CYBER RISK MANAGEMENT WITH THE HELP OF ARTIFICIAL INTELLIGENCE IN SMES: ANALYSIS OF BARRIERS AND NEEDS

Lukas Holder[0000-0002-9272-6671]
Institute of Business Economics and Industrial Sociology, Graz University of Technology

Abstract: *Cyber Risk Management is a critical concern for Small and Medium Enterprises as they increasingly become attractive targets for cyber-attacks. Despite this, many Small and Medium Enterprises lack awareness about the growing cyber threats they face. With artificial intelligence tools' emergence, opportunities and threats for cyber attackers and defenders have heightened. Small and Medium Enterprises require resources and knowledge to protect themselves against cyber-attacks effectively. Social engineering attacks like phishing emails or malware-infected websites are common in the digital landscape. This paper provides an overview of barriers and needs in Cyber Risk Management for Small and Medium Enterprises, based on a literature review conducted via Web of Science, Scopus, and Google Scholar. The current state of Cyber Risk Management in Small and Medium Enterprises is analyzed, focusing on identified shortcomings. Additionally, the availability of AI tools for Small and Medium Enterprises is examined, and best practice examples are provided to guide Small and Medium Enterprises in improving their cybersecurity.*

Keywords: Cybersecurity, Cyber-Risk-Management, Artificial Intelligence

1. INTRODUCTION

In recent years, cyber security has become an enormous issue for companies. Small and Medium Enterprises (SMEs) have emerged as desirable targets. In these companies, there is usually no dedicated cyber risk management, if there is any risk management. This neglect of cyber security can lead to existentially threatening damage. Computer networks are becoming more complex. More and more machines and systems are being added to these networks and thus offer more and more attack surfaces for harmful cyber-attacks. Phishing, malware, and ransomware attacks are widely spread and do not only target large corporations (Bin & Ali, 2022).
Artificial intelligence (AI) is also a factor that has caused more and more turmoil in recent years, notably in recent months. Artificial intelligence can become a danger in the cyberspace, especially for SMEs, but it can also be used to protect against attacks (Kant & Johannsen, 2022). Cybercrime can be reduced with the help of this technology, and attacks can be detected and averted. With AI, decisions can also be made in crucial cyber risk management. Above all, malware can be identified with the help of AI-based tools. (Jakka et al., 2022).
To find out exactly how aware SMEs are of the seriousness of the situation, this research analyses the current literature using a systematic literature review. This literature review aims to analyze the current threats in the cyber environment of SMEs. In section 2, possible risks that threaten SMEs are searched for and explored in more detail. Section 3 explains the threats in more detail and explains possible counter-strategies. These are described in best practice examples. A small focus is set on Artificial Intelligence.

2. Systematic Literature Review

The Systematic Literature Review (SLR) guidelines by Wright et al., (2007) were used as orientation. This paper explains a simple seven-step plan to help create an SLR. The seven steps are the definition of a research question, the creation of a search protocol, the literature search, the data extraction, a quality appraisal, a data analysis and results and finally the interpretation of the results. To begin the systematic literature review, the following research question was asked first:
"What are the current cyber risks SMEs face, and what is the role of Artificial Intelligence in cyber security?"
The databases Web of Science, Scopus, and Google Scholar were searched. Scopus, the largest citation database for peer-reviewed literature, offers a dynamic and configurable search system. In the first search, the following search string was used: (TITLE-ABS-KEY (smes AND cyber AND security). This string yielded 196 results. The second search extended the string to (TITLE-ABS-KEY (artificial AND intelligence AND smes AND cyber AND security), which got 15 results. The second search was conducted on Web of Science, a comprehensive research database and citation index provided by Clarivate Analytics. It was chosen because

it has a curated, published, peer-reviewed content database. The same two search strings were used to search. The first search yielded 107, and the second 12 results. The last search was conducted on Google Scholar, a freely accessible web search engine provided by Google that focuses on academic literature. This database lacks a configurable search system, and the search terms yielded 34.200 and 15.900, respectively. However, only the first few pages are relevant results, and none of the papers found were new.
Exclusions and inclusion criteria were defined to narrow the search further following limitations. The language of the literature was kept in English only. Only information technology (IT), operational technology (OT), Computer Engineering Business, and Management literature were used. Articles and conference papers were included, whereas books and book chapters were excluded.
After a title analysis, the individual abstracts of the papers were reviewed for relevance. In the end, 69 papers remained that were equipped with relevant information. These articles were sorted by title and year, and relevant risks were extracted. Mendeley was used to sort the research results, where entries found twice were eliminated.
The following paragraphs show some of the more interesting papers. Haastrecht et al. (2021) show some promising findings in their work. They identify many threats SMEs face, like malware attacks, ransomware attacks, Phishing, and DoS and DDoS attacks. In their paper, they write about cyber threat intelligence (CTI) to improve collective cybersecurity resilience and want to bring this strategy to SMEs. Haastrecht et al. (2021) published a second paper in which they write about motivating SMEs using Self-Determination Theory (SDT) to implement cyber risk management and conduct a cyber risk assessment.
Artificial intelligence was also a focus of the investigation. Rawindaran et al. (2021) write about the cost benefits of using machine learning features in Network Intrusion Detection systems NIDs for cyber security. They mention a cyber pandemic where the pattern recognition of machine learning tools can be used to protect data and prevent cyber-attacks. Automated security event responses are the focus of the research of Fraley & Cannady (2017). In combination with Neural Networks, or Deep Neural Networks, a vast amount of data can be analyzed, and different patterns could be found that indicate threats like data leaks or network intrusions.

3. RESULTS AND DISCUSSION

This Section presents the results of the systematic literature review. It is interesting to look at the publication years of the individual papers. Figure 1 shows that in the early 2000s, hardly any articles were published on cyber security in SMEs. Cybersecurity was a generally new topic, and much basic research had to be done. Around the beginning of the 2010s, interest in this area began to take root. Cyber security concepts were concretized and also applied to SMEs. Only at the end of the 2010s can one see the beginning of an upswing. Especially the years during and after the COVID-19 pandemic show a significant increase in interest in the topic. Cyber security naturally became a big issue here with the forced digitalization. Smaller companies have also brought their networks online and thus offered a large surface for potential attacks. The need for solutions and information about risks has naturally also increased.

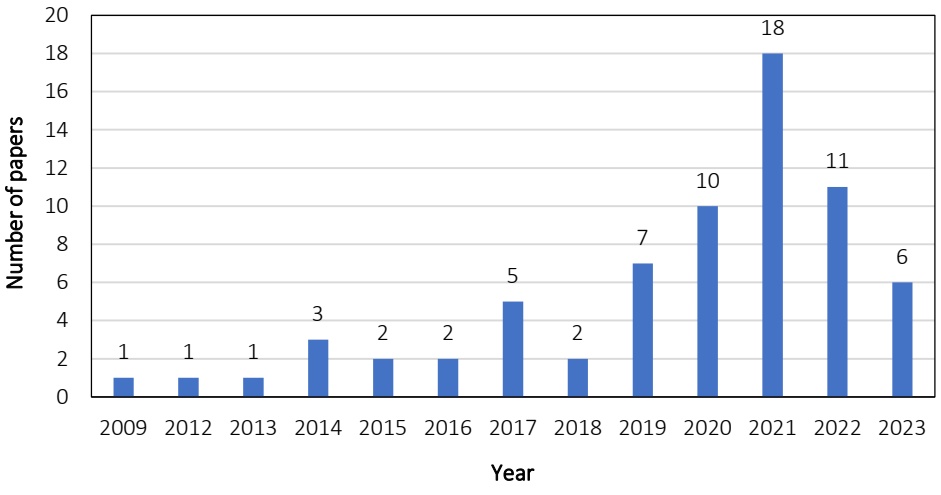

Figure 1: Publication Year of the Found Research Results (N=69)

In Figure 2, it can be seen that the main threat from SMEs is malware attacks. Malware is malicious software that can enter corporate networks through multiple routes. It is often a carelessly clicked link that leads to

an infection. There are many different types of malware. Ransomware, spyware, and adware were explicitly mentioned in the papers. Ransomware usually locks a system and demands a ransom to rerelease it. Spyware is used to steal data such as passwords, and adware is an annoying ad that gets stuck in the PC's software, usually the browser.

The second most frequently mentioned attack is phishing. The term phishing is made up of the word's password and fishing. The attacker tries to appear as a trustworthy person or institution to steal sensitive data from the victim via email, telephone, or text message. Spear phishing was also mentioned. This is a phishing attack that targets a specific person or company. Phishing and spear phishing belong to the group of social engineering attacks where the social characteristics of people are actively exploited to obtain information (Bada & Nurse, 2019).

In third place, there is another point that has often been mentioned. Lack of awareness was noted in 24 articles. The management has much catching up to do in this area. In addition to this problem, there is a lack of resources, a lack of knowledge, and the a of cyber risk management. The management must inform their staff about potential risks, provide enough funding, and help keep the potential of cyber threats as low as possible. Employees, in general, could be a risk to the company's cyber security. A lack of training can make them susceptible to social engineering attacks like phishing attacks, and they could become an insider threat. This can happen intentionally or unintentionally. Weak passwords can lead to data breaches or identity theft. It can be seen that the human factor can lead to a variety of problems (Kalhoro et al., 2022).

Denial of Service or Distributed Denial of Service attacks, also known as DoS and DDoS attacks, specifically target servers or web applications to interrupt the service of these systems. In general, the network of SMEs is constantly strained (Pawar & Palivela, 2022). Be it attacks like the Man in the Middle attack, where an attacker interposes himself between two communicating systems, or an Eavesdropping attack where communications of networks are intercepted and essential data is stolen (Zeadally et al., 2020).

The networking of devices and the ever-smarter development of companies also lead to new risks and areas of attack. Internet of Things threats have become increasingly relevant in recent years. Smartphones, old machines connected to the company network, or laptops carried from the company network to public networks for home offices offer new attack opportunities (Vakakis et al., 2019).

Not only threats from the company can become dangerous, but stakeholders can also lead to problems. External bank accounts can get hacked and robbed of funding or cloud services used by the company to store data, which can get breached and lead to many problems.

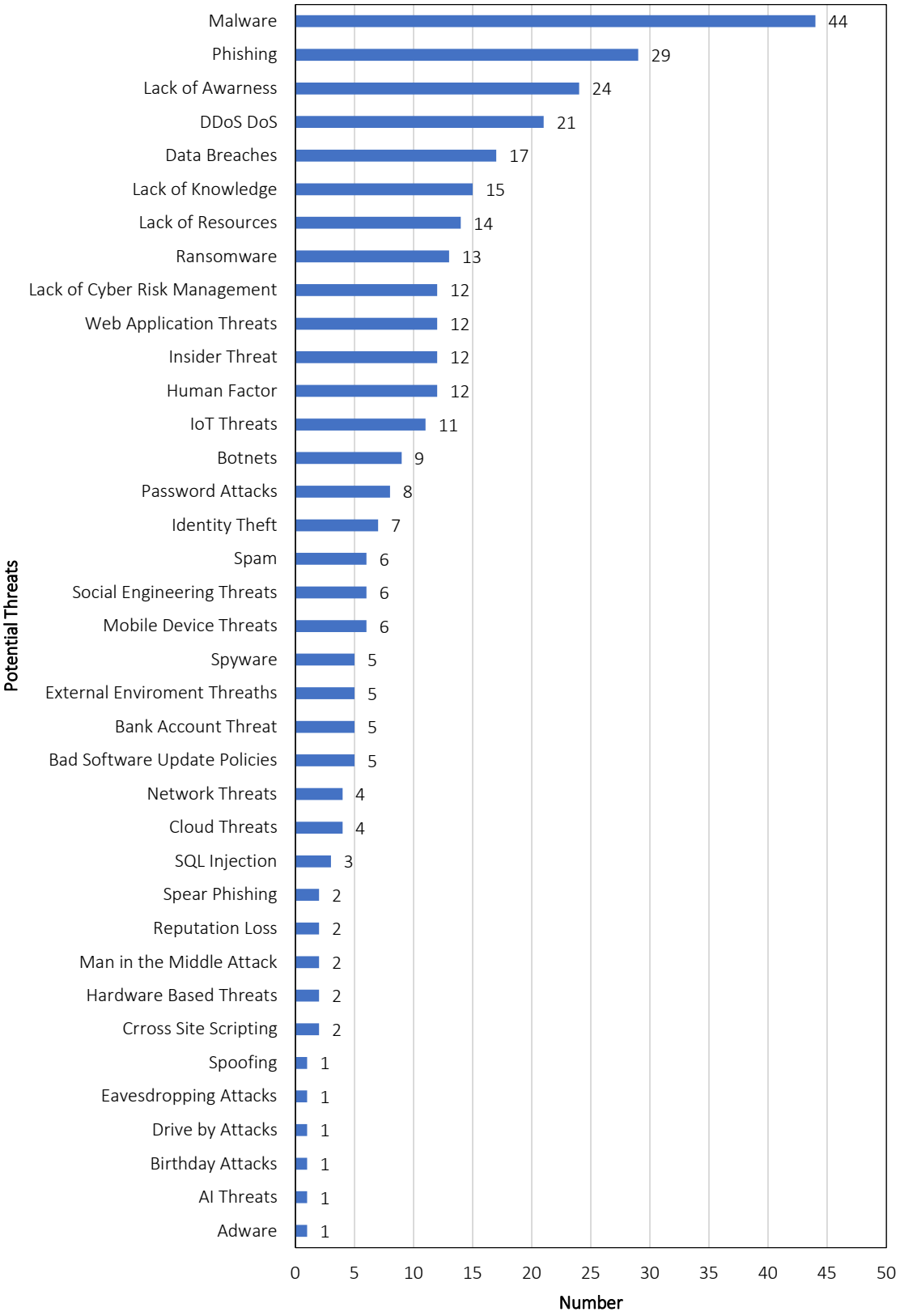

Figure 2: Cyber Threats mentioned and discussed in the Literature (N=325)

3.1 Best Practice Examples and Potential Barriers

Most of the formerly mentioned threats can be reduced or even avoided with straightforward policies and steps in the right direction. However, most SMEs face a barrier. Often, there is a lack of financial resources, or the companies are overconfident in cyber security (Alahmari & Duncan, 2021). Emer et al. (2021) have provided examples of how to mitigate those cyber risks and threats, and some of the strategies shown can be implemented without the need for enormous resources or knowledge. Proper cyber risk management is the key to a working cyber security strategy. First of all, a risk assessment should be conducted with a focus on cyber risk.

Low-hanging fruits like antivirus software and a proper firewall can help guard the system and prevent cyber-attacks. Those systems will be able to detect most malware and lower the chance of a network intrusion or data breach. To combat human-based threats, companies need to inform and train their employees about cyber-attack risks. Proper user management is also advantageous. Employees only get the rights for systems they need and use during their workday. This mitigates the risks of intentional or unintentional human-based threats. Methods such as two-factor authentication and regular password updates with precise specifications should be implemented to combat employee threats further.

Investing in artificial intelligence and machine learning solutions is undoubtedly a sound decision, as highlighted Rawindaran & Jayal (2021), who discuss the application of AI tools in intrusion detection. These tools enable the detection and prevention of malware attacks and their associated damage. The constantly evolving cyber threat landscape presents persistent challenges in cybersecurity for companies. In response, the adoption of artificial intelligence has given rise to both offensive and defensive strategies in the realm of cyber warfare. Offensive AI enhances the efficiency and effectiveness of cyber-attacks, while defensive AI is geared towards fortifying cybersecurity measures. For small and medium-sized enterprises, which often struggle with limited resources, effective defensive cybersecurity solutions are of immense importance. In light of this, the integration of AI-based defenses has become imperative. Although AI primarily serves as a protective measure, it's crucial to recognize that attackers are increasingly leveraging AI for a wide array of sophisticated attacks, as highlighted by Kant & Johannsen.

4. CONCLUSIONS

In conclusion, this paper highlights the critical importance of cyber risk management for Small and Medium Enterprises and the need for increased awareness and resources to protect against cyber-attacks effectively. The systematic literature review conducted in this research provides valuable insights into the current state of cyber risk management in SMEs, focusing on identified barriers and needs. The findings reveal that malware attacks, phishing, lack of awareness, and denial of service attacks are among SMEs' significant threats.

One significant aspect discussed in the paper is the role of artificial intelligence (AI) in cyber security. AI has the potential to both enhance cyber-attack capabilities and strengthen defense mechanisms. It can detect and prevent attacks, identify malware, and make informed decisions in cyber risk management. Incorporating AI tools and technologies can significantly benefit SMEs in improving their cybersecurity posture.

The publication analysis presented in the paper indicates a growing interest in cyber security for SMEs, particularly in recent years. The increased attention can be attributed to the evolving cyber threat landscape and the digitalization trends accelerated by events such as the COVID-19 pandemic. As SMEs increasingly rely on digital systems and networks, effective cyber risk management solutions become paramount.

Overall, this research emphasizes the importance of addressing the identified barriers and needs in cyber risk management for SMEs. It provides best practice examples and highlights the potential of AI tools in mitigating cyber risks. By raising awareness, allocating sufficient resources, and adopting appropriate cyber risk management strategies, SMEs can enhance their cybersecurity resilience and protect their critical assets from cyber threats. The insights and recommendations presented in this paper serve as a valuable resource for SMEs seeking to strengthen their cyber risk management practices in the face of an evolving threat landscape.

REFERENCES

Alahmari, A. A., & Duncan, R. A. (2021, July 1). Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs. *Proceedings of the 13th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2021*. https://doi.org/10.1109/ECAI52376.2021.9515166

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Bin, A., & Ali, A. (2022). *Cybersecurity Infrastructure adoption Model for Malware Mitigation in Small Medium Enterprises (SME)*. *August*, 6–8.

Emer, A., Unterhofer, M., & Rauch, E. (2021). A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises. *IEEE Engineering Management Review*, *49*(2), 98–109. https://doi.org/10.1109/EMR.2021.3078077

Fraley, J. B., & Cannady, J. (2017, May 10). The promise of machine learning in cybersecurity. *Conference Proceedings - IEEE SOUTHEASTCON*. https://doi.org/10.1109/SECON.2017.7925283

Haastrecht, M. Van, Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Adrian, R., Baumgartner, L., Fricker, S., Ruiz, J. F., Armas, E., Brinkhuis, M., & Spruit, M. (2021). *A Shared Cyber Threat Intelligence Solution for SMEs*. 1–21.

Jakka, G., Yathiraju, N., & Ansari, M. F. (2022). *Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management*. *6*(3), 6156–6165.

Kalhoro, S., Ayyasamy, R. K., Jebna, A. K., Kalhoro, A., Krishnan, K., & Nodeson, S. (2022). *How Personality Traits Impacts on Cyber Security Behaviors of SMEs Employees*. 635–641.

Kant, D., & Johannsen, A. (2022). *Evaluation of AI-based use cases for enhancing the cyber secu- rity defense of small and medium-sized companies (SMEs)*. 1–8.

Pawar, S., & Palivela, D. H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1). https://doi.org/10.1016/j.jjimei.2022.100080

Rawindaran, N., & Jayal, A. (2021). *Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries*.

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2021). Cost benefits of using machine learning features in NIDS for cyber security in UK small medium enterprises (SME). *Future Internet*, *13*(8). https://doi.org/10.3390/fi13080186

Vakakis, N., Nikolis, O., Ioannidis, D., Votis, K., & Tzovaras, D. (2019). Cybersecurity in SMEs: The smart-home/office use case. *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD*, *2019-Septe*. https://doi.org/10.1109/CAMAD.2019.8858471

Van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021, August 17). A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3465481.3469199

Wright, R. W., Brand, R. A., Dunn, W., & Spindler, K. P. (2007). How to write a systematic review. *Clinical Orthopaedics and Related Research*, *455*, 23–29. https://doi.org/10.1097/BLO.0b013e31802c9098

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access*, *8*, 23817–23837. https://doi.org/10.1109/ACCESS.2020.2968045

APPENDIX 1. List of paper used for the Systematic Literature Review

Title of the Paper	Year	Author
The severity and effects of Cyber-breaches in SMEs: a machine learning approach	2023	Arroyabe et al.
Small-Scale Cyber Security	2023	Osborn & Simpson
Data-driven Intrusion Detection System for Small and Medium Enterprises	2023	Elezaj et al.
Cybersecurity Awareness and Capacities of SMEs	2023	Erdogan et al.
Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors	2023	Sukumar et al.
It Won't Happen to Me: Surveying SME Attitudes to Cyber-security	2022	Wilson et al.
Improving Cybersecurity Awareness Among SMEs in the Manufacturing Industry	2022	Johansson et al.
How Personality Traits Impacts on Cyber Security Behaviors of SMEs Employees	2022	Kalhoro et al.
Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime	2022	Rawindaran & Jayal
LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)	2022	Pawar & Palivela
Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management	2022	Jakka et al.
Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs)	2022	Kant & Johannsen
Machine learning approach for intrusion detection systems as a cyber security strategy for Small and Medium Enterprises	2022	Baci et al.
Capability oriented RE for Cybersecurity and Personal Data Protection: Meeting the challenges of SMEs	2022	Kavakli
SENTINEL - Approachable, tailor-made cybersecurity and data protection for small enterprises	2022	Trantidou et al.
Cybersecurity Infrastructure adoption Model for Malware Mitigation in Small Medium Enterprises (SME)	2022	Bin & Ali
A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs	2021	Renaud & Ophoff
Intrusion Detection System using Autoencoder based Deep Neural Network for SME Cybersecurity	2021	Ubaidillah et al.
Investigating Cyber Security Factors Influencing The Perception Behavioral Intention of Small and Medium Enterprise	2021	Bisma et al.
A Shared Cyber Threat Intelligence Solution for SMEs	2021	Haastrecht et al.
A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs	2021	Haastrecht et al.
A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises	2021	Emer et al.
Classifying SMEs for Approaching Cybersecurity Competence and Awareness	2021	Shojaifar & Järvinen
Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME)	2021	Rawindaran et al.
Cyber risk management in SMEs: insights from industry surveys	2021	Hoppe et al.
Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment	2021	Boletsis et al.
Exploring Cybersecurity Ecosystem in the Middle East: Towards an SME Recommender System	2021	Ahmed & Nanath
Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal	2021	Antunes et al.
Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs	2021	Alahmari & Duncan
It's Not My Problem: How Healthcare Models Relate to SME Cybersecurity Awareness	2021	Pickering et al.
Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries	2021	Rawindaran, Jayal, & Prakash
On Strengthening SMEs and MEs Threat Intelligence and Awareness by Identifying Data Breaches, Stolen Credentials and Illegal Activities on the Dark Web	2021	Pantelis et al.
Practical Autonomous Cyberhealth for resilient Micro, Small and Medium-sized Enterprises	2021	Mantas et al.
The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses	2021	Tam et al.
Towards Cybersecurity Risk Management Investment: A Proposed Encouragement Factors Framework for SMEs	2021	Alahmari & Duncan

A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs	2020	Armenia et al.
Calculated risk? A cybersecurity evaluation tool for SMEs	2020	Benz & Chatterjee
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	2020	Radanliev et al.
Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda	2020	Ozkan & Spruit
Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence	2020	Alahmari & Duncan
Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity	2020	Zeadally et al.
Intelligent Detection and Recovery from Cyberattacks for Small and Medium-Sized Enterprises	2020	Lopez et al.
Systematic Approach to Cyber Resilience Operationalization in SMEs	2020	Carías et al.
The dark side of data science - An empirical study of cyber risks in German SMEs	2020	Ulrich et al.
The business benefits of cyber security for SMEs	2020	Lloyd
A Novel Cybersecurity Framework for Countermeasure of SME's in Saudi Arabia	2019	Ajmi et al.
Survey and Lessons Learned on Raising SME Awareness about Cybersecurity	2019	Ponsard et al.
Predicting CyberSecurity Incidents using Machine Learning Algorithms: A Case Study of Korean SMEs	2019	Mohasseb et al.
Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)	2019	Bada & Nurse
Defining a New Composite Cybersecurity Rating Scheme for SMEs in the U.K.	2019	Rae & Patel
Cybersecurity in SMEs: The Smart-Home/Office Use Case	2019	Vakakis et al.,
A big data framework for network security of small and medium enterprises for future computing	2019	Kyun et al.
Towards a Cyber Security Label for SMEs: A European Perspective	2018	Ponsard et al.
Exploring SME cybersecurity practices in developing countries Exploring SME cybersecurity practices in developing countries	2018	Kabanda et al.
The Promise of Machine Learning in Cybersecurity	2017	Fraley & Cannady
Managing Cybersecurity and e-Commerce Risks in Small Businesses	2017	Raghavan et al.
Effective Cyber Security Strategies for Small Businesses	2017	Cook
Cyber-Security Policy Decisions in Small Businesses	2017	Patterson
A state of the art survey - Impact of cyber-attacks on SME's	2017	Saleem & Ande
How South African SMEs address cyber security: the case of web server logs and intrusion detection	2016	Kent et al.
Cyber Security & Ethical Hacking For SMEs	2016	Berger & Jones
A Conceptual Model of an Intelligent Platform for Security Risk Assessment in SMEs	2015	Arenda
The cyber security in SMEs in Poland and Tanzania	2015	Nycz et al.
Small to Medium Enterprise Cyber Security Awareness: An Initial Survey of Western A eastern Australian Business	2014	Valli et al.
Cybersecurity Information Sharing: a Framework for Information Security Management in UK SME Supply Chains	2014	Lewis et al.
Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs	2014	Osborn
Cyber Security: Small Firms under Fire	2013	Hayes & Bodhani
Cyber Security Scenarios and Control for Small and Medium Enterprises	2012	Sangani & Vijayakumar
SMEs and Cybersecurity Threats in E-Commerce	2009	Sharma et al.