Cyber risk assessment in small and medium-sized enterprises

Sukumar, Arun; Mahdiraji, Hannan Amoozad; Jafari-Sadeghi, Vahid

DOI:
10.1111/risa.14092

Citation for published version (Harvard):
Sukumar, A, Mahdiraji, HA & Jafari-Sadeghi, V 2023, 'Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors', *Risk Analysis*, vol. 43, no. 10, pp. 2082-2098. https://doi.org/10.1111/risa.14092

DOI: 10.1111/risa.14092

ORIGINAL ARTICLE

Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors

Arun Sukumar[1] | Hannan Amoozad Mahdiraji[2] | Vahid Jafari-Sadeghi[3]

[1] Bristol Business School, University of the West of England, Bristol, UK

[2] School of Business, University of Leicester, Leicester, UK

[3] Aston Business School, Aston University, Birmingham, UK

Correspondence
Vahid Jafari-Sadeghi, Aston Business School, Aston University, Aston Triangle, Birmingham, B4 7ET, the United Kingdom.
Email: v.jafari-sadeghi@aston.ac.uk

Abstract

The role played by information and communication technologies in today's businesses cannot be underestimated. While such technological advancements provide numerous advantages and opportunities, they are known to thread organizations with new challenges such as cyberattacks. This is particularly important for small and medium-sized enterprises (SMEs) that are deemed to be the least mature and highly vulnerable to cybersecurity risks. Thus, this research is set to assess the cyber risks in online retailing SMEs (e-tailing SMEs). Therefore, this article employs a sample of 124 small e-tailers in the United Kingdom and takes advantage of a multi-criteria decision analysis (MCDA) method. Indeed, we identified a total number of 28 identified cyber-oriented risks in five exhaustive themes of "security," "dependency," "employee," "strategic," and "legal" risks. Subsequently, an integrated approach using step-wise weight assessment ratio analysis (SWARA) and best–worst method (BWM) has been employed to develop a pathway of risk assessment. As such, the current study outlines a novel approach toward cybersecurity risk management for e-tailing SMEs and discusses its effectiveness and contributions to the cyber risk management literature.

KEYWORDS

cyber risk, cybersecurity, e-tailers, MCDA, SMEs

1 | INTRODUCTION

In the last decade, the waves of digital transformation have forced small and medium-sized enterprises (SMEs) to adopt and equip their business models with ever-evolving technologies (Jafari-Sadeghi et al., 2021). Be it online shopping (Tarhini et al., 2018) or running supply chains of firms (Dallasega et al., 2018), technological advancement has created new and exciting business opportunities (Soomro et al., 2016), and it has also led to new challenges that altered organizational designs, the ability to manage data, and a new source of risks (Calabrese et al., 2019; Jafari-Sadeghi, 2021; Shah et al., 2019). Indeed, emerging obstacles such as information security and cyber risks have resulted in widespread financial and nonfinancial losses (Arcuri et al., 2017). In this vein, SMEs are deemed to face the same levels of cybersecurity issues as their larger counterparts, however, limited resources and capabilities made them fragile against cyber risks (Baggott & Santos, 2020; Benz & Chatterjee, 2020). That is, cyber risk management and preparation emerge as crucial competencies for not only survival but also the growth of small firms (Chatterjee, 2019; Hoppe et al., 2021).

Given that, in recent years, cybersecurity has become increasingly popular among scholars (e.g., Krombholz et al., 2015; Kshetri, 2018), several shortcomings have been found in extant research. To begin with, a considerable body of cybersecurity literature has explored the risk management strategies, technical issues, organizational design, awareness, and mitigation options in large enterprises (Cains et al., 2021; Shah et al., 2019). However, little is known about the extent to which SMEs deal with cyber risks. Given that SMEs are often major stakeholders of larger firms, they are considered potential targets for cyber attackers to penetrate larger counterparts (Better Business Bureau, 2017). This is particularly important as a survey at National Center for the Middle Market (2016) highlights that "55% of SME companies lack either an up-to-date cyber-risk strategy or any defined cyber-risk strategy at all" (Benz & Chatterjee, 2020). Hence, more studies are required to explore the level of preparedness, risk assessment strategies, and defense capabilities in dealing with cybersecurity issues within small enterprises such as e-tailing SMEs (online retailing SMEs that provide product/service offering to customers via the Internet). Online retailing SMEs constitute one of the largest adaptors of internet and communication technologies (Hånell et al., 2019) and given the potential impact of cyber risks, it is important to identify the risks these SMEs face and assess them in their contextual setting.

Second, emerging research on SMEs and their ability to manage cyber risks although is increasing, is still fragmented. For instance, Ključnikov et al. (2019) examined the success factors of information security in SMEs, while Ponsard and Grandclaudon (2019) addressed the different applicable standards and guidelines for safeguarding SMEs from cyber threats. Other works have also noted the importance of cybersecurity to SMEs, that is, ethical hacking (Berger & Jones, 2016), network security tools (Iyamuremye & Shima, 2018), security management (Markakis et al., 2019), and compliance challenges (Lloyd, 2020). However, there is a gap in the literature to comprehensively provide the types of cyber risks associated with small enterprises that mostly operate on online platforms. Such categorization seems crucial due to the nature of cyber risks. According to Ratten (2019), cyber threats are complex, some are purely system vulnerabilities while others arise because of human actors. Threats involve sociotechnical factors (Hills & Atkinson, 2016) and organizational contexts play an important role in their interpretation and estimation (Grant et al., 2014).

Third, regarding methodological perspectives, current approaches to risk analysis (also known as technical risk analyses) are based on the quantification of risk. that is, the product of probability and impact of consequence and has come under criticism from researchers (Ganin et al., 2020; Renn, 1998). Ganin et al. (2020) argue that technical risk analyses are inadequate in dealing with everchanging cyber threat scenarios that are not well known or have not been characterized before. The oversimplification of risk masks the true nature of threats and does not allow true analysis to be bought forward (Paté-Cornell et al., 2018; Renn, 2021). In the context of SMEs, their unique firm characteristics, uncertain organizational contexts, and the lack of previous historical data make it difficult to employ traditional methods to characterize risk. An alternative to address risks in an SME context is to employ MCDA, in this approach, instead of risk assessment, the focus is shifted to risk-based decision making that is aimed at developing risk values that can be used for building indexes or scorecards (Triantaphyllou, 2000). The risk metrics are quantified either in their natural units or on the constructed scale and integrated depending on context-specific goals or priorities (Velasquez & Hester, 2013). The developed indexes or scorecards also help in charting the course of action or alternative mitigation strategies (Velasquez & Hester, 2013). That is, MCDA studies in risk management are growing (e.g., Ganin et al., 2020) and are now increasingly used as alternative approaches to traditional technical risk analysis techniques (e.g., Kiker et al., 2005; Wu et al., 2016).

Therefore, this article focuses on the nature of e-tailing SMEs and strives to address two distinct research objectives. Risk-based decision making can help in prioritizing risks and in the better deployment of scarce organizational resources. Accordingly, the first objective of this article attempts to consolidate the literature on cyber risks from the perspective of e-tailing SMEs. Subsequently, the second objective seeks to propose an analysis procedure to measure the importance of identified cyber risk scenarios and prioritize them based on their ranking, which contributes to risk management in the context of cybersecurity for small e-tailers. To address these research objectives, this article takes advantage of a multilayer MCDA method to explore and examine a total number of 28 identified cyber-oriented risks in five themes. When it comes to risk assessment, Shamala et al. (2017) argue that inaccurate and vague data can lead to incorrect decisions. Hence, to cope with the uncertainty and improve the process of analyzing risks, we employed an integrated approach of using step-wise weight assessment ratio analysis (SWARA) and best–worst method (BWM) to develop a pathway of risk assessment considering uncertainty.

The rest of the article is structured as follows. The next section explores the literature on cyber risks in the context of e-tailing SMEs as well as current approaches toward cyber risk assessment. It is followed by a detailed discussion regarding the methodological aspects of the integrated SWARA-BWM approach. The subsequent section delves into the case study and the results of the application SWARA-BWM approach, while the final section discusses the results of the study and highlights the key contribution of this work.

2 | LITERATURE REVIEW

It has been well established that with the rapid growth of information and communication technologies, there has been an increase in cyber risks in recent years (Radanliev et al., 2020). SMEs are not immune to the threats posed by the use of information and communication technologies studies have noted that SMEs may be more vulnerable to cyber threats when compared to larger firms (Payne, 2018; Sangani & Vijayakumar, 2012; Singh et al., 2022). Authors have noted several reasons for the vulnerability of SMEs to cybersecurity threats, they include lack of awareness (Topping et al., 2014), lack of resources (Kurpjuhn, 2015; Renaud, 2016; Satyanarayana et al., 2022), ignorance of employees (Henson & Garfield, 2016), absence of internal guidelines and standards (Ponsard et al., 2018), and high dependence on third-party vendors (Javaid & Iqbal, 2017). The manifestation of cyber threats and the resulting damages to both financial and reputational themes have been recognized and highlighted (Eling & Schnell, 2016).

TABLE 1 Cybersecurity studies in an SME context

Theme	References
SMEs' awareness of cyber threats and mitigation strategies	Payne, 2018; Topping, 2017; Harsch et al., 2014
SME cybersecurity readiness	Eilts & Levy, 2018; Teh & Kee, 2019; Osborn, 2014
SME supply chains and cybersecurity	Lewis, et al, 2014; Henson & Sutcliffe, 2013.
Regional studies on cyber risks and SMEs	Kent et al., 2016; Nycz et al., 2015; Asgary et al., 2020
Social engineering and SMEs	Osei & Yeboah-boateng, 2013; Onwubiko & Lenaghan, 2007
Evaluation tools	Benz & Chatterjee, 2020; Javaid & Iqbal, 2017; Burggraf et al., 2018
Business continuity	Mallinder & Drabwell, 2013; Sadok & Bednar, 2016
Information security and SMEs	Ključnikov et al., 2019; Yigit Ozkan et al., 2020; Brunner et al., 2018

In general, the topic of cybersecurity has been researched extensively, for example, the nature of cyber threats and their mitigation (Azmi et al., 2018; Kshetri, 2018; Nieto et al., 2019), human–computer interactions and resulting threats (Gupta et al., 2017; Heartfield et al., 2016; Krombholz et al., 2015), social engineering attacks (Gupta et al., 2017), technical aspects of cybersecurity (Stallings, 2019), standards, policies, and procedures (Bozkus Kahyaoglu & Caliyurt, 2018), identity fraud management (Shah et al., 2019), and MCDA approach to cyber risk assessment (Ganin et al., 2020). These works though addressing different aspects of cybersecurity have been developed either in the context of larger firms or hypothetical examples. Sangani and Vijayakumar (2012) note that large firms have the technological expertise to safeguard their company's information assets and the resources to safeguard against cyber threats through capital investment in security tools and employee training, however when it comes to SMEs, their resource constraints can be a barrier to address cyber threats and may expose them to financial and reputational damages.

While extensive studies have examined the impact of information and communication technology usage from an SME perspective (Mustafa & Yaakub, 2018), studies about their cyber risks and assessment are still emerging. A study by Eilts and Levy (2018) noted the cybersecurity awareness of SMEs while Lewis et al. (2014) addressed cybersecurity pertaining to SME supply chains. Decision making in small-scale IT users was studied by Osborn and Simpson (2017), with cybersecurity practices of SMEs in developing countries explored by Kabanda et al. (2018). Table 1 notes the major themes studied in relation to cybersecurity in the context of SMEs.

Examining the literature, we can notice that when it comes to cyber risks, there are very few studies that have looked into either assessment or risk evaluation in an SME context. From the perspective of online retailing SMEs, there are knowledge gaps in how risk is prioritized, how risks are assessed, and plans for mitigation. When one takes into account, the differences in firm characteristics and entrepreneurial risk profiles of individuals associated with SMEs (Ratten, 2019), there is a dearth of research examining how cyber risk management is undertaken in SMEs. The study of cyber risk management practice in SMEs is important because of the role played by them in the socioeconomic development of a nation. For example, a recent statistic notes that there are 5.9 million SMEs in the United Kingdom, contributing to an estimated 52% of total turnover (Department for Business Energy and Industrial Strategy, 2019). Forty-five percent of microenterprises have websites, and the website sales of SMEs alone were credited at 96.3 billion pounds in 2018 (Office for National Statistics, 2019). SMEs form a significant user base for the adoption of information and communication technologies and as such, a fertile ground for the manifestation of cyber risks.

Contrasting to the contribution of SMEs, a recent study also notes that four in ten SMEs have experienced cyberattacks in the 12 months (Rae & Patel, 2019) and only 14% of microenterprises are actively involved in Information and Communication Technology (ICT) risk assessments (Office for National Statistics, 2019). Given the contribution of SMEs and the lack of risk assessment techniques in their context, there is a need to address this. The existing approaches either based on technical risk analyses (PRA) or risk-based decision analysis (MCDA) have not specifically targeted SMEs nor have attempted to develop a framework for assessment and management. It is in addressing this gap, that we set our article, its main aim is to propose a model of MCDA—here an integrated approach of SWARA and BWM to develop a cyber-risk classification approach to e-tailing SMEs.

Core unified risk framework (CURF) developed by Wangen et al. (2018), provides a comprehensive framework of currently available approaches to information security risk assessment (ISRA). In their work, they have analyzed 11 ISRA methods and have developed a framework for comparing the methods for their completeness. The framework assesses the different methods, and functional approaches to risk management, that is, focusing on threats, and vulnerabilities and often based on risk equations (probabilities and impact). Apart from Wangen et al. (2018), other notable studies have looked into ISRA scope and methods (for example, see OCTAVE, Alberts & Dorofee, 2002; FAIR, Freund, 2015; NIST SP 800–30, Fenz et al., 2014).

Though there is considerable coverage in the development and comparison of different ISRA methods, there are a few drawbacks that are common in the approaches. Firstly, considered as a common themes in many of the approaches is the use of probabilites in risk quantification. in complex systems and in systems where there is lack of historical data, estimation of probabilities is difficult. Second, in the observed methods, the description of risks is poor, if the risk knowledge is inadequate, then it limits the predictive power of the approach (Wangen et al., 2018). Third, the approaches rely on properties and a predefined set of criteria, the approaches are top-down and miss the contextual factors that can contribute to complexity and uncertainty. The approaches lack a bottom-up philosophy, trying to connect to factors and contexts that reflect true uncertainties and risk knowledge. Finally, the more important limitation of the methods observed is the lack of importance given to human motivational elements and judgments in the context of cyber risks (Green et al., 2022; Wangen et al., 2018).

In our study of cyber risks in the context of online retailing SMEs, the use of the abovementioned approaches has drawbacks, first it has been noted that SMEs have poor risk awareness/knowledge, especially in cyber risks (Osborn & Simpson, 2017; Ponsard & Grandclaudon, 2019) and in general higher-order risk management approaches (Gao et al., 2013). Probability-based data and historical data to support the above approaches are difficult to obtain in SME contexts. Small and microbusinesses are usually owner-led and the informal operating environment may not truly capture intentions, judgments, and decision making and their impact on risk assessment (Falkner & Hiebl, 2015). To overcome this difficulty and to develop a holistic picture of the cyber risks of e-tailing SMEs, we examined the literature for cyber risk classification in general and more specifically of SMEs. In their study of e-business firms, Beck et al. (2002) have classified cyber risks along the traditional lines of strategy, operational, legal, and financial domains. The work was conceptual and lacked empirical verification of the classification of risks. Similarly, Scott (2004) has developed a classification scheme for e-business risks. The classification framework is developed along the dimensions of policy, strategy, and operations. In developing the classification framework, Scott (2004) has identified 16 different e-business risks and has grouped them along the areas of policy, strategy, and operations based on empirical evidence.

A further holistic approach to cyber risk classification was attempted by Grant et al. (2014); they developed a broader risk classification specific to SMEs. Their work involved the development of five major risk themes and 24 individual risk items that explored the different risk elements that SMEs face. Of the developed classification frameworks and their relevance to SMEs, we can notice that only the work done by Grant et al. (2014), has an SME backdrop. The other frameworks and the risks analyzed were not SME-specific nor broad enough to highlight the different cyber risks e-tailing SMEs may face. Adapting the work done by Grant et al. (2014), we propose the five exhaustive risk themes and individual sub-risks as a foundation for the analysis of the SWARA-BWM integrated approach. The adapted risk themes and individual sub-risks are highlighted in Table 2.

Cyber risk assessment via MCDA methods has been considered by scholars previously. Linkov et al. (2006, 2007) presented a comparative assessment of risk via different MCDA methods (Linkov et al., 2006, 2007; Sukumar et al., 2022). Similarly, the application of MCDA methods in assessing risks relevant to contaminated sediment case studies was investigated (Yatsalo et al., 2007). Some years later, the integrated top-down and bottom-up approaches to risk standards were analyzed (Linkov et al., 2014). More recently, various applications of MCDA approaches in risk assessment in the area of engineering and environment were presented (Linkov et al., 2020; Sadraei et al., 2022). As it is obvious from previous literature, employing MCDA approaches; especially, the integrated, hybrid, and multilayer versions in risk assessment has been frequently considered by scholars (Ali et al., 2019). As a result, in this manuscript, the authors have designed an integrated MCDA approach to assess cyber risks in the specific case of e-tailing SMEs.

3 | HYBRID SWARA-BWM APPROACH FOR CYBER RISK ASSESSMENT

Numerous risk analysis methods are being employed in setting priorities for protecting the infrastructures of SMEs, large-scale companies, etc. One of the most popular ones is the “Risk = Threat × Vulnerability × Consequence (R = TVC)” approach (Linacre et al., 2005). In 2008, some potential restrictions and limitations of this method were presented (Cox, 2008). As a consequence, it was analyzed that the R = TVC approach is not strong enough to guide resource allocations to effectively optimize risk reductions. Even 4 years later in 2012, the same scholar modified the classical version to overcome the previous limitations in risk reduction (Cox, 2012). Nonetheless, the efficiency and effectiveness of resource allocations still were not entirely resolved. In this regard, the integrated MCDM methodology recommended in this article is trying to determine and assess the importance of each cyber risk via an optimal nonlinear mathematical model. In this way, the resource allocation for each identified cyber risk of e-tailing SMEs is going to be based on an effective, efficient, and optimal approach toward risk reduction.

MCDA is a set of methods used to support and facilitate complicated decision-making dilemmas and challenges within organizations (Rezaei et al., 2018). These approaches are generally classified into two major streams known as multiattribute decision-making (MADM) methods and multiobjective decision-making (MODM) methods (Mokhtarzadeh et al., 2018; Taghavifard et al., 2018). As in this article, the main objective is to assess and prioritize cyber risks (as criteria) from the perspective of e-tailing SMEs, the MADM era is relevant and multi-objective models and methods are not required. Moreover, MADM methods are often applied to support managers and researchers through three main objectives including (i) measuring the importance or weights of criteria, factors, indicators, risks, etc. (ii) measuring the score of alternatives or options and ranking or sorting them considering multiple criteria, (iii) analyzing the relationship amongst the factors, criteria, risks, etc. to provide the causal

TABLE 2 Cyber risks and their explanations

Risk	Codes	Description
Security	SR_1	Risk of attack from viruses, worms, malicious software
	SR_2	Risk of credit/debit card fraud and misuse
	SR_3	Risk of denial of service attacks
	SR_4	Risk of identity theft
	SR_5	Risk of attack from hackers or crackers
	SR_6	Risk of fraudulent emails (Phishing and social engineering)
	SR_7	Risk of illegal capture of data in online transit
Dependency	DR_1	Risk of dependency on website developers, payment systems
	DR_2	Risk of dependency on suppliers and partners
	DR_3	Risk of a lack of technical knowledge
	DR_4	Risk of technologies becoming legacy systems and obsolete
	DR_5	Risk of company's technologies failing from technical support
	DR_6	Risk of poor leadership
	DR_7	Risk of increase in competition
Employee	ER_1	Risk of reputation damage due to poor customer satisfaction and fulfilment
	ER_2	Risk of the security-related incident due to inadequate training
	ER_3	Risk of damage to information assets by current employees
	ER_4	Risk of damage to information assets by former employees
Strategic	TR_1	Risk of not having appropriate financial models/measures
	TR_2	Risk of not following adequate standards, policies, and procedures
	TR_3	Risk of not having trust promoting symbols and signs on the website
Legal	LR_1	Risk of intellectual property violations
	LR_2	Risk of noncompliance to local and foreign laws
	LR_3	Risk of unfamiliar local and international tax regimes

relationship and a basic conceptual model (Jafari-Sadeghi et al., 2022).

Since in this research, the authors are measuring the importance or the weights of the cyber risks from the perspective of e-tailing SMEs, and the methods relevant to the first objective are required. These methods are basically classified into two major categories including the data-oriented methods and the expert-based approaches; nonetheless, hybrid methods also could be used in mixed circumstances (Amoozad Mahdiraji et al., 2020). If the criteria are qualitative, difficult to measure, and the required data are not available, then expert-based methods are applicable (Mahdiraji et al., 2021). Expert-based methods focus on a limited number of qualified experts instead of a high number of respondents (i.e., between 3 and 15). These experts share their experience and intuition via specific questionnaires and linguistic variables (Razavi Hajiagha et al., 2018). As real-world data regarding all identified cyber risks are not available, measuring them is difficult and some of them are qualitative; hence, the authors have employed these methods. There are many methods in this regard (Mahdiraji et al., 2019). Considering the advantages of BWM compared to the other methods discussed in the literature by Rezaei (2015), this method has been employed to overcome the obstacles and limitations of BWM, the authors have designed an integrated version of SWARA-BWM in this manuscript.

BWM is a method to extract the weights or importance of criteria, risks, threats, etc. that was presented by Rezaei (2015). Known as the most cited article in the area of the weighting method since 2010. Some different approaches to BWM have been already introduced in deterministic and uncertain situations (Mahdiraji et al., 2019, 2020).

BWM has been employed in many types of research in recent years. The integrations and applications of this method have been analyzed and presented (Mi et al., 2019).

In this article, the nonlinear approach of BWM (Rezaei, 2015) integrated with SWARA is employed and described as follows:

1. Determine the set of risks known as $(\{C_1.C_2.\dots.C_n\})$.
2. Define the best (most important) and worst (least important) risks by experts' opinions. The most critical risk is noted by (B) and the worst is shown by (W). In this research, a modification of this step is performed. To identify B and W in this research, a SWARA is proposed. To this matter, based on the final rank obtained from the SWARA method the best and worst risks are chosen as the following steps.

TABLE 3 Sample questionnaire for the best against other criteria

Security risks							
Best compare to others	**Risk of denial of service attacks**	**Risk of attack from hackers or crackers**	**Risk of debit/credit card fraud and misuse**	**Risk of identity theft**	**Risk of fraudulent emails (phishing and social engineering)**	**Risk of Illegal capture of data in online transit**	**Risk of attack from viruses, worms, malicious software**
Risk of attack from viruses, worms, malicious software						▨	1

Fill in the blanks with a number from 1 to 9. The gray box indicates a comparison of the best (most important risk) with the worst (least important risk); thus, should have the highest number. Moreover, the value of 1 is used for comparing the best with the best.

2.1. Sort the identified risks based on the mean point of the questionnaire used in the survey. Then, calculate the set point of each risk known S_j as follows based on Keršulienė et al. (2010). Note that, P_j illustrates the mean point of each risk based on the survey.

$$S_j = \begin{cases} P_j, \ j = 1 \\ \left|P_j - P_{j-1}\right|, \ j > 1 \end{cases} \tag{1}$$

2.2. Obtain the primary coefficient for each cyber risk K_j as follows:

$$K_j = \begin{cases} 1, \ j = 1 \\ S_j + 1, \ j > 1 \end{cases} \tag{2}$$

2.3. Calculate the initial weight known as Q_j as follows:

$$Q_j = \begin{cases} 1, \ j = 1 \\ \frac{Q_{j-1}}{K_j}, \ j > 1 \end{cases} \tag{3}$$

2.4. Calculate the normalized weights for each cyber risk as follows. Afterwards, opt for the highest W_j as the best and the lowest as the worst for the BWM method as an input.

$$W_j = \frac{Q_j}{\sum_{j=1}^{n} Q_j}, \text{ for all } j \tag{4}$$

3. Determine the preference of the most critical cyber risk over other risks by a number between 1 and 9 known as ($A_B = (A_{b1}, A_{b1}, \ldots, A_{bn})$) by each expert through a designed questionnaire as shown in Table 3 (sample).
4. Determine the preference of all risks over the least critical cyber risk by a number between 1 and 9 known as ($A_W = (A_{1w}, A_{2w}, \ldots, A_{nw})$) by each expert through a designed questionnaire as presented in Table 4 (sample).
5. The optimal weights are emanated by solving the nonlinear (NLP) model of (5) by LINGO or GAMS software known as ($W_j^k = \{W_1^k, W_2^k, \ldots, W_n^k\}$) for expert k_{th}.

$$\min \xi$$

st:

$$\left|\frac{W_B}{W_j} - A_{bj}\right| \le \xi; \text{ for all } j$$

$$\left|A_{jw} - \frac{W_j}{W_W}\right| \le \xi; \text{ for all } j$$

$$\sum W_j = 1,$$

$$W_j \ge 0, \text{ for all } j \tag{5}$$

6. The compatibility rate of comparisons for each expert is resulted by Equation (6) where CR^k is the consistency rate of the kth expert. In this research, CR less than 0.2 is acceptable.

$$CR^k = \frac{\xi^*}{CI}, \text{ for all } k \tag{6}$$

Note that CI determines the consistency index adopted from Table 3 as highlighted in Table 5.

The hybrid SWARA-BWM approach has been illustrated in Figure 1.

4 | CASE STUDY AND RESULTS

Using the risks and sub-risks listed in Table 1, a survey was conducted among UK SME e-tailers asking them to rank the risks according to their importance. The questionnaire was sent to 750 UK-based small e-tailers, with 124 responding to the survey (16.5% response rate). The firms were randomly selected from the FAME database and the selection criteria included the following:

TABLE 4 Sample questionnaire for other criteria on the worst

	Comparing other risks with the worst	Risk of illegal capture of data in online transit
Security Risks	Risk of denial of service attacks	
	Risk of attack from hackers or crackers	
	Risk of debit/credit card fraud and misuse	
	Risk of identity theft	
	Risk of fraudulent emails (phishing and social engineering)	
	Risk of illegal capture of data in online transit	1
	Risk of attack from viruses, worms, malicious software	

Fill in the blanks with a number from 1 to 9. The gray box indicates a comparison of the best (most important risk) with the worst (least important risk); thus, should have the highest number. Moreover, the value 1 is used for comparing the worst with the worst.

TABLE 5 Consistency index (Rezaei, 2015)

a_{BW}	1	2	3	4	5	6	7	8	9
Consistency Index	0	0.44	1	1.63	2.3	3.00	3.73	4.47	5.23

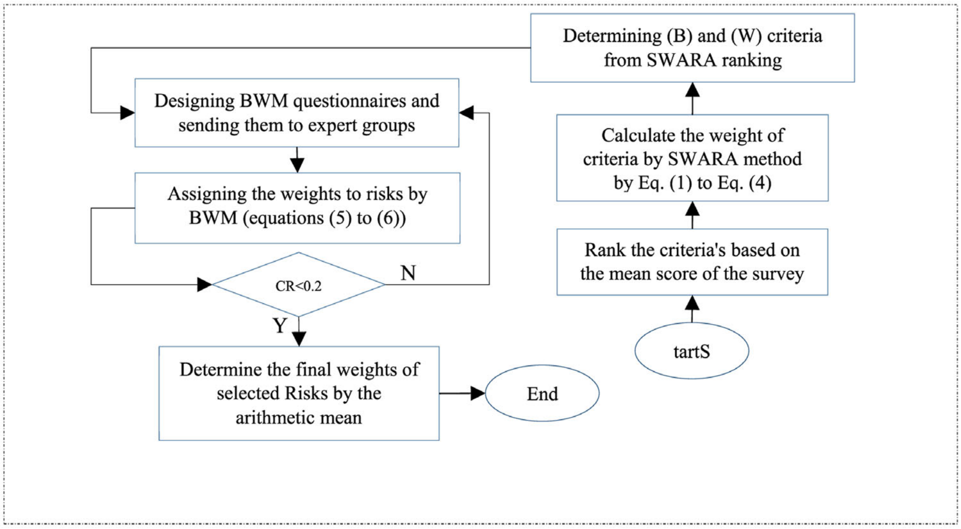
Determining (B) and (W) criteria from SWARA ranking
Designing BWM questionnaires and sending them to expert groups
Calculate the weight of criteria by SWARA method by Eq. (1) to Eq. (4)
Assigning the weights to risks by BWM (equations (5) to (6))
Rank the criteria's based on the mean score of the survey
CR<0.2
N
Y
tartS
Determine the final weights of selected Risks by the arithmetic mean
End

FIGURE 1 The proposed approach

- The e-tailers fitted with the UK definition of SMEs.
- The e-tailers were based in the United Kingdom and had no subsidiaries or were part of subsidiaries.
- The business was selling a product/service through its website.
- Has been in operation for more than 3 years.

The initial parts of the questionnaire focused on addressing the demographic and respondent details of the SME, while the second part of the questionnaire focused on collecting data on the risk perception of the identified risks. A seven-point Likert scale (1 being extremely high risk to 7 No risk at all) was used to collect data on risk perception and the mean scores of the respondents to the identified risks and sub-risks are given in Table 6.

By implementing Equations, (1)–(4), the results of the SWARA method are presented in Table 7. The initial importance of each risk is derived from the mean rating in Table 6.

Based on Table 7, the most important and the least important risks in each category are determined using the SWARA method. As a result, the B (best) and W (worst) of each category are calculated. To measure the importance of each risk using BWM, data were also collected from a panel of experts. The experts were asked to participate and fill out the relevant questionnaires based on the risk identified in Table 2. The

TABLE 6 Mean rating of the risks

Risk	Codes	Description	Mean rating
Security	SR_1	Risk of attack from viruses, worms, malicious software	2.39
	SR_2	Risk of credit/debit card fraud and misuse	2.84
	SR_3	Risk of denial of service attacks	2.99
	SR_4	Risk of identity theft	3.01
	SR_5	Risk of attack from hackers or crackers	3.13
	SR_6	Risk of fraudulent emails (phishing and social engineering)	3.18
	SR_7	Risk of illegal capture of data in online transit	3.29
Dependency	DR_1	Risk of dependency on website developers, payment systems	3.89
	DR_2	Risk of dependency on suppliers and partners	3.92
	DR_3	Risk of a lack of technical knowledge	4.34
	DR_4	Risk of technologies becoming legacy systems and obsolete	4.52
	DR_5	Risk of company's technologies failing from technical support	4.56
	DR_6	Risk of poor leadership	4.73
	DR_7	Risk of increase in competition	5.42
Employee	ER_1	Risk of reputation damage due to poor customer satisfaction and fulfilment	3.60
	ER_2	Risk of the security-related incident due to inadequate training	5.05
	ER_3	Risk of damage to information assets by current employees	5.28
	ER_4	Risk of damage to information assets by former employees	5.30
Strategic	TR_1	Risk of not having appropriate financial models	4.15
	TR_2	Risk of not following adequate standards, policies and procedures	4.46
	TR_3	Risk of not having trust promoting symbols and signs on the website	3.78
Legal	LR_1	Risk of intellectual property violations	4.7
	LR_2	Risk of non-compliance to local and foreign laws	5.11
	LR_3	Risk of unfamiliar local and international tax regimes	5.45

expert panel for this study was composed of individuals who have considerable knowledge of cybersecurity management. Table 8 explains the knowledge base and qualifications of the experts.

By employing six experts' opinions and based upon questionnaire samples presented in Tables 3 and 4; besides using the model (4) and LINGO software, the weight of each risk based upon expert opinion is presented in Table 9.

Calculating the consistency ratio for the responses from the experts, we have Table 10. As it is clear, all experts have provided responses and comparisons with reliable and acceptable consistency (less than 0.2).

The final weights of each risk as calculated by the hybrid SWARA-BWM method are given in Table 11.

5 | DISCUSSION AND IMPLICATIONS

This research article's main objectives were to consolidate the literature on cyber risks in the context of e-tailing SMEs. Cyber risks have the potential to affect both SMEs and large organizations; while the risks, their assessment and mitigating strategies have been studied in-depth in the context of large firms, less focus was paid to the cyber risks, and their assessment in the context of small and medium-sized. This research explores this less focused area, it identified 28 cyber-oriented risks in the context of e-tailing SMEs and has demonstrated that the combined approach of BWM and SWARA can be used to integrate empirical data and expert knowledge for assigning risk scores based on criteria.

TABLE 7 Weight of risks by step-wise weight assessment ratio analysis (SWARA)

		S_j	K‘	Q_j	W_j
Security	Risk of attack from viruses, worms, malicious software (B)	4.610	4.610	1.000	0.230
	Risk of credit/debit card fraud and misuse	0.450	1.450	0.690	0.158
	Risk of denial of service attacks	0.150	1.150	0.600	0.138
	Risk of identity theft	0.020	1.020	0.588	0.135
	Risk of attack from hackers or crackers	0.120	1.120	0.525	0.121
	Risk of fraudulent emails (phishing and social engineering)	0.050	1.050	0.500	0.115
	Risk of illegal capture of data in online transit (W)	0.110	1.110	0.450	0.103
Dependency	Risk of dependency on website developers, payment systems (B) hardware vendors	3.110	3.110	1.000	0.220
	Risk of dependency on suppliers and partners	0.030	1.030	0.971	0.213
	Risk of a lack of technical knowledge	0.420	1.420	0.684	0.150
	Risk of technologies becoming legacy systems and obsolete obsolete	0.180	1.180	0.579	0.127
	Risk of company's technologies failing from technical support	0.040	1.040	0.557	0.122
	Risk of poor leadership	0.170	1.170	0.476	0.105
	Risk of increase in competition (W)	0.690	1.690	0.282	0.062
Employee	Risk of reputation damage due to poor customer satisfaction (B)	3.400	3.400	1.000	0.484
	Risk of security-related incident due to inadequate training	1.450	2.450	0.408	0.198
	Risk of damage to information assets by current employees	0.230	1.230	0.332	0.161
	Risk of damage to information assets by former employees (W)	0.020	1.020	0.325	0.158
Strategic	Risk of not having trust promoting symbols and signs on the website (B)	3.220	3.220	1.000	0.437
	Risk of not having appropriate financial models/measures	0.370	1.370	0.730	0.319
	Risk of not having policies and procedures (W)	0.310	1.310	0.557	0.244
Legal	Risk of intellectual property violations (B)	2.300	2.300	1.000	0.447
	Risk of noncompliance to local and foreign laws	0.410	1.410	0.709	0.317
	Risk of unfamiliar local and international tax regimes (W)	0.340	1.340	0.529	0.236

Table 11 denotes, the final ranking of the risk based on the hybrid SWARA-BWM method. In the importance of risks, literature has noted that SMEs give more importance to security risks (Brass & Sowell, 2021), but our ranking notes that SMEs are more concerned with the risks associated with legal, strategic, and employee domains when compared to security (Zabalawi et al., 2021). The highest weighting was achieved by intellectual property violations (0.597), followed by trust symbols on the transacting websites (0.577), and reputation damage (0.487). Security and dependency risks are often highlighted as major areas of concern to SMEs (Jia et al., 2021) who do not score highly in our method. The risk scenarios associated with security and dependency, that is, identity thefts, denial of service attacks, technical knowledge, etc., were not considered important in comparison with some of the risk scenarios in employee and strategy-related domains. One possible explanation for this could be that SMEs are gaining confidence when it comes to dealing with security challenges, there is a fundamental level of awareness that is helping them to identify and deal with security threats. The increased adoption of ICT by SMEs and efforts by agencies to promote cyber security awareness may contribute to a lower rating of these risks (Stjepic et al., 2021). The weighting also points out that the effect of technology influence may be weaning and the core business values of providing good customer service and being trustworthy (Zhu, 2021) are major areas of concern and drivers for success in e-tailing SMEs.

The lack of importance to security and dependency-related risk is also noted in the variation present in expert ratings. When it came to experts, the variation in opinion decreases with the importance associated with risks. Typically, in security and dependency risk themes, the variation seen is higher in comparison with the employee, strategic, and legal risk areas (Figure 2).

Furthermore, when it comes to consistency, the same pattern emerges, the experts are more consistent when it comes to strategic, legal, and employee risks and less so in the context of security and dependency risk themes (Figure 3). Experts are more consistent in their decision while evaluating strategic, legal, and employee risks. However, when it comes to dependency and security risks, their opinion varies leading to low consistency.

The existing literature on SME cyber risk management is sparse. Few studies that have been undertaken have focused on risk classification (Dewitt et al., 2022; Grant et al, 2014)

TABLE 8 Experts' information

Expert field	Experience and qualifications
Industry	Work as a chief information officer with a big online retailer. In the past, he has worked with companies like Amazon and IBM. Has more than 15 years of information security experience and has professional qualifications including Certified Information Systems Auditor.
Academic	This expert (a professor) has been researching small businesses for more than 20 years. Has extensive publications and is an expert in the study of small businesses. The expert is the editor of a highly ranked journal associated with small business and entrepreneurship
Industry	Head of creative village specializing in arts and crafts. The village has nearly 30 businesses and for the past 20 years, the expert has been supporting small businesses to set shop and helping them to grow their business
Government	An executive at a Growth Hub. Has more than 12 years of experience in supporting tech-based start-ups and leads the government initiative to promote more technology-based startups and accelerate high-growth firms.
Technology	The expert leads one of the most prominent online fraud detecting firms in the country. The expert specializes in phishing and social engineering attacks and currently, her firm assesses the vulnerability of large and medium-sized companies to phishing and employee-based threats. Has been in this field since 2002.
Legal	This expert specializes in online trading and has been advising large and small firms on the legal and IP aspects of selling online. Has more than 10 year's online legal experience.

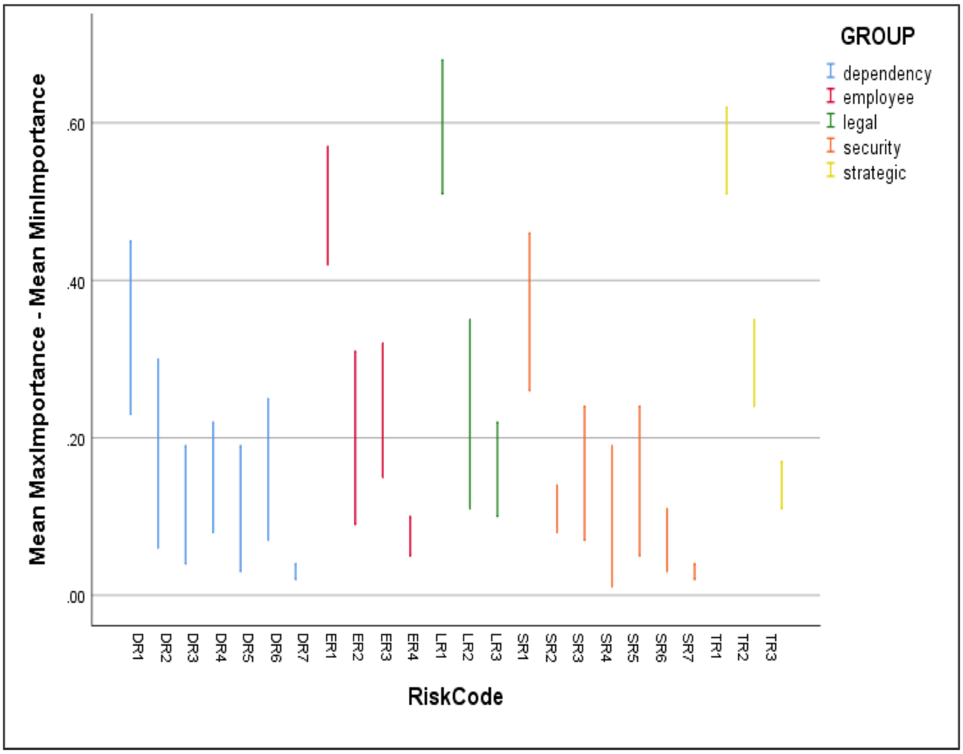

FIGURE 2 Experts' risk rating variation

and others on success factors (Ključnikov et al, 2019). Our work extends the current work done in risk classification in the context of SMEs. It extends the work done by Grant et al (2014) and goes further in the assessment of the threats by using an MCDA approach. The work by Grant et al (2014) was built on theories of risk perception, that is, psychometric paradigm and social amplification of risk. This work contributes toward our understanding of cyber threat perception and lays the foundation for future work in cyber threat perception and how it influences mitigating strategies.

Our findings provide an alternative approach to cyber risk assessment using MCDA. The MCDA approach moves away from probability-based analyses and provides the basis for the integration and synthesis of data from different sources to provide a ranking that can help in informed and evidence-based decision making. The actual data for this work were collected from surveys conducted with UK-based e-tailing SMEs and expert opinions. Though the results are developed in the context of e-tailing SMEs, it is limited by the range of risk identified, Black Swan events

TABLE 9 Weight of risk by each expert

	Risk	Weights by experts' opinion					
		E1	**E2**	**E3**	**E4**	**E5**	**E6**
Security	Risk of attack from viruses, worms, malicious software	0.26	0.36	0.46	0.39	0.37	0.34
	Risk of credit/debit card fraud and misuse	0.14	0.1	0.11	0.08	0.08	0.12
	Risk of denial of service attacks	0.14	0.08	0.07	0.24	0.14	0.15
	Risk of identity theft	0.19	0.15	0.011	0.1	0.1	0.1
	Risk of attack from hackers and crackers	0.21	0.22	0.1	0.05	0.24	0.21
	Risk of fraudulent emails (phishing and social engineering)	0.04	0.05	0.11	0.1	0.03	0.05
	Risk of illegal capture of data in online transit	0.02	0.03	0.04	0.03	0.03	0.03
Dependency	Risk of dependency on website developers, payment systems	0.230	0.370	0.340	0.450	0.390	0.420
	Risk of dependency on suppliers and partners	0.090	0.060	0.080	0.110	0.300	0.130
	Risk of lack of technical knowledge	0.190	0.050	0.040	0.080	0.050	0.100
	Risk of technologies becoming legacy systems and obsolete	0.220	0.110	0.080	0.120	0.110	0.120
	Risk of company's technologies failing from technical support	0.190	0.170	0.180	0.070	0.030	0.100
	Risk of poor leadership	0.070	0.210	0.250	0.120	0.080	0.100
	Risk of increase in competition	0.020	0.030	0.030	0.040	0.030	0.030
Employee	Risk of reputation damage due to poor customer satisfaction and fulfilment	0.42	0.42	0.45	0.54	0.57	0.52
	Risk of security-related incident due to inadequate training	0.31	0.31	0.22	0.09	0.22	0.27
	Risk of damage to information assets by current employees	0.18	0.18	0.25	0.32	0.16	0.15
	Risk of damage to information assets by former employees	0.1	0.1	0.09	0.05	0.06	0.06
Strategic	Risk of not having trust promoting symbols and signs on the website	0.510	0.530	0.580	0.530	0.570	0.620
	Risk of not having appropriate financial models	0.350	0.300	0.310	0.300	0.290	0.240
	Risk of not following adequate standards, policies, and procedures	0.140	0.170	0.110	0.170	0.140	0.140
Legal	Risk of intellectual property violations	0.51	0.53	0.51	0.68	0.68	0.67
	Risk of noncompliance to local and foreign laws	0.35	0.3	0.35	0.22	0.22	0.11
	Risk of unfamiliar local and international tax regimes	0.14	0.17	0.14	0.1	0.1	0.22

TABLE 10 Expert's consistency ratio (CR)

	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5	Expert 6
Security risk	0.10	0.08	0.19	0.17	0.13	0.09
Dependency risk	0.12	0.13	0.19	0.17	0.17	0.17
Employee risk	0.03	0.03	0.06	0.11	0.02	0.03
Strategic risk	0.03	0.01	0.06	0.01	0.04	0.02
Legal risk	0.03	0.02	0.03	0.01	0.01	0.01

TABLE 11 Final weights of each risk by SWARA-BWM

	Risks	Final weights
Security	Risk of attack from viruses, worms, malicious software	0.363
	Risk of credit/debit card fraud and misuse	0.105
	Risk of denial of service attacks (DoS)	0.137
	Risk of identity theft	0.109
	Risk of attack from hackers and crackers	0.172
	Risk of fraudulent emails (phishing and social engineering)	0.063
	Risk of illegal capture of data in online transit	0.030
Dependency	Risk of dependency on website developers, payment systems	0.367
	Risk of dependency on suppliers and partners	0.128
	Risk of lack of technical knowledge	0.085
	Risk of technologies becoming legacy systems and obsolete	0.127
	Risk of company's technologies failing from technical support	0.123
	Risk of poor leadership	0.138
	Risk of increase in competition	0.030
Employee	Risk of reputation damage due to poor customer satisfaction and fulfillment	0.487
	Risk of the security-related incident due to inadequate training	0.237
	Risk of damage to information assets by current employees	0.207
	Risk of damage to information assets by former employees	0.077
Strategic	Risk of not having trust promoting symbols and signs on the website	0.557
	Risk of not having appropriate financial models	0.298
	Risk of not following adequate standards, policies, and procedures	0.145
Legal	Risk of intellectual property violations	0.597
	Risk of noncompliance to local and foreign laws	0.258
	Risk of unfamiliar local and international tax regimes	0.145

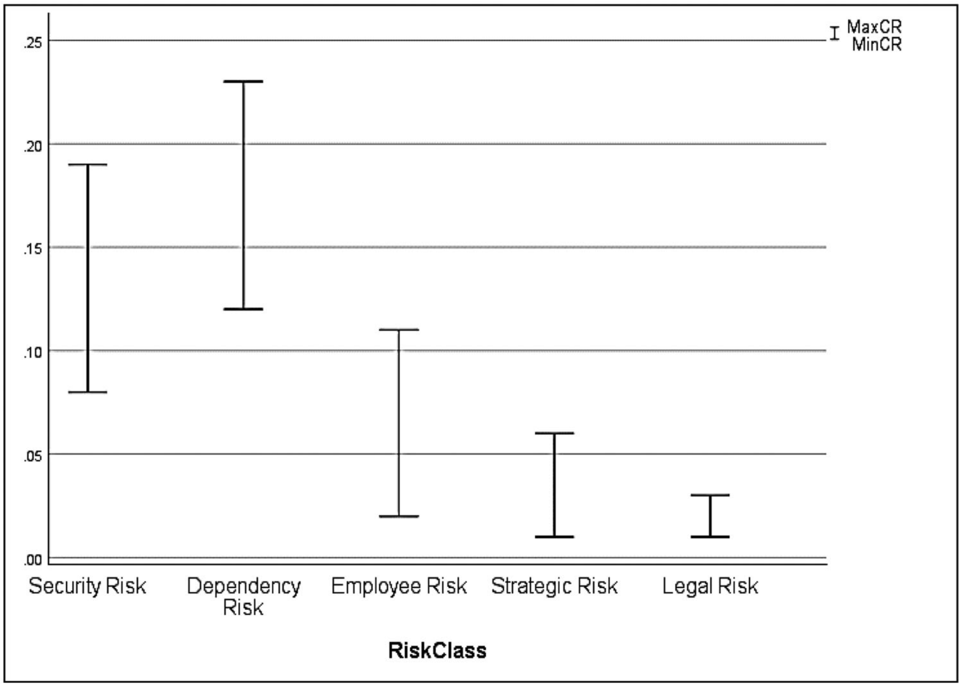

FIGURE 3 Experts' consistency ratio variation

especially can change the perception, uncertainties, and risk assessment.

The interconnected ICT systems and their extension to mobile platforms raise the complexity levels and probability of Black Swan events happening. The results obtained in the study are also based on weights; this has drawbacks as it depends on expert opinions. From a practical perspective, the risk ranking approach elicited here can be used in practice and is flexible enough to accommodate changing risk scenarios. The combined approach can be used by owners/managers of SMEs to plan mitigation measures or as a source for gathering risk knowledge and further information. Given the nature of cyber risks and the significant uncertainties associated with their threats and consequences, the above case study is an illustrative example of how the combination of BWM and SWARA, an MCDA approach allows for the amalgamation of data from different sources to make informed and validated risk management decision. Given the inclusion of expert opinion, the approach is flexible, that is, it can be used to assess cyber risks in other sectors and industries. Thus, widening its practical contribution beyond SMEs/retail industries. From a policy perspective, when it comes to SMEs, the focus from agencies and other stakeholders has mainly been on creating awareness of cyber threats. Risk mitigation strategies are often considered expensive and are not designed specifically in the context of SMEs or customized to their needs. This research has shown that cyber threat assessment can be designed for SMEs and future policy decisions need to take into account SMEs' education on systematic risk threat assessment. Rather than awareness sessions, the policy could be oriented toward risk assessment in the context of cyber threats for SMEs.

6 | CONCLUSION

The BWM method was developed in 2015 and has been widely used for evaluating in interdisciplinary areas such as architecture (e.g., Mahdiraji et al., 2018), healthcare (e.g., Karimi et al., 2020; Liao et al., 2019), transportation (e.g., Munim et al., 2020; Omrani et al., 2020), education (e.g., Ishizaka & Resce, 2020), and services and operations (e.g., Chen et al., 2020). This article is the first to implement this popular method in evaluating cyber risks. Previous relevant research focused on using only statistical-based methods to evaluate cyber risks, however, recently the application of decision-making methods in risk assessment is also noted (Ganin et al., 2020).

Since 2015, much technical development in BWM has been in exploring scheduling and classification in various contexts (Mi et al., 2019). One of the main challenges in using the BWM approach is the process of determining the most important (best) and least important (worst) criteria. In all the previous work, this was done with the help of experts or individuals, in this research we have deviated from this approach to develop a more robust mechanism to determine criteria. We have used SWARA as the principal method in determining the most and least important sub-criteria in each risk category. The data for SWARA come from real-world SMEs, rather than just depending on expert opinions. Individually, each method has its deficiencies, for example, in BWM, it is the problem of determining the best and worst criteria whereas, in SWARA, it is the nonuse of consistency ratios and weights not emanating from optimization approaches. These issues are solved by using a hybrid approach, where the strengths of each method complement one another and negate the deficiencies. The multistage decision-making approach BWM-SWARA addresses limitations regarding each method if used separately.

This study's focus was on the cyber risk assessment of e-tailing SMEs. By using multidecision criteria analysis, this work developed a risk classification framework specific to online retailing SMEs. The current methods in risk assessment are highly skewed toward the use of probabilities, this poses challenges in environments where the complexity makes it hard to determine realistic probabilities or scenarios where the absence of historical data weakens the predictive power of the risk models developed. In practice, probabilistic models are complex and in environments such as SMEs, they are difficult to develop and use. Especially, SME characteristics such as the informal working mechanisms, duality of roles (owner/manager), and absence of procedures and controls can make it difficult to apply probability-based models. There are calls for alternative approaches in cybersecurity risk management, specifically, the use of competitive methods. This work precisely addresses this call, by using an integrated approach of BWM and SWARA, it can develop a risk ranking specific to e-tailing SMEs that can help decisionmakers to prioritize and better manage risk. In unknown scenarios, this integrated approach provides a route to analyzing risk.

From the decision-making perspective, limitations are recognized. First of all, the methods used in this research are deterministic approaches with crisp numbers in decision making. However, considering the current uncertainty and changing environment, it is suggested to implement uncertain approaches in this regard. Classical uncertainty methods such as fuzzy sets and gray systems alongside modern uncertain approaches including interval fuzzy sets (IFs), hesitant fuzzy sets (HFs), hesitant fuzzy linguistic term sets (HFLTs), and interval-valued intuitionistic fuzzy sets (IVIFs) are recommended. Furthermore, the data gathered in this research are cross-functional, thus, the methods used are static decision-making methods. Nevertheless, dynamic decision-making methods including stratified decisions making are useable to assess the effect of time on the importance of cyber risks. Eventually, the combination of the methods used in this research is chosen by the authors based on their possibility and popularity. However, there are other evaluation methods to determine the importance of cyber risks. Hybrid approaches from other methods including FARE (Factor Relationship), pairwise comparison, LINMAP (Linear Programming Technique for Multidimensional Analysis of Preference), and SECA (simultaneous evaluation of criteria and alternatives) could also be investigated in future studies.

ACKNOWLEDGMENTS

The authors would like to thank the editors and anonymous reviewers for their insightful comments that significantly improved the manuscript. We disclose any funding or other competing interests.

ORCID

Vahid Jafari-Sadeghi https://orcid.org/0000-0003-3083-6119

REFERENCES

Alberts, C. J., & Dorofee, A. J. (2002). *Managing information security risks-The OCTAVE approach*. (p. 471). Pearson Education.

Ali, Y., Awan, M. A., Bilal, M., Khan, J., Petrillo, A., & Khan, A. A. (2019). Risk assessment of China-Pakistan fiber optic project (CPFOP) in the light of multi-criteria decision making (MCDM). *Advanced Engineering Informatics*, *40*, 36–45.

Amoozad Mahdiraji, H., Hafeez, K., & Razavi Hajiagha, S. H. (2020). Business process transformation in the financial market: A hybrid BPM-ELECTRE TRI for redesigning a securities company in the Iranian stock market. *Knowledge and Process Management*, *27*(3), 211–224.

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). How does cyber crime affect firms? The effect of information security breaches on stock returns. *CEUR Workshop Proceedings*, *1816*(2015), 175–193.

Asgary, A., Ozdemir, A. I., & Özyürek, H. (2020). Small and medium enterprises and global risks: Evidence from manufacturing SMEs in Turkey. *International Journal of Disaster Risk Science*, *11*(1), 59–73. https://doi.org/10.1007/s13753-020-00247-0

Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, *3*(2), 258–283. https://doi.org/10.1080/23738871.2018.1520271

Baggott, S. S., & Santos, J. R. (2020). A risk analysis framework for cyber security and critical infrastructure protection of the U.S. electric power grid. *Risk Analysis*, *40*(9), 1744–1761. https://doi.org/10.1111/risa.13511

Beck, M., Drennan, L., & Higgins, A. (2002). *Managing e-risk*. Association of British Insurers.

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Berger, H., & Jones, A. (2016). Cyber security & ethical hacking for SMEs. Proceedings of the 11th International Knowledge Management in Organizations Conference on The Changing Face of Knowledge Management Impacting Society. pp. 1–6. https://doi.org/10.1145/2925995.2926016

Better Business Bureau. (2017). State of cybersecurity among small businesses in North America. Council of Better Business Bureaus.https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360–376. https://doi.org/10.1108/MAJ-02-2018-1804

Brass, I., & Sowell, J. H. (2021). Adaptive governance for the internet of things: Coping with emerging security risks. *Regulation & Governance*, *15*(4), 1092–1110.

Brunner, M., Mussmann, A., & Breu, R. (2018). Introduction of a tool-based continuous information security management system: An exploratory case study. Proceedings - 2018 IEEE 18th International Conference on Software Quality, Reliability, and Security Companion, QRS-C 2018, pp. 483–490. IEEE. https://doi.org/10.1109/QRS-C.2018.00088

Burggraf, P., Dannapfel, M., Bertling, M., & Xu, T. (2018). Return on CPS (RoCPS): An evaluation model to assess the cost effectiveness of cyber-physical systems for small and medium-sized enterprises. PICMET 2018 - Portland International Conference on Management of Engineering and Technology: Managing Technological Entrepreneurship: The Engine for Economic Growth, Proceedings, October, pp. 1–9. IEEE. https://doi.org/10.23919/PICMET.2018.8481980

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2021). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), 1643–1669. https://doi.org/10.1111/risa.13687

Calabrese, R., Andreeva, G., & Ansell, J. (2019). "Birds of a feather" fail together: Exploring the nature of dependency in SME Defaults. *Risk Analysis*, *39*(1), 71–84. https://doi.org/10.1111/risa.12862

Chatterjee, D. (2019). Should executives go to jail for cybersecurity breaches? *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 1–3.

Chen, Z., Ming, X., Zhou, T., Chang, Y., & Sun, Z. (2020). A hybrid framework integrating rough-fuzzy best-worst method to identify and evaluate user activity-oriented service requirements for a smart product-service system. *Journal of Cleaner Production*, *253*, 119954. https://doi.org/10.1016/j.jclepro.2020.119954

Cox Jr, L. A. (2008). Some limitations of "risk = threat× vulnerability× consequence" for risk analysis of terrorist attacks. *Risk Analysis: An International Journal*, *28*(6), 1749–1761.

Cox Jr, L. A. (2012). Evaluating and improving risk formulas for allocating limited budgets to expensive risk-reduction opportunities. *Risk Analysis: An International Journal*, *32*(7), 1244–1252.

Dallasega, P., Rauch, E., & Linder, C. (2018). Industry 4.0 as an enabler of proximity for construction supply chains: A systematic literature review. *Computers in Industry*, *99*, 205–225. https://doi.org/10.1016/j.compind.2018.03.039

Department for Business Energy and Industrial Strategy. (2019). Business population estimates for the UK and the Regions 2019. Author.

Dewitt, S., Jafari-Sadeghi, V., Sukumar, A., Aruvanhalli Nagaraju, R., Sadraei, R., & Li, F. (2022). Family dynamics and relationships in female entrepreneurship: An exploratory study. *Journal of Family Business Management*. Advance online publication. https://doi.org/10.1108/JFBM-01-2022-0013

Eilts, D., & Levy, Y. (2018). Towards an empirical assessment of cybersecurity readiness and resilience in small businesses. *KSU Proceedings on Cybersecurity Education, Research and Practice*. https://digitalcommons.kennesaw.edu/ccerp/2018/practice/2

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

Falkner, E. M., & Hiebl, M. R. W. (2015). Risk management in SMEs: a systematic review of available evidence. *Journal of Risk Finance*, *16*(2), 122–144. https://doi.org/10.1108/JRF-06-2014-0079

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management and Computer Security*, *22*(5), 410–430. https://doi.org/10.1108/IMCS-07-2013-0053

Freund, J. (2015). Measuring and managing information risk. In *Measuring and managing information risk*. Butterworth-Heinemann. https://doi.org/10.1016/c2013-0-09966-5

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*(1), 183–199. https://doi.org/10.1111/risa.12891

Gao, S. S., Sung, M. C., & Zhang, J. (2013). Risk management capability building in SMEs: A social capital perspective. *International Small Business Journal*, *31*(6), 677–700. https://doi.org/10.1177/0266242611431094

Grant, K., Edgar, D., Sukumar, A., & Meyer, M. (2014). Risky business: Perceptions of e-business risk by UK small and medium sized enterprises (SMEs). *International Journal of Information Management*, *34*(2), 99–122. https://doi.org/10.1016/j.ijinfomgt.2013.11.001

Gupta, S., Singhal, A., & Kapoor, A. (2017). A literature survey on social engineering attacks: Phishing attack. Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016, pp. 537–540. IEEE. https://doi.org/10.1109/CCAA.2016.7813778

Green, E., Sukumar, A., Jafari-Sadeghi, V., Pandya, K., & Khavarinezhad, S. (2022). Analysis of factors impeding access to finance in internet-enabled crowdfunding: A systematic literature review. *International Journal of Technology Transfer and Commercialisation*, https://doi.org/10.1504/IJTTC.2022.10049235

Hajiagha, S. H. R., Mahdiraji, H. A., & Hashemi, S. S. (2018). Total area based on orthogonal vectors (Taov) as a novel method of a multi-criteria decision aid. *Technological and Economic Development of Economy*, *24*(4), 1679–1694.

Hånell, S. M., Rovira Nordman, E., Tolstoy, D., & Özbek, N. (2019). "It's a new game out there": e-commerce in internationalising retail SMEs. *International Marketing Review*, *37*(3), 515–531. https://doi.org/10.1108/IMR-03-2018-0107

Harsch, A., Idler, S., & Thurner, S. (2014). Assuming a state of compromise: A best practise approach for SMEs on incident response management. Proceedings - 8th International Conference on IT Security Incident Management and IT Forensics, IMF 2014, pp. 76–84. IEEE. https://doi.org/10.1109/IMF.2014.13

Heartfield, R., Loukas, G., & Gan, D. (2016). You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. *IEEE Access*, *4*, 6910–6928. https://doi.org/10.1109/ACCESS.2016.2616285

Henson, R., & Garfield, J. (2016). What attitude changes are needed to cause SMEs to take a strategic approach to information security? *Athens Journal of Business & Economics*, *2*(3), 303–317. https://doi.org/10.30958/ajbe.2-3-5

Henson, R., & Sutcliffe, D. (2013). A model for proactively insuring SMEs in the supply chain against cyber risk. Atiner Conference Paper Series: SME2013-0547. Pp. 1–19.

Hills, M., & Atkinson, L. (2016). Towards cyber-resilient and sustainable SMEs: The case study of added value from a large IT Re-seller. In Hills, M. (Ed.). *Why* cyber security is a socio-technical challenge*: N*ew concepts and practical measures to enhance detectio*n* (pp. 71–80). Nova Science Publishers.

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. *Journal of Risk Finance*, *22*(3/4), 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Ishizaka, A., & Resce, G. (2020). Best-worst PROMETHEE method for evaluating school performance in the OECD's PISA project. *Socio-Economic Planning Sciences*, *73*, 100799. https://doi.org/10.1016/j.seps.2020.100799

Iyamuremye, B., & Shima, H. (2018). Network security testing tools for SMEs (small and medium enterprises). Proceedings of 4th IEEE International Conference on Applied System Innovation 2018, ICASI 2018, pp. 414–417. IEEE. https://doi.org/10.1109/ICASI.2018.8394272

Jafari-Sadeghi, V. (2021). Internationalisation, risk-taking, and export compliance: A comparative study between economically advanced and developing Country. *International Journal of Entrepreneurship and Small Business*, *43*(3), 384–408. https://doi.org/10.1504/IJESB.2021.10039076

Jafari-Sadeghi, V., Mahdiraji, H. A., Devalle, A., & Pellicelli, A. C. (2022). Somebody is hiding something: Disentangling interpersonal level drivers and consequences of knowledge hiding in international entrepreneurial firms. *Journal of Business Research*, *139*, 383–396.

Jafari-Sadeghi, V., Garcia-Perez, A., Candelo, E., & 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*(2021), 100–111. https://doi.org/10.1016/j.jbusres.2020.11.020

Javaid, M. I., & Iqbal, M. M. W. (2017). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). International Conference on Communication Technologies, ComTech 2017, October, pp. 78–90. IEEE. https://doi.org/10.1109/COMTECH.2017.8065754

Jia, Y., Yuan, B., Xing, L., Zhao, D., Zhang, Y., Wang, X., Liu, Y., Zheng, K., Crnjak, P., Zhang, Y., Zou, D., & Jin, H. (2021, November). Who's in control? On security risks of disjointed iot device management channels. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, pp. 1289–1305. Association for Computing Machinery.

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Karimi, H., Sadeghi-Dastaki, M., & Javan, M. (2020). A fully fuzzy best–worst multi attribute decision making method with triangular fuzzy number: A case study of maintenance assessment in the hospitals. *Applied Soft Computing Journal*, *86*, 105882. https://doi.org/10.1016/j.asoc.2019.105882

Kent, C., Tanner, M., & Kabanda, S. (2016). How South African SMEs address cyber security: The case of web server logs and intrusion detection. 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies, EmergiTech 2016, pp. 100–105. IEEE. https://doi.org/10.1109/EmergiTech.2016.7737319

Keršuliene, V., Zavadskas, E. K., & Turskis, Z. (2010). Racionalaus ginčų sprendimo būdo nustatymas taikant naują kriterijų svorių nustatymo metodą, pagrįstą nuosekliu laipsnišku poriniu kriterijų santykinės svarbos lyginimu. *Journal of Business Economics and Management*, *11*(2), 243–258. https://doi.org/10.3846/jbem.2010.12

Kiker, G. A., Bridges, T. S., Varghese, A., Seager, P. T. P., & Linkov, I. (2005). Application of multicriteria decision analysis in environmental decision making. *Integrated Environmental Assessment and Management*, *1*(2), 95–108. https://doi.org/10.1897/IEAM_2004a-015.1

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: Factors of success. *Entrepreneurship and Sustainability Issues*, *6*(4), 2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Kshetri, N. (2018). The economics of cyber-insurance. *IT Professional*, *20*(6), 9–14.

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud and Security*, *2015*(3), 5–7. https://doi.org/10.1016/S1361-3723(15)30017-8

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. (2014). Cybersecurity information sharing: a framework for sustainable information security management in UK SME supply chains. Twenty Second European Conference on Information Systems, 2014, pp. 1–15.

Liao, H., Mi, X., Yu, Q., & Luo, L. (2019). Hospital performance evaluation by a hesitant fuzzy linguistic best worst method with inconsistency repairing. *Journal of Cleaner Production*, *232*, 657–671. https://doi.org/10.1016/j.jclepro.2019.05.308

Linacre, N. A., Koo, B., Rosegrant, M. W., Msangi, S., Falck-Zepeda, J., Gaskell, J., Komen, J., Cohen, M. J., & Birner, R. (2005). Security analysis for agroterrorism: applying the threat, vulnerability, consequence framework to developing countries. EPTD Discussion Paper 138. International Food Policy Research Institute.

Linkov, I., Satterstrom, F. K., Yatsalo, B., Tkachuk, A., Kiker, G. A., Kim, J., Bridges, T. S., Seager, T. P., & Gardner, K. (2007). Comparative assessment of several multi-criteria decision analysis tools for management of contaminated sediments. In Linkov, I., Kiker, G. A., Wenning, R. J. (Eds). *Environmental security in harbors and coastal areas* (pp. 195–215). Springer.

Linkov, I., Satterstrom, F. K., Kiker, G., Batchelor, C., Bridges, T., & Ferguson, E. (2006). From comparative risk assessment to multi-criteria decision analysis and adaptive management: Recent developments and applications. *Environment International*, *32*(8), 1072–1093.

Linkov, I., Anklam, E., Collier, Z., DiMase, D., & Renn, O. (2014). Risk-based standards: Integrating top-down and bottom-up approaches. *Environment, Systems, and Decisions*, *34*, 134–137.

Linkov, I., Moberg, E., Trump, B. D., Yatsalo, B., & Keisler, J. M. (2020). *Multi-criteria decision analysis: Case studies in engineering and the environment*. CRC Press.

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud and Security*, *2020*(2), 14–17. https://doi.org/10.1016/S1361-3723(20)30019-1

Mahdiraji, H. A., Arzaghi, S., Stauskis, G., & Zavadskas, E. K. (2018). A hybrid fuzzy BWM-COPRAS method for analyzing key factors of sustainable architecture. *Sustainability*, *10*(5), 1–26. https://doi.org/10.3390/su10051626

Mahdiraji, H. A., Kazimieras Zavadskas, E., Kazeminia, A., & Abbasi Kamardi, A. (2019). Marketing strategies evaluation based on big data analysis: a CLUSTERING-MCDM approach. *Economic Research-Ekonomska Istraživanja*, *32*(1), 2882–2892.

Mahdiraji, H. A., Zavadskas, E. K., Arab, A., Turskis, Z., & Sahebi, I. G. (2021). Formulation of manufacturing strategies based on an extended Swara method with intuitionistic fuzzy numbers: An automotive industry application. *Transformations in Business & Economics*, *20*(2), 346–374.

Mahdiraji, H. A., Zavadskas, E. K., Skare, M., Kafshgar, F. Z. R., & Arab, A. (2020). Evaluating strategies for implementing industry 4.0: a hybrid expert oriented approach of BWM and interval valued intuitionistic fuzzy TODIM. *Economic Research-Ekonomska Istraživanja*, *33*(1), 1600–1620.

Mallinder, J., & Drabwell, P. (2013). Cyber security: a critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber attack. *Journal of Business Continuity & Emergency Planning*, *7*(2), 103–111.

Markakis, E., Nikoloudakis, Y., Mastorakis, G., Mavromoustakis, C. X., Pallis, E., Sideris, A., Zotos, N., Antic, J., Cernivec, A., Fejzic, D., Kulovic, J., Jara, A., Drosou, A., Giannoutakis, K., & Tzovaras, D. (2019). Acceleration at the edge for supporting SMEs Security: The FORTIKA paradigm. *IEEE Communications Magazine*, *57*(2), 41–47. https://doi.org/10.1109/MCOM.2019.1800506

Mi, X., Tang, M., Liao, H., Shen, W., & Lev, B. (2019). The state-of-the-art survey on integrations and applications of the best worst method in decision making: Why, what, what for and what's next? *Omega (United Kingdom)*, *87*, 205–225. https://doi.org/10.1016/j.omega.2019.01.009

Mokhtarzadeh, N. G., Mahdiraji, H. A., Beheshti, M., & Zavadskas, E. K. (2018). A novel hybrid approach for technology selection in the information technology industry. *Technologies*, *6*(1), 34.

Munim, Z. H., Sornn-Friese, H., & Dushenko, M. (2020). Identifying the appropriate governance model for green port management: Applying analytic network process and best-worst methods to ports in the Indian Ocean Rim. *Journal of Cleaner Production*, *268*, 122156. https://doi.org/10.1016/j.jclepro.2020.122156

Mustafa, H. K., & Yaakub, S. (2018). Innovation and technology adoption challenges: Impact on SMEs' company performance. *International Journal of Accounting, Finance and Business*, *3*(15), 57–65. www.ijafb.com

National Center for the Middle Market. (2016). National center for middle market study. https://www.middlemarketcenter.org/

Nieto, A., Acien, A., & Fernandez, G. (2019). Crowdsourcing analysis in 5G IoT: Cybersecurity threats and mitigation. *Mobile Networks and Applications*, *24*(3), 881–889. https://doi.org/10.1007/s11036-018-1146-4

Nycz, M., Martin, M. J., & Polkowski, Z. (2015). The cyber security in SMEs in Poland and Tanzania. Proceedings of the 2015 7th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2015, pp. AE27–AE34. IEEE. https://doi.org/10.1109/ECAI.2015.7301182

Office for National Statistics. (2019). E-Commerce and ICT Activity, UK: 2018. November, 1. Author.

Omrani, H., Amini, M., & Alizadeh, A. (2020). An integrated group best-worst method – Data envelopment analysis approach for evaluating road safety: A case of Iran. *Measurement: Journal of the International Measurement Confederation*, *152*, 107330. https://doi.org/10.1016/j.measurement.2019.107330

Onwubiko, C., & Lenaghan, A. P. (2007). Managing security threats and vulnerabilities for small to medium enterprises. 2007 IEEE Intelligence and Security Informatics, pp. 244–249. IEEE. https://doi.org/10.1109/isi.2007.379479

Osborn, E. (2014). Sources of the perceived lack of cyber security in SMEs. Centre for Doctoral Training (CDT) in Cyber Security Technical Paper. https://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e/download_file?file_format=pdf&safe_filename=01-15.pdf&type_of_work=Research+paper

Osborn, E., & Simpson, A. (2017). On small-scale IT users' system architectures and cyber security: A UK case study. *Computers and Security*, *70*, 27–50. https://doi.org/10.1016/j.cose.2017.05.001

Osei, E., & Yeboah-boateng, E. O. (2013). Social engineering of social engineers & corporate espionage agents: How prepare are SMEs in developing economies? *Journal of Electronics & Communications Engineering Research*, *1*(3), 14–22.

Paté-Cornell, M. E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis*, *38*(2), 226–241. https://doi.org/10.1111/risa.12844

Payne, B. K. (2018). White-collar cybercrime: White-collar crime, cybercrime, or both? *Criminology, Criminal Justice, Law and Society*, *19*(3), 16–32.

Ponsard, C., & Grandclaudon, J. (2019). Survey and guidelines for the design and deployment of a cyber security label for SMEs. In Mori, P., Furnell, S., & Camp, O. (Eds.), *Communications in computer and information science* (Vol. 977, pp. 240–260). Springer International Publishing. https://doi.org/10.1007/978-3-030-25109-3_13

Ponsard, C., Grandclaudon, J., & Dallons, G. (2018). Towards a cyber security label for SMEs: A European perspective. Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Madeira, Portugal, pp. 426–431. https://doi.org/10.5220/0006657604260431

Radanliev, P., De Roure, D., Page, K., Nurse, J. R. C., Mantilla Montalvo, R., Santos, O., Maddox, L., & 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). https://doi.org/10.1186/s42400-020-00052-8

Rae, A., & Patel, A. (2019). Defining a new composite cybersecurity rating scheme for SMEs in the U.K. In Heng, J. & Lopez, S. H. (Eds.), *Lecture notes in computer science* (Vol. 11879, pp. 362–380). Springer. https://doi.org/10.1007/978-3-030-34339-2_20

Ratten, V. (2019). The effect of cybercrime on open innovation policies in technology firms. *Information Technology and People*, *32*(5), 1301–1317. https://doi.org/10.1108/ITP-03-2018-0119

Renaud, K. (2016). How smaller businesses struggle with security advice. *Computer Fraud and Security*, *2016*(8), 10–18. https://doi.org/10.1016/S1361-3723(16)30062-8

Renn, O. (1998). Three decades of risk research: Accomplishments and new challenges. *Journal of Risk Research*, *1*(1), 49–71. https://doi.org/10.1080/136698798377321

Renn, O. (2021). New challenges for risk analysis: systemic risks. *Journal of Risk Research*, *24*(1), 127–133. https://doi.org/10.1080/13669877.2020.1779787

Rezaei, J. (2015). Best-worst multi-criteria decision-making method. *Omega*, *53*, 49–57. https://doi.org/10.1016/j.omega.2014.11.009

Rezaei, J., van Roekel, W. S., & Tavasszy, L. (2018). Measuring the relative importance of the logistics performance index indicators using Best Worst Method. *Transport Policy*, *68*(2017), 158–169. https://doi.org/10.1016/j.tranpol.2018.05.007

Sadok, M., & Bednar, P. M. (2016). Information security management in SMEs: Beyond the IT challenges. HAISA, 2016, Frankfurt, Germany. Pp. 209–219. http://dblp.uni-trier.de/db/conf/haisa/haisa2016.html#SadokB16

Sadraei, R., Biancone, P., Lanzalonga, F., Jafari-Sadeghi, V., & Chmet, F. (2022). How to increase sustainable production in the food sector? Mapping industrial and business strategies and providing future research agenda. *Business Strategy and the Environment*. Advance online publication. https://doi.org/10.1002/bse.3244

Sangani, N. K., & Vijayakumar, B. (2012). Cyber security scenarios and control for small and medium enterprises. *Informatica Economica Journal*, *16*(2), 58–71.

Satyanarayana, K., Chandrashekar, D., Sukumar, A., & Jafari-Sadeghi, V. (2022). How does international entrepreneurial orientation influence firms' internationalization? – An exploration with Indian software product top management teams. *International Journal of Entrepreneurial Behavior & Research*, *28*(7). https://doi.org/10.1108/IJEBR-07-2021-0530

Scott, J. E. (2004). Measuring dimensions of perceived e-business risks. *Information Systems and E-Business Management*, *2*(1), 31–55. https://doi.org/10.1007/s10257-003-0026-y

Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: promising organisational practices. *Information Technology and People*, *32*(5), 1125–1129. https://doi.org/10.1108/ITP-10-2019-564

Shamala, P., Ahmad, R., Zolait, A., & Sedek, M. (2017). Integrating information quality dimensions into information security risk management (ISRM). *Journal of Information Security and Applications*, *36*, 1–10. https://doi.org/10.1016/j.jisa.2017.07.004

Singh, R., Chandrashekar, D., Subrahmanya, B., Sukumar, A., & Jafari-Sadeghi, V. (2022). Network cooperation and economic performance of SMEs: Direct and mediating impacts of innovation and internationalisation. *Journal of Business Research*, *148*(September 2022), 116–130. https://doi.org/10.1016/j.jbusres.2022.04.032

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stallings, W. (2019). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley Professional.

Stjepić, A. M., Pejić Bach, M., & Bosilj Vukšić, V. (2021). Exploring risks in the adoption of business intelligence in SMEs using the TOE framework. *Journal of Risk and Financial Management*, *14*(2), 58.

Sukumar, A., Jafari-Sadeghi, V., Xu, Z., & Tomlins, R. (2022). Young students and desire to social entrepreneurship: The impact of government's role. *International Journal of Entrepreneurship and Small Business*, *46*(4), 526–553. https://doi.org/10.1504/IJESB.2022.10049315

Taghavifard, M. T., Mahdiraji, H. A., Alibakhshi, A. M., Zavadskas, E. K., & Bausys, R. (2018). An extension of fuzzy SWOT analysis: An application to information technology. *Information (Switzerland)*, *9*(3), 1–19. https://doi.org/10.3390/info9030046

Tarhini, A., Alalwan, A. A., Al-Qirim, N., Algharabat, R., & Masa'deh, R. (2018). An Analysis of the Factors Influencing the Adoption of Online Shopping. *International Journal of Technology Diffusion*, *9*(3), 68–87. https://doi.org/10.4018/ijtd.2018070105

Teh, S. S., & Kee, D. M. H. (2019). The readiness of small and medium enterprises for the industrial revolution 4.0. *GATR Global Journal of Business Social Sciences Review*, *7*(4), 217–223. https://doi.org/10.35609/gjbssr.2019.7.4(2)

Topping, C. (2017). The role of awareness in adoption of government cyber security initiatives: A study of SMEs in the UK. https://www.diva-portal.org/smash/get/diva2:1127292/FULLTEXT01.pdf

Topping, C., Bada, M., & Sasse, A. (2014). The role of awareness in the adoption of government cyber security initiatives: A study of SMEs in the UK. Global Cyber Security Capacity Centre, Independent (July), 71. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1127292&dswid=5770

Triantaphyllou, E. (2000). Multi-criteria decision making methods. In *Applied optimization* (pp. 5–21). Springer. https://doi.org/10.1007/978-1-4757-3157-6_2

Velasquez, M., & Hester, P. (2013). An analysis of multi-criteria decision making methods. *International Journal of Operations Research*, *10*(2), 56–66.

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, *CURF. International Journal of Information Security*, *17*(6), 681–699. https://doi.org/10.1007/s10207-017-0382-0

Wu, W., Kou, G., & Peng, Y. (2016). Group decision-making using improved multi-criteria decision making methods for credit risk analysis. *Filomat*, *30*(15), 4135–4150. https://doi.org/10.2298/FIL1615135W

Yatsalo, B. I., Kiker, G. A., Kim, J., Bridges, T. S., Seager, T. P., Gardner, K., Satterstrom, F. K., & Linkov, I. (2007). Application of multicriteria decision analysis tools to two contaminated sediment case studies. *Integrated Environmental Assessment and Management: An International Journal*, *3*(2), 223–233.

Yigit Ozkan, B., Spruit, M., Wondolleck, R., & Burriel Coll, V. (2020). Modelling adaptive information security for SMEs in a cluster. *Journal of Intellectual Capital*, *21*(2), 235–256. https://doi.org/10.1108/JIC-05-2019-0128

Zabalawi, E. A., Bakhouche, A., & El Chaar, R. (2021). Risk management: Minimizing the triple risks–strategic, financial, and operational. In Webb, H. C., Al Numairy, H., & Wu, W. (Eds.). *Innovation management and growth in emerging economies* (pp. 206–225). IGI Global.

Zhu, F. (2021). *The impact of high technology on the economy*. In 2021 5th Annual International Conference on Data Science and Business Analytics (ICDSBA), pp. 323–327. IEEE.

How to cite this article: Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*, 1–17. https://doi.org/10.1111/risa.14092