

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص إدارة مخاطر



العنوان باللغة العربية

تقييم تأثير التقنيات الناشئة (e.g., AI, IoT) على إدارة مخاطر الأمن السيبراني.

إعداد الطالب/ فهد بن احمد الهديان

إشراف/ د. وليد عبدالجواد سليمان صديق

د. الفيصل عبدالحميد محمد حسن

العام الدراسي:

2023

Executive Summary

This study delves at the impact that cutting-edge innovations like AI and IoT are having on the field of cybersecurity risk management. The paper shows the increasing use of AI in cybersecurity practices, highlighting its revolutionary effect on the way difficult cybersecurity issues are approached, especially in the areas of threat detection, incident response, and vulnerability management. Security flaws and limited device processing power are slowing the widespread adoption of IoT as AI's use continues to grow. Cybersecurity resilience in a dynamic threat landscape requires attention to ethical considerations and legal frameworks for AI, as well as the adoption of standardized security procedures for the Internet of Things (IoT). This study lays the groundwork for future cybersecurity research and innovation by providing crucial insights for practitioners, researchers, and policymakers.

Contents

Executive Summary 2

Chapter One: Introduction 4

Research Objectives 6

Chapter Two: Literature Review 6

AI in Cybersecurity: Applications and Benefits 6

IoT Devices and Security Challenges 8

Cybersecurity Risk Management Strategies and Best Practices 10

Recent Research and Identified Gaps 12

Chapter 3 Methodology 14

Research Design and Approach 14

Surveys 14

Interviews 15

Sample Selection 15

Data Analysis Methods 15

Chapter 4: Findings 15

Chapter 5: Discussion 18

Chapter 6: Conclusion 20

References 22

Assessing the Impact of Emerging Technologies (e.g., AI, IoT) on

Cybersecurity Risk Management

Chapter One: Introduction

Cyberspace is an eternal conflict, where both sides must continually adapt to stay one step ahead of their respective enemies. The nature of cyber dangers in today's rapidly evolving digital world is not fixed; rather, it is a fluid

phenomenon subject to constant change. Those charged with protecting digital assets—whether people, businesses, or governments—must thus constantly adapt in order to stay one step ahead of an ever-expanding collection of threats. Artificial intelligence (AI) and the Internet of Things (IoT) are two transformational and disruptive forces that have permanently etched the 21st century into our globally interconnected world. These technological behemoths have invaded many facets of our life, providing several advantages. But their widespread use in modern life has left a complicated shadow, filled with novel and nuanced cybersecurity issues (Lee, 2020).In the field of cybersecurity, Artificial Intelligence (AI) has emerged as a key enabler, providing a plethora of new tools and breakthroughs that are fundamentally altering the field. Tools and algorithms driven by artificial intelligence have proven their ability to identify, respond to, and mitigate risks more quickly and accurately than conventional systems. Cybersecurity has been revolutionized by the advent of automated threat detection, incident response, and vulnerability management (Radanliev et al., 2018). These skills are crucial in a world where cyberattacks are becoming more complex and destructive, aiming at anything from essential infrastructure to private data. Artificial intelligence (AI) offers a glimmer of hope by offering a paradigm shift in how these dangers are addressed. The fact that AI can facilitate predictive analytics increases the technology's allure. This presents an exciting opportunity for preventative security measures, which may be used by a wide

variety of businesses to head off attacks before they even begin. AI offers a ray of hope in a world where cyber dangers are growing in size and sophistication, providing a smart and proactive way to protect against them (Raban & Hauptman, 2018). IoT, or the Internet of Things, has become deeply embedded in our daily lives with the development of AI. The way we live, work, and interact with our environments has been profoundly altered by a complex network of networked devices, including smart appliances, medical equipment, industrial sensors, and more. This massive consolidation has opened up a wealth of opportunities, including better medical treatment, more efficient manufacturing, and more enjoyable daily life. However, as these gadgets have become more commonplace, a plethora of security flaws have also come to light. There is a unique and difficult mix of threats that must be handled due to the lack of established security procedures and the low computing capacity of many IoT devices (Radanliev et al., 2020). The threats to cybersecurity posed by emerging technologies are not hypothetical or far off in the future; they are already permeating our daily lives and the places where we operate. They exist now, and we must pay attention to them right away. Both possibilities and difficulties have arisen in the field of cybersecurity as a result of the rise of AI and IoT as dominant forces in the digital world. There are concerns regarding ethical usage and potential biases in AI, despite the fact that it holds the promise of improved threat identification, incident response, and vulnerability management. While the

Internet of Things (IoT) has the potential to provide enormous advantages, it also presents significant security issues due to the lack of established security procedures and the distinctive computing limits of IoT devices. The challenge in this area of study is figuring out how AI and the Internet of Things will affect the already fraught field of cybersecurity risk management.

Research Objectives

Organizations, governments, and people all need to adjust their cybersecurity plans to keep up with the ever-changing nature of cyber threats. This study is important because it has the potential to:

- (1) Enhance our understanding of how AI and IoT influence cybersecurity risk management.
- (2) Provide practical insights and best practices for organizations to adapt their cybersecurity strategies in response to the evolving threat landscape.
- (3) Offer policy and regulatory recommendations, particularly in areas related to IoT security standards and AI ethics.
- (4) Contribute to the development of an advanced framework for the integration of AI and IoT into **cybersecurity risk management**.

Chapter Two: Literature Review

AI in Cybersecurity: Applications and Benefits

When it comes to protecting against ever developing cyber threats, artificial intelligence (AI) has shown to be a game-changer. The use of AI in this field has many potential uses and benefits, and might significantly alter the way cybersecurity is approached. Artificial intelligence (AI) has brought a proactive and adaptable new method to the field of detecting and preventing threats. When it comes to identifying potential dangers in real time, AI-powered systems much outperform rule-based approaches (Taddeo, 2019). These systems are able to quickly detect possible security breaches by recognizing patterns and abnormalities in network traffic and system behavior using machine learning techniques and large datasets. By reducing the amount of time it takes to identify threats, this improved capacity lessens the severity and effect of assaults. Furthermore, AI's ability to identify risks covers a broad range of threats, including malware, ransomware, APTs, and even zero-day vulnerabilities. Cybersecurity solutions powered by AI can keep businesses one step ahead of thieves and help them respond quickly to new vulnerabilities by constantly assessing new and emerging threats. Artificial intelligence (AI) is a revolutionary development in the field of incident response. With the use of machine learning and natural language processing, AI systems can automatically handle security situations. Automating these processes considerably shortens reaction times and lessens the impact of

cyberattacks. Incident response enabled by artificial intelligence isn't limited to simple detection; it also helps in mitigating and containing threats (Muheidat & Tawalbeh, 2021). AI helps with incident containment by isolating compromised systems and applying security fixes or deploying countermeasures to stop further damage and spread. Further, AI is superior to human beings when it comes to vulnerability management, since it improves risk detection and prioritization. Computers powered by AI are capable of scanning whole data centers for security flaws in both hardware and software. In order to identify vulnerabilities, these systems examine past data, system settings, and patch management details. Artificial intelligence (AI) provides predictive analytics beyond vulnerability discovery, determining the likelihood of an attack and the possible harm to an organization. With this foresight, businesses can concentrate on fixing the most pressing security holes first. Artificial intelligence improves the effectiveness and accuracy of vulnerability management in this way. Artificial intelligence's predictive analytics skills are crucial in a world where cyber threats are continually developing and growing more complex, in addition to its function in threat detection and incident response. Artificial intelligence technologies may alert businesses to possible security breaches in advance by identifying patterns and correlations in data. Organizations can be more proactive in the face of a constantly shifting threat landscape thanks to these predictive skills, which play a crucial role in lowering the total risk to digital assets. However, there are moral questions

that arise when AI is used in cyber security. Inheriting biases from training data might compromise the objectivity of AI threat identification and mitigation. The employment of AI in offensive cyber operations also raises moral questions, calling for a middle ground between safety and abuse. In order for AI to be effectively used in cybersecurity, these moral concerns must be resolved. To guarantee impartial and equitable results in danger assessment and response, researchers and practitioners are hard at work developing strategies for bias prevention in AI systems. Further, talks are occurring to define acceptable rules and procedures about the ethical limits of AI in offensive cyber operations. The use of AI and the benefits it brings to cybersecurity are expansive and game-changing, strengthening protections in many different ways. It is clear that AI plays a vital role in creating the future of cybersecurity, from the proactive protection against changing threats to the effective management of vulnerabilities and the ethical issues related with AI. We will investigate the actual effects of AI and the difficulties and opportunities that arise when implementing it in real-world cybersecurity settings as we progress through this study.

IoT Devices and Security Challenges

Healthcare, industrial applications, and consumer-focused services are just some of the fields that have been revolutionized by the advent of the Internet of Things (IoT). However, several security concerns have been raised as a

result of the exponential growth of IoT devices. Internet of Things (IoT) devices have become critical to providing state-of-the-art medical treatment and remote health monitoring to patients. Health and fitness trackers, smart medical gadgets, and telemedicine systems all fall under this category. They pose serious security concerns, but have the potential to enhance patient outcomes and access to healthcare services. The safety of patients' personal information is of paramount importance. Cybercriminals frequently target individuals' health records because of the extreme sensitivity and intimate nature of this data. Unauthorized access to patient information due to vulnerabilities in IoT healthcare equipment might compromise privacy and expose individuals to different types of fraud and identity theft. Further, malevolent actors may exploit vulnerabilities in medical equipment to alter therapy and patient care, which can have fatal outcomes (Sadique, Rahmani & Johannesson, 2018). When it comes to optimizing processes, boosting automation, and boosting operational efficiency, IoT devices play a crucial role in the industrial sector. These tools are necessary in areas where failure might have catastrophic consequences, such as in utilities, factories, and logistics centers. However, security concerns have been raised due to the introduction of IoT devices into these critical infrastructures. The potential financial and safety costs of an IoT device attack in the manufacturing industry are high. Blackouts and financial losses might result, for instance, from a cyberattack on the Internet of Things (IoT) systems at a power plant.

The same is true for the manufacturing industry; accidents might occur if the security of industrial IoT devices is compromised. Smart home appliances and wearables are only two examples of the kinds of consumer applications of IoT devices that have seen rapid acceptance due to their ease and efficacy.

However, these gadgets present new security risks. Internet of Things (IoT) gadgets in smart homes can operate as cyberattack entry points, allowing hackers to compromise residents' privacy, convenience, and safety. Smart locks, security cameras, and home automation systems are all vulnerable to infiltration and privacy violations if they fall into the wrong hands (Tawalbeh, Muheidat, Tawalbeh & Quwaider, 2020). Furthermore, fraudsters now have a much larger attack surface to exploit because of the widespread use of IoT devices in consumer applications. The lack of established security procedures for IoT devices is a problem that affects every industry. The development of many IoT devices sometimes prioritizes utility and cost-effectiveness above strong security measures. Due to the absence of universally accepted security protocols, IoT devices can easily be compromised. Cybercriminals can take advantage of these flaws to steal information, take control of systems, or launch DDoS assaults. Many devices in the Internet of Things have low processing power, which creates their own security risk. The memory and processing capability of these devices is sometimes insufficient to implement adequate security protocols. This makes them easy prey for hackers who can take advantage of their lack of processing power to compromise their

networks and systems. Harnessing the full potential of IoT devices requires addressing the security concerns they provide. Organizations, legislators, and technology manufacturers must work together to establish standardized security procedures and best practices as IoT continues to develop and become more integrated into our everyday lives. Additionally, people should always be on guard to secure their Internet of Things devices, checking for updates, using robust passwords, and doing frequent vulnerability scans. The security concerns connected with the Internet of Things can be reduced if these issues are resolved.

Cybersecurity Risk Management Strategies and Best Practices

To protect digital assets and lessen the impact of a wide variety of cyber threats, solid cybersecurity risk management must be in place. It includes a wide variety of tactics and guidelines that businesses should follow to safeguard their digital infrastructure. The process of identifying and evaluating potential threats is crucial to managing cybersecurity risks. The first stage is a thorough search for possible cyber hazards within the company (Lee, 2021). It requires an in-depth familiarity with the assets, network architecture, and security holes that make up an organization's digital landscape. Risk assessment is an ongoing procedure that must change along with the evolving nature of potential dangers. A company's risk profile can be better understood when the value, weaknesses, and dangers associated with its digital assets

have been identified. After a danger has been identified, the next important step is to take action to lessen or respond to that risk. In this step, you'll work on formulating plans and procedures to deal with the threats you've pinpointed. It includes things like keeping an eye out for potential dangers and devising a plan of action in the event of an occurrence. Cybersecurity rules, access restrictions, intrusion detection systems, and incident response plans are all examples of potential risk mitigation measures (Jarjoui & Murimi, 2021). The creation of an incident response plan, outlining actions to be performed in the event of a security incident, is an important part of risk reduction. Specific steps, reaction groups, channels of communication, and barriers to spread should all be outlined in this strategy. In order to effectively manage cybersecurity risks, education and training are essential. In order to foster a security-aware workforce, companies must place a premium on employee education and training. Employees who are well-informed are more likely to spot security risks, follow procedures, and take appropriate action during security crises. Training for cybersecurity has to cover best practices, security awareness, and how to spot phishing efforts, which continue to be a common attack vector (Dias et al., 2021). A well-coordinated and successful response to a security breach depends on everyone in the business being familiar with the incident response strategy. Risk management relies heavily on constant surveillance and evaluation. The threat environment is ever-changing as new exploits and entry points are discovered. It is crucial to

conduct constant vulnerability and threat assessments. Companies need to keep attentive by using intrusion detection systems, security information and event management (SIEM) systems, and threat intelligence feeds. Penetration testing and vulnerability scanning, two components of regular security audits, can help reveal vulnerabilities before they are exploited by hackers. Third-party risk management provides an extra safety net. Companies' exposure to risk can be affected by the security practices of their suppliers and service providers. To effectively manage risks, it is necessary to evaluate the suppliers' and partners' cyber hygiene. By doing this evaluation, we can guarantee that our trusted partners also adhere to our strict security policies. Best practices in cybersecurity risk management include keeping an organized and transparent incident response strategy. To guarantee a swift and effective reaction to a security breach, it is important to frequently practice this strategy with all key parties. Cybersecurity risk management is a multi-faceted process that requires firms to recognize, evaluate, and lessen their exposure to cyber threats. Organizations may improve their security posture and resilience in the face of a constantly shifting threat landscape by implementing comprehensive security measures, continuing education, third-party risk management, and incident response plans. In order to keep up with the ever-changing nature of cyber risks, companies need to implement comprehensive risk management strategies that include constant monitoring, evaluation, and adaptation.

Recent Research and Identified Gaps

New studies in the realm of cybersecurity have shed light on the ever-changing world of digital security, especially in regards to the impact of AI and the IoT. But this ever-evolving subject keeps throwing up huge holes in our knowledge that must be filled with more research if we are to deepen our understanding and improve our defenses. There have been encouraging findings from studies examining the use of AI in cyber defense. AI has already begun to show its revolutionary potential in the security industry through its use in threat detection, incident response, and vulnerability management. There is an urgent need to investigate the practical efficacy of AI-driven security solutions as they become more widespread. There are still a lot of unknowns. For instance, what are the limits of these AI systems' prediction powers, and how do they adjust to new threats? Harnessing the full potential of AI-driven cybersecurity solutions requires an understanding of their performance in a variety of organizational scenarios and an ever-changing threat landscape. Ethical questions of the use of AI in cybersecurity are also an important topic of study. It is a challenging problem that needs more investigation to guarantee that AI algorithms are unbiased and that the use of AI in offensive cyber operations follows ethical norms. New studies in the field of Internet of Things and cybersecurity have revealed previously unknown dangers and weaknesses caused by the explosion of linked gadgets.

Research has detailed the threats posed by the Internet of Things to several sectors, including the medical, manufacturing, and retail sectors. Tackling these security issues, however, is no easy feat. More study is needed to create standardized security procedures for IoT devices so that they can withstand cyberattacks. Research into the unique security needs of various industries and the development of sector-specific countermeasures is also essential.

Protecting patient privacy and the reliability of medical equipment are two examples. Protecting vital infrastructure from cyberattacks is a top priority in industrial settings. The consumer market is focused on protecting connected homes and private information. The increased connection provided by a 5G network presents both benefits and threats to the security of the Internet of Things, and hence warrants more study. The intersection of AI and IoT in the realm of cyber security is an area that has received insufficient attention in recent studies. While research into AI and IoT separately has been extensive, the combined implications of these two trends on security procedures have received less attention. Research into the ways in which AI may improve the safety of Internet of Things gadgets and networks holds considerable promise. How can IoT environments be connected with AI-driven threat detection systems so that new threats may be detected and countered quickly?

Understanding the practical ramifications of this convergence of technology is essential. Finally, the best practices and techniques for managing cybersecurity risks need to be continuously evaluated. Recent studies have

highlighted the significance of risk assessment, prevention, knowledge, and surveillance. But a thorough analysis of how these techniques have been implemented in the real world across different industries is required. How effective are various approaches to risk management in various business settings? What problems and obstacles arise during their implementation, and how may they be fixed? Further research is needed into standardizing incident response plans and evaluating the risk management practices of third parties. While we have made great gains in our understanding of the effects of AI and the Internet of Things on cybersecurity in recent years, there are still many questions that need answering. The convergence of AI and IoT; the creation of standardized security protocols for IoT; the evaluation of risk management strategies in a variety of organizational settings; the practical application of AI-driven cybersecurity tools; and so on. In order to better protect ourselves and react to the ever-changing cybersecurity threat landscape, it is crucial to fill these knowledge gaps.

Chapter 3 Methodology

This study uses a mixed-method approach, which means that it collects and analyzes data in both qualitative and quantitative ways. This methodological approach offers a thorough and multifaceted investigation of how new technologies, like as AI and IoT, affect the management of cybersecurity threats.

Research Design and Approach

This study employs a descriptive and exploratory methodology to better understand cybersecurity risk management in the presence of artificial intelligence and the internet of things. The research topic was better understood because to the mixed-method approach, which capitalized on the advantages of both qualitative and quantitative studies. Interviews and focus groups, for example, were qualitative approaches that gave in-depth insights and context, while surveys and polls were quantitative methods that allowed for more comprehensive data collecting and statistical analysis.

Surveys

Surveys were prepared and sent out to cybersecurity specialists, IT workers, and enterprises that make use of AI and IoT to collect quantitative data. Most of the questions in the surveys focused on respondents' successes, failures, and recommendations for improving cybersecurity in the age of AI and the Internet of Things. The goals of the survey were to collect quantitative data on the use of AI and IoT in cybersecurity, the pros and cons seen by respondents, and the degree to which businesses have incorporated these technologies into risk management.

Interviews

Experts in cybersecurity, creators of AI and IoT technologies, and IT decision-makers were interviewed in-depth to compile the qualitative data. These in-depth discussions illuminated the complexities and opportunities inherent to incorporating AI and IoT into cybersecurity risk management. Participants' willingness to talk about their own lives and the world at large was increased by the use of open-ended inquiries. Interviews are a great method for learning about nuanced issues and recording detailed accounts of people's lives.

Sample Selection

The research parameters included a section for random sampling. One key motivation for using a random sample strategy was to reduce the potential for selecting biased volunteers for the study. Right after the sampling, the research was able to incorporate a total of 20 participants.

Data Analysis Methods

The surveys' quantitative data were examined statistically. Quantitative results were summarized and presented using descriptive statistics including frequencies, percentages, and measures of central tendency. Insightful patterns and trends in respondents' perspectives and experiences with AI and IoT in cybersecurity were shown by this investigation. Conversely, theme analysis was utilized in the study of qualitative interview data. The method relied on extracting, interpreting, and reporting overarching themes from the qualitative data.

Chapter 4: Findings

Significant insights into how Artificial Intelligence (AI) and the Internet of Things (IoT) might be used to improve cybersecurity and risk management have emerged from this study's data analysis phase. The study used a combination of quantitative and qualitative research techniques, including questionnaires and in-person interviews. The most important results and analyses are presented here. Insight into the use of artificial intelligence and internet-of-things technology in cyber defense is provided by the survey's findings. According to the statistics, a sizable number of businesses are already using AI in their cybersecurity initiatives. 30% of those surveyed said they used systems powered by AI to look for threats, while another 40% said they used the technology to handle incidents and safeguard against security flaws. This shows widespread belief in AI's ability to strengthen data protection measures. However, just 30% of respondents confirmed using IoT devices for security purposes, suggesting that more work has to be done to integrate IoT into cybersecurity. These Internet of Things uses case studies covered a wide range of industries, from healthcare to manufacturing to consumer products. In terms of cyber security, the data shows that IoT adoption is rising but becoming more deliberate. The poll also investigated how businesses deal with potential threats posed by AI and IoT. Most notably,

eighty percent of respondents claimed to have established, thorough plans for managing cybersecurity risks. Methods such as risk assessment, incident preparation, and constant surveillance of potential dangers were implemented. Such actions are indicative of a preventative strategy for handling cybersecurity threats. In addition, qualitative data gathered via in-depth interviews with cybersecurity specialists gives granular insights into the difficulties, best practices, and recurring themes associated with the influence of AI and the Internet of Things on cybersecurity risk management. Ethical concerns about using AI for cybersecurity came up often in the interviews. Several professionals have stressed the significance of checking AI algorithms for bias and making sure they act ethically. It was recognized that there is a hurdle in using AI for security purposes without compromising on ethics. The low computing power of many IoT devices was cited as a major obstacle. Due to the difficulty of circumventing this restriction, it represents a novel threat to information security. There is a dire need to address resource restrictions in IoT security, according to experts. Once more, it was thought that incorporating AI and IoT into cybersecurity would be a difficult task. Experts noted that there were obstacles to establishing full integration of AI and IoT components with preexisting security infrastructure and guaranteeing compatibility between such components.

Fig 1: Data showing the usage of emerging technologies for various purposes

Educating and training workers to develop a security mindset was highlighted by experts. Staff workers who have received enough training are better able to spot security risks and follow procedures. Training in all aspects of cybersecurity was identified as a must-have. However, one of the recommended approaches is constant scanning for security holes and threats. The use of intrusion detection systems, threat intelligence feeds, and security information and event management (SIEM) systems were all stressed by the experts. It was determined that creating uniform incident response plans was an essential best practice. For efficient incident management, these plans lay out specific steps to take, who should do what, how to communicate, and how to keep things contained. The ever-changing nature of cyber dangers was a common subject. Experts stressed that the danger landscape is always changing, calling for vigilant security solutions that can keep up with the shifting threats. The interviews showed how various industries have varied security needs. Security solutions for the healthcare, industrial, and consumer sectors must address the unique requirements and risks of each. At long last, the need of merging AI and IoT in cybersecurity has been acknowledged by experts. The practical consequences of this convergence, which provide enormous benefits, have been recognized as a potential area for further study.

Chapter 5: Discussion

The results of this study provide light on how the fields of cybersecurity risk management and artificial intelligence (AI) would be affected by the convergence of these two developing technologies. With an emphasis on the role of artificial intelligence (AI), the specific security problems offered by the Internet of Things (IoT), and a comparison of current cybersecurity risk management approaches with study findings, this part interprets the findings in the context of the research goals. We also discuss the possible effects of policy and regulation. The study's overarching goal was to evaluate how AI and the Internet of Things have altered the way we handle cybersecurity threats. According to the results, firms are progressively using AI into their cybersecurity processes, which is consistent with the stated goals. When it comes to finding threats, dealing with incidents, and managing vulnerabilities, AI is not only common but also highly influential. This uptake is indicative of the growing trend toward proactive and insightful cyber defense. However, enterprises are taking more time to fully realize the benefits of the Internet of Things (IoT) when it comes to cybersecurity. IoT devices have their own set of security difficulties that call for industry-specific and standardized security methods. The results highlight the game-changing function of AI in cyberspace. When it comes to detecting abnormalities and potential breaches in real time, AI-powered systems shine. By analyzing massive databases for anomalies and trends, machine learning models improve the precision of threat detection. In a world where threats are always changing, this

preventative strategy is a game-changer. Automated incident response driven by AI saves time and improves efficiency when dealing with security breaches. With the use of machine learning and natural language processing, AI systems can recognize and react to dangers on their own, drastically cutting down on reaction times and collateral damage. The results show how AI has the ability to completely change the way incidents are handled by improving efficiency and effectiveness. Vulnerability management is simplified by AI since flaws are discovered automatically and countermeasures are suggested. This foresight helps businesses be more resistant to new hazards. In conclusion, AI improves cybersecurity by helping to spot threats more accurately, responding quickly to incidents, and managing vulnerabilities proactively.

The study's findings shed light on the problems caused by the Internet of Things across industries. Safety of patient information and medical equipment is of utmost importance in the healthcare industry. IoT healthcare equipment have security flaws that might allow hackers to access sensitive patient information and even change their treatment plans. The priority for the manufacturing industry is to prevent cyberattacks on vital infrastructure. There is a potential for serious economic and safety ramifications due to the integration of IoT devices in power plants and industrial. Securing smart homes and private information is a major concern for the consumer

technology industry. Intruders and privacy violators may gain access to a smart home using an unauthorized IoT device. Cybercriminals have a much larger target area to work with because to the widespread adoption of IoT devices.

According to the data, many businesses have established procedures for handling cybersecurity risks. Strategies include figuring out what risks there are and how to deal with them, as well as always keeping an eye on things. Consistent with these procedures, the studies' findings highlight the value of preventative risk management. Current practices and research findings lend credence to the importance of standardizing incident response strategies and continuously monitoring for possible threats and vulnerabilities. Particularly for Internet of Things (IoT) security standards and artificial intelligence (AI) ethics, the findings have legislative and regulatory consequences. Regulations and standards are necessary to guarantee the ethical and impartial use of AI to security procedures as its role in cybersecurity grows. Healthcare data privacy and security, critical infrastructure protection, and consumer application privacy and security are all policy issues that need further focus. To counteract the risks posed by so many moving parts, it is crucial that standardized security standards be developed for the Internet of Things. It is important to build regulatory frameworks to guarantee the safety of IoT devices, especially in industries where they will have a major influence.

Chapter 6: Conclusion

Emerging technologies, such as Artificial Intelligence (AI) and the Internet of Things (IoT), are having a profound effect on cybersecurity risk management, and this study has unearthed key insights into this influence. The results not only demonstrate the revolutionary impact of AI, but also illuminate the specific security issues brought on by the widespread use of IoT devices across industries. Some of the most important results show that businesses are increasingly using AI for cybersecurity purposes, particularly for automating their responses to incidents and spotting vulnerabilities ahead of time. This uptake demonstrates how AI has the ability to radically alter security procedures, allowing businesses to keep up with ever-evolving cyber threats. The cautious incorporation of IoT in cybersecurity, on the other hand, emphasizes the need for established security procedures and industry-specific solutions. Vulnerabilities in networked devices and networks are becoming increasingly pressing due to security concerns in healthcare, industrial, and consumer applications. This study has important implications for the fields of cybersecurity practice, study, and policymaking. The research results provide useful advice for firms seeking to modify their approach to cybersecurity in light of the ever-changing nature of the threats they face. The findings have

important legislative and regulatory implications, since they highlight the need for ethical concerns in AI and for standardized security safeguards for IoT devices. Improving knowledge, providing useful insights, and maybe creating cutting-edge frameworks for incorporating AI and IoT into cybersecurity risk management are all examples of how this work contributes to the subject of cybersecurity. These improvements enable businesses to keep their data and digital assets safe in an ever-changing threat scenario. Future research directions are essential since the subject of cybersecurity continues to develop at a breakneck rate. Investigating how artificial intelligence and the internet of things (IoT) may complement one another to strengthen cybersecurity is an exciting area of study. Standardized security procedures for IoT devices and ethical issues in AI should continue to be at the forefront of research efforts. In an area where risks are always shifting, continuous evaluation and adaptation are also essential. This study lays the groundwork for future investigation and innovation in the subject of cybersecurity, which is essential for coping with the new threats posed by AI and the Internet of Things.

References

Dias, F. M., Martens, M. L., de Paula Monken, S. F., da Silva, L. F., & Santibanez-Gonzalez, E. D. R. (2021). Risk management focusing on the best practices of data security systems for healthcare. International Journal of Innovation, 9(1), 45-78.

Jarjoui, S., & Murimi, R. (2021). A framework for enterprise cybersecurity risk management. In Advances in cybersecurity management (pp. 139-161).

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. Future internet, 12(9), 157.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659-671.

Muheidat, F., & Tawalbeh, L. A. (2021). Artificial intelligence and blockchain for cybersecurity applications. In Artificial Intelligence and Blockchain for Future Cybersecurity Applications (pp. 3-29).

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. foresight, 20(4), 353-363.Radanliev, P., De Roure,

D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. Computers in industry, 102, 14-22.

Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., ... & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. Cybersecurity, 3(1), 1-21.

Sadique, K. M., Rahmani, R., & Johannesson, P. (2018). Towards security on internet of things: applications and challenges in technology. Procedia Computer Science, 141, 199-206.

Taddeo, M. (2019). Three ethical challenges of applications of artificial intelligence in cybersecurity. Minds and Machines, 29, 187-191.

Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.

Appendices

Appendix 1: Questionnaire: Assessing the Impact of Emerging Technologies on Cybersecurity Risk Management

Part 1: Demographics

1. Gender:

- Male
- Female
- Other (please specify)

2. Age:

- Under 18
- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65 or over

3. Educational Background:

- High School
- Bachelor's Degree
- Master's Degree
- Doctoral Degree

- Other (please specify)

4. Current Role:

- Cybersecurity Professional
- IT Manager
- AI/ IoT Developer
- IT Decision Maker
- Other (please specify)

Part 2: AI and Cybersecurity 5. Are you currently using AI-based tools or systems in your organization's cybersecurity practices?

- Yes
- No

6. If you answered "Yes" to the previous question, please describe the specific AI-based tools or systems you are using in your cybersecurity practices.

7. How has AI impacted your organization's ability to detect and respond to cybersecurity threats? (Select all that apply)

- Improved threat detection
- Faster incident response

- Better vulnerability management

- Other (please specify)

8. Have you encountered any ethical concerns related to the use of AI in cybersecurity? If so, please describe them.

Part 3: IoT and Cybersecurity

9. Are you currently using any IoT devices or technology for security purposes within your organization?

- Yes

- No

10. If you answered "Yes" to the previous question, please describe the specific IoT devices or technologies you are using for security purposes.

11. What are the major security challenges you've encountered in integrating IoT devices into your organization's cybersecurity practices?

12. Do you believe that the implementation of IoT devices pose unique security risks when compared to traditional IT devices and networks?

- Yes

- No

- Not sure

Part 4: Cybersecurity Risk Management 13. What cybersecurity risk management strategies has your organization currently implemented? (Select all that apply)

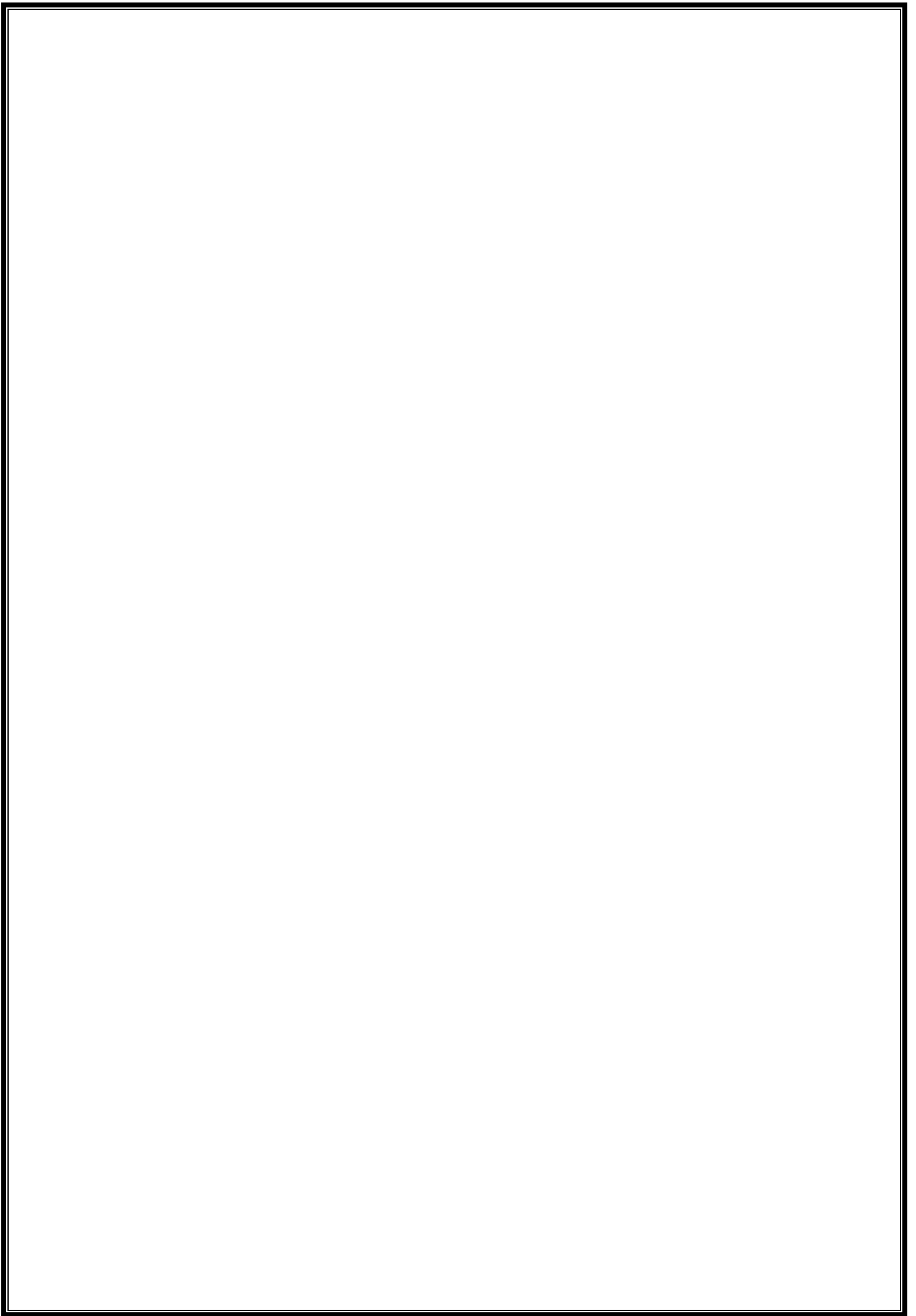
- Risk assessment
- Incident response planning
- Constant threat monitoring
- Employee training and education
- Third-party risk management
- Other (please specify)

14. How do you think AI and IoT can enhance or impact the effectiveness of your current cybersecurity risk management strategies?

Part 5: Overall Reflection

15. In your opinion, what are some of the most significant benefits of incorporating AI together with IoT technologies into cybersecurity risk management?

16. What are some of the major challenges or obstacles do you foresee in fully integrating AI and IoT into cybersecurity practices?



Midocean University

College of Management

Department of Risk management

Title in English

**Assessing the impact of emerging technologies (e.g., AI, IoT) on
cybersecurity risk management**

Prepared by:

Fahad Ahmed Alhodayan

Supervised by:

PhD. Waleed sulaiman

PhD. Alfaisal Abdelhameed

Year:2023