



CYBERSECURITY AND RISK MANAGEMENT: SAFEGUARDING ENTREPRENEURS IN THE DIGITAL AGE

Dr. Saud Ilahi

Designation: Assistant Professor Department: Business Administration

Institute: Jazan University District: Jazan City: Jazan State: Jazan, KSA.

Email: drsaudilahi@gmail.com

Article History

RECEIVED DATE : 01/07/2023

REVISED DATE: 30/09/2023

ACCEPTANCE DATE : 05/10/2023

Abstract

Introduction: The focus of this study is to evaluate the way cyber security and risk management procedures can help entrepreneurs safeguard in this digital age. Objectives have been set according to the aim of this study and the questions have been prepared to conduct the entire research properly.

Literature Review: The benefits of technology in business and the way security systems need to be installed to get all the benefits effectively have been discussed. Challenges entrepreneurs face in online or technology-based business have been mentioned. The ways of implementing cyber security policies to get rid of all cyber threats have also been discussed.

Methodology: various online sources have been chosen to collect data, apart from that, secondary data has been collected to add historical information to this research.

Findings: Collected data was analysed in this part when thematic analysis was done. Themes have been made to justify all the information accurately. This has helped in answering the question raised in this research.

Discussion: This part discussed all the valuable points. The need to implement a risk assessment framework to rectify the specific risks, early detection of risk to implement a faster mitigation process, constant monitoring and regular employee training to make a strong business team can help entrepreneurs in safeguarding their businesses.

Conclusion: The process the study followed to conduct and complete the research is mentioned in this part. The detailed discussion regarding the topic in this study is able to help all in informing the way entrepreneurs can be safeguarded through cyber security and risk management.

CCLicense CC-BY-NC-SA 4.0	Keywords: Risk assessment, Cyber threat, business growth, encryption, early detection, safeguarding entrepreneurs.
------------------------------	---

Introduction

Technology has evolved immensely and this has created both opportunities and risks for all. In the matter, Elia *et al.* (2020), explained along with the increasing growth of the internet and technology, cyber security has become an important component. In order to safeguard newly introduced businesses and entrepreneurs, managing cyber risk and providing proper security to prevent any threat has become necessary. As opined by, Jafari-Sadeghi *et al.* (2021) the growing potential of technology has made businesses reliant on it which also increases the cyber risk to a higher extent. Thus, managing the risk in this digital age for entrepreneurs is crucial and for that cyber security measures can be helpful extremely.

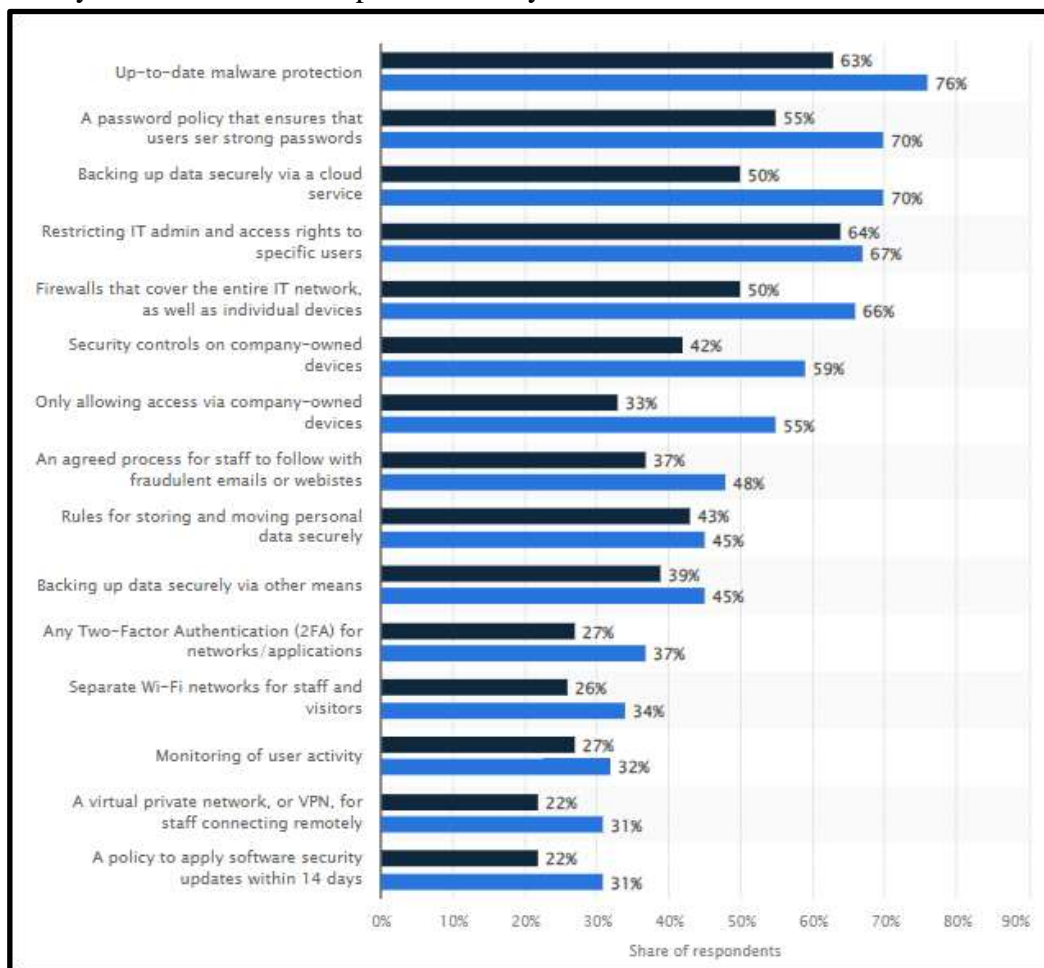


Figure 1: Percentage of used cyber security policies in the UK business
(Source: Statista, 2023)

Figure 1 highlights the cyber rules and protection processes businesses and charities have implemented. 76% of businesses have implemented updated malware protection, whereas 34%

of businesses have installed different WiFi networks for employees and visitors (Statista, 2023). It can also be seen that most charities, 64%, are following the common rule of restricting IT administration and access rights to distinctive users (Statista, 2023).

This has been indicated as a significant approach for UK businesses to take control of risk and manage entrepreneurial jobs effectively. Thus, the role of cyber security and its distinctive forms have been a great help for entrepreneurs in this digital era of ruling the world.

Aim

This study aims to evaluate the way cyber security and risk management procedures can help entrepreneurs safeguard in this digital age.

Research Objectives

RO1: To discover the role of the digital world and technology in the business of entrepreneurs

RO2: To discover the challenges entrepreneurs face in their digital business

RO3: To understand the role of cyber security and risk management in safeguarding the business

RO4: To analyse the process of implementing robust cyber security policies and procedures to safeguard the entrepreneurs of the digital age

Research Questions

RQ1: How do technology and the digital world impact the business development of entrepreneurs?

RQ2: What are the challenges entrepreneurs often face in their digital businesses?

RQ3: What is the role of cyber security and risk management in safeguarding their business?

RQ4: How can robust cyber security policies and procedures be implemented to safeguard the entrepreneurs of the digital age?

Literature Review

Role of technology and digital modes in the development of business for entrepreneurs

Technology plays a pivotal role in the growth of businesses in the modern age. In this matter, von Briel *et al.* (2021), explained leveraging technology in the digital age is not just about getting competitive advantages as it has become a fundamental need to become successful. It can be seen that online presence through websites has helped entrepreneurs establish a storefront that can inform clients and customers about the offerings of the business. Here, Ben Arfi and Hikkerova (2021), mentioned marketing through digital platforms has made it easier for entrepreneurs to reach a maximum audience in a limited time.

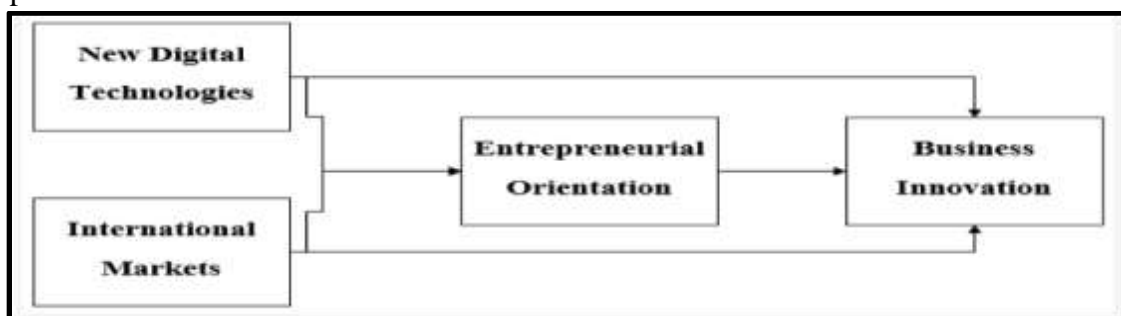


Figure 2: Impact of technology in business innovation

(Source: Vadana *et al.* 2020)

It can also be seen that e-commerce platforms help entrepreneurs in managing online sales overseas and manage payment efficiently. According to, Alford and Jones (2020), different tools of data analysis have helped entrepreneurs to understand the purchasing behaviour of the customer and watch trends in the market effectively. Data-driven decision-making has helped entrepreneurs achieve success immensely. It can also be seen from the discussion of, Vadana *et al.* (2020), that managing supply chain and logistics for entrepreneurs has become easier through the digital mode of business. Thus, it is said that technology has helped entrepreneurs in developing businesses effectively.

Discovering the challenges faced by entrepreneurs in digital business

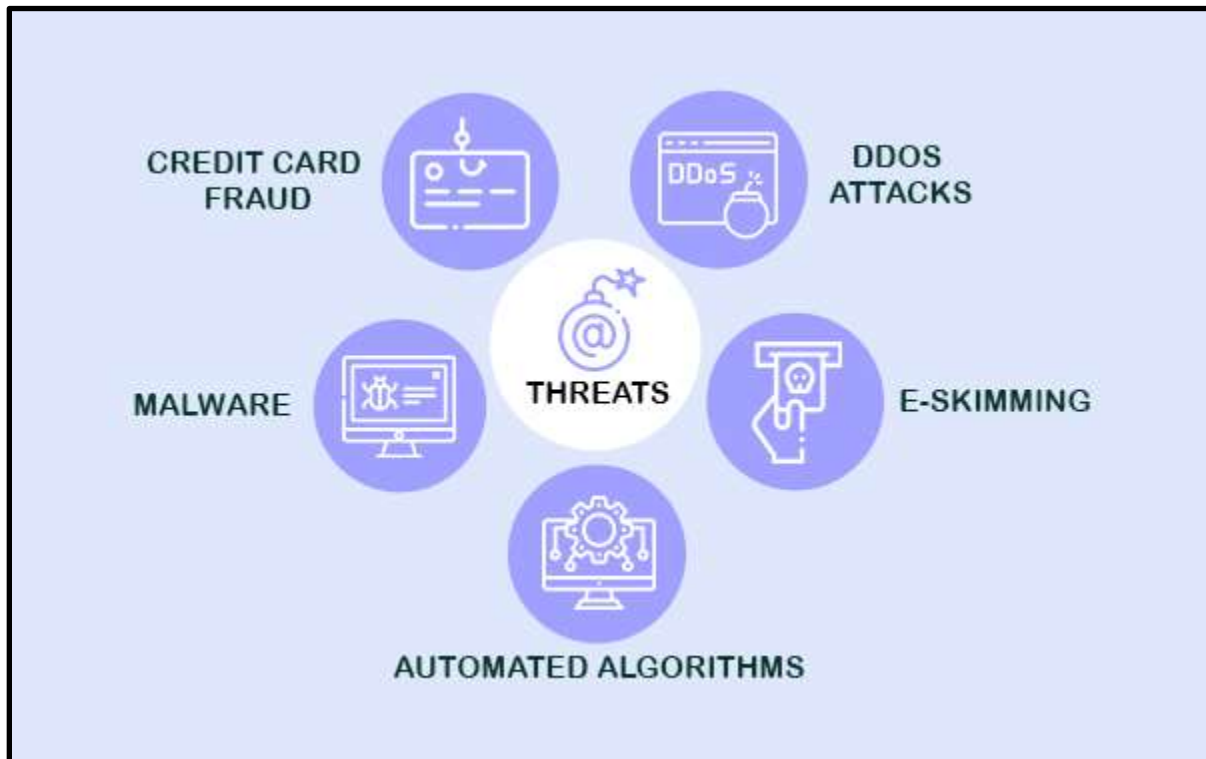


Figure 3: Cyber threat in online entrepreneurship

(Source: Kraus *et al.* 2019)

Digital space for business is highly competitive as multiple startups and new market entries vying for attention. Secundo *et al.* (2021), mentioned, standing out in a crowded business place where competition is high is quite tough. The challenges in maintaining security for entrepreneurs is the toughest matter in the digital age business. According to, Kraus *et al.* (2019), many businesses face leakage of company revenue of market share unauthorised way due to a lack of digital security. On the other hand, managing the personal information of customers can be highly challenging for entrepreneurs while doing online business. In this matter, Jafari-Sadeghi *et al.* (2021), added a technical malfunction or cyber attack can lead to a breach of the personal information of companies which also risks employees' lives. Ransomware and phishing attacks can also damage the business which brings challenges for entrepreneurs. Payment management and maintaining good rapport with shareholders have become challenges due to

cyber threats. Thus, the management of risk in the digital age of doing business is highly important and needs proficiency.

Evaluating the role of cyber security and risk management in safeguarding business

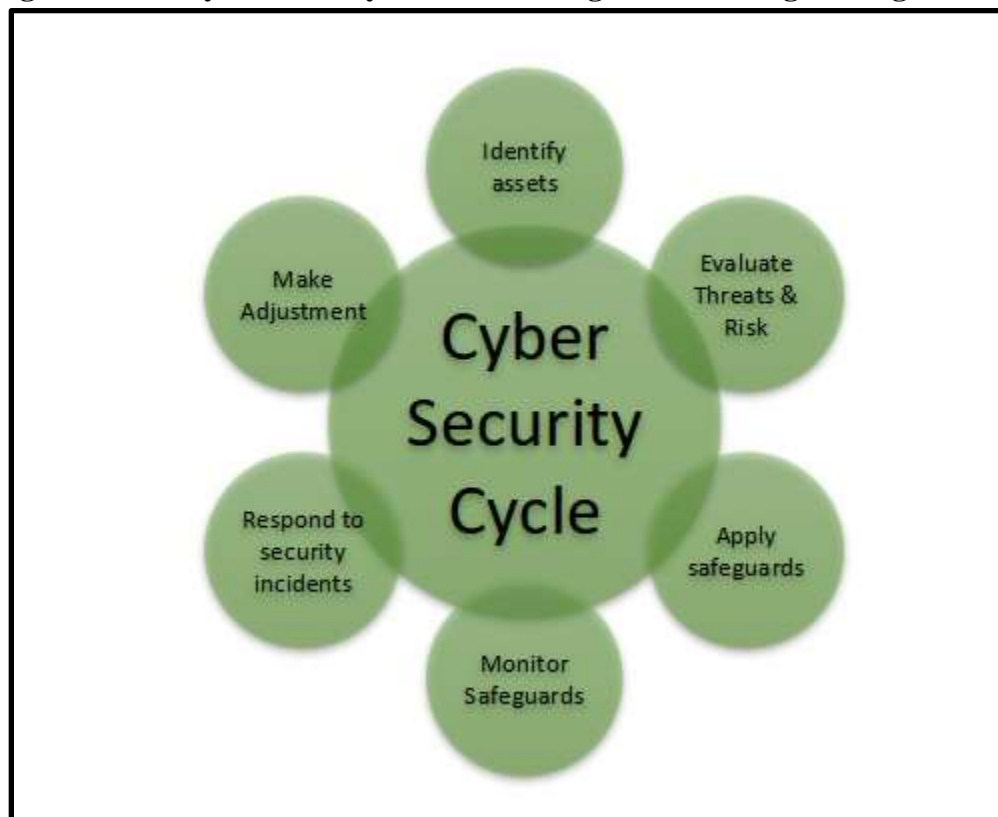


Figure 4: Policies in cyber security

(Source: Mandviwalla and Flanagan, 2021)

Cyber security measures like encryption, control over access and a string fraud detection system can safeguard all the sensitive information of a business. In this context, Bican and Brem (2020), mentioned risk management in business is able to help in identifying threats and analysing the impact of the threats. It can be seen that risk management protocols can help entrepreneurs develop continuity and disaster recovery plans in business to ensure the fastest recovery of business defects. According to, Mandviwalla and Flanagan (2021), using cloud-based software to secure data storage is able to lower the risk of data breach and hacking. It can be seen that cyber security management and safeguarding business can be costly, however, it prevents the high cost associated with data breaches and legal actions effectively. Risk control incorporates incident retort arranging into the comprehensive risk management framework. Thus, it can be comprehended that cyber security and risk management help in safeguarding entrepreneurs effectively.

Process of implementing robust cyber security policies to safeguard the entrepreneurs of the digital age

It is important to consider factors like the industry of business, the nature of digital assets and the landscape of risk in order to implement cyber security effectively. Here, Ratten and Jones

(2021), stated rectification of the cyber threats and vulnerabilities efficiently is highly important to understand the measure of cyber security needs to be implemented. Later, contacting a dedicated cyber security team who is eligible to manage risks is required. Implementation of the data classification system according to the sensitivity of data is important. According to, Lopez *et al.* (2021), ensuring the cyber security policies are well aligned with business regulations is highly important. It is crucial to ensure that only authorised individuals or teams are eligible to have access to the sensitive data of a business. Apart from that, Stine *et al.* (2020), mentioned, that paying enough to access cloud-based software partners is able to protect the data of entrepreneurs which increases customer as well as employee satisfaction. Encrypting online business mode can help in detecting any fraudulent activity at an early stage.

Theoretical Framework

System theory

System theory is an effective approach of understanding the complex system which is closely interconnected with all its components. In this matter, Markovsky and Dörfler (2021), stated, system theory provides a framework to understand the way all the components of a system work together to achieve a particular goal as a whole. In the context of risk management for entrepreneurs by safeguarding business through proper cyber security, system theory helps in informing all the components of business that is technology, people, and external environment. System theory is able to promote a holistic view of the cyber security posture of a company (Becvar *et al.* 2023). It helps entrepreneurs in identifying the vulnerabilities and weaknesses in the entire system which can help in resolving the issue faster.

Literature Gap

This study has collected historical data to present all the valuable information thus, the views of entrepreneurs have not been gathered. It can be seen that the use of highly secured devices in business can help in safeguarding entrepreneurs effectively however, due to limited resources, choosing the cheaper option can become the first choice of startups (AlGhamdi *et al.* 2020). This creates a gap between successful businesses and cyber attract. Choosing a secondary method of researching for this study also implements a gap in this literature as getting real-time information has been restricted due to that. The dual effect of technology needed to be discussed in brief to understand the threat projection in the online business of entrepreneurs in the digital age which is insufficient. Hence, all this lack has created a gap in this literature.

Methodology

In this research, a variety of online sources have been used to collect accurate information regarding the role of cyber security and risk management in safeguarding entrepreneurs. This has helped in analysing all the information in the further part of the study through the “theoretical analysis” process. Conceptual understanding is able to be improved through the theoretical analysis of all collected information (Mazhar *et al.* 2021). The process of collecting existing information is also cost and time-effective and highly useful as it consists of the value of peer review.

Findings

Theme 1: Establishing a comprehensive risk assessment framework can help in safeguarding entrepreneurs

Developing and implementing a structured framework for managing risks is important to identify, and validate potential risks of cyber security particularly to the business operation of an entrepreneur. In this matter, Alahmari and Duncan (2020), stated conducting a thorough risk analysing process can help in identifying weaknesses effectively. Later, it is important to evaluate the strength of each risk on the business. A lack of understanding of the specific risk area can affect negatively and cost money to the business (Lee, 2021). Not all risks have similar importance, the risk assessment framework helps entrepreneurs in prioritising all the risks based on their potential and type of occurrence. Most entrepreneurs have limited resources, thus, having a risk assessment framework is able to help in making proper decisions about where and how to invest in cyber security to get a proper cure in business (Landoll, 2021). It can also be seen that the risk-assessing framework provides a proactive process of managing risk which is better than reacting to the risk after it has been materialised. Hence, the overall discussion in this part has helped in understanding that a risk management framework needs to be used to implement proper cyber security measures for entrepreneurs in business.

Theme 2: Establishment of a continuous monitoring and incident response credibility can help in reducing cyber risks

Continuous monitoring of the activity of the digital and tech-based applications can help in getting real-time visibility into the system and network effectively. It is able to help an entrepreneur and its team detect any malicious or suspicious behaviour in the system or network (Hawamleh *et al.* 2020). Constant monitoring is able to help in responding immediately to any security incidents. According to, Hasan *et al.* (2021), rapid mitigation of cyber threats is highly important to lower the losses, and risk of losing all vital documents. Thus, the threats need to be detected early stage for which continuous monitoring is truly highly effective. On the other hand, the risk related to online platforms can also harm the safety of customers of a business, where the early detection of risk can help in safeguarding customers which ultimately protects the reputation of an entrepreneur. Instantaneous incident reaction declines the amount of downtime caused by cyber incidents (Georgiadou *et al.* 2022). This is critical for firm continuity as extended downtime is able to result in financial losses and reputational harm. Therefore, the discussion on this theme has helped in understand that early detection of threats in a business can be done through continuous monitoring of the system and network that can protect the image of entrepreneurs effectively.

Theme 3: Implementation of continuous employee training and awareness programs can help in managing cyber risk effectively

Cyber threat is not only restricted to the eligibility of a software application, it also considers the eligibility of a person to handle technology and the digital world. Ali *et al.* (2020), mentioned continuous employee training and programs for awareness regarding cyber threats and controlling measures can help businesses handle risks better. Management of risk in vulnerable

times can become easier when employees have enough knowledge to take accurate action. Training of all employees can help entrepreneurs to inform them of the importance of a unique ID and password for all individuals to protect the safety of personal and company information (Svilicic *et al.* 2019). Increasing familiarity with the case incidents of cyber-attacks can help employees detect any suspicious movement in the business network at an early stage. Awareness, on the other side, can help in informing the types, ways and potential of different threats and the way of taking immediate mitigation steps to lower the risks (Del Giorgio Solfa, 2022). Thus, the constant training and awareness programme for the employees in a business can help entrepreneurs handle business better.

Discussion

The collection of secondary data has helped in defining all the vital points in this study. The analysis of the collected data has helped to understand the value of proper encryption, using strong passwords and restricted or well-protected devices for business purposes (Dicuonzo *et al.* 2019). It can be seen that using upgraded malfunction detection tools can help in preventing most of the common cases of threat in the digital world. The cyber security network needs to be implemented at the early stage of detecting the weaknesses of a network (Lee, 2020). The use of systems in this study has helped in understanding the way all the components in a system are codependent to fight against a threat or affected together. It was also highlighted in this study that, all the aspects of threats have different cures, thus, the type of courage and potential of damaging the business need to be analysed to implement cyber security measures. There are policies and procedures to establish a strong cyber-protected network for businesses (Androjna *et al.* 2020). However, it can be costly but it is able to help reduce the cost of handling legal actions after data breaches.

Conclusion

This study has conducted thorough research to inform the way cyber security is important for risk management in business to safeguard entrepreneurs. Many forms of security measures are available to help businesses to handle cyber risks effectively. The aims and objectives have been set properly which has helped in conducting the entire research constructively. Theoretical discussion has shown the link between system theory to the cyber network securing measures. The thematic analysis in this study has helped to explain the vital points of all the collected data.

References

- Alahmari, A. and Duncan, B., 2020, June. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1-5). IEEE.
- Alford, P. and Jones, R., 2020. The lone digital tourism entrepreneur: Knowledge acquisition and collaborative transfer. *Tourism Management*, 81, p.104139.
- AlGhamdi, S., Win, K.T. and Vlahu-Gjorgievska, E., 2020. Information security governance challenges and critical success factors: Systematic review. *Computers & security*, 99, p.102030.

- Ali, O., Shrestha, A., Chatfield, A. and Murray, P., 2020. Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, 37(1), p.101419.
- Androjna, A., Brcko, T., Pavic, I. and Greidanus, H., 2020. Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, 8(10), p.776.
- Becvar, R.J., Becvar, D.S. and Reif, L.V., 2023. *Systems theory and family therapy: A primer*. Rowman & Littlefield.
- Ben Arfi, W. and Hikkerova, L., 2021. Corporate entrepreneurship, product innovation, and knowledge conversion: the role of digital platforms. *Small Business Economics*, 56, pp.1191-1204.
- Bican, P.M. and Brem, A., 2020. Digital business model, digital transformation, digital entrepreneurship: Is there a sustainable “digital”? *Sustainability*, 12(13), p.5239.
- Del Giorgio Solfa, F., 2022. Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry. *International Journal of Technology, Innovation and Management (IJTIM)*, 2.
- Dicuonzo, G., Galeone, G., Zappimulso, E. and Dell'Atti, V., 2019. Risk management 4.0: The role of big data analytics in the bank sector. *International Journal of Economics and Financial Issues*, 9(6), pp.40-47.
- Elia, G., Margherita, A. and Passiante, G., 2020. Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process. *Technological forecasting and social change*, 150, p.119791.
- Georgiadou, A., Mouzakis, S., Bounas, K. and Askounis, D., 2022. A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, 62(3), pp.452-462.
- Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R., 2021. Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, p.102726.
- Hawamleh, A.M.A., Alorfi, A.S.M., Al-Gasawneh, J.A. and Al-Rawashdeh, G., 2020. Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology*, 63(5), pp.7894-7899.
- Jafari-Sadeghi, V., Garcia-Perez, A., Candelo, E. and Couturier, J., 2021. Exploring the impact of digital transformation on technology entrepreneurship and technological market expansion: The role of technology readiness, exploration and exploitation. *Journal of Business Research*, 124, pp.100-111.
- Jafari-Sadeghi, V., Garcia-Perez, A., Candelo, E. and Couturier, J., 2021. Exploring the impact of digital transformation on technology entrepreneurship and technological market expansion: The role of technology readiness, exploration and exploitation. *Journal of Business Research*, 124, pp.100-111.

- Kraus, S., Palmer, C., Kailer, N., Kallinger, F.L. and Spitzer, J., 2019. Digital entrepreneurship: A research agenda on new business models for the twenty-first century. *International Journal of Entrepreneurial Behavior & Research*, 25(2), pp.353-375.
- Landoll, D., 2021. *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press.
- Lee, I., 2020. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future internet*, 12(9), p.157.
- Lee, I., 2021. Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), pp.659-671.
- Lopez, C.A., Castillo, L.F. and Corchado, J.M., 2021. Discovering the value creation system in IoT ecosystems. *Sensors*, 21(2), p.328.
- Mandviwalla, M. and Flanagan, R., 2021. Small business digital transformation in the context of the pandemic. *European Journal of Information Systems*, 30(4), pp.359-375.
- Markovsky, I. and Dörfler, F., 2021. Behavioral systems theory in data-driven analysis, signal processing, and control. *Annual Reviews in Control*, 52, pp.42-64.
- Mazhar, S.A., Anjum, R., Anwar, A.I. and Khan, A.A., 2021. Methods of data collection: A fundamental tool of research. *Journal of Integrated Community Health (ISSN 2319-9113)*, 10(1), pp.6-10.
- Ratten, V. and Jones, P., 2021. Entrepreneurship and management education: Exploring trends and gaps. *The International Journal of Management Education*, 19(1), p.100431.
- Secundo, G., Gioconda, M.E.L.E., Del Vecchio, P., Gianluca, E.L.I.A., Margherita, A. and Valentina, N.D.O.U., 2021. Threat or opportunity? A case study of digital-enabled redesign of entrepreneurship education in the COVID-19 emergency. *Technological forecasting and social change*, 166, p.120565.
- Statista, 2023 (Online) Which of the following rules or controls, if any, do you have in place? Available at: <https://www.statista.com/statistics/586660/implemented-cyber-security-rules-or-controls-by-uk-businesses/> Accessed on 29th October, 2023]
- Stine, K., Quinn, S., Witte, G. and Gardner, R.K., 2020. Integrating cybersecurity and enterprise risk management (ERM). *National Institute of Standards and Technology*, 10.
- Svilicic, B., Kamahara, J., Celic, J. and Bolmsten, J., 2019. Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU Journal of*
- Vadana, I.I., Torkkeli, L., Kuivalainen, O. and Saarenketo, S., 2020. Digitalization of companies in international entrepreneurship and marketing. *International Marketing Review*, 37(3), pp.471-492.
- von Briel, F., Selander, L., Hukal, P., Lehmann, J., Rothe, H., Fürstenau, D., Recker, J., Jarvenpaa, S., Yoo, Y., Alpar, P. and Wurm, B., 2021. Researching digital entrepreneurship: Current issues and suggestions for future directions. *Communications of the Association for Information Systems*, 48, pp.284-304.