Taylor & Francis
Taylor & Francis Group

Journal of Computer Information Systems

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ucis20

Cybersecurity Resilience in SMEs. A Machine Learning Approach

Juan Carlos Fernandez de Arroyabe, Marta F. Arroyabe, Ignacio Fernandez & Carlos F. A. Arranz

To cite this article: Juan Carlos Fernandez de Arroyabe, Marta F. Arroyabe, Ignacio Fernandez & Carlos F. A. Arranz (01 Sep 2023): Cybersecurity Resilience in SMEs. A Machine Learning Approach, Journal of Computer Information Systems, DOI: 10.1080/08874417.2023.2248925

To link to this article: https://doi.org/10.1080/08874417.2023.2248925

Published online: 01 Sep 2023.

JOURNAL OF COMPUTER INFORMATION SYSTEMS
https://doi.org/10.1080/08874417.2023.2248925

Taylor & Francis
Taylor & Francis Group

Cybersecurity Resilience in SMEs. A Machine Learning Approach

Juan Carlos Fernandez de Arroyabe[a], Marta F. Arroyabe[a], Ignacio Fernandez[b], and Carlos F. A. Arranz[c]

[a]University of Essex, Colchester, UK; [b]Loughborough University, Loughborough, UK; [c]University of Greenwich, London, UK

ABSTRACT

This study investigates cybersecurity resilience in small and medium-sized enterprises (SMEs), focusing on three key aspects: the capacity to handle potential cyber incidents, the ability to recover from such incidents, and the capability to adapt in the face of possible cyber threats. Grounded in the Resource-Based View (RBV) framework, we conduct an empirical investigation utilizing a survey of 239 UK SMEs. The study makes a theoretical and methodological contribution, with significant implications for managers. First, the study highlights the lack of SMEs' engagement with the management of cybersecurity and finds cybersecurity incidents to be the most important factor in driving resilience, as compared to cybersecurity capabilities. Moreover, the study also extends the RBV theory, emphasizing the importance of the interaction between cybersecurity capabilities affecting SMEs' cybersecurity resilience. Second, the study showcases the potential of statistical methods, particularly machine learning techniques to identify the relationships between the factors affecting SMEs' cybersecurity.

KEYWORDS

Cybersecurity; resilience; SMEs; cybersecurity incidents; cybersecurity impacts; cybersecurity systems

Introduction

Cybersecurity is emerging as a critical capability for organizational survival and growth.[1–4] Caldwell[5] and Choo[6] point out that companies are exposed to cybersecurity incidents, considering both the potential risks of the internet, electronic commerce, the digitalization of companies, and the use of Internet of Things (IoT). The connected nature of enterprises means that firms' information systems (IS) connect to the network, and can be a potential source of attacks, which can affect the operability and resilience of enterprises.[7–9] For example, the implementation of digital technologies such as big data implies the storage of information, which can potentially be stolen.[10] The incorporation of industrial robots connected to the Industrial Internet of Things (IIoT), or the use of smart devices, can be subject to potential attacks, for example, tampering attacks, which impact the integrity of systems or applications, or denial of service (DoS), which impacts the availability of systems and applications.[1,11] In general, firms are exposed to attacks such as spyware, malware, DoS, ransomware or phishing among others, and the devices of the firms can serve as possible entry points for cyberattacks.[1] In this context, cybersecurity appears in organizations as a key element to guarantee the firms' resilience, allowing the development of their activities without affecting their operability.

The study explores cybersecurity resilience in small and medium-sized enterprises (SMEs), addressing several gaps. Given the crucial role of SMEs in the economy, both in terms of employment and production, it becomes essential to ensure their operational continuity is not compromised by cybersecurity incidents. Compared to large firms, SMEs face substantial challenges in terms of the capability (e.g., knowledge and skills) and capacity (e.g. financial and time resources) to plan and implement cybersecurity and their digital transformation.[12,13] Since previous studies have mostly focused on large organizations,[14–17] it is crucial to explore how SMEs behave in terms of resilience, which refers to their capacity to withstand, recover from, and adapt to potential cyber incidents.[18]

The first gap concerns the lack of understanding regarding how cybersecurity is currently being managed in SMEs.[1] The existing literature indicates that many SMEs perceive cybersecurity as unimportant,[12] believing they are unlikely to be targeted by cyber threats. However, empirical research reveals that SMEs are indeed targeted, either by automated attacks or deliberate ones, and they can serve as entry points for cybersecurity attacks into the supply chain of larger enterprises.[19] This perception of cybersecurity among SMEs leads to a lack of attention toward cybersecurity management, resulting in increased vulnerabilities for these businesses and the potential risk of operational

CONTACT Marta F. Arroyabe mf17255@essex.ac.uk Essex Business School, University of Essex, Wivenhoe Park, Colchester CO4 3SQ, UK

disruptions.[1,20,21] Considering this, several studies emphasize the vital importance of investigating and understanding how cybersecurity management clarifies in SMEs.[1,22,23]

Second, our research aims to address a gap that has been overlooked by previous studies. While previous research has concentrated primarily on technical and operational aspects, we aim to examine the impact of both cybersecurity management, as well as cyberattacks, on the cybersecurity resilience of SMEs.[2,6,20] Other researchers such as Conteh and Schmick,[4] and Fernandez De Arroyabe and Fernandez de Arroyabe[12] have also observed the challenge of establishing a relationship between the types of incidents, cybersecurity management, and their impact on firm management.

To address these gaps, we conduct an empirical analysis framed in the resource-based view (RBV). Thus, in line with the works of Bharadwaj[24] and Jalali and Kaiser,[3] our study introduces the concept of cybersecurity capabilities as crucial organizational capacities. These capabilities emerge from the interaction between resources and competencies, resulting in the development of routines, procedures, and processes that collectively form cybersecurity capabilities within organizations. Furthermore, our study aligns with the findings of Cavusoglu et al.[25] which emphasize the significant connection between cybersecurity capabilities and organizational performance. The effectiveness and strength of an organization's cybersecurity capabilities directly influence its overall performance. The empirical study takes the SMEs as the unit of analysis, employing survey data from 239 UK SMEs in 2022. We will combine regression methods with machine learning techniques. To the explanatory potential of regression methods, we add the potential of machine learning in prediction and simulation. In business research, the application of machine learning methodology offers a unique approach to analyzing complex systems characterized by numerous interactions.[26,27] This is the case of cybersecurity management in firms, which is characterized by interactions and correlations between variables.[12,28] Furthermore, in the field of cybersecurity, there may be instances where the response is low due to a lack of knowledge regarding incidents and their impacts; in such cases, the utilization of methods, like machine learning techniques, allows us to establish causal relationships.[26]

Conceptual framework

The resource-based view (RBV) theory is a management framework that emphasizes a firm's internal resources and capabilities as primary sources of competitive advantage.[29] According to this theory, the unique combination of resources and capabilities within a firm determines its potential for achieving sustainable competitive advantage and superior performance in the market. Specifically, capabilities refer to a firm's capacity to deploy resources, often in combination, using organizational processes to achieve specific objectives.[29] These capabilities are a result of learning, organizational resources, and the firm's historical experiences.[29,30] Learning occurs through practice and experimentation, enabling tasks to be performed more effectively.[29] Moreover, extensive research in strategic management and organizational science has demonstrated that differences in the configuration of organizational resources and capabilities explain much of the variation in organizational performance.[31–33]

The RBV framework has a long tradition in the field of IT systems. For instance, Bharadwaj[24] introduced the concept of IT as an organizational capability, highlighting the significance of IT resources and their effective deployment in creating a competitive advantage. Similarly, Jalali and Kaiser[34] view cybersecurity capability as an organizational capacity and examine the challenges associated with its development within organizations. They aim to gain a deeper understanding of the complexities involved in capability development, particularly in the context of cybersecurity. Furthermore, studies have shown that the configuration of cybersecurity capabilities is closely linked to organizational performance, and there are considerable variations in how different companies structure their cybersecurity resources.[25]

The connected nature of enterprises means that IT systems connect to the network increasing their exposure to cybersecurity incidents. Thus, companies are exposed to cyberattacks, which are constantly growing, becoming more sophisticated, and diversified in nature, which makes it challenging for companies to safeguard themselves.[1,4,35] Cybersecurity attacks can occur in various ways, depending on the attacker's objectives, the method of execution, and the attacker's identity. The literature identifies different types of adversaries that use various techniques, including phishing, malware or web attacks, and the exploitation of vulnerabilities arising from the incorrect use of IT systems within organizations. ENISA has classified various types of attacks in cyberspace,[36] including malware, which accounts for 30% of all cyberattacks. Other attacks include website and domain attacks to steal personal information and bank details, as well as phishing attempts that seek to impersonate identities and deploy malware. Apart from external attacks, internal staff can also cause security breaches, either intentionally or unintentionally.

ENISA (2020) highlights the importance of this type of threat, noting that 77% of data leaks in firms result from insider-relate-dated incidents.

In this context, cybersecurity in organizations arises intending to protect IT systems, consisting of a set of measures, strategies, organizational processes and procedures aimed at alleviating the risks and vulnerabilities of their information systems.[37] In general, companies allocate resources to create cybersecurity capabilities, structured in various configurations that form the cybersecurity management of the firms. The main objective of these capabilities is not only to effectively reduce potential losses due to cybersecurity incidents but also to enhance the overall performance of their operations.[38] The configuration of these cybersecurity capabilities can vary, encompassing both operational aspects and cybersecurity capabilities of a strategic and organizational nature.[39,40] These can range from cybersecurity capabilities that develop actions of an operative nature to capabilities actions of a strategic and organizational nature.[39,40] First, we can talk about *cybersecurity control mechanism*, where the firm develops cybersecurity routines and procedures, which include activities such as *software updates*, the use of *firewalls* and *malware scanning*, as well as *network security measures*, which can be combined with secure communication methods such as *VPN* and *data encryption*.[11,35,41] Second, regarding *cybersecurity management*, companies introduce measures of organizational and strategic nature concerning their cybersecurity, such as the assignment of *teams* for the management of information security, the development of *policies and cybersecurity risk assessment systems* (for example, ISO 27000s, Cyber essentials), or including cybersecurity issues in the *meetings* of the senior managers of the companies.[39,40]

Research questions

We assess the cybersecurity resilience of SMEs by following the conceptualization provided by the National Institute of Standards and Technology.[a],[18] Our study focuses on three key aspects: the capacity to operate in the face of potential cybersecurity incidents, the ability to recover from such cybersecurity incidents, and finally, the capability to adapt to possible cybersecurity incidents. Based on these aspects, we formulate three research questions for our study.

The first research question considers the capacity to work against potential cybersecurity incidents, which is measured by the cybersecurity impact on SMEs. The impact of cybersecurity incidents extends beyond the IT systems of a firm and affects its overall business continuity, reputation, and supply chains. These consequences entail financial and economic costs, including income loss, increased expenses for additional staffing, and the need for new measures to prevent future breaches.[36] As emphasized by Couce-Vieira et al.[42] (2020) and Fernandez de Arroyabe and Fernandez de Arroyabe,[12] incidents can also have implications for other intangible assets, such as corporate reputation. For instance, a Forbes Insights[43] report showed that 46% of organizations suffered reputational and brand value damage following a cybersecurity incident. Additionally, Couce-Vieira et al.[42] pointed out that incidents have effects not only on the firm but also on its stakeholders, highlighting the importance of proper management of the information communicated to customers and shareholders. Fernandez de Arroyabe and Fernandez de Arroyabe[12] further emphasized the responsibility that companies have to their customers and the administration, which may result in compensation and associated costs.

In this context, the first research question asks how SMEs perceive which factors affect the economic and managerial impact on the SME. For this, we consider that the impact is a balance between the cybersecurity incidents and the configuration of cybersecurity capability.

RQ1: *How do cybersecurity incidents and cybersecurity capabilities affect the economic and managerial impact in SMEs?*

Second, an important aspect of resilience in SMEs is the recovery time from a cybersecurity incident. A cybersecurity incident not only has economic and reputational repercussions for companies but also paralyzes their activities.[12] In this sense, the capability to recover the activity will depend on both internal and external variables.[37] As internal variables, we can consider the degree of development and the implementation of cybersecurity. In this sense, cybersecurity capabilities not only prevent incidents, mitigating the vulnerabilities of the SMEs but also propose action procedures for firms to recover after an incident. ISO 27,000 highlights the need for business continuity plans, setting the procedures and routines for companies to follow to return to their activity.[39] Moreover, the recovery time is affected by the severity of the incidents, i.e., the degree of damage produced in the companies. For example, for damages for data theft, if there is a backup, the firm's

[a]NIST (2023) define cyber resilience as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources (NIST SP 800-172).

activity can be resumed; for damage to the IT infrastructure, with adequate segregation of the systems, the activity can be resumed; even a DoS attack can be prevented and recovered with the right cybersecurity measures.[8,11] There is variability in the recovery time from hours to days or months, with the consequent damages for the SMEs. Therefore, it is to be expected that the incidents, as well as the damage produced by them, have an impact on the recovery time of SMEs.

Our second research question asks which factors affect the recovery time of SMEs. Thus, we consider cybersecurity capabilities, cybersecurity incidents, and cybersecurity impact.

RQ2: *How do cybersecurity capabilities, cybersecurity incidents and cybersecurity impact affect the recovery time of SMEs?*

Finally, we consider one last aspect of the cybersecurity resilience of SMEs, namely the ability to adapt to possible cybersecurity incidents and their economic and managerial impact. In this sense, the investment in cybersecurity systems, both at operational and strategic levels, provides cybersecurity capabilities for SMEs. Thus, developing IT routines and procedures for software updates, malware detection and network security, VPN, and data encryption, will mitigate the firm's vulnerabilities.[39] Moreover, in line with ISO 27,000, the creation of cybersecurity systems in companies not only involves the development and implementation of operational measures but also implies both organizational and strategic decisions concerning the cybersecurity of companies, from the assignment of equipment for the management of information security, development of cybersecurity risk assessment policies and systems, even including cybersecurity issues in the meetings of companies' senior.[39] All these measures have the objective of developing procedures and routines that allow the correct functioning of the firm and its personnel, mitigating or reducing the cybersecurity vulnerabilities of the companies.

In this context, we pose a third research question that explores which factors affect the creation of cybersecurity capabilities in SMEs. To do this, we consider factors such as cybersecurity impact and cybersecurity incidents, as elements that affect the development of cybersecurity capabilities in SMEs.

RQ3: *How do cybersecurity incidents and cybersecurity impact affect the development of cybersecurity capabilities in SMEs?*

Methodology and data

For this research, we have conducted a survey of UK SMEs. The fieldwork was conducted between February and May 2022, being the analysis period 2019–2022. The SMEs were drawn from the Free Company Data Product, which is a publicly accessible directory containing basic data (e.g., company name, address, postcode, local authority, and industry classification) of live companies on the register from the UK's Companies House. We employed a web crawler and a web scrapper to obtain the contact addresses of the companies. The survey was carried out via the Internet, consisting of two waves, and ensuring a balance across sectors. The sample data in the study consists of 239 SMEs.

The distribution of the sample is made up of a high percentage (77.8%) of micro-enterprises (1 to 9 employees); with less representation of small companies (16.4%) (10 to 49 employees), and medium-sized companies (50 to 249 employees) (5.8%). Our sample covers 19 different sectors. The most represented sectors are *professional, scientific and technical activities* (SIC: 74909), *agents involved in the sale of a variety of goods* (SIC: 46190), *manufacture of loaded electronic boards activities* (SIC: 26120), *business support service activities* (SIC: 82990), *human health activities* (SIC: 86900), *amusement and recreation activities* (SIC: 93290), and *repair of computers and peripheral equipment* (95110). Finally, we have found a homogeneous geographical distribution of the sample in the UK.

To ensure both the robustness of the survey and the results, we first analyzed the responses obtained in the two waves, and we did not find significant discrepancies between the two waves. Second, we performed checks of the survey to verify the robustness of the questionnaires and answers, testing the common method variance (CMV) and common method bias (CMB), following the method of Podsakoff et al.[44] The analysis identified eight distinct constructs that collectively account for 63.55% of the variance. The first factor accounts for 17.031% of the variance, which falls below the recommended threshold of 50%. Consequently, we can infer that common method variance (CMV) and common method bias (CMB) are not a significant concern in our findings.

Measures

The first group of variables refers to the cybersecurity capabilities of SMEs. Following previous works,[11,12] we classify cybersecurity capabilities into two variables. The first variable refers to the operational and control cybersecurity capabilities, where the SMEs have created

operational and control processes and routines for cybersecurity during the period 2019 to 2022. Following Fernandez de Arroyabe and Fernandez de Arroyabe,[12] and Cucoranu et al.[11] the items chosen in this question are: i) Regular software updates (including patching); ii) Encrypting or securing data; iii) Malware protection; iv) Use of VPN; v) Firewalls and network security; vi) Identity and Access Management; vii) Physical security controls on firm-owned devices; viii) Only allowing access via firm-owned devices; ix) A segregated guest wireless network; and x) Regular backing up data securely. Additionally, following Arranz et al. (2021), the variable *cyber-controls* were formed as a cumulative index of the 10 types of cybersecurity capabilities (Alpha Cronbach: 917).

The second variable refers to the strategic and organizational processes and procedures in the implementation of cybersecurity capabilities in SMEs, during the period 2019 to 2022. Following Fernandez de Arroyabe and Fernandez de Arroyabe,[1] the question is multi-item: i) An outsourced provider that manages your cybersecurity; ii) Staff members with information security or governance responsibilities; iii) A formal policy or policies in place covering cybersecurity risks; iv) Invested in threat intelligence; v) An independent cybersecurity assessment; vi) Any business-as-usual health checks that are undertaken regularly; and vii) Formal cybersecurity discussions with the CEO, board or equivalent. As in the previous variable, we create a new variable *cyber-management*, as a cumulative index of the seven items (Cronbach Alpha: 879).

The following variable refers to the perception of cybersecurity incidents (successful or unsuccessful) that occurred within the firm in the last months. Thus, following Fernandez de Arroyabe and Fernandez de Arroyabe,[12] and Cucoranu et al.[11] we have determined a series of cybersecurity incidents, such as: i) Phishing or spear phishing; ii) Ransomware; iii) Viruses, spyware or malware; iv) Attacks that try to take down the companies' website or online services; v) Unauthorized use of computers, networks or servers by staff, even if accidental (insider incident); vi) Unauthorized use or hacking of computers, networks or servers by people outside your organization; vii) Hacking or attempted hacking of online bank accounts; and ix) Denial of service (DoS or DDoS). The *cyber-incidents* variable is created as a cumulative index of previous items (Cronbach Alpha: 760).

The next variable refers to the level of cybersecurity impacts in economic and management terms in SMEs (*cyber-impacts*). In line with Fernandez de Arroyabe and Fernandez de Arroyabe,[12] we consider the following outcomes: i) Stopped the business-as-usual activities; ii) Negative impact on the revenue or share value; iii) Repair or recovery costs; iv) Fines from regulators or authorities or associated legal costs; and v) Reputational damage and loss of customer trust. The *cyber-impacts* variable is created as a cumulative index of previous items (Cronbach Alpha: 716).

The last variable refers to how long did it take to restore business operations (*recovery time*): i) No time at all; ii) Less than a day; iii) Between a day and under a week; iv) Between a week and under a month; v) One month or more; and vi) Still not back to normal.

Following the literature on cybersecurity and to control our results, we have included three control variables. The first one is the *size* of the firms. Using a Likert scale from 1 to 3, where 1 corresponds to companies with 1 to 9 employees, 2 corresponds to companies with 10 to 49 employees, and finally, 3 corresponds to companies with 50 to 250 employees.

The second control variable is the firm's *growth* in turnover since 2017, rated on a Likert scale from 1 to 4. A score of 1 indicates no growth, 2 indicates growth of less than 10% per year, 3 indicates growth between 10% and 20%, and finally, 4 indicates growth exceeding 20%.

The last variable measures the degree of *digitalization* of the company, considering the following digital technologies: cloud computing, Artificial Intelligence, smart devices, robotics, big data, blockchain, and high-speed infrastructure. This variable is measured as an accumulative index of the seven digital technologies, ranging from 0 for companies that haven't adopted any digital technologies to 7 for those that have adopted all of them.

Empirical analysis

Regarding the first research question (RQ1), how *cyber-control, cyber-management* and *cyber-incidents* affect the firm in economic and management terms (*cyber-impact*), we conduct a linear regression analysis. To do this, we use cyber-impact as the dependent variable, and cyber-control, cyber-management, and cyber-incidents as independent variables. The econometric model is:

$$\begin{aligned} \textit{Cyber-impact} = {} & \textit{constant} + \beta_1(\textit{Cyber-control}) \\ & + \beta_2(\textit{Cyber-management}) \\ & + \beta_3(\textit{Cyber-incidents}) + e \end{aligned}$$

Moreover, we combine regression analysis with machine learning methods, more specifically artificial neural networks (ANN). That is, to the explanatory power of regression models in causal analyses, we want to add the exploratory power of ANN models, especially in the case of the existence of non-linear

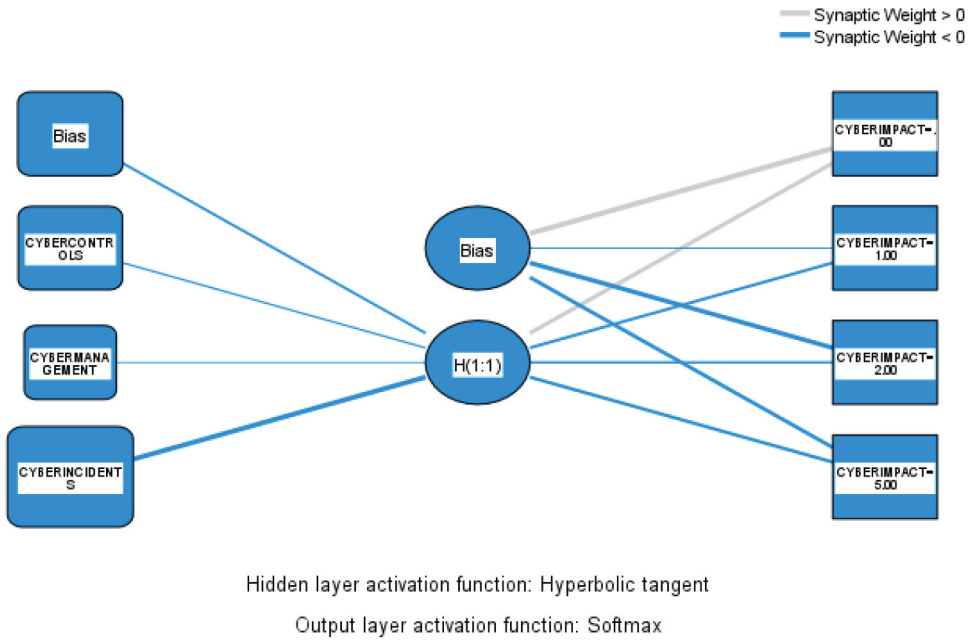

Figure 1. ANN-MLP architecture for RQ1.

relationships between input variables and multiplicity of interactions.[26] For the simulation with ANN, we use the multilayer perceptron (MLP). Specifically, the architecture of a multilayer perceptron (MLP) consists of an input layer, one or more hidden layers, and an output layer. By connecting the neurons in the hidden and output layers with their respective weights, it becomes possible to analyze the interaction between the input variables.

To develop the ANN-MLP architecture, we adopted the methodology of Wang[45] and Fernandez de Arroyabe et al.[1] (see Annex Table A1). The design process entails the determination of the number and size of hidden layers. This is, the number of inputs and outputs of the network is determined by the number of input and output variables, whereas the number and size of hidden layers are determined through a trial-and-error approach involving several combinations of the number of hidden layers and neurons,[b] [1,46] with various activation functions tested to identify the optimal architecture that minimizes the error. Additionally, we employ the backpropagation algorithm for learning, which adjusts the connection weights of each neuron, reducing the error. The econometric model is:

$$Cyber\text{-}impact = f(Cyber\text{-}control; Cyber\text{-}management; Cyber\text{-}incidents)$$

Figure 1 and Table 1 present the results of the ANN-MLP architecture for RQ1, the software used for the simulation was SPSS. The options chosen to design the ANN-MLP architecture are:

(1) In the design process, the number of hidden layers was chosen to range between 1 and 50.
(2) The activation function can be hyperbolic tangent or sigmoidal or SoftMax.
(3) The learning algorithm uses backpropagation.[c] The parameters chosen for the algorithm were: the number of interactions, the learning rate, and the moment. In our study, we set the number of interactions (n) to 10,000. The learning rate (β) is another important variable, as it controls the magnitude of the weight changes in each iteration. Typically, the learning rate falls between 0.05 and 0.5. Finally, the moment factor (α) accelerates the convergence of the weights. Yegnanarayana[47] suggests that a value close to 1, such as 0.9, is an appropriate choice.

[b] To accurately model function approximation, Ciurana et al.[46] suggest that a two-layer neural network is typically adequate.

[c] This learning algorithm decides the connection weights of each neuron, readjusting the weights and minimizing the error. The equation for modifying the algorithm weights is shown below.
$\Delta wji(n+1) = \varepsilon.\mu pi.\ xpi + \beta \Delta wji(n)$
Being, wji = weight neuron i and j
n = number of interactions
ε = learning rate
μpi = neuron j error for pattern p
xpi = output of neuron i for pattern p
β =momentum

Table 1. ANN-MLP architecture of RQ1.

Output variable	ANN architecture	Activation Functions	Error Function	Input variables
Cyberimpact	3-1-1	• Hyperbolic tangent • Identity (SoftMax)	Cross-entropy	• Cyber-incidents • Cyber-controls • Cyber-management

Figure 1 revealed that the optimal architecture for predicting cybersecurity impact is 3-1-1. This architecture consists of three neurons in the input layer, one neuron in the hidden layer, and one neuron in the output layer.[d] After various simulations, the hyperbolic tangent function was used as the activation function for the hidden layer, while the SoftMax function was used for the output layer.

Regarding the second research question (RQ2), we performed an ordinal logistic regression analysis, employing *recovery time* as the dependent variable, and *cyber-control*, *cyber-management, cyber-impact and cyber-incidents* as independent variables. Ordinal logistic regression allows the use of variables with multi-items, such as recovery time, which ranges from 1 to 7. The econometric model for regression analysis is:

$$\begin{aligned} Recovery\text{-}time = {} & constant + \beta_1(Cyber\text{-}control) \\ & + \beta_2(Cyber\text{-}management) \\ & + \beta_3(Cyber\text{-}incidents) \\ & + \beta_4(Cymer\text{-}impact) + e \end{aligned}$$

As in the previous research question, we also simulate with ANN-MLP, Figure 2 and Table 2 show the architecture of the network, following previous specifications for the design of the ANN-MLP architecture. The econometric model is:

$$\begin{aligned} Recoverytime = {} & g(Cyber\text{-}control; Cyber\text{-}management; \\ & Cyber\text{-}incidents; Cyber\text{-}impact) \end{aligned}$$

$$\begin{aligned} & Cyber\text{-}control, Cyber\text{-}management \\ & = h(Cyber\text{-}incidents; Cyber\text{-}impact) \end{aligned}$$

Regarding the third research question (RQ3), we have simulated with ANN-MLP, using two input variables, *cyber-impact* and *cyber-incidents*, and as output variables *cyber-control and cyber-management*. Figure 3 and Table 3 show the ANN-MLP architecture, following the previous design process.

Analysis and results

First, our survey reveals a limited understanding among SMEs of successful and unsuccessful incidents as evidenced by the low response rate of these items. Of the answers obtained, ransomware, DoS, website attacks, phishing, and hacking were the most mentioned, in addition to incidents of an internal nature such as the unauthorized use of devices. Second, our results show how cybersecurity capabilities configurations are being managed in SMEs. Regarding cybersecurity control capabilities, we observe that the most frequently used are software updates (49%), firewalls, and backing up (40%); VPN, access management, and network segregation are used by less than 20% of companies. Furthermore, companies combine various cybersecurity control capabilities, between 4 and 7, being the most frequent software updates, firewall and malware protection, which are combined with access management measures, physical controls or VPN. Regarding cybersecurity management capabilities, only 10% of companies use some cybersecurity management procedure, such as outsourcing management, the assignment of personnel to assume these responsibilities or the setting of policies for cybersecurity. Additionally, our results reveal little use of several systems simultaneously, such as the existence of personnel and discussions on the board of companies, or the establishment of cybersecurity policies. Moreover, the most frequent cybersecurity impact is the stoppage of activities and costs derived from the damages of the incidents. Very infrequent are direct economic losses for the firm, damage to the firm's reputation or problems with the authorities. As for the recovery time, approximately 80% of the responses received indicate that the cybersecurity incident was resolved in less than an hour, with repairs being more infrequent in a day or a week.

Regarding RQ1, Table 4 shows the results of the linear regression analysis. The results show that cyber-controls ($\beta = -.027$; $p < .05$) and cyber-incidents ($\beta = .309$; $p < .001$) have an impact on SMEs, with negative and positive signs, respectively. The results show that the cyber-management variable is not significant.[e]

For robustness checks of regression analysis, we employ ANN-MLP. Firstly, we evaluated the fitting

[d]The ANN-MLP processing is performed considering the output variable as discrete (Likert scale), in the entire range of the variable.

[e]In order to corroborate the robustness of the model, we have performed various types of regressions, considering the diversity of relationship typologies between the dependent and independent variables (*logistic; linear; quadratic and cubic*), and the best fit has been obtained with a relationship linear between variables (R^2: 411).

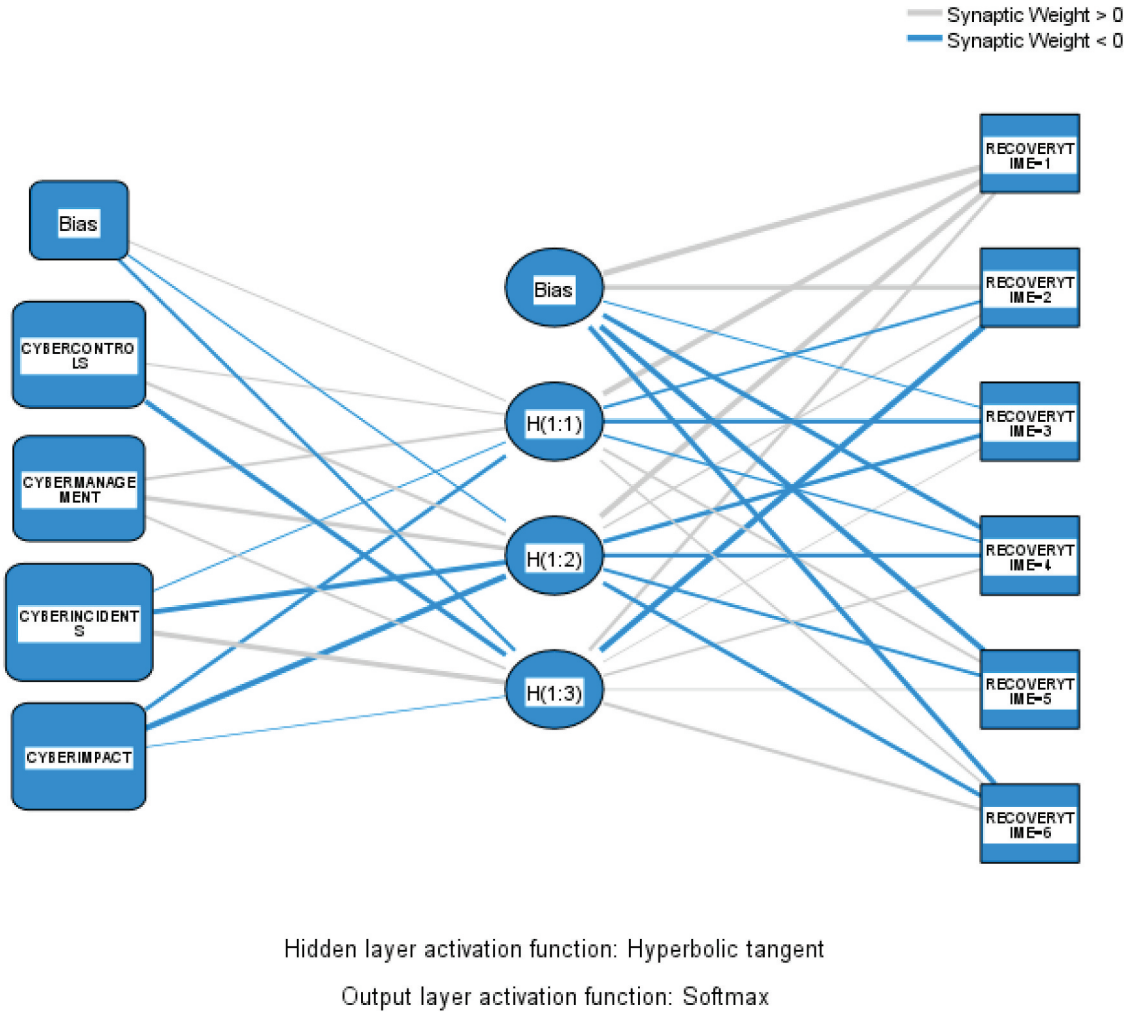

Figure 2. ANN-MLP architecture for RQ2.

Table 2. ANN-MLP architecture of RQ2.

Output variable	ANN architecture	Activation Functions	Error Function	Input variables
Recovery time	4-3-1	• Hyperbolic tangent • Identity (SoftMax)	Cross-entropy	Cyber-incidents Cyber-controls Cyber-management Cyber-impact

of the ANN-MLP design by applying cross-entropy error in the training and testing phases. The results showed that the percentage of incorrect predictions was 7.4% and 5.3%, respectively. Secondly, we assessed the predictability of our models using the ROC curve,[f] which is a graph of sensitivity versus specificity that indicates the classification performance. The accuracy of the model is higher when the curve moves away from the 45-degree line. Our ROC curve revealed that the selected architecture can predict more than 80% of the output variable values (see Figure 1). Figure 4 illustrates the ROC curve for each significant value of the variable cyber-impact, which ranges from 0 to 5, showcasing the diversity of impacts experienced by SMEs, ranging from 1 to 5. Additionally, it is evident from the analysis that cases in which SMEs perceived three or four types of impact are not significant.

Additionally, from the simulation with ANN-MLP, Figure 5 shows the normalized importance of each input variable on the output variable. The normalized importance is estimated with Garson's

[f]The ROC (Receiver Operating Characteristics) curve is a graphical representation of the trade-off between sensitivity and specificity, which shows how well a binary classification model is able to distinguish between positive and negative classes. The closer the ROC curve is to the upper left corner of the plot, the better the classification performance of the model. In other words, if the curve moves away from the 45-degree diagonal line, the accuracy of the model is higher.

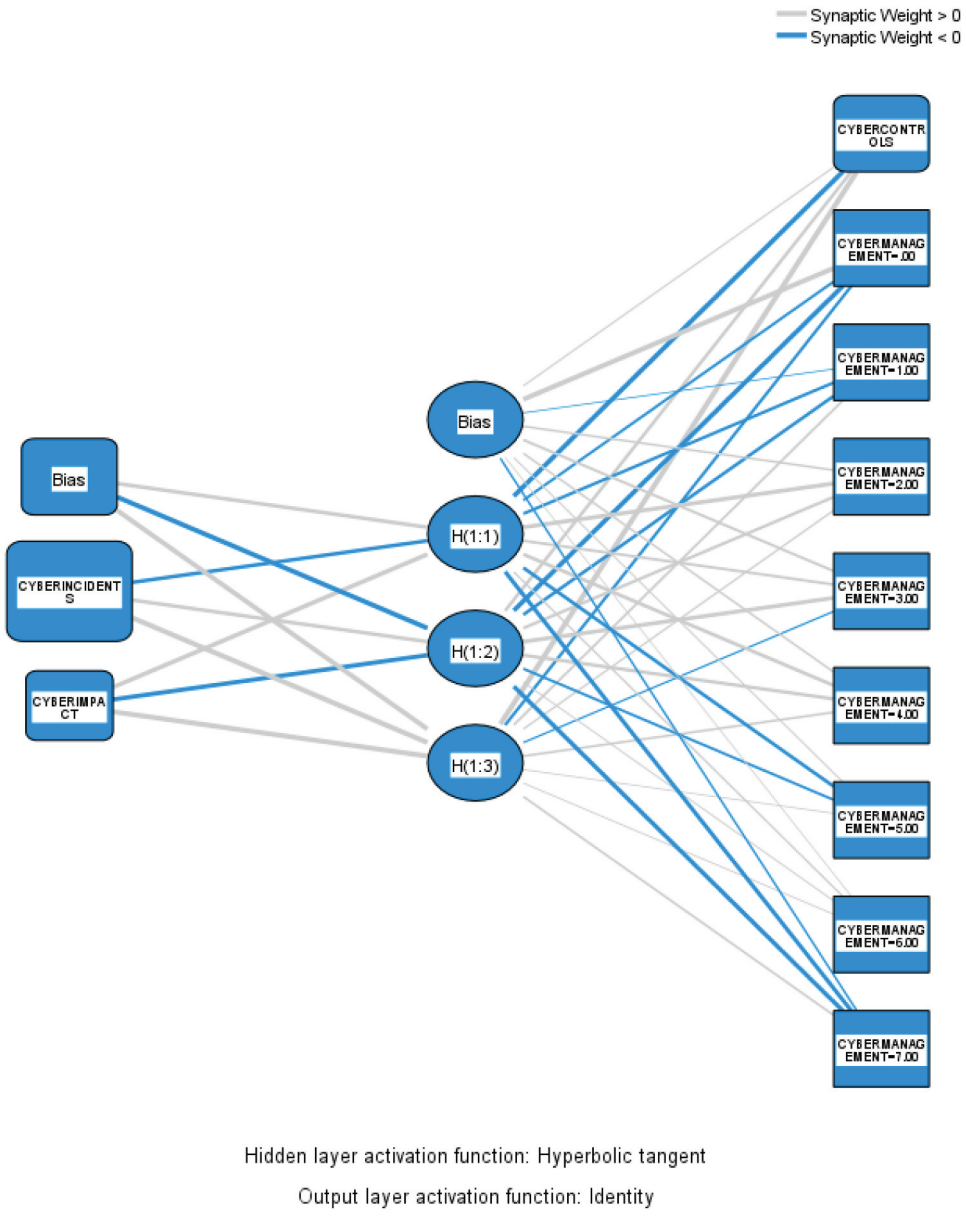

Figure 3. ANN-MLP architecture for RQ3.

Table 3. ANN-MLP architecture of RQ1.

Output variable	ANN architecture	Activation Functions	Error Function	Input variables
Cyber-controls Cyber-management	2-3-2	• Hyperbolic tangent • Identity (SoftMax)	Cross-entropy	Cyber-incidents Cyber-impact

algorithm, where the relative importance of each input variable arises as the absolute sum of the weights of each variable in each neuron and layer.[48] Our results show that cyber-incidents have the highest importance on cyber-impact (cyber-incidents: 593; 100% normalized value), followed by cyber-controls (cyber-controls: 289; 48.7% normalized value), while cyber-management, has the least importance (cyber-management: 118; 19.8% normalized value).

Regarding RQ2, Table 5 shows the results of the ordinal logit regression analysis.[g] Our results show that cyber-management has a negative and significant effect ($\beta = -.411$; $p < .001$), cyber-control a negative and significant effect ($\beta = -.237$; $p < .01$), and cyber-impact a positive and significant effect

[g]Furthermore, we check various types of regression, analyzing the relationship between the dependent and independent variables, and we observe that the non-linear (logistic) relationship has the best fit.

Table 4. Regression analysis of RQ1.

Variables	Estimate	Estimate	Estimate	Estimate	Estimate	VIF
CYBERCONTROLS		−.031*			−.027*	1.411
		(.010)			(.013)	
CYBERMANAGEMENT			−.080		−.004	1.401
			(.026)		(.025)	
CYBERINCIDENTS				.265***	.309***	1.372
				(.027)	(.027)	
Size	−.180***	−.110***	−.123***	−.162**	−.118***	1.034
	(.015)	(.012)	(.015)	(.021)	(.017)	
Growing	.044**	.075**	.099**	.082**	.055**	1.077
	(.013)	(.020)	(.031)	(.028)	(.019)	
Digitalisation	.289***	.250***	.237***	.218***	.201***	1.294
	(.024)	(.021)	.(021)	(.020)	(.023)	
R^2		.065	.071	.317	.401	

*$p < .05$; **$p < .01$; ***$p < .001$.

($\beta = 1.759$ $p < .001$). However, while in the multiple regression model, the impact of cyber-incidents is not significant, the individual regression analysis has a positive and significant impact ($\beta = .118$; $p < .05$), highlighting the limitations of the regression analysis with unbalanced samples.

To further investigate the findings from our previous analysis of RQ2, we utilized an ANN-MLP simulation. Our assessment of the simulation's robustness indicates that it is highly reliable, as evidenced by a low rate of incorrect predictions in training and testing phases (15.2% and 11.1%, respectively). Additionally, we utilized a ROC curve to evaluate the predictability of our models, and the results indicate that they can predict over 80% of output variable values (see Figure 6). Figure 6 shows the degree of significance of each of the possible items of the recovery time variable.

Additionally, from the simulation with ANN-MLP, Figure 7 shows the normalized importance of each input variable on the output variable. Our results show similar importance across the different factors of interest in SMEs' recovery time: cyber-impact (cyber-impact: 289; 100% normalized value), cyber-incidents (cyber-incidents: 272; 94.3% normalized value), cyber-control (cyber-control: 239; 82.8% normalized value), and cyber-management (cyber-management: 200; 69.2% normalized value).

Regarding RQ3, we have performed a simulation with ANN-MLP. The simulation shows an acceptable level of robustness (incorrect predictions 20.8% and 18.9%; ROC values greater than 50%). Figure 8 shows the ROC curve for each of the values of the cyber-management variable. Regarding the results, Figure 9 shows the normalized importance of each input variable on the output variables (cyber-controls and cyber-management). We observe that cyber-incidents have the highest importance (cyber-incidents: 769; 100% normalized value) on cybersecurity capabilities in SMEs, and to a lesser extent, cyber-impact shows less importance (cyber-impact: 231; 30.13% normalized value).

Discussion

First, our analysis explores the cybersecurity resilience in SMEs. Regarding the perception that SMEs have and manage cybersecurity, the results are in line with previous works that indicate the myopia that cybersecurity has for SMEs. Our results corroborate previous works that highlight that most SMEs underestimate the cyber tools and techniques they should use compared to large companies. For instance, our results support previous studies noting that SMEs tend to use weak protection systems, forgetting software updates and the development of cybersecurity policies and routines,[12] and do not seek international certifications such as the ISO 27000s.[12,23] Moreover, the results show that, fundamentally, SMEs use basic protection operating systems, such as firewalls, antivirus protection, and software updates, showing that routines, procedures, policies, and strategic decisions on cybersecurity are anecdotal or scarce in SMEs. Additionally, the results extend the understanding of the myopia of SMEs regarding cybersecurity management,[12,20,23,49] meaning that staff may engage in risky practices that may affect safety.[1,9,35,36] Fernandez de Arroyabe and Fernandez de Arroyabe[12] highlight that risk practices by employees are the main causes of cyber-breaches in SMEs since automatic attacks do not usually have a high level of severity. Following Benz et al.[50] and Mayadunne and Park,[23] we can conclude that the IT infrastructure in an SME is often composed of a small team and has an inadequate security budget, which is a significant disadvantage in dealing with cybersecurity threats.

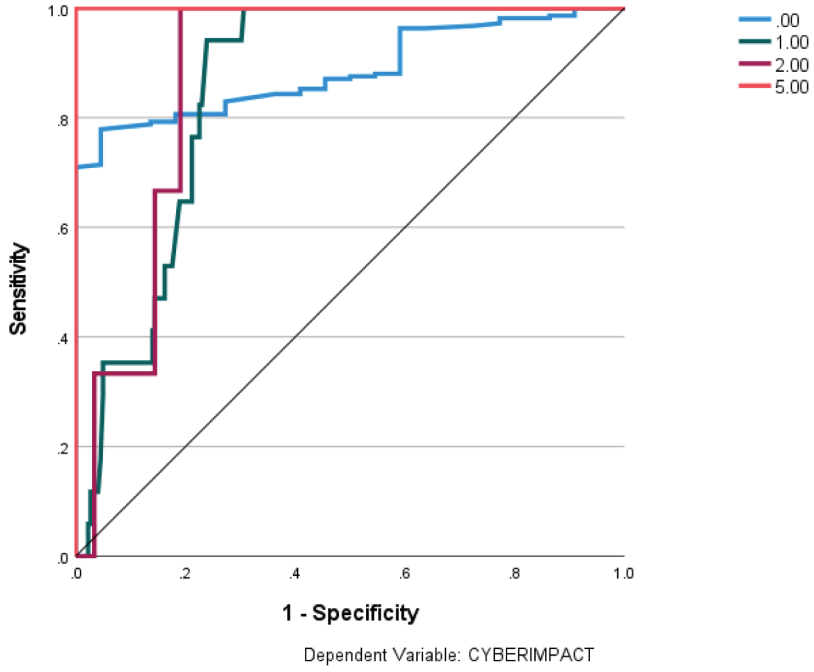

Figure 4. ROC curve for analysis of the robustness of ANN_MLP (RQ1).

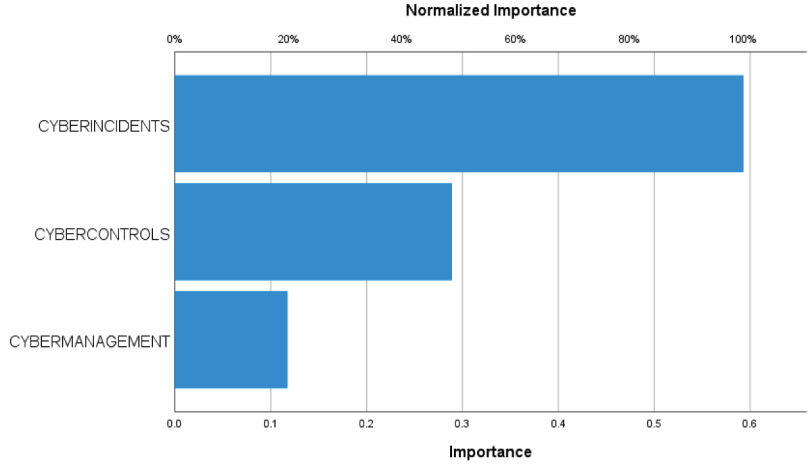

Figure 5. RQ1 normalised importance in cybersecurity impact.

Table 5. Regression analysis of RQ2.

Variables	Estimate	Estimate	Estimate	Estimate	Estimate	Estimate	VIF
CYBERMANAGEMENT		−.310***				−.411***	1.218
		(.150)				(.199)	
CYBERIMPACT			1.501***			1.759***	1.599
			(.334)			(.333)	
CYBERCONTROLS				−.218**		−.237**	1.110
				(.110)		(125)	
CYBERINCIDENTS					.118*	.021	1.728
					(.121)	(.205)	
Size	.118***	.092***	.097***	.089***	.072***	.055***	1.023
	(.023)	(.015)	(.013)	(.018)	(.018)	(.010)	
Growing	.192***	.110***	.123***	.150***	.151***	.144***	1.100
	(.102)	(.099)	(.077)	(.125)	(.123)	(.132)	
Digitalisation	.142***	.118***	.113***	.117***	.120***	.109***	1.336
	(.098)	(.095)	(.094)	(.104)	(.107)	(.099)	
−2 Log Likelihood		66.189	51.630	90.125	79.549	103.652	
Chi-Square		8.991	31.073	6.110	32.094	60.339	
Sig.		.000	.000	.000	.000	.000	
Cox and Snell		.112	.219	.094	.180	.389	
Nagelkerke		.107	.295	.081	.163	.411	
McFadden		.055	.197	.052	.045	.257	

*$p < .05$; **$p < .01$; ***$p < .001$.

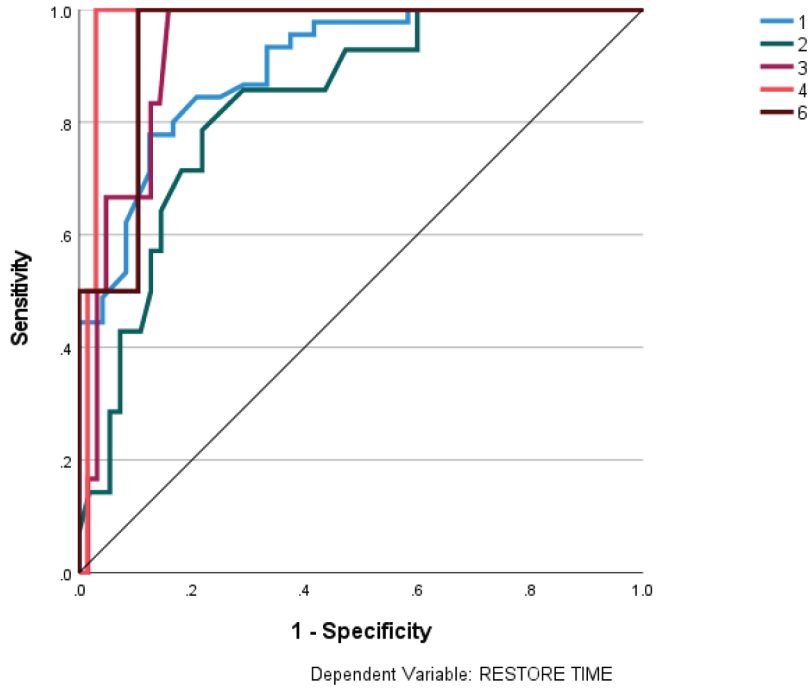

Figure 6. ROC curve for analysis of the robustness of ANN_MLP (RQ2).

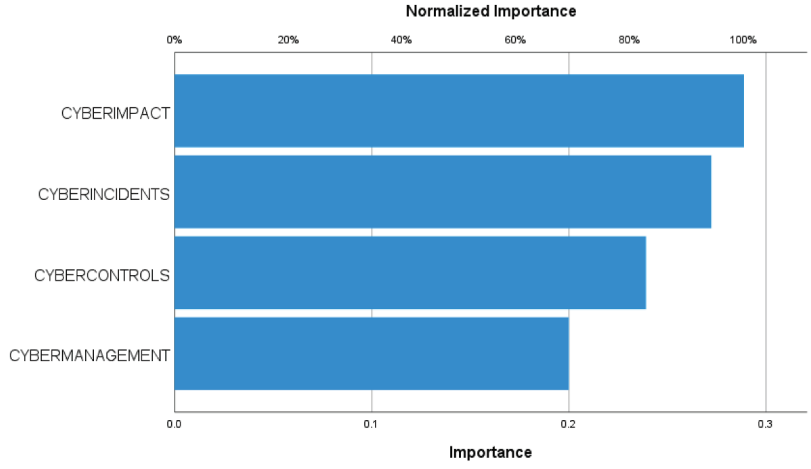

Figure 7. RQ2 normalised importance in recovery time.

Second, regarding SMEs' perception of cybersecurity incidents, the results show limited knowledge of the cybersecurity incidents they received and the impact that these have in economic and management terms. Although the literature pointed out that SMEs are under the threat of cybersecurity incidents, such as data breaches, data destruction, and DoS, which can negatively affect the activities of SMEs,[23,35,49,50] our results show myopia in terms of cybersecurity incidents and impact. This corroborates previous works that indicate how SMEs underestimate cybersecurity threats, considering that the attacks are not directed at them due to their smaller size.[12,23,49] Moreover, we want to highlight that from the responses received, the cybersecurity incidents have little impact, as shown by the majority of the SMEs in our study, for which the recovery time is less than an hour. This is in contrast to previous works that indicate how cybersecurity incidents produce a significant impact on SMEs, in terms of economic losses, reputation, and business continuity.[36,50]

Regarding the first dimension of cybersecurity resilience (RQ1) which investigates which factors affect the cybersecurity impact in SMEs, the results show that external threats and attacks, and internal capabilities, in

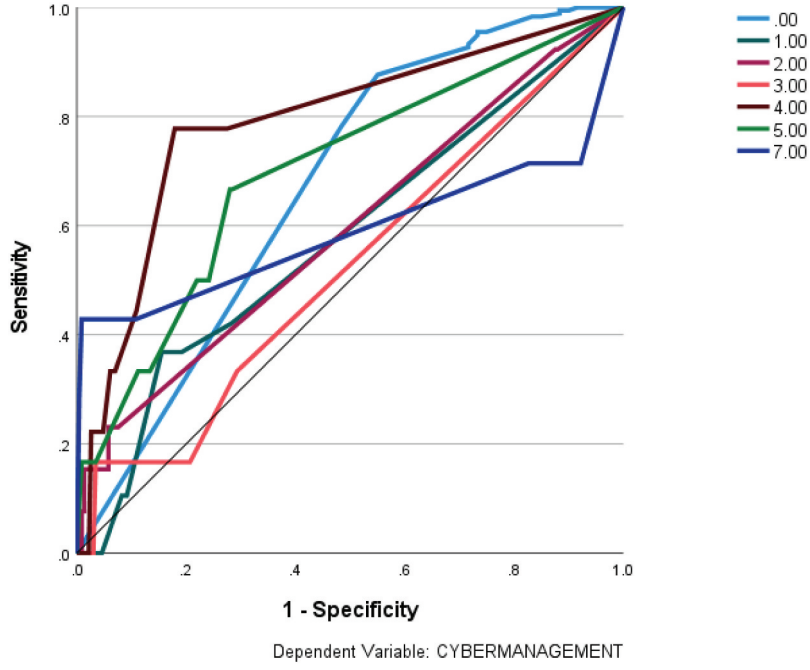

Figure 8. ROC curve for analysis of the robustness of ANN_MLP (RQ3).

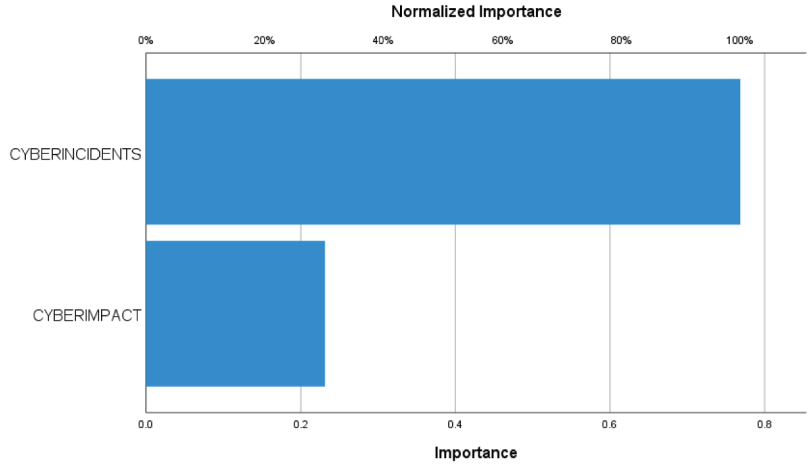

Figure 9. RQ3 normalised importance in cybersecurity management capabilities.

the form of cybersecurity control capabilities, and cybersecurity management capabilities are relevant drivers. In particular, cybersecurity incidents have the highest effect on the cybersecurity impact, in comparison to the internal management of cybersecurity. This highlights the perception of low relevance that SMEs have of protection capabilities against incidents on cybersecurity impact.[51–53] Moreover, also, we see that cybersecurity control capabilities have a higher impact than cybersecurity systems and policies, in line with previous studies that note the negligible role of cybersecurity policies and procedures in SMEs, being almost exclusively the management of cybersecurity focused on mechanisms and operating control procedures.[12,39] Therefore, we can conclude that the cybersecurity impact, as an element of the resilience of the SME, is based on cybersecurity incidents.

Regarding the second dimension of cybersecurity resilience (RQ2), which explores which factors affect the recovery time, the results show that damages produced by the cybersecurity incidents, as well as the cybersecurity incidents themselves, stand out over the rest of the protection capabilities. Moreover, in line with previous literature, we highlight the limited weight that the SME perceives of internal cybersecurity capabilities in recovery time.[12,20,49] Furthermore, we can conclude that the resilience of SMEs is perceived through the degree of severity

of the incidents and their impact, rather than on the firm's management in terms of cybersecurity capabilities.

Finally, the third dimension of cybersecurity resilience, explores how cybersecurity impacts and cybersecurity incidents affect investment in developing cybersecurity capabilities for SMEs. This question engages with the literature on cybersecurity,[54,55] indicating that investment in cybersecurity capabilities in SMEs is affected by cybersecurity incidents and cybersecurity impacts. From our analysis, we consider that this does not occur with the same intensity, since the perception that SMEs have of cybersecurity incidents is greater than the effect of cybersecurity impacts. From these results, we can extend the cybersecurity literature,[51,52,55] pointing out that the severity of the incidents, and the damage produced affect the investment in cybersecurity, but with different intensity. In general, we observe that there is not only interaction between factors, direct and indirect, but also to understand the management of cybersecurity in the SME we must consider the feedback effects between factors, between severity of incidents, cybersecurity impact and cybersystems in the SMEs.

Conclusion

This paper aims to analyze the cybersecurity resilience in SMEs, focusing on three dimensions of resilience such as the ability to work in situations of potential cybersecurity incidents, the ability to recover from those cybersecurity incidents, and finally, the ability to adapt to potential cybersecurity incidents. From our study, we can conclude that the resilience of SMEs is fundamentally affected by cybersecurity incidents, with the cybersecurity impact and cybersecurity capabilities of SMEs being less relevant. In general, we observe the myopia of the SME toward the management of cybersecurity, having as a main challenge the cybersecurity incidents that may occur in the SME.

The paper makes significant contributions in the domain of RBV, offering theoretical and methodological advancements, with practical implications for managers. Firstly, the study validates the application of RBV theory in the context of IT systems, specifically by considering cybersecurity capabilities as organizational capabilities. Additionally, the research extends the RBV theory by emphasizing the crucial role of interactions between cybersecurity capabilities and cybersecurity incidents, and their collective impact on cybersecurity resilience. This highlights the importance of how organizations respond to and recover from cybersecurity challenges. Furthermore, the study reinforces previous findings by demonstrating the effect of cybersecurity capabilities on the performance of SMEs. The paper underscores how investing in and developing cybersecurity capabilities can directly influence the overall performance and success of SMEs in the contemporary digital landscape. In conclusion, the paper offers valuable insights into the RBV theory's application to the IT domain, specifically focusing on cybersecurity capabilities as organizational assets. It also contributes to the advancement of the RBV theory by emphasizing the significance of the interplay between cybersecurity capabilities and incidents in shaping an organization's cybersecurity resilience. Lastly, the study underscores the positive impact of cybersecurity capabilities on the performance of SMEs, emphasizing the importance of investing in cybersecurity measures in today's increasingly interconnected business environment.

From our research, we have identified some contributions to cybersecurity in SMEs. Unlike previous literature that indicated that the SME has scarce resources, which resulted in inadequate cybersecurity management, the findings indicate that the approach of SMEs toward cybersecurity is reactive and short-sighted, which contrasts with the strategic decisions of larger organizations that prioritize prospective, proactive, and anticipatory capacity in their behavior. Consequently, we suggest a series of actions to be taken at the organizational level. Firstly, organizations should involve decision-makers at all levels in updating themselves on cybersecurity matters. For instance, organizations could focus on developing information channels and training programs for senior management to ensure their active participation in cybersecurity management. Secondly, organizations should develop forward-looking systems to proactively identify potential cybersecurity incidents, and business vulnerabilities in the cyber environment. Furthermore, SMEs should consider strengthening the integration of cybersecurity systems and applying routines and procedures that allow proper management of it. The almost exclusive use of the control mechanism is not enough, considering that a high percentage of incidents and vulnerabilities derive from the inappropriate use of policies and procedures by the staff of the SMEs. Therefore, control mechanisms need to be reinforced by involving SMEs in obtaining cybersecurity standards.

From a methodological point of view, we believe that the use of statistical methods, particularly ML techniques, allows us to identify cause-effect relationships between the factors that affect cybersecurity in SMEs. That is, the use of machine learning algorithms is very appropriate in the field of cybersecurity, where the lack of information on the part of firm managers is common, which translates into unbalanced databases, or situations where mutual interactions and correlation problems between variables may exist. In this situation, the combined use of regression methods with ANN allows us to obtain robust models of the relationships between variables.

The present study is not exempt from limitations, despite the robustness of the methodology used. First, the study focused on SMEs in the UK. Future studies could address the study of these same issues in other countries and larger samples, to consider the existence of the geographical scope in the behavior of the SMEs in the management of cybersecurity. Secondly, future studies should extend the understanding of RBV, considering addressing the dynamics of cybersecurity capabilities, taking into account the interaction and feedback of factors such as the severity of incidents, the effectiveness and efficiency of cybersecurity systems, and the perception of the vulnerability of SMEs.

Acknowledgment

We thank Adam Joinson, Joanna Syrda and participants at the Digital Security by Design (DSbD) All Hands events for helpful comments.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The work was supported by the UKRI Discribe Hub+, Digital Security by Design (DSbD) Programme, funded through the Economic and Social Research Council [ES/V003666/1].

References

1. Fernandez de Arroyabe IF, Arranz CF, Arroyabe MF, de Arroyabe JCF. Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: a UK survey for 2018 and 2019. Comput Secur. 2023;124:102954. doi:10.1016/j.cose.2022.102954.
2. Ekelund S, Iskoujina Z. Cybersecurity economics – balancing operational security spending. Inf Technol People. 2019;32(5):1318–42. doi:10.1108/ITP-05-2018-0252.
3. Jalali MS, Siegel M, Madnick S. Decision-making and biases in cybersecurity capability development: evidence from a simulation game experiment. J Strategic Inf Syst. 2019;28(1):66–82. doi:10.1016/j.jsis.2018.09.003.
4. Conteh NY, Schmick PJ. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. Int J Adv Comput Res. 2016;6(23):31–43. doi:10.19101/IJACR.2016.623006.
5. Caldwell T. Plugging the cyber-security skills gap. Comput Fraud Secur. 2013;2013(7):5–10. doi:10.1016/S1361-3723(13)70062-9.
6. Choo KR. The cyber threat landscape: challenges and future research directions. Comput Secur. 2011;30(8):719–31. doi:10.1016/j.cose.2011.08.004.
7. Weishäupl E, Yasasin E, Schryen G. Information security investments: an exploratory multiple case study on decision-making, evaluation and learning. Comput Secur. 2018;77:807–23. doi:10.1016/j.cose.2018.02.001.
8. Srinidhi B, Yan J, Tayi GK. Allocation of resources to cyber-security: the effect of misalignment of interest between managers and investors. Decis Support Syst. 2015;75:49–62. doi:10.1016/j.dss.2015.04.011.
9. Wright RT, Jensen ML, Thatcher JB, Dinger M, Marett K. Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. Inf Syst Res. 2014;25(2):385–400. doi:10.1287/isre.2014.0522.
10. Mallinder J, Drabwell P. Cyber security: a critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber-attack. J Bus Contin Emer Plan. 2014;7:103–11.
11. Cucoranu IC, Parwani AV, West AJ, Romero-Lauro G, Nauman K, Carter AB, Balis UJ, Tuthill MJ, Pantanowitz L. Privacy and security of patient data in the pathology laboratory. J Pathol Inform. 2013;4(1):4. doi:10.4103/2153-3539.108542.
12. Fernandez De Arroyabe I, Fernandez de Arroyabe JC. The severity and effects of cyber-breaches in SMEs: a machine learning approach. Enterp Inf Syst. 2023;17(3):1942997. doi:10.1080/17517575.2021.1942997.
13. European Commission. The digital economy and society index (DESI). 2020. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72352.
14. Hayes J, Bodhani A. Cyber security: small firms under fire. Eng Technol. 2013;8(6):80–83. doi:10.1049/et.2013.0614.
15. Osborn E. Business versus technology: sources of the perceived lack of cyber security in SMEs. CDT Technical Paper 01/15. University of Oxford; 2015.
16. Ponsard C, Grandclaudon J, Dallons G. Towards a cyber security label for SMEs: a European perspective. Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018). Funchal - Madeira, Portugal: Science and Technology Publications; 2018. p. 426–431.
17. Valli C, Martinus IC, Johnstone MN. Small to medium enterprise cyber security awareness: an initial survey of Western Australian business. Proceedings of International Conference on Security and Management. Las Vegas, USA: CSREA Press; 2014. p. 71–75.
18. NIST. Glossary. Computer security resource center (CSR). National Institute for Standards and Technology; 2023. https://csrc.nist.gov/glossary/term/cyber_resiliency.
19. DCMS. Cyber security breaches survey 2021. 2021. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021.
20. Benaroch M. Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. Inf Syst Res. 2018;29(2):315–40. doi:10.1287/isre.2017.0714.
21. Shin YY, Lee JK, Kim M. Preventing state-led cyberattacks using the bright internet and internet peace principles. J Assoc Inf Syst. 2018;19(3):152–81. doi:10.17705/1jais.00488.
22. Renaud K, Ophoff J. A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. Organ Cybersecur J. 2021;1(1):24–46. doi:10.1108/OCJ-03-2021-0004.

23. Mayadunne S, Park S. An economic model to evaluate information security investment of risk-taking small and medium enterprises. Int J Prod Econ. 2016;182:519–30. doi:10.1016/j.ijpe.2016.09.018.
24. Bharadwaj AS. A resource-based perspective on information technology capability and firm performance: an empirical investigation. MIS Q. 2000;24(1):169–96. doi:10.2307/3250983.
25. Cavusoglu H, Cavusoglu H, Son JY, Benbasat I. Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources. Inf Manage. 2015;52(4):385–400. doi:10.1016/j.im.2014.12.004.
26. Alpaydin E. Machine learning. The MIT Press; 2021. doi:10.7551/mitpress/13811.001.0001.
27. Paliwal M, Kumar UA. Neural networks and statistical techniques: a review of applications. Expert Syst Appl. 2009;36(1):2–17. doi:10.1016/j.eswa.2007.10.005.
28. Warkentin M, Johnston AC, Walden E, Straub DW. Neural correlates of protection motivation for secure IT behaviors: an fMRI examination. J Assoc Inf Syst. 2016;17(3):194–211. doi:10.17705/1jais.00424.
29. Teece DJ. The foundations of enterprise performance: dynamic and ordinary capabilities in an (economic) theory of firms. Acad Manage Perspect. 2014;28 (4):328–52. doi:10.5465/amp.2013.0116.
30. Suddaby R, Coraiola D, Harvey C, Foster W. History and the micro-foundations of dynamic capabilities. Strateg Manag J. 2020;41(3):530–56. doi:10.1002/smj.3058.
31. Grant RM. Toward a knowledge-based theory of the firm. Strateg Manag J. 1996;17:109–22. doi:10.1002/smj.4250171110.
32. Barney J. Firm resources and sustained competitive advantage. J Manage. 1991;17(1):99–120. doi:10.1177/014920639101700108.
33. Peteraf M. The cornerstones of competitive advantage: a resource-based view. Strateg Manag J. 1993;14:179–91. doi:10.1002/smj.4250140303.
34. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. J Med Internet Res. 2018;20(5):e10059. doi:10.2196/10059.
35. Jensen ML, Dinger M, Wright RT, Thatcher JB. Training to mitigate phishing attacks using mindfulness techniques. J Manage Inf Syst. 2017;34(2):597–626. doi:10.1080/07421222.2017.1334499.
36. ENISA. ENISA threat landscape 2020: cyber attacks becoming more sophisticated, targeted, widespread and undetected. European Union Agency For Cybersecurity; 2020. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends.
37. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — information security controls. Geneva: ISO/IEC; 2022.
38. Bose R, Luo X, Liu A. Investigating security investment impact on firm performance. Int J Account Inf Manag. 2014;22(3):194–208. doi:10.1108/IJAIM-04-2014-0026.
39. ISO. ISO/IEC 27001: 2017 - information security management. ISO/IEC; 2016. http://www.iso.org/iso/iso27001 .
40. ISO/IEC 15408-1:2009. Information technology – security techniques – evaluation criteria for IT security – Part 1: introduction and general model. ISO/IEC; 2018. https://www.iso.org/standard/50341.html.
41. Rakas SB, Timcenko V, Kabovic M, Kabovic A. Cyber security issues in conductor temperature and meteorological measurement based DLR system. Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion (MedPower 2016). Belgrade (Serbia): IET; 2016. p. 1–7.
42. Couce-Vieira A, Insua DR, Kosgodagan A. Assessing and forecasting cybersecurity impacts. Decis Anal. 2020;17(4):356–74. doi:10.1287/deca.2020.0418.
43. Forbes Insights. The reputational impact of it risk. FALLOUT; 2014. https://images.forbes.com/forbesinsights/StudyPDFs/IBM_Reputational_IT_Risk_REPORT.pdf.
44. Podsakoff PM, MacKenzie SB, Lee JY, Podsakoff NP. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J Appl Psychol. 2003;88(5):879. doi:10.1037/0021-9010.88.5.879.
45. Wang Q. Artificial neural networks as cost engineering methods in a collaborative manufacturing environment. Int J Prod Econ. 2007;109(1):53–64. doi:10.1016/j.ijpe.2006.11.006.
46. Ciurana J, Quintana G, Garcia-Romeu ML. Estimating the cost of vertical high-speed machining centres, a comparison between multiple regression analysis and the neural networks approach. Int J Prod Econ. 2008;115(1):171–78. doi:10.1016/j.ijpe.2008.05.009.
47. Yegnanarayana B. Artificial neural networks. New Delhi (India): PHI Learning Pvt. Ltd; 2009.
48. Ibrahim OM. A comparison of methods for assessing the relative importance of input variables in artificial neural networks. J Appl Sci Res. 2013;9:5692–700.
49. Kabanda S, Tanner M, Kent C. Exploring SME cybersecurity practices in developing countries. J Organ Comput Electron Commerce. 2018;28(3):269–82. doi:10.1080/10919392.2018.1484598.
50. Benz M, Chatterjee D. Calculated risk? A cybersecurity evaluation tool for SMEs. Bus Horiz. 2020;63(4):531–40. doi:10.1016/j.bushor.2020.03.010.
51. Menard P, Bott GJ, Crossler RE. User motivations in protecting information security: protection motivation theory versus self-determination theory. J Manage Inf Syst. 2017;34 (4):1203–30. doi:10.1080/07421222.2017.1394083.
52. Posey C, Roberts TL, Lowry PB. The impact of organizational commitment on insiders' motivation to protect organizational information assets. J Manage Inf Syst. 2015;32(4):179–214. doi:10.1080/07421222.2015.1138374.
53. Chan M, Woon IMY, Kankanhalli A. Perceptions of information security at the workplace: linking information security climate to compliant behavior. Int J Inf Privacy Secur. 2005;1(3):18–41. doi:10.1080/15536548.2005.10855772.
54. Vance A, Siponen M, Pahnila S. Motivating is security compliance: insights from habit and protection motivation theory. Inf Manage. 2012;49(3–4):190–98. doi:10.1016/j.im.2012.04.002.
55. Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur. 2012;31(1):83–95. doi:10.1016/j.cose.2011.10.007.

Annex

Table A1. Steps of the ANN design.

1. Choice of the ANN typology	• We choose the ANN architecture with Multilayer Perceptron (MLP)
2. Design of architecture of ANN-MLP	• The network accuracy and efficiency are dependent on various parameters: hidden nodes, activation functions, training algorithm parameters and characteristics such as normalization and generalization. • The number of inputs and outputs is given by the number of available input and output variables. • The number and size of hidden layers are determined by testing several combinations of the number of hidden layers and the number of neurons. • The types of activation functions, for the hidden layer, we can use sigmoid logistic (values from 0 to 1), hyperbolic tangent (−1 to 1), and softmax function for the activation function of the output layer.
3. Choice of the learning algorithm	• We are going to use Backpropagation. This learning algorithm determines the connection weights of each neuron, readjusting the weights and minimizing the error.
4. Learning stage	• To avoid problems of overfitting and consumption of processing time, we divided the sample randomly into three subsamples (training, testing and holdout). • In the training stage, the weights and links between nodes are determined, to minimize the error. In the validation stage, the generalizability of the obtained architecture is checked. Lastly, the holdout data is used to validate the model.