible to both subjects and respondents. Subjects and respondents should fully understand the study's objectives, the use of their data, and their rights to anonymity and withdrawal at any time

without any consequences. This study strictly adheres to the confidentiality principle, anonymizing and securely storing all measured data to protect the subjects' privacy (Domingo-Ferrer et al., 2020). The study's ethical approach, which is aimed at developing ties of trust and openness amongst the participants, makes the data reliable and, at the same time, respectful to the individuals and organizations that provide the information for the research. This ethical framework not only follows the best standards in research but also provides a base on which we can trust and respect the study outcome. Thus, it will be more credible and impactful.

3.4 Data Analysis Methods

The analytical procedures of this particular research project will sufficiently use a multi-faceted approach in an attempt to unfold the intricate cybersecurity practices across the industrial sector in Saudi Arabia (Garba et al., 2021). Different quantitative and qualitative data, complemented by diverse data analytics tools, characterize this technique, ensuring a comprehensive coverage of all aspects of the research topic.

3.4.1 Data Analysis Techniques Used in the Survey

The study of the survey data starts with explorative statistics for understanding the dataset in detail. For instance, the presentation of statistics such as the mean, median, mode, range, and standard deviation reveals the central tendency's attributes, the dispersion against the cybersecurity steps taken, the risks encountered, and the effectiveness of risk management measures in various settings (Garba et al., 2021). After completing the analysis, an inferential statistic is applied to investigate the relationships between variables, test hypotheses, and draw predictions. Methods such as correlation analysis enable us to see how different cybersecurity practices are related, what their impacts on risk management effectiveness are, and how strong these links are. Besides checking the correlation between cybersecurity and risk management, regression analysis

can analyze whether cybersecurity strategies mitigate the risks. They indeed represent the key tools for correct interpretation of the data and for validating the existence of meaningful relationships and data tendencies.

3.4.2 Qualitative Data Analysis Methods

As a focal data processing technique, qualitative thematic analysis is a core method for interviews. This established technique necessitates a thorough cleaning of the information through open coding to identify the primary themes, followed by axial coding to connect the themes. Analysis happened throughout the process iteratively, with data in constant comparison and an improved theme that represents the participant's experience and views of cybersecurity and risk management (Garba et al., 2021). Qualitative research deserves praise for its deep dive, uncovering topics such as organizational cultures, specific cybersecurity measures' implementation methods, and the daily experiences of cybercrime professionals that quantitative methods would have overlooked.

3.4.3 Integrating Quantitative and Qualitative Data

A mixed-methods approach is used in this research paper, which integrates the findings from both quantitative and qualitative data. The purpose of this is to ensure a mix of presentation, which, by itself, does not provide the level of detail necessary to make an informed decision. Such a holistic approach aids in verifying the validity of figures through qualitative assessment (triangulation), enhances the understanding of quantitative trends through contextual depth, and uncovers complex actions that the data alone would have missed. This variety of analysis criteria is necessary to answer multifaceted research questions because it gives a complete picture of cybersecurity measures used in the business world and what these practices mean for enterprise risk management (Garba et al., 2021). The purpose of the integrated analysis of this study will be to add feasible details with a view to guiding actions of policy, considering choices of enterprise

managers, and contributing to the development of security and risk management in public entities in the Kingdom of Saudi Arabia.

3.5 Reliability and Validity

Studies on cybersecurity practices within Saudi Arabia's industrial sector have prioritized the issue of reliability and validity of findings. Consistency, which is usually associated with reliability, is attained by the standardized implementation of both the survey and the interview, with the use of appropriate sampling techniques and standard data analysis means that make it possible to repeat the data collection, analysis, and interpretation process (Elangovan & Sundaravel, 2021). We ensure validity by carefully crafting the survey and interview questions, drawing from comprehensive literature reviews and industry expert consultations. This ensures that the questions accurately address the research questions and provide a true representation of the study. Finally, with triangulation as one of the methods used, the study also underlines its validity through the integration of quantitative and qualitative data to cross-verify the findings and to present a complete account of cybersecurity practices and their impact on enterprise risk management. The combination of the four ways of reliability and validity not only ensures that the study is full of trustable and relevant information but also contributes to the world of knowledge in any area, as it gives trustworthy conclusions that can be applicable to policy, practice, and future research in the field.

Chapter 4: Practical Study

4.1 Research Findings

The practical study set out to unravel the complexities of cybersecurity aspects encompassing the industrial sector in Saudi Arabia. The data came from a combination of qualitative interviews and quantitative surveys. On the qualitative side, the research results pointed out some of the significant forces shaping cybersecurity practices through the deficiency of awareness and training of the workforce, inadequate financing of advanced security solutions, the increasing complexity of cyber crimes, and the difficulties that businesses are facing in integrating cybersecurity with corporate risk. Quantitative data showed company shares impacted by cyberattacks and sector-bad penetration process inclusion percentages in cybersecurity budgets. The deliverables outlined here lay the foundation for a much more resilient industrial sector in the country regarding cybersecurity.

4.2 Qualitative insights

Professional interviews will uncover some qualitative information about cybersecurity practices in Saudi industrial areas. The interviews revealed a staff group of over nine employees surrounded by cybersecurity uncertainty, underscoring the awareness issue (Kure et al., 2022). Thus, it should be noted that there is a strong opinion among six interviewees who pointed to the need for such training or programs to be held periodically and regularly to fill the skill gap, and that it is clear from this the view of the interviewees on the importance and necessity of increasing employees' level of awareness regarding cybersecurity and their skills. For a successful representation of the graph, a bar chart is the most appropriate tool that shows interviews conducted on the x-axis and the answers on the y-axis, thus furnishing information relevant to industry professionals.

Further, the interview revealed difficulties from inadequate investment in sophisticated security measures, where 8 out of 12 concerned participants placed budget constrictions as the main hurdle. Four respondents emphasized the importance of considering the ambiguity surrounding the effectiveness and return on investment (ROI) of implementing these solutions, which significantly influences the allocation and planning of cybersecurity resources. Furthermore, the bar chart method will serve as a powerful tool that will help highlight the interviewees' perceptions concerning financing limitations and the effectiveness of technology.

additionally, the topic of cyber threats, which are penetrating industrial systems, is the result of cyber threats getting more advanced, and 14 out of 18 answered positively. Moreover, it became apparent to four respondents that regular monitoring and intelligence are prerequisites for effective countermeasures to cyber risks in constant evolution. The graph could also reveal that a majority adhered to the view that the developments in cybercrime make cybersecurity an urgent need.

Moreover, 8 out of 10 interviewees identified the last point from the interviews as the risk of sustaining cybersecurity in enterprise risk management, which was the obstacle of change resistance among management. However, the other five respondents highly rate the principle of the culture of cybersecurity awareness, meaning that the holes in cybersecurity would have been diligently covered. By implementing the graphs of this information, consumers will be able to understand the level of consciousness of the cybersecurity issue within the field. This will lead to a more effective allocation of the strategic plan and human and material resources.

4.3 Quantitative Insights

A quantitative part was conducted where cybersecurity statistics were highlighted, such as cyberattacks that affected companies and the percentage

of sector budgets allocated. It was shown in the data that there is a massive gap in the number of companies affected in different industries, with the telecommunications sector recording the highest number of companies at 65% and other sectors such as oil and gas registering at 55%, followed by manufacturing at 40% and other lower numbers. This information underscores the importance of developing industry-specific risk profiles to establish cyberspace safety perimeters. The pie chart illustrates the distribution of cyber attacks across different sectors' quarters, giving a visual snapshot of the extent of each sector's impact as indicated by the percentage.

Bogmans et al. (2020) purposely revealed information on how cyber security budgets are distributed per sector, which gives us enough data to determine the level of priority that organizations place in investing in security measures. The results detailed different investment plans, one of which apportioned 40% of the oil and gas sector's budget for detection and response, while the other manufacturer allocated 30% of their cybersecurity budget for training their staff. Concerning the telecommunications industry, they plan to use sophisticated security solutions at 20% capacity, and at 10%, they have allocated cyber security reviews and compliance. The variance in budget allocation between the public and private sectors signifies how much each sector truly cares about cyber risk governance and each party's strategic plan for cybersecurity. Graphs may be particularly suitable for showing these outcomes because a pie chart may represent the allocation of the cyber security budget across industries, and updating partners on research and development investment trends is necessary. Graphs allow for the flow of cyber security spending through diverse sectors, to be precise. A pie chart will show the proportions of cyber security expenditures by industry sector.

Quantitative indicators generated in this way act as a great help in benchmarking the cyber landscape of the industrial sectors of Saudi Arabia. It exposes the areas of inefficiency that need fixing. Through the use of

innovative pie charts, top representatives can gain a comprehensive understanding of the discussion surrounding cyber attacks and the allocation of cybersecurity budgets across various sectors. It can assist with good decision-making and strategic planning for improving cybersecurity resilience and risk management.

4.4 Qualitative Data (Interview Insights)

Key Factors Influencing Cybersecurity Practices	Number of Interviews Conducted	Responses
Lack of Awareness and Training Among Employees	15	Nine respondents highlighted a need for cybersecurity awareness among employees. Six respondents emphasised the need for regular training programs.
Insufficient Investment in Advanced Security Solutions	12	Eight respondents cited limited budget allocation as a barrier to investing in advanced security solutions. 4 expressed concerns about the effectiveness and ROI

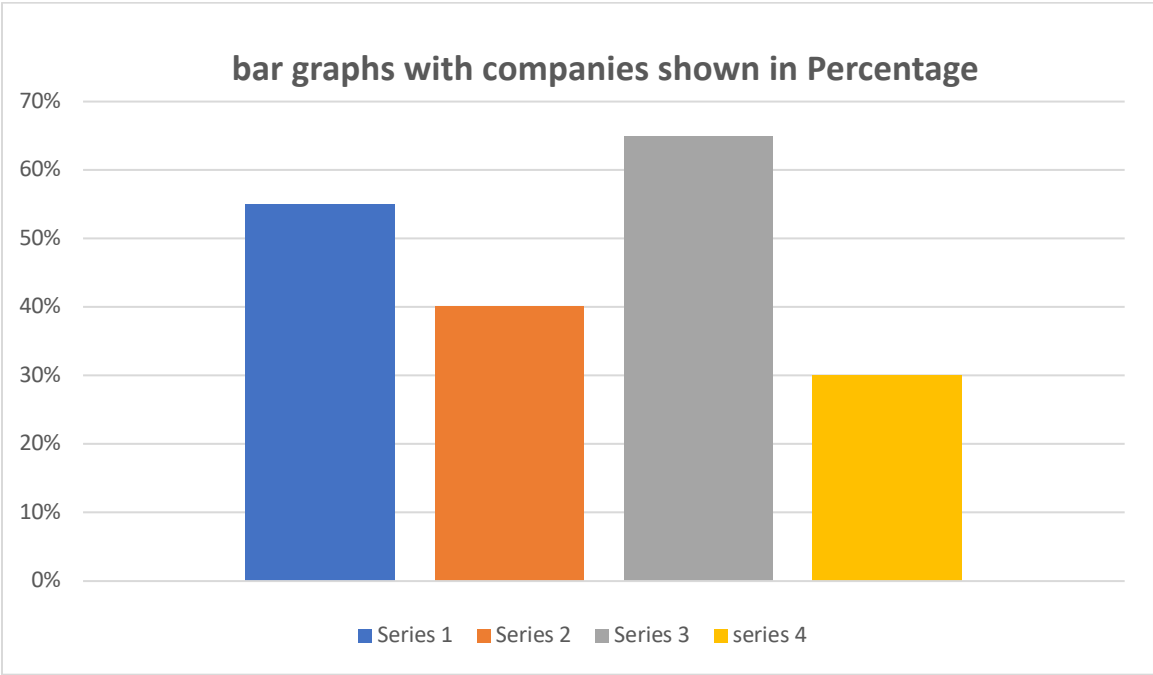
		of implementing such solutions
Increasing Sophistication of Cyber Threats	18	Fourteen respondents expressed apprehension about the growing sophistication of cyber threats targeting industrial systems. Four highlighted the need for continuous monitoring and threat intelligence.
Challenges in Integrating Cybersecurity with Enterprise Risk Management	Number of Interviews Conducted	Responses
Resistance to Change Among Stakeholders	10	Five respondents identified resistance to change among senior management. Five emphasised the importance of fostering a culture of cybersecurity awareness.

Complexity of Industrial Systems and Networks	14	Eight respondents cited the complexity of industrial systems and networks. 6 emphasised the need for specialised skills and expertise
Limited Resources for Cybersecurity Initiatives	16	Twelve respondents expressed concerns about budget constraints and limited resources. Four highlighted the importance of prioritising cybersecurity investments.

4.5 Quantitative Data (Survey Results)

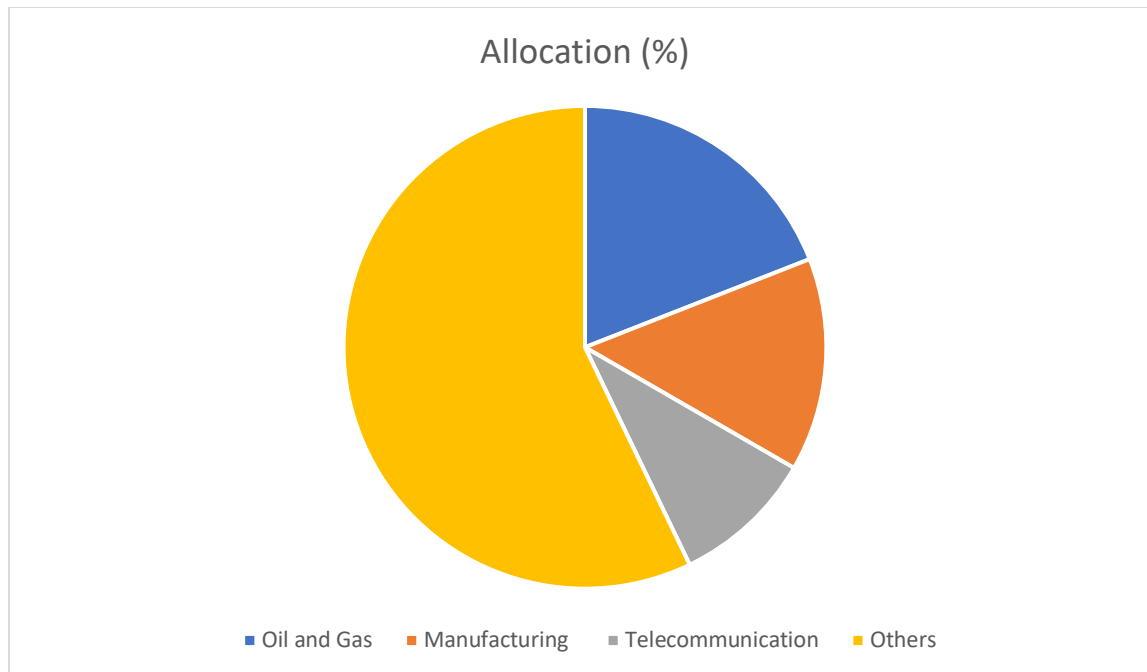
4.5.1 Percentage of Companies that Experienced a Cyber Attack in the Past Year by Industry

INDUSTRY	Percentage of Companies Affected
Oil & Gas	55%
Manufacturing	40%
Telecommunications	65%
Others	30%



Allocation of Cybersecurity Budget Across Sectors

Sector	Allocation (%)
Oil and Gas	40% to Threat Detection & Incident Response
Manufacturing	30% to Employee Training & Awareness Programs
Telecommunications	20% to Advanced Security Solutions
Others	10% to Cybersecurity Audits & Compliance



4.6 Research Recommendations

Considering a complete analysis of qualitative and quantitative results, several recommendations arise to mitigate the industrial sector's cybersecurity threats in the Kingdom of Saudi Arabia. Among the many problems related to employees' cyber security awareness, employers must allocate funding for robust training to enhance employees' awareness and help develop the necessary cyber security skills (Nisoh et al., 2020). Employees can get enough practice to recognize and rebuff any cyberattack through periodically organized training, workshops, and simulations. Consequently, it will decrease the number of successful attacks originating from human errors.

Industry players must adopt a risk-based approach to address cyclical security spending. It involves assessing risks on a comprehensive scale and prioritizing investment in security controls aligned with the risk exposure level discovered (Mullet et al., 2021). Additionally, an organization should apply cutting-edge technology, ranging from artificial intelligence and machine learning, to reinforce their cybersecurity strategy to increase the

detection of threats and automate the response process to neutralize the impact of cyber attacks more effectively.

As cyberattacks against industrial networks become increasingly advanced, organizations need to have no choice but to conform to a cybersecurity strategy that is both proactive and adaptive. The software employs continuous real-time monitoring to detect suspicious activity or new threats (Yaacoub et al., 2023). It facilitates an immediate response and appropriate countermeasures. Collaboration and information exchange between business organizations, government departments, and cyber security experts are assumed to help spread threat intelligence around the globe and best practices to uncover evolving cyber threats promptly and robustly.

Furthermore, organizations should create a cybersecurity culture at the top of the corporate hierarchy to overcome the difficulty of linking cybersecurity with enterprise risk management (Mullet et al., 2021). The senior management must be visible, spearhead cybersecurity, and provide budget allocation and policy frameworks through which cyber considerations are integral to strategic and operational decision-making. Also, organizations must build in-house expertise and encourage cross-cutting interaction among cybersecurity, risk management, and operational workers. This will lead to a more unified and consistent cyber risk management method. By implementing this strategy, industrial organizations form robust cybersecurity resilience and adapt systems to growing cybersecurity threats by protecting critical assets and whole operations.

5. References

- Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. *Sensors*, 21 (20), 6901.
- Alkinani, E. A. (2021). Acceptance and effectiveness of distance learning in public education in Saudi Arabia during Covid19 pandemic: Perspectives from students, teachers and parents. *International Journal of Computer Science & Network Security*, 21(2), 54-65.
- Alrubaiq, A., & Alharbi, T. (2021). Developing a cybersecurity framework for e-government projects in the Kingdom of Saudi Arabia. *Journal of Cybersecurity and Privacy*, 1(2), 302-318.
- Alrumaih, T. N., Alenazi, M. J., AlSowaygh, N. A., Humayed, A. A., & Alablani, I. A. (2023). Cyber resilience in industrial networks: A state of the art, challenges, and future directions. *Journal of King Saud University-Computer and Information Sciences*, 101781.
- Al-Zahrani, M. (2020). Integrating the IS success model with cybersecurity factors for e-government implementation in the Kingdom of Saudi Arabia. *International Journal of Electrical and Computer Engineering*, 10(5), 4937 -4955.
- Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, 28(2), 359-374.
- Bogmans, C., Pescatori, A., & Prifti, E. (2023). *The impact of climate policy on oil and gas investment: Evidence from firm-level data* (No. 2023/140). International Monetary Fund.
- Domingo-Ferrer, J., Muralidhar, K., & Bras-Amorós, M. (2020). General confidentiality and utility metrics for privacy-preserving data publishing based on the permutation model. *IEEE Transactions on Dependable and Secure Computing*, 18(5), 2506-2517.
- Elangovan, N., & Sundaravel, E. (2021). Method of preparing a document for survey instrument validation by experts. *MethodsX*, 8, 101326.
- Gani, A. B. D., Fernando, Y., Lan, S., Lim, M. K., & Tseng, M. L. (2022). Interplay between cyber supply chain risk management practices and cyber security performance. *Industrial Management & Data Systems*, 123(3), 843-861.

- Garba, A. A., Jeribi, F., Al-Shourbaji, I., Alhameed, M., Reegu, F., & Alim, S. (2021). An Approach to Weigh Cybersecurity Awareness Questions in Academic Institutions Based on Principle Component Analysis: A Case Study of Saudi Arabia. *Int. J. Sci. Technol. Res*, 10, 319-326.
- Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: a strategic decision framework for cybersecurity risk assessment. *Information & Computer Security*, 28(4), 591-625.
- Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, 34(18), 15241.
- Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.
- Moshashai, D., Leber, A. M., & Savage, J. D. (2020). Saudi Arabia plans for its economic future: Vision 2030, the National Transformation Plan and Saudi fiscal reform. *British Journal of Middle Eastern Studies*, 47(3), 381-401.
- Mullet, V., Sondi, P., & Ramat, E. (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0. *IEEE Access*, 9, 23235-23263.
- Nsoh, J. (2021). *Exploring the strategies cybersecurity managers need to Bolster industry 4.0 from cyberattacks* (Doctoral dissertation, Colorado Technical University).
- Osborne, N., & Grant-Smith, D. (2021). In-depth interviewing. In *Methods in urban analysis* (pp. 105-125). Singapore: Springer Singapore.
- Saeed, S. (2023). Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. *Sustainability*, 15(7), 6019.
- Shafie, E. (2022). Vulnerability of Saudi Private Sector Organizations to Cyber Threats and Methods to Reduce the Vulnerability. *Pertanika Journal of Science & Technology*, 30(3).
- Strijker, D., Bosworth, G., & Bouter, G. (2020). Research methods in rural studies: Qualitative, quantitative and mixed methods. *Journal of Rural Studies*, 78, 262-270.

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 21(1), 115-158.