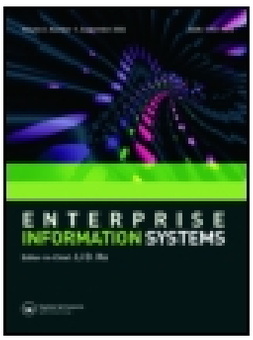

Enterprise Information Systems

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/teis20

The severity and effects of Cyber-breaches in SMEs: a machine learning approach

Ignacio Fernandez De Arroyabe & Juan Carlos Fernandez de Arroyabe

To cite this article: Ignacio Fernandez De Arroyabe & Juan Carlos Fernandez de Arroyabe (2021): The severity and effects of Cyber-breaches in SMEs: a machine learning approach, Enterprise Information Systems, DOI: 10.1080/17517575.2021.1942997

To link to this article: https://doi.org/10.1080/17517575.2021.1942997

Published online: 30 Jun 2021.

ENTERPRISE INFORMATION SYSTEMS
https://doi.org/10.1080/17517575.2021.1942997

Taylor & Francis
Taylor & Francis Group

The severity and effects of Cyber-breaches in SMEs: a machine learning approach

Ignacio Fernandez De Arroyabe[a,b] and Juan Carlos Fernandez de Arroyabe[c]

[a]Data Services, Commercial Banking, Lloyds Banking Group, UK; [b]Cyber Security Centre, Warwick Manufacturing Group (WMG), University of Warwick, UK; [c]Essex Business School, University of Essex, Elmer Approach, Southend-on-Sea, UK

ABSTRACT

In this paper, we investigate cyber breaches and their effects on small and medium enterprises (SMEs), considering the role that cybersecurity plays in SMEs, and the importance that SMEs have in the economy. Using the Cyber Security Breaches Survey data, the first contribution extends previous works confirming that SMEs receive a wide variety of breaches. Secondly, we have characterized the degree of severity of breaches in SMEs, based on disruption time and their cost. Our last contribution consists of determining the effect and severity of breaches in SMEs in terms of economic, financial and management impacts.

ARTICLE HISTORY
Received 4 December 2020
Accepted 10 June 2021

KEYWORDS
Cyber breaches; *smes*; *severity*; *effects*; *artificial neural network*

1. Introduction

The study of cyber breaches and their effect on companies has become a critical element in businesses' strategic management (Lezoche and Panetto 2020; Ashibani et al., 2017; Chronopoulos, Panaousis, and Grossklags 2018; Fielder, 2016). This is because, not only does the impact of an attack affect a company in terms of information systems (IS), but also the protection of cybersecurity is increasingly highlighted in terms of business continuity, company reputation, repercussions to supply chains, as well as legal implications. Moreover, companies are developing indicators and metrics for assessing their level of protection and the probability of suffering a cyber breach as an element that has a significant impact on the economic and financial reputation of the business[1] (see, for example, Pirounias, Mermigas, and Patsakis 2014).

In this context, the literature has addressed the analysis of breaches generated in companies, as well as the effect on those companies (Heartfield et al. 2018; Conteh and Schmick 2016; Gatrner Group 2014). Despite these important contributions, the relationship between breaches and their potential impact on companies has generated diverse and inconclusive results (see, for example, Couce-Vieira, Insua, and Kosgodagan 2020). This is due to several reasons. First, it is problematic to identify breaches in companies (Bland et al. 2020; Wang and Zhang 2020; Seibold et al. 2020; Sahoo and Gupta 2019; Heartfield et al. 2018; Choo 2011). Most of the existing research has focused on

CONTACT Juan Carlos Fernandez de Arroyabe jcfern@essex.ac.uk Essex Business School, University of Essex, Elmer Approach, Southend-on-Sea, UK

investigating a certain typology of attacks and on studying cases of companies, without considering a wider spectrum of possible types of attacks that companies may receive (Garre, Pérez, and Ruiz-Martínez 2021; Dahiya and Gupta 2020). Second, the study of cyber-breach impact has been limited to a purely technical and operational aspect, with few studies that have considered other types of impacts on companies (for example, economic, financial and management) (Couce-Vieira, Insua, and Kosgodagan 2020). This has occurred due to the low permeability of cybersecurity management in companies,[2] which, derived from its complexity and technical specificity, makes it difficult for company managers to get involved (Ahmad et al. 2019; Cavusoglu et al. 2015; Srinidhi, Yan, and Tayi 2015).

In this paper, we will investigate this gap, studying cyber breaches and their impact on companies. To do this, we make various assumptions in terms of defining the framework of our research. First, we assume that there is a wide spectrum of cyber breaches in companies, and, therefore, variability in the types of effect they produce. Unlike previous studies, the methodology followed in this paper is based on the statistical analysis of the types of breaches and their effect on companies. Second, we will study the case of small and medium-sized enterprises (SMEs), covering a gap in the literature that has mainly focused on large companies (Ponsard, Grandclaudon, and Dallons 2018; Osborn 2015; Valli, Martinus, and Johnstone 2014; Hayes and Bodhani 2013). SMEs are known to play a key role in the global economy. For example, in European countries, they employ two thirds of the workforce and generate around 60% of the GDP (Müller, Buliga, and Voigt 2018). Moreover, SMEs have had little coverage in terms of cybersecurity compared with large companies (Osborn 2015), even though approximately 72% of breaches occur in SMEs (Fielder et al. 2016). These attacks, depending on the severity, generate disruptions in SMEs, which can affect business operations and prevent staff from carrying out their daily work, to the extent that 60% of small companies cannot maintain their business six months after a cyberattack (Aguilar 2015). Third, this paper conducts a cause-effect analysis from a methodological point of view (Somya Sahoo and Gupta 2019). To do this, using artificial neural networks (ANNs) for the prediction and simulation, we establish the relationship between breaches and their effects in SMEs. Machine learning methodology permits the analysing of multiple business and management research questions, in which the multiplicity of interactions and complexity are their main characteristics (Arranz and Fernandez de Arroyabe 2010; Somers and Casal 2009). This is the case in the management of cybersecurity in companies, in which the breaches have multiple consequences for these companies, involving multiple interactions between variables (Couce-Vieira, Insua, and Kosgodagan 2020). Moreover, previous studies on cybersecurity in companies relied on survey data, which is characterised by a low response rate, because of the difficulty of identifying both attacks and threats and the impact on companies (Cyber Security Breaches Survey 2017). In this sense, the use of methods with a high level of robustness, such as machine learning ones, allows us to build a causal relationship in cases with a low response (Minbashian, Bright, and Bird 2010; Somers and Casal 2009).

Therefore, our research question investigates breaches and their effects on SMEs. To do this, we will first analyse *the severity of breaches in SMEs*. After characterising the typology of the breaches, we will consider their degree of severity, measuring them in terms of disruption time and estimated cost for the companies. The first question (RQ1) is: *How do breaches affect SMEs in terms of severity?* Second, we will establish a causal relationship

between breaches and their effects on SMEs. Unlike previous works, which have focused exclusively on the results of breaches, in terms of damage to software or the destruction and alteration of data (Dahiya and Gupta 2020), we consider that SMEs have both the capacity to react and decide on when they face breaches. Following Couce-Vieira, Insua, and Kosgodagan (2020), the impact of breaches will not only be analysed in terms of damage to the information system (IS) infrastructure but also in terms of the economic, financial and management impact for SMEs. Therefore, our second research question (RQ2) is: *What is the impact of breaches in SMEs?* For the empirical study, we make use of the Cyber Security Breaches Survey data, which collects information on the management of cybersecurity in UK companies (Cyber Security Breaches Survey 2016, 2017). This survey contains data on the breaches suffered by companies, the security measures they used, as well as the outcome of the breaches. The final sample consists of 1,348 UK SMEs in the period 2016–2017.

2. Method

2.1 Conceptual background

Information system (IS) security can be defined as a set of measures, strategies and methodologies targeted at alleviating the risks and vulnerabilities of the information systems (ISO/IEC 2014; CLUSIF 2008). Organizations make use of IS security to prevent or minimise the impact of attacks[3] and threats on the IS. The ENISA (2018) defines a cyber breach as a violation of the security policy of a system to affect its integrity or availability, leading to unauthorised access or attempted access to a system.

The typology of breaches is very diverse considering the variety of attacks that companies can receive. We can find a wide typology of attacks, as these are intensifying, diversifying and becoming more sophisticated (Mendhurwar and Mishra 2019; Contech and Schimick, 2016; Mallinder and Drabwell 2014). Moreover, the ways in which cyber-attacks occur are varied, depending on the objectives, who produces them or the method of execution. In general, in the literature, we can find external attacks carried out by different types of adversaries,[4] from phishing, malware or web attacks, to the exploitation of vulnerabilities derived from the incorrect use of IS in the company. For example, the latest ENISA report identifies 15 categories of attacks and breaches for cyberspace (ENISA 2020), among which the following stand out: 1) malware or malicious software, which is responsible for 30% of all registered cyberattacks, with consequent damage to the operation of the companies' IS; 2) attacks on websites and domains, aiming to steal personal information or bank details from users; 3) phishing, which is widely used and seeks to supplant identity (of a trusted or legitimate third party) in order to both steal personal information and deploy malware; and 4) data breaches, which are the result of cyberattacks that lead to the loss or theft of data. In addition to these external attacks, we must consider the *insider threat*, which can come from the misuse that the company's staff makes of the IS, either voluntarily or involuntarily, causing a security breach. ENISA (2020) highlights the importance of this type of threat, noting that 77% of company data breaches are caused by internal threats.

Moreover, in addition to the typology of breaches, a complete characterisation of them in terms of their effect on companies requires the analysing of the frequency of their

occurrence. At first sight, a more exposed company will receive more attacks and, as a consequence, greater potential damage to the company is to be expected; however, this is not always the case. CLUSIF (2008) point out that while approximately 80% of breaches exploit common vulnerabilities, only 5% to 10% of the attacks present serious risks for organisations (Gatrner Group 2014). Moreover, Cohen (1997) and Choo (2011) pointed out that the most infrequent attacks are those that do the most damage to companies. Therefore, this means variability in effects on organisations, considering both the degree of exposure of the company and the severity of the breaches. Jeong, Lee, and Lim (2019) point out that organisations could reduce the investment in security systems by assessing and ranking the frequency and severity of the risks.

2.2 SMEs and cybersecurity

The internet has become the most important asset of SMEs for their businesses (Müller, Buliga, and Voigt 2018). Thus, SMEs develop their businesses through the internet, which, together with the main characteristics of SMEs, such as a high degree of flexibility in adapting to the client, multitasking staff and a focus on the innovative development of products or services, increases their competitiveness. The internet, however, also brings some negative aspects, such as the higher exposure of SMEs' IS to attacks and threats of the internet space (Osborn 2015).

Regarding the relationship between SMEs and cybersecurity, this can be described as controversial (Ponsard, Grandclaudon, and Dallons 2018; Osborn 2015; Sangani and Vijayakumar 2012). First, most small and medium-sized businesses feel that IS security is not their primary concern, which is reflected in minimal annual cybersecurity budgets (Osborn 2015). This is due to the fact that SME managers evaluate that the level of risk is very low as compared with large companies, therefore having a false sense of security (Osborn 2015; Valli, Martinus, and Johnstone 2014). Moreover, in most situations, Osborn (2015) finds that SMEs do not have clear steps to implement cybersecurity processes due to the diversity and number of devices,[5] which, together with low adherence to procedures and standards, makes the implementation of standards an impossible task (Ponsard, Grandclaudon, and Dallons 2018; Sangani and Vijayakumar 2012).

However, the literature shows that SMEs have a high level of risk, noting that approximately more than half of attacks are directed at them (Aguilar 2015; Osborn 2015). Hayes and Bodhani (2013) point out that the main reason for this is that SMEs are easy targets with a good value versus risk ratio, and therefore they receive a variety of attacks. First, SMEs are falling victim to automated attacks as a result of their online presence. These usually consist of phishing (or *spear-phishing*) emails to lure victims to fake sites that will instal malware (Wright et al. 2014). There are also botnet infections, where devices in SMEs get infected and become part of a botnet controlled by a command and control (C&C) server (Garre, Pérez, and Ruiz-Martínez 2021). Second, SMEs receive attacks as inputs to larger targets (Ponsard, Grandclaudon, and Dallons 2018; Sangani and Vijayakumar 2012). That is, the adversaries know that there is the possibility that smaller partners are the weakest link to get to a larger organisation, as information exchanges can spread across several entities – for example, when these SMEs are a supplier of large companies (Sung, Kim, and Chang 2018). Finally, another type of attack is based on the use that SMEs make of their computing resources (Jang-Jaccard and Nepal 2014). As we have previously

pointed out, since SMEs do not consider themselves to be a target of computer attacks, they neglect procedures, implementation and awareness of possible attacks, allowing adversaries to exploit the vulnerabilities of these companies.

2.3 Research model

As mentioned above, our research looks at both breach types and their effect on SMEs. Based on a cause-effect analysis, our research model is shown in Figure 1.

- First, after identifying the type of breaches suffered by SMEs, we will determine the *severity of the breaches*.[6] As we have previously pointed out, we consider that not all breaches have the same degree of severity for the company. To estimate severity, the literature uses two types of variables (Conteh and Schmick 2016; Heartfield et al. 2018). The first is the service replacement time (*disruption time*), with the most severe attacks being those that require the most time to normalise the service in the company. The second is the *cost of the breaches* for the firm. Couce-Vieira, Insua, and Kosgodagan (2020) and the Cyber Security Breaches Survey (2017) pointed out that the cost of breaches[7] includes estimates of the lost business costs, improvements and implementation of software, and systems costs, and extra expenses on staff and expert advice costs.
- Second, regarding the *effect that breaches* have on SMEs, following Couce-Vieira, Insua, and Kosgodagan (2020), we consider that these have *economic, financial and management implications* for the company. Thus, financial and economic cost implications range from the loss of revenue, or the increase in costs as a consequence of hiring additional staff, to implications in the image and management of the company, such as the need to inform customers or stakeholders, or the introduction of new measures needed to prevent or protect against future breaches. Additionally, Couce-Vieira, Insua, and Kosgodagan (2020) pointed out that breaches have an impact on other types of intangible assets such as corporate reputation. For example, a Forbes Insights (2014) report indicates that 46% of organisations had suffered reputational and brand equity damage as a result of an attack. Moreover, Couce-Vieira, Insua, and Kosgodagan (2020) pointed out that the impact of breaches not only affects the company but also has implications for its stakeholders, highlighting the importance of knowing how to correctly manage the information transmitted to customers and shareholders. Also, Ekelund and Iskoujina (2019) highlight the

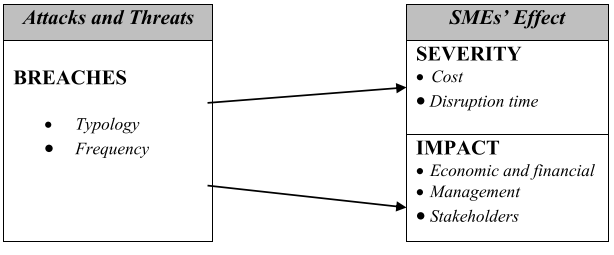

Figure 1. Research model: breaches and the effect in the SMEs.

responsibility that companies have to their clients and to the administration, which can translate into compensation and associated costs.[8] Therefore, breaches not only have economic, financial and management implications for the company but also the firm's environment can be threatened by its practices, and by how the company manages its cybersecurity.

2.4 Empirical study

2.4.1. Survey

In this study, the unit of analysis is the firm, and the data is collected from the Cyber Security Breaches Survey (2016, 2017). The Cyber Security Breaches Survey is a survey of UK firms, commissioned by the Department for Culture, Media and Sport (DCMS), which is part of the National Cyber Security Programme. The data was collected by Ipsos MORI, together with the Institute for Criminal Justice Studies at the University of Portsmouth, following the standard of the Code of Practice for Official Statistics.

The sample was obtained using the government's Inter-Departmental Business Register (IDBR), which includes UK firms across all sectors and is the main source for government surveys at the firm level and the compilation of national statistics. The final sample consisted of 1,348 UK SMEs. A random probability telephone survey of UK businesses was undertaken from 24 October 2016 to 11 January 2017[9] .

The survey was designed to collect information about a range of topics related to cybersecurity. First, the survey asked about firms' perception of cybersecurity; for example, their approach to the management of cybersecurity risks, their level of awareness, their attitude towards cybersecurity, their perception on the information and guidance available on cybersecurity, and the reasons why managers thought cybersecurity was important. Second, the survey covered topics related to firms' own experiences with cybersecurity; for example, their previous experiences with cybersecurity breaches, the impact and nature of these breaches, and their managerial approach and expenditures on cybersecurity.

The questionnaire was developed by Ipsos MORI and the Institute for Criminal Justice Studies (ICJS) in three stages: The first stage consisted of a stakeholder workshop and interviews involving Government, business and cyber security provider representatives across 13 organisations.[10] The objective of this stage was to clarify the key cyber security issues facing businesses today. The second stage consisted of cognitive testing interviews with 10 businesses. This stages was intended to test comprehension of the new questions for 2017 and any technical terms used (e.g. ransomware). The last stages was a pilot survey, consisting of 30 interviews.

2.4.2. Measures

The first group of variables identifies the types of breaches in companies. To do this, and in line with our research model (Figure 1), we use two variables: *typology* and *frequency of the breaches*.

- The first variable measures the *typology of the most frequent breaches* (BREACHES) in companies. The questionnaire considers that breaches can be produced both by

external hacker attacks through malware, phishing or spam, as well as by insider incidents derived from the incorrect use of information systems or sabotage situations. The Cyber Security Breaches questionnaire asks the following question: *Have any of the following happened to your organisation in the last 12 months?* The questionnaire measures this variable with eight items (see Table).

- The second variable measures the *frequency* (FREQUENCY) of the occurrence of breaches in companies. For this, the questionnaire asks the following question: *Approximately, how often in the last 12 months did you experience any of the cybersecurity breaches or attacks you mentioned?* Table shows the results of the survey.

The second group of variables measures the *severity of the breaches*. For this, and in line with the literature, we have used three variables:

- The first variable is a subjective measure of the company's perception of the *most disruptive breach* based on the breach's typology, as defined in the questionnaire. To do this, the questionnaire asks the following question: *I would like you to think about the one cybersecurity breach, or related series of breaches or attacks, that caused the most disruption to your organisation in the last 12 months*. Table collects the results of the responses.
- The second variable measures the severity of the breaches by the *time of disruption* (TIME), in which the firms recover their services. The questionnaire asks the following question: *As far as you know, how long was it, if any time at all, between this breach or attack occurring and is it identified as a breach?* The answers are displayed in Table.
- The last variable measures the *cost of cybersecurity breaches* (COSTS) for firms. The questionnaire asks the following question: *Approximately how much, if anything, do you think the cybersecurity breaches or attacks you have experienced in the last 12 months have cost your organisation financially?* This includes both direct and indirect costs or damages. Table shows the distribution of expenses based on the number of SMEs.

The last variable measures the *impact of the breaches* in SMEs. With this variable, we measure the impact of breaches on the company in financial, management and economic terms, also considering the responsibility that the firm has to its environment.

- Regarding the measurement of the *impact of breaches* (IMPACT) on SMEs, the questionnaire asks the following multi-item question (Table): *And have any of these breaches or attacks impacted your organisation in any of the following ways?*

2.4.3. Robustness of survey

Following the method of Podsakoff et al. (2003), the robustness of the survey has been tested through the common method variance (CMV). This analysis reveals six distinct latent constructs that account for 69.02% of the variance. The first factor accounts for 17.35% of the variance, which is below the recommended limit of 50%. This result suggests CMV is not a concern in the results of our survey.

2.4.4. ANN: procedure and design

In this paper, we estimate the research models, using an artificial neural network (ANN). This statistical model mimics biological neural networks to model complex patterns and prediction problems, allowing the analysis and prediction of complex relationships (non-linear and multiple interactions) in causal studies (Arranz and Fernandez de Arroyabe 2010; Somers and Casal 2009). The ANNs are models that employ parallel information-processing structures for interpreting outcomes. At the same time, they are capable of adjusting their framework to increase the reliability of the model (Minbashian, Bright, and Bird 2010).

Regarding the typology of ANNs, for this application, we have used the multilayer perceptron (MLP) (Figure 2). Given the particular purposes of the application, the MLP model usually leads to the most satisfactory results, as reported in Bourilkov (2019). In MLP, neurons are organised in several layers, the first one being the input layer and the last one the output layer. Between input and output layers there could be several other hidden layers (Figure 2). The number of hidden layers has an important role in determining the generalisation ability of the MLP (Minbashian, Bright, and Bird 2010).

For the ANN-MLP design procedure, we propose five steps to design the ANN-MLP architecture, following the works of Wang (2007) and Ciurana, Quintana, and Garcia-Romeu (2008), as can be seen in Table 1.

Regarding the design of the ANN-MLP architecture for the analysis, we have established the following causal models with the objective to answer the research questions (RQs) posed.

- *Research question (RQ1)*: Model 1 determines the *severity* of breaches in SMEs. As an input variable we have the *breaches typology* (BREACHES), and as an output variable both the *cost of the breaches* (COSTS) and the *disruption time* (TIME).
- *Research question (RQ2)*: Model 2 simulates the *impact of breaches* (IMPACT) in SMEs. The input variable is the *breaches typology* (BREACHES) and the output variable the *impact* of the breaches (IMPACT).

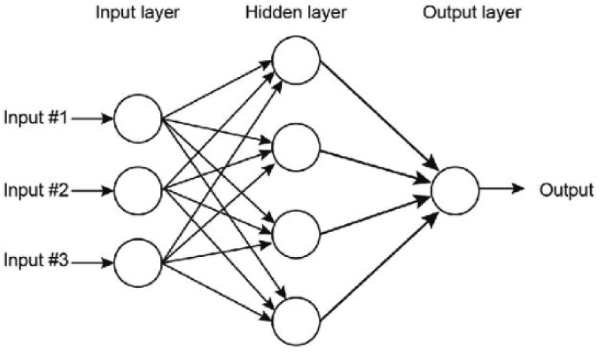

Figure 2. ANN Multilayer Perceptron (MLP) architecture. Source: Manning, Sleator, and Walsh (2014)

Table 1. Steps of the ANN-MLP procedure.

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 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 used a sigmoid logistic (values from 0 to 1) and a hyperbolic tangent (-1 to 1), and an identity function for the activation function of the output layer.
3. Choice of the learning algorithm	• We are going to use is 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.
4. Sensitive analysis	• A sensitive analysis is developed to quantify the influence of each input variable on the output variables.

Source: Arranz, Arguello, and Fernandez de Arroyabe (2021)

Following Wang (2007), and Arranz and Fernandez de Arroyabe (2010), this paper uses a trial and error procedure for the design of the ANN-MLP architecture. The structure has been selected after having tested the ANN-MLP configurations with a different number of hidden layers, different number of neurons for each level, and different activation functions. While the number of inputs and outputs of the proposed network is given by the number of available input and output variables, the number and size of hidden layers is determined by testing several combinations of the number of hidden layers and the number of neurons. Master (Masters 1993) and Bishop (1995) pointed out that the choice of an appropriate number of hidden neurons is important; if too few are used there would be few resources to solve the adjustment problem while the use of too many neurons would increase the training time and will cause over-fitting. In general, experimentation with different numbers of hidden layers and different units is the most common method, existing certain rules to limit the number of experiments. In this line, Ciurana, Quintana, and Garcia-Romeu (2008) and Mohrotra (1997) pointed out that for a function approximation a two-layer neural network is usually sufficient, to accurately model any type of function. Regarding the number of neurons in each hidden layer, Hegazy et al. (1994) proposed that the number of neurons should be 0.75 m or m, where m is the number of input neurons. Master (Masters 1993) established a rule that is based on the combination of input and output neurons. As a criterion, the number of units in the hidden layer should not exceed the number of input variables (Bishop 1995). An extremely small number of units in the hidden layer compared to the number of input variables does not usually give a good result (Masters 1993; Bishop 1995).

The results of the two architectures for the two models are shown in Table 2. For example, for Model 1, the structure is 9-7-7, which means that there are 9, 7 and 7 neurons in the input, hidden and output layers respectively. For the hidden layer, the activation function was the hyperbolic tangent and for the output layer the identity function was employed. In Table 3, we show the various experiments. The initial criteria were to experiment with both one hidden layer and two hidden layers, and a maximum number of units in each hidden layer equal to the number of variable inputs.

3. Results and discussion

In terms of descriptive analysis, the sample is composed of 1,348 SMEs, of which 37.52% of the firms included have less than nine employees; a similar percentage (35.5%) corresponds to firms with ten to 49 employees, and 26.9% from 50 to 249 employees. For the online services offered by the sampled companies, the questionnaire divides them into seven different categories, from emails, websites and social media sites to bank accounts

Table 2. ANN-MLP architecture for interaction analysis.

Model	Output variable	ANN architecture	Activation Functions	Error
Model 1	Severity of the Breaches	9-7-7	• Hyperbolic tangent • Identity	Sum-Square
Model 2	Impact of the Breaches	9-9-11	• Hyperbolic tangent • Identity	Sum-Square

Table 3. Design of ANN-MLP architecture*.

Number of Hidden Layer		1				2															
Number of Neurons	Hidden Layer 1	9	8	7	6	9				8				7				6			
	Hidden Layer 2	-	-	-	-	9	8	7	6	9	8	7	6	9	8	7	6	9	8	7	6
Error % (Disruption Time)		24.8	24.2	23.8	24.5	26.0	25,4	26.9	27.2	27.1	27.7	27.9	28.2	31.4	31.9	31.5	33.4	36.8	36.1	35.4	36.2
Error (Costs)		.429	4.03	.383	.399	.550	.553	.589	.601	.538	.524	.670	.689	.663	.691	.704	.752	.673	.698	.739	.733

*This table has been obtained with hyperbolic tangent and softmax as activation functions

Table 4. Identification of breaches in SMEs*.

Variable	Typology of Breaches	Count	%
BREACHES 1	Computers becoming infected with ransomware	141	10.5
BREACHES 2	Computers become infected with other viruses, spyware or malware	234	17.4
BREACHES 3	Attacks that try to take down your website or online services	60	4.5
BREACHES 4	Hacking or attempted hacking of online bank accounts	48	3.6
BREACHES 5	People impersonating your organisation in emails or online	238	17.7
BREACHES 6	Staff receiving fraudulent emails or being directed to fraudulent websites	492	36.5
BREACHES 7	Unauthorised use of computers, networks or servers by staff, even if accidental	39	2.9
BREACHES 8	Unauthorised use or hacking of computers, networks or servers by people outside your organisation.	66	4.9

*Total: 1,348 SMEs

for the clients. In general, the majority of the sampled firms provide online services that relate to emails (93.2%), followed by websites (86.1%), online bank payments (72.1%) and, to a lesser extent, the development of digital marketing via social network sites (59.1%). Finally, the results show a low level of activity of the sampled companies in online ordering, and paying or booking services (26.7%). In order to analyse the degree of integration for firms in the use of online services, the results show that in most cases, around 80% of the sample, companies simultaneously use between three and five online services. In particular, the use of email, websites, online bank payment and social network sites is evident in 34.1% of the firms. Moreover, we have performed an analysis of variance (ANOVA) to determine if there are significant differences between the firm size and integration of online services in SMEs. From our analysis, we observe that the level of integration of online services is not homogeneous in companies (ANOVA, significance level: .000), finding that there is a positive correlation between the largest number of online services integrated into the company and its size (correlation: .240; $p < .001$).

Table 4 shows the results of the breaches typology in the sample. First, from our results, we can confirm that SMEs are subject to a wide variety of attacks. From breaches produced by social engineering attacks, such as phishing; automated attacks, such as injecting ransomware with the aim of hijacking information; non-automated attacks, with malware aiming to penetrate the company's network; or breaches produced by the improper use of the company's assets. Therefore, despite the perception of many SME managers, SMEs are exposed to hacker attacks. Second, in terms of the typology of breaches in SMEs, our results show that the most commonly identified type of breaches (36.5%) is *staff receiving a fraudulent email or being directed to fraudulent sites* (BREACHES 6), followed by *people impersonating their organisation via emails or online* (17.7%) (BREACHES 5), and *computers infected with other viruses, spyware or malware* (17.4%) (BREACHES 2). Other types of breaches are much less commonly identified, with frequency rates below 10% in most of the cases. As we can see, the results are in line with previous studies (Wright et al. 2014), which point out that the main attacks have a social nature, and highlight the importance of this type of attack, which is based on a lack of procedures and a lack of knowledge of the company's personnel of cybersecurity policies (Ponsard, Grandclaudon, and Dallons 2018). Moreover, we see how malware attacks have their importance in SMEs, in line with previous works (Valli, Martinus, and Johnstone 2014; Sangani and Vijayakumar 2012). Sangani and Vijayakumar (2012) and Osborn (2015) highlighted the lack of adequate protection of the IS in SMEs, either due to the diversity

Table 5. Frequency of breaches in SMEs*.

Variables	Frequency	Count	%
FREQUENCY 1	Once only	226	34.6
FREQUENCY 2	More than once but less than once a month	183	28.0
FREQUENCY 3	Roughly once a month	96	14.7
FREQUENCY 4	Roughly once a week	71	10.9
FREQUENCY 5	Roughly once a day	35	5.4
FREQUENCY 6	Several times a day	42	6.4

*Total: 653 SMEs

of devices or the lack of knowledge in their cybersecurity management; these are an important source of vulnerabilities in SMEs.

Table 5 displays the frequency of occurrence of the breaches experienced by SMEs. First, we observe that approximately 653 SMEs, 48.4% of the sample, have responded to this question, which suggests that over half of the SMEs sampled are not aware of the breaches occurring in their companies. We have carried out a preliminary check to see if there are biases in the answers. In a similar way as in previous questions, we have performed an analysis of variance (ANOVA) to determine if there are significant differences between SMEs and the frequencies of breaches. The ANOVA results show a homogeneous behaviour, without there being significant differences in the SMEs, either due to the size of the company (ANOVA, significance level: .685) or the number of online services integrated into it (ANOVA, significance level: .227). Second, Table 4 shows that approximately 80% of the SMEs report having suffered attacks either only once or less than once per month at most, with daily or very frequent attacks representing only 10% of responses. Previous analysis of our results could indicate that the SMEs are not a target of cybersecurity attacks due to the infrequency of the breaches. However, if we consider that the most infrequent attacks are pointed out in the literature as being the most damaging to firms, our initial assumption must change. That is, attacks aimed at penetrating the company's network have the characteristic of occurring in certain situations and with a very low level of frequency (Conteh and Schmick 2016; Gatrner Group 2014; Peggy et al., 2011). In this same line, we can place the threats produced by the employees from the use of the company's devices, or the fraudulent use of these. Moreover, automated attacks without a defined objective are constantly present, with a high frequency. In this line, Walli et al. (Valli, Martinus, and Johnstone 2014) point out that these attacks are usually easily detected by the conventional protection systems, without causing significant damage to companies.

In order to examine the behaviour pattern of breaches in SMEs, we have performed an analysis of variance (ANOVA) to see if there are differences based on the frequency of occurrence in each type of breach (Table 6). To do this, we have created a variable, with a value of 1 if the attacks are *infrequent* (frequency between once and more than a month), and a value of 2 if the breaches are very *frequent* (if the frequency is between daily and a month). Firstly, we see that in BREACHES 1 and 2, which correspond to *SME computers being infected with both ransomware and other types of viruses (spyware or malware)*, there are significant differences regarding the frequency of occurrence and, consequently, two different groups are generated in each type of breach. The first, the more infrequent group, corresponds in both types of breaches to approximately 75% of the cases in the sample, with the other group representing approximately 25% of the

Table 6. Frequency and typology of breaches in SMEs.

			Frequency (%)	
Variables	**F**	**Sig.**	1*	2**
BREACHES 1	8.806	.003	73.4	26.6
BREACHES 2	27.975	.000	75.9	24.1
BREACHES 3	2.826	.093	*Non-significant*	
BREACHES 4	3.035	.082	*Non-significant*	
BREACHES 5	.245	.621	*Non-significant*	
BREACHES 6	91.584	.000	52.7	47.3
BREACHES 7	.038	.845	*Non-significant*	
BREACHES 8	.381	.537	*Non-significant*	

*Frequency between once and more than a month
**Frequency between daily and a month.

cases, which occur with a daily to a monthly frequency. An interpretation of these two groups of breaches corresponds to non-automated attacks, which are more infrequent, but with more sophistication and tailored towards SMEs. This can be a case of ransomware and also specific malware; this group of attacks are usually launched by motivated adversaries (financial gain mostly) (Sahoo and Gupta 2019; Heartfield et al. 2018) and are usually very harmful to SMEs. The second group corresponds to automated attacks that usually target a large sample of companies at the same time. These types of attacks tend to be less sophisticated since attackers try to infect as many systems as possible with exactly the same malware, which makes them ineffective or easily neutralised given the diversity of systems and security measures of SMEs (Osborn 2015). Secondly, the results show that also BREACHES 6, which corresponds to the *SME staff receiving fraudulent email or being directed to fraudulent sites*, displays significant differences in the frequency of this type of breach. In this case, about half of the breaches are infrequent, and the other half have a high frequency. As in the previous case, we can talk about targeted attacks (more infrequent), such as spear-phishing, in which the attacker has knowledge of the victims and tries to convince them to go to a fraudulent site using that familiarity, or automated attacks, generic and very frequent attacks, which are usually the classic phishing that most people receive (for example, a common one is an email about an HMRC tax refund, in which the attacker encourages the victim to follow a link to get a tax refund by inputting their bank account details).

3.1. The severity of the breaches

Regarding our first research question (*the severity level of the breaches and what their effect on SMEs is*), Table 7 collects the perception of SMEs with respect to the disruptiveness of breaches. Out of the responses obtained, the *staff receiving fraudulent emails or being directed to fraudulent websites* (BREACHES 6) is the most severe breach in the perception of SMEs, having a response greater than 10% (248 of SMEs: 18.4%), with the rest of the breaches having answers lower than 10%. First, we see that the results show a poor response, which we can interpret as a consequence of the scarcity of knowledge and consideration that cybersecurity has in SMEs, corroborating previous works (Ponsard, Grandclaudon, and Dallons 2018; Osborn 2015). Second, in line with Jensen et al. (2017) and Walli et al. (Valli, Martinus, and Johnstone 2014), the results point out that the most severe breaches in the perception of SMEs are those derived from social engineering

Table 7. Typology of breaches in SMEs and perception of the severity*.

Variable	Typology of Breaches	Count	%
BREACHES 1	Computers becoming infected with ransomware	78	5.8
BREACHES 2	Computers become infected with other viruses, spyware or malware	126	9.3
BREACHES 3	Attacks that try to take down your website or online services	29	2.2
BREACHES 4	Hacking or attempted hacking of online bank accounts	22	1.6
BREACHES 5	People impersonating your organisation in emails or online	101	7.5
BREACHES 6	Staff receiving fraudulent emails or being directed to fraudulent websites	248	18.4
BREACHES 7	Unauthorised use of computers, networks or servers by staff, even if accidental	5	0.4
BREACHES 8	Unauthorised use or hacking of computers, networks or servers by people outside your organisation	28	2.1

*Total: 1,348 SMEs

Table 8. The disruption time in the SMEs*.

Time disruption	Count	%
• Immediate	425	66.2
• Within 24 hours	162	25.2
• Within a week	40	6.2
• Within a month	9	1.4
• Within 100 days	4	.6
• Longer than 100 days	2	.3

*Total: 642 SMEs

attacks, such as phishing. According to Liginlal, Sim, and Khansa (2009), these results are consistent with the fact that social engineering attacks are more visible to company management and noticeable to any company employee (other types, such as spyware, are more difficult to detect), considering that company managers make infrequent updates to their cybersecurity status (Cybersecurity Breaches, 2017). We can conclude that there is limited usefulness of subjective measures[11] to analyse the severity of breaches in SMEs.

Complementary to this analysis, we have analysed the severity of the breaches using two objective measures, such as the *disruption time* produced by the breaches, and the *cost* that the breaches entail for SMEs. As in previous questions, we have carried out a confirmatory analysis, to check if in the response obtained there was a bias derived from the *size* or the *online services* of the SMEs, confirming that the response is homogeneous, as shown by the two variance analyses carried out for both variables (ANOVA, significance level: .244; significance level: .126). The results in Table 8 show the *disruption time*. We see that 91.4% of breaches are resolved in less than 24 hours. Less than 1% are those that last for more than one month. Regarding the *cost* of breaches (Table 9), the response of SMEs varies from a minimum amount to £100,000, with the average expense being approximately £2,000. Therefore, from our results, we see that the attacks received by SMEs are not very severe, combining both recovery time and cost, contradicting previous results that highlight the high level of severity of attacks, indicating that 60% of SMEs will disappear after six months.

In order to identify the typology of breaches and their severity, we have performed a causal analysis with an ANN multilayer perceptron (MLP). Figure 3 shows the architecture of the neural network used to model the severity of attacks, using the *types of breaches* as input variables, and the *disruption time* and *cost* as output variables. We

Table 9. The costs of the breaches in the SMEs*.

Costs (£)	Frequency	%
0 to 199	411	70.9
200 to 999	57	9.8
1,000 to 9,999	79	13.6
10,000 to 100,000	33	5.7

Total: 580 SMEs

have previously considered the robustness of the model. Modelling with ANN-MLP shows an ability to predict both the *cost* and the *disruption time*, with an error of 23.8% in the case of the *disruption time*, and in the case of the *cost* with a continuous scale, it is 0.383. Moreover, the correlation between the expected and actual output variables is 0.633 and 0.729, both for *cost* and *disruption time*. Therefore, we can point out high robustness or the explanatory capacity of the model.

Table 10 shows the normalised importance of the severity of breaches in the *costs* and *disruption time*. It is observed that BREACHES 7 (*unauthorised use of computers, networks or servers by staff*: 100%) is the one that produces the highest severity both in *cost* and *disruption time*. At a second level are BREACHES 4 (*hacking or attempted hacking of online bank accounts*: 64.1%) and BREACHES 8 (*unauthorised use or hacking of computers, networks or servers by people outside your organisation*: 60.5%). At a lower level are BREACHES 6 (*staff receiving fraudulent emails or being directed to fraudulent websites*: 43.0%) and BREACHES 5 (*people impersonating your organisation in emails or online*: 38.6%). The rest of the breaches have a normalised impact of less than 30%. More in detail, in Table 11, we see the independent impact for each output variable. We see that there is a slight difference. Thus, regarding the *cost of disruption*, we see that the one with the greatest effect is BREACHES 3 (*attacks that try to take down your website or online services*: 100%), followed by BREACHES 7 (*unauthorised use of computers, networks or servers by staff, even if accidental*: 78.4%). Moreover, in the case of *disruption time*, it is BREACHES 7 (*unauthorised use of computers, networks or servers by staff, even if accidental*: 100%) which reports a greater effect here. Our results are in line with previous studies that highlight how direct attacks on the commercial and financial infrastructure of a company represent significant damage to firms (Lezoche and Panetto 2020; Heartfield, 2018; Chaudhry et al. 2011). Moreover, our results corroborate that the inappropriate use of SMEs' devices has a greater severity, such as, for example, not having an appropriate password policy (password length and characters, together with the expiration of the passwords) and/or leaving an unprotected network due to improper use of safe environments, which allows the entry of attacks and loss of control, producing significant damage in terms of loss of business activities and information (ISO 2016; ISO/IEC 15,408–1: 2009, 2018). These results reinforce the need to establish appropriate cybersecurity policies, procedures, awareness and training in SMEs, together with cyber insurance cover to enable rapid business recovery, but also to update protection and security controls (ISO/IEC 15,408–1: 2009, 2018; Cenfetelli and Bassellier 2009).

Therefore, as a discussion on what the degree of breach severity is in SMEs, our results show a low level of breach severity both in costs for the SMEs and in the time to solve the disruption. This may explain the controversial relationship between cybersecurity and SMEs, noted in the literature (Ponsard, Grandclaudon, and Dallons 2018; Osborn 2015;

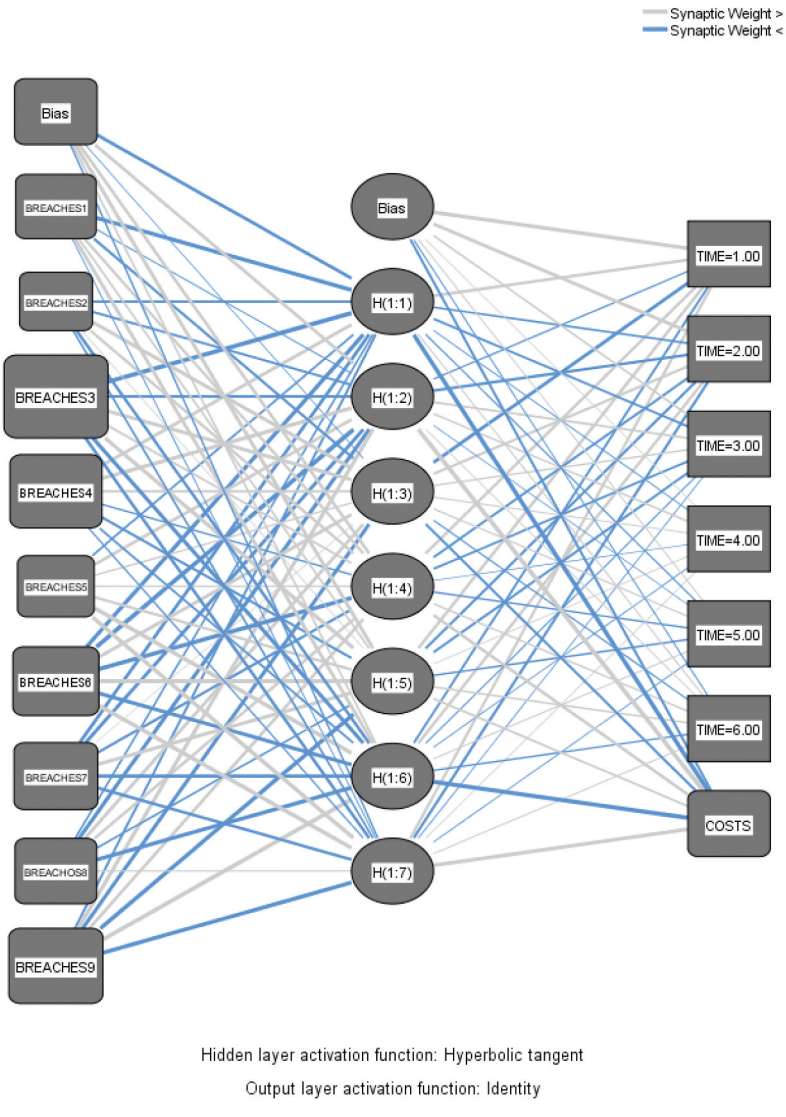

Figure 3. ANN Multilayer Perceptron (MLP) architecture for breaches and cost and time disruption.

Sangani and Vijayakumar 2012). On the one hand, this low level of severity of our results, together with the scarcity of updates that managers make for cybersecurity problems (Cyber Security Breaches Survey 2017), may explain why SMEs do not feel like cyberattack targets. However, from our results, we see that SMEs are subject to all types of attacks. In line with Wright et al. (2014), phishing plays an important role in small and medium-sized companies, taking advantage of the low level of preparation of employees. Second, our results corroborate previous studies that SMEs receive attacks as inputs to larger targets (Ponsard, Grandclaudon, and Dallons 2018; Sangani and Vijayakumar 2012). Finally, the exposure of SMEs to the internet makes them subject to automatic attacks, corroborating previous studies that indicate their low degree of severity (Jang-Jaccard and Nepal 2014; Sangani and Vijayakumar 2012). Moreover, we must highlight the severity of breaches

Table 10. The importance of the severity of the breaches in the costs and disruption time*.

Variables	Typology of Breaches	Value	Normalise
BREACHES 1	Computers becoming infected with ransomware	.064	28.8%
BREACHES 2	Computers become infected with other viruses, spyware or malware	.063	28.1%
BREACHES 3	Attacks that try to take down your website or online services	.064	28.6%
BREACHES 4	Hacking or attempted hacking of online bank accounts	.143	64.1%
BREACHES 5	People impersonating your organisation in emails or online	.086	38.6%
BREACHES 6	Staff receiving fraudulent emails or being directed to fraudulent websites	.096	43.0%
BREACHES 7	Unauthorised use of computers, networks or servers by staff, even if accidental	.223	100.0%
BREACHES 8	Unauthorised use or hacking of computers, networks or servers by people outside your organisation	.135	60.5%

*Simulation: ANN-MLP 9-7-7; Error (Costs): 0.383; Error (Time): 23.8%

Table 11. The importance of the severity of the breaches in the costs and disruption time*.

		Time Disruption		Costs	
Variables	Typology of Breaches	Value	Normalise	Value	Normalise
BREACHES 1	Computers becoming infected with ransomware	.050	19.8%	.124	72.1%
BREACHES 2	Computers become infected with other viruses, spyware or malware	.045	17.9%	.111	64.4%
BREACHES 3	Attacks that try to take down your website or online services	.178	70.9%	.172	100.0%
BREACHES 4	Hacking or attempted hacking of online bank accounts	.194	77.4%	.130	75.5%
BREACHES 5	People impersonating your organisation in emails or online	.036	14.3%	.098	57.0%
BREACHES 6	Staff receiving fraudulent emails or being directed to fraudulent websites	.042	16.6%	.084	48.8%
BREACHES 7	Unauthorised use of computers, networks or servers by staff, even if accidental	.250	100.0%	.135	78.4%
BREACHES 8	Unauthorised use or hacking of computers, networks or servers by people outside your organisation	.104	41.5%	.112	65.2%

*Simulation: ANN-MLP 9-7-7; Robustness, Error (Costs): 0.383; Error (Time): 23.8%

Table 12. Impact of breaches in SMEs.

Variable	Impacts	Count	%
IMPACT 1	Stopped staff from carrying out their day-to-day work	182	13.5
IMPACT 2	Loss of revenue or share value	31	2.3
IMPACT 3	Additional staff time to deal with the breach or attack.	247	18.3
IMPACT 4	Any other repair or recovery costs	120	8.9
IMPACT 5	New measures needed to prevent or protect against future breaches or attacks	264	19.6
IMPACT 6	Fines from regulators or authorities, or associated legal costs	0	0
IMPACT 7	Reputational damage	4	0.3
IMPACT 8	Prevented provision of goods or services to customers	24	1.8
IMPACT 9	Discouraged you from carrying out a future business activity you were intending to do	46	3.4
IMPACT 10	Complaints from customers	18	1.3
IMPACT 11	Goodwill compensation or discounts are given to customers	248	18.4

produced by the misuse of SMEs' devices. In line with Osborn (2015) and Ponsard, Grandclaudon, and Dallons (2018), this last point reinforces the need for SMEs to adhere to international standards, for example, the family of ISO 27000s.

3.2. Impact of breaches in SMEs

Table 12 provides information on the second research question, *how breaches impact on SMEs*. The impact is considered in the survey as the reaction of the firm to the breaches, in terms of management, financial and economic impacts, involving both the company and its environment. As in previous questions, we have verified the existence of biases in the

responses, and we see that there are significant differences (ANOVA, significance level: .000), showing an increase in the response as the company has a larger size and more integrated online services. Furthermore, we can confirm that there is a positive correlation in the higher response as companies increase in size and the number of integrated online services. In line with previous studies, our results show that as dependence on online services increases, SME managers increase their interest and concern about cybersecurity. Regarding the results, Table 12 shows that the most common impacts of breaches in SMEs are IMPACT 5 (*decision to implement new measures that prevent further attacks*: 19.6%), IMPACT 3 (*additional time from the staff to deal with the attack itself*: 18.3%), as well as IMPACT 11 (*compensations to customers*: 18.4%) and IMPACT 1 (*stopped staff from carrying out their day-to-day work*: 13.5%). From our results, we can confirm that breaches have both economic and financial implications for companies, in terms of costs, customer compensation and denial of service (Pérez-González, Preciado, and Solana-Gonzalez 2019; Jensen et al. 2017; Herath and Rao 2009; Liginlal, Sim, and Khansa 2009). Moreover, an important conclusion is that the existence of breaches produces a reaction in SMEs in terms of management to protect themselves against future attacks. This result is in line with the reactive role that SMEs play in terms of cybersecurity (Chan, Woon, and Kankanhalli 2005). However, unlike other studies, which have highlighted loss of reputation damage or legal costs as impacts, especially in large firms, we see from our results that in the case of SMEs these are insignificant (Forbes Insights 2014).

Regarding the causal effect that different types of breaches have on SMEs, Figure 4 shows the ANN-MLP architecture of the causal relationship between breaches and their impact. The robustness of the model is high. Thus, it is observed that the prediction capacity of our model is greater than 85% in all cases, both for values 0 and 1, producing a robust model to predict the effects of attacks. Moreover, the correlation between the expected and actual output variables is higher than 0.750. These results show a high ability to predict, considering the model error.

Table 13 shows the normalised importance of the *causal effect between the different breach typologies and the impact generated*. From the results, we can conclude that breaches related to malware attacks have a greater impact on the economic losses of a company, both in terms of additional staff costs and service interruptions. On the other hand, SMEs introduce cybersecurity measures as a result of the existence of breaches derived from both malware attacks and the inappropriate use of IS facilities by staff. In this sense, Osborn (2015) and Sangani and Vijayakumar (Sangani and Vijayakumar 2012) have pointed out the reactive nature of SMEs in terms of their relationship with cybersecurity, which means that breaches are a driver in investment for security measures and the implementation of security standards. Moreover, in terms of image, and relationships with clients and authorities, breaches related to the misuse of IS are the ones that have the most impact (Couce-Vieira, Insua, and Kosgodagan 2020). Unlike hacker attacks that are easily understood by company stakeholders, cybersecurity problems caused by the inappropriate use of IS by company personnel, with the consequent problems of operation and responsibility, require in many cases financial compensation or a thorough explanation (Couce-Vieira, Insua, and Kosgodagan 2020; Posey, Roberts, and Lowry 2015), which result in losses of corporate reputation and demotivation to start new businesses. These highlight the need for additional cover for security incidents, which could be solved by having cyber insurance cover.

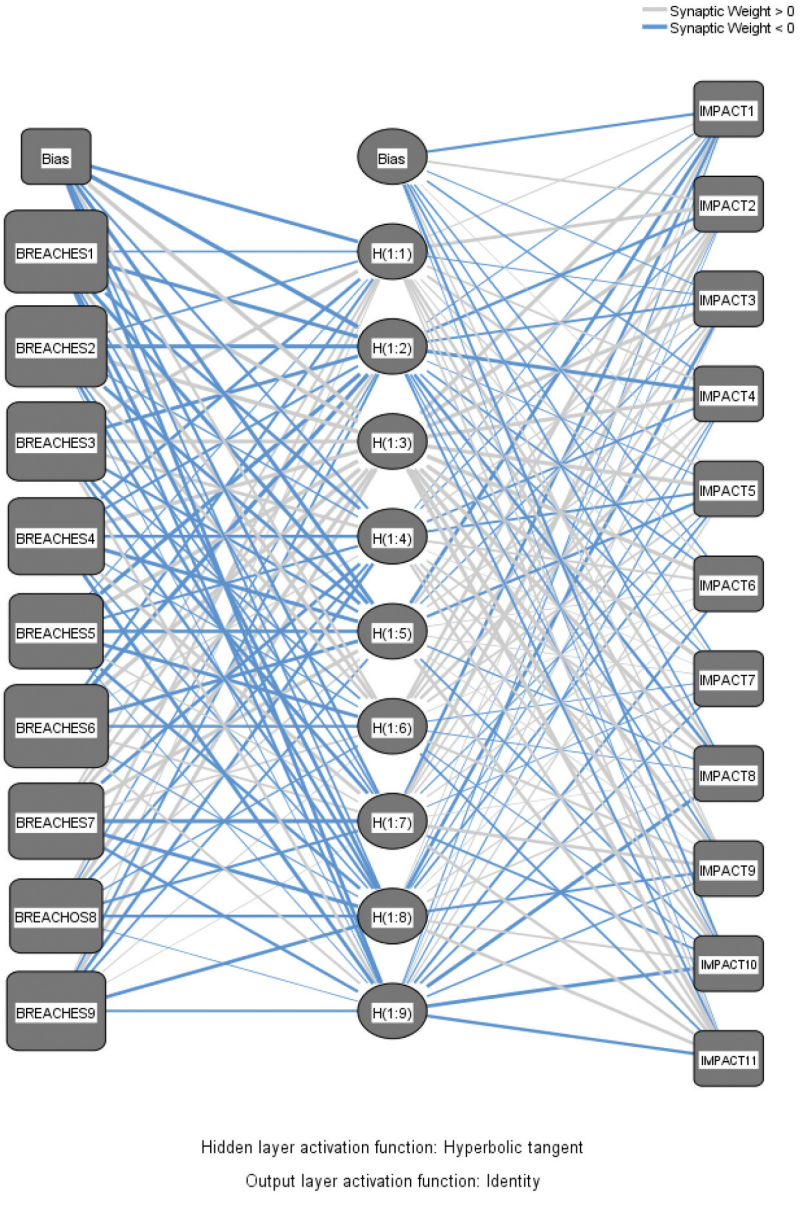

Figure 4. ANN Multilayer Perceptron (MLP) architecture for breaches and impacts.

Finally, from our results, it can be confirmed that breaches have an effect on SMEs in economic, financial and management terms. While previous work highlighted operational and technical problems (Sahoo and Gupta 2019; Valli, Martinus, and Johnstone 2014), our results confirm the economic and financial effects that breaches have in terms of lost revenue. Moreover, our results are in line with previous works that highlight the effect that breaches produce in the relationship with clients and with the administration (Couce-Vieira, Insua, and Kosgodagan 2020), especially in the case of misuse of the IS of SMEs.

Table 13. The normalise importance of the breaches and the impacts in the SMEs*.

Variables	Normalise Importance										
	IMPACT 1	**IMPACT 2**	**IMPACT 3**	**IMPACT 4**	**IMPACT 5**	**IMPACT 6**	**IMPACT 7**	**IMPACT 8**	**IMPACT 9**	**IMPACT 10**	**IMPACT 11**
BREACHES 1	100%	41%	37%	92%	9%	-	21%	14%	27%	22%	45%
BREACHES 2	61%	18%	100%	61%	95%	-	13%	23%	25%	43%	18%
BREACHES 3	23%	25%	36%	7%	54%	-	44%	41%	12%	20%	45%
BREACHES 4	18%	100%	14%	30%	41%	-	38%	8%	23%	48%	39%
BREACHES 5	7%	60%	50%	39%	68%	-	18%	20%	18%	17%	38%
BREACHES 6	17%	32%	11%	44%	47%	-	33%	18%	14%	11%	72%
BREACHES 7	22%	63%	27%	100%	100%	-	45%	100%	100%	100%	100%
BREACHES 8	35%	59%	34%	97%	43%	-	100%	26%	78%	26%	23%

Lastly, the results differ in terms of the impact they have on corporate reputation (ENISA 2020; Gatrner Group 2014).

4. Conclusion

Our paper has analysed the cyber breaches produced in SMEs, as well as their effect and severity in management, economic and financial terms. We have combined statistical analysis with the use of machine learning, using a causal analysis to model the effect of breaches in SMEs.

From a cybersecurity point of view, our first group of contributions extends the literature on SMEs' security (Müller, Buliga, and Voigt 2018; Ponsard, Grandclaudon, and Dallons 2018; Hayes and Bodhani 2013). Firstly, we extend previous works confirming that SMEs are targets of cyberattacks either directly or as part of the supply chain of other larger companies. Thus, SMEs receive a wide variety of breaches, through malware in automated and non-automated attacks, followed by attacks of a social nature (social engineering), exploiting staff vulnerabilities, even those derived from the misuse of the IS in SMEs. Secondly, unlike previous works, we have characterised the degree of severity of breaches in SMEs, based on disruption time and their cost. Our last contribution consists of determining the effect of breaches in SMEs in economic, financial and management terms, highlighting the differential aspects concerning large companies.

From a policy-making point of view, our work highlights the need to develop adequate policies and procedures in SMEs for the development of cybersecurity systems in conjunction with appropriate training and awareness campaigns. Firstly, unlike previous studies that justified the non-existence of protection methods against possible cyberattacks and threats, based on the consideration that SME managers have of cybersecurity, as well as the little adherence that SMEs have to the application of policies, and finally the diversity of IS in them, we consider the need to adhere to these types of standards or best practices of security in companies. Secondly, we highlight the importance of breaches derived from the misuse of IS in SMEs by their staff. Therefore, we consider a crucial element is to involve SME employees in training and awareness campaigns, which will reduce breaches that occur in this way. Finally, we highlight the need to involve SME managers in decisions to invest in cybersecurity systems and cyber insurance, stressing the problems that this may entail for the company, not only in terms of cost and denial of services, but also in responsibilities with its stakeholders and loss of corporate reputation.

Our last contribution is framed from a methodological point of view. We consider that the use of statistical methods, in particular, machine learning techniques, allows us to identify the cause-effect relationships between breaches and their impact on SMEs. Firstly, the use of statistical techniques and adequate surveys allows us to characterise the behaviour of companies in terms of cybersecurity. Secondly, the use of machine learning is very appropriate in the field of cybersecurity, where the lack of information from company managers and correlation problems between variables is common, allowing us to obtain robust modelling of the relationships between variables.

Finally, like any other, our study is not free from limitations. First, although our study uses an important and significant sample, perhaps later studies should expand the sample to different countries, testing the non-existence of bias in our results. Also, although our study used the

Cyber Breaches Innovation Survey as a questionnaire, subsequent studies should focus on other alternative measures to test the results and avoid possible measurement biases.

Notes

1. Insurance and financial institutions use it as part of the liability of a company to be able to recover from a cyber breach or the likelihood of a company having a cyber breach (ABI 2020).
2. In line with the Cybersecurity Breaches Survey (2017), which indicates that approximately less than 15% of managers receive daily or weekly updates on cybersecurity in companies in the UK. Cybersecurity has been focused on IT departments, with little relation to the rest of the company.
3. A cyberattack is a set of offensive actions against information systems, producing a security incident in the firm (CLUSIF 2008).
4. Adversaries, in this context, could be anything from competitors, to nation states or nation state sponsored hackers, to financially motivated individuals (Chaudhry et al. 2011).
5. Osborn (2015) highlighted that SMEs have an average of 2.92 devices, with desktops being the most used, followed by smartphones and tablets. For internet access, this study indicates that ADSL modems, ADSL wireless and 3 G/4 G wireless are the most used systems; however, a high level of ignorance of the different connection possibilities stands out. Regarding protection systems, the study indicates that the main cybersecurity countermeasures are firewalls, virus scanners, malware scanners and spam killers; however, regarding the maintenance of cybersecurity system updates, a high percentage of SMEs were unaware of how frequent these updates needed to be.
6. Ifinedo's (2012) concept of *perceived severity of an attack and breaches* refers to the differences in the degree of seriousness by which attacks and threats are perceived and in the potential harm of the attack. In the context of the firm and, particularly, for IT systems, this potential harm can be measured in terms of the costs and legal liability for the company.
7. According to Kaspersky Lab (2017), cyberattacks cost an average of $1.3 million per business in 2017 in North America, 11% more than in 2016. For SMEs, the average cost of recovery amounts to $117,000.
8. For example, when a company suffers a data breach, following GDPR, the Information Commissions Office (ICO) can fine a said SME 10 million euros (or the equivalent in sterling), or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher.
9. Obtaining the data through a telephone survey has some advantages. First, the use of random-probability sampling to avoid selection bias. Second, the inclusion of micro and small businesses, which ensures that the findings are representative of the whole UK business population and not skewed towards larger businesses. And finally, a telephone data collection approach, which aims to also include businesses with less of an online presence (compared to online surveys).
10. The stakeholders were: The Cabinet Office, The Centre for the Protection of National Infrastructure (CPNI), Government Communications Headquarters (GCHQ), The Home Office, 6 UK industry representative bodies, and 3 professional cyber security or software organisations.
11. In this paper we differentiate between *subjective* and *objective*. While *subjective* is based on the response perceived by the manager, *objective* refers to the response measure using *cost* and *time of disruption*.

Conflicts of interest

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

References

ABI (2020). "*Cyber Risk Insurance*." The Association of British Insurers. https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/

Aguilar, L. A. (2015). "*The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses*." US Securities and Exchange Commission. https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

Ahmad, A., J. Webb, K. C. Desouza, and J. Boorman. 2019. "Strategically-motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack." *Computers & Security* 86: 402–418. doi:10.1016/j.cose.2019.07.001.

Arranz, N., and J. C. Fernandez de Arroyabe. 2010. "Efficiency in Technological Networks, an Approach from Artificial Neural Networks (ANN)." *International Journal of Management Science and Engineering Management* 5 (6): 453–460. doi:10.1080/17509653.2010.10671137.

Arranz, N., N. L. Arguello, and J. C. Fernandez de Arroyabe. 2021. "How Do Internal, Market and Institutional Factors Affect the Development of Eco-innovation in Firms?" *Journal of Cleaner Production* 297: 126692. doi:10.1016/j.jclepro.2021.126692.

Ashibani, Y., and Q. H. Mahmoud. 2017. "Cyber Physical Systems Security: Analysis, Challenges and Solutions." *Computers & Security* 68: 81–97. doi:10.1016/j.cose.2017.04.005.

Bishop, C. M. 1995. *Neural Networks for Pattern Recognition*. Oxford, UK: Oxford University Press.

Bland, J. A., M. D. Petty, T. S. Whitaker, K. P. Maxwell, and W. A. Cantrell. 2020. "Machine Learning Cyberattack and Defense Strategies." *Computers & Security* 92: 101738. doi:10.1016/j.cose.2020.101738.

Bourilkov, D. 2019. "Machine and Deep Learning Applications in Particle Physics." *International Journal of Modern Physics A* 34 (35): 1930019. doi:10.1142/S0217751X19300199.

Cavusoglu, H., H. Cavusoglu, J. Y. Son, and I. Benbasat. 2015. "Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources." *Information & Management* 52 (4): 385–400. doi:10.1016/j.im.2014.12.004.

Cenfetelli, R., and G. Bassellier. 2009. "Interpretation of Formative Measurement in Information Systems Research." *MIS Quarterly* 33 (4): 689–708. doi:10.2307/20650323.

Chan, M., I. Y. Woon, and A. Kankanhalli. 2005. "Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior." *Journal of Information Privacy and Security* 1 (3): 18–41. doi:10.1080/15536548.2005.10855772.

Chaudhry, P. E., S. S. Chaudhry, S. A. Stumpf, and H. Sudler. 2011. "Piracy in Cyber Space: Consumer Complicity, Pirates and Enterprise Enforcement." *Enterprise Information Systems* 5 (2): 255–271. doi:10.1080/17517575.2010.524942.

Choo, K. R. 2011. "The Cyber Threat Landscape: Challenges and Future Research Directions." *Computers & Security* 30 (8): 719–731. doi:10.1016/j.cose.2011.08.004.

Chronopoulos, M., E. Panaousis, and J. Grossklags. 2018. "An Options Approach to Cybersecurity Investment." *IEEE Access* 6: 12175–12186. doi:10.1109/ACCESS.2017.2773366.

Ciurana, J., G. Quintana, and M. L. Garcia-Romeu. 2008. "Estimating the Cost of Vertical High-speed Machining Centers, a Comparison between Multiple Regression Analysis and the Neural Approach." *International Journal of Production Economics* 115 (1): 171–178. doi:10.1016/j.ijpe.2008.05.009.

CLUSIF. 2008. *Risk Management. Concepts and Methods*. Paris: Club de la Securite Infomatique.

Cohen, F. 1997. "Information System Attacks: A Preliminary Classification Scheme." *Computers & Security* 16 (1): 29–46. doi:10.1016/S0167-4048(97)85785-9.

Conteh, N. Y., and P. J. Schmick. 2016. "Cybersecurity: Risks, Vulnerabilities and Countermeasures to Prevent Social Engineering Attacks." *International Journal of Advanced Computer Research* 6 (23): 31–43. doi:10.19101/IJACR.2016.623006.

Couce-Vieira, A., D. R. Insua, and A. Kosgodagan. 2020. "Assessing and Forecasting Cybersecurity Impacts." *Decision Analysis* 17 (4): 356–374. doi:10.1287/deca.2020.0418.

Cyber Security Breaches Survey (2016). "*Official Statistics. Cyber Security Breaches Survey 2017*." Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017

Cyber Security Breaches Survey (2017). "*Official Statistics. Cyber Security Breaches Survey 2017*." Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

Dahiya, A., and B. B. Gupta. 2020. "Multi Attribute Auction Based Incentivized Solution against DDoS Attacks." *Computers & Security* 92: 101763. doi:10.1016/j.cose.2020.101763.

Ekelund, S., and Z. Iskoujina. 2019. "Cybersecurity Economics – Balancing Operational Security Spending." *Information Technology & People* 32 (5): 1318–1342. doi:10.1108/ITP-05-2018-0252.

ENISA. 2018. *Reference Incident Classification Taxonomy*. Luxembourg: European Union Agency for Cybersecurity.

ENISA. 2020. *Insider Threat ENISA. Threat Landscape*. Luxembourg: European Union Agency for Cybersecurity.

Fielder, A., E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi. 2016. "Decision Support Approaches for Cyber Security Investment." *Decision Support Systems* 86: 13–23. doi:10.1016/j.dss.2016.02.012.

Forbes Insights (2014). "The Reputational Impact of It Risk." FALLOUT. https://images.forbes.com/forbesinsights/StudyPDFs/IBM_Reputational_IT_Risk_REPORT.pdf

Garre, J. T. M., M. G. Pérez, and A. Ruiz-Martínez. 2021. "A Novel Machine Learning-based Approach for the Detection of SSH Botnet Infection." *Future Generation Computer Systems* 115: 387–396. doi:10.1016/j.future.2020.09.004.

Gatrner Group (2014). "*Top 10 Strategic Predictions for 2015*." Gartner Group. http://www.gartner.com/technology/home.jsp

Hayes, J., and A. Bodhani. 2013. "Cyber Security: Small Firms under Fire." *Engineering & Technology* 8 (6): 80–83.

Heartfield, R., G. Loukas, S. Budimir, A. Bezemskij, J. R. Fontaine, A. Filippoupolitis, and E. Roesch. 2018. "A Taxonomy of Cyber-physical Threats and Impact in the Smart Home." *Computers & Security* 78: 398–428. doi:10.1016/j.cose.2018.07.011.

Hegazy, T., Fazio, P., and Moselhi, O. (1994). Developing practical neural network applications using back-propagation. *Computer-Aided Civil and Infrastructure Engineering*, *9*(2): 145–159.

Herath, T., and H. R. Rao. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations." *European Journal of Information Systems* 18 (2): 106–125. doi:10.1057/ejis.2009.6.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory." *Computers & Security* 31 (1): 83–95. doi:10.1016/j.cose.2011.10.007.

ISO (2016). "ISO/IEC 27001: 2013 - *Information Security Management*." ISO/IEC. http://www.iso.org/iso/iso27001

ISO/IEC. 2014. *International Standard ISO/IEC 27000: Information Technology-Security Techniques - Information Security Management Systems - Overview and Vocabulary*. Geneva: ISO/IEC.

Jang-Jaccard, J., and S. Nepal. 2014. "A Survey of Emerging Threats in Cybersecurity." *Journal of Computer and System Sciences* 80 (5): 973–993. doi:10.1016/j.jcss.2014.02.005.

Jensen, M. L., M. Dinger, R. T. Wright, and J. B. Thatcher. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques." *Journal of Management Information Systems* 34 (2): 597–626. doi:10.1080/07421222.2017.1334499.

Jeong, C. Y., S. Y. T. Lee, and J. H. Lim. 2019. "Information Security Breaches and IT Security Investments: Impacts on Competitors." *Information & Management* 56 (5): 681–695. doi:10.1016/j.im.2018.11.003.

Kaspersky (2017). "For Business IT Security: Cost Center or Strategic Investment? Investigating the New Business Attitude Towards IT Security Budgets." Kaspersky For Business. https://go.kaspersky.com/rs/802-IJN-240/images/IT%20Security%20Econmics%20Report%209.18.17.pdf

Lezoche, M., and H. Panetto. 2020. "Cyber-Physical Systems, a New Formal Paradigm to Model Redundancy and Resiliency." *Enterprise Information Systems* 14 (8): 1150–1171. doi:10.1080/17517575.2018.1536807.

Liginlal, D., I. Sim, and L. Khansa. 2009. "How Significant is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management." *Computers & Security* 28 (3–4): 215–228. doi:10.1016/j.cose.2008.11.003.

Mallinder, J., and P. Drabwell. 2014. "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.

Manning, T., R. D. Sleator, and P. Walsh. 2014. "Biologically Inspired Intelligent Decision Making: A Commentary on the Use of Artificial Neural Networks in Bioinformatics." *Bioengineered* 5 (2): 80–95. doi:10.4161/bioe.26997.

Masters, T. 1993. *Practical Neural Network Recipes in C++*. San Francisco, California: Morgan Kaufmann.

Mendhurwar, S., and R. Mishra. 2019. "Integration of Social and IoT Technologies: Architectural Framework for Digital Transformation and Cyber Security Challenges." *Enterprise Information Systems* 1–20. doi:10.1080/17517575.2019.1600041.

Minbashian, A., J. E. Bright, and K. D. Bird. 2010. "A Comparison of Artificial Neural Networks and Multiple Regression in the Context of Research on Personality and Work Performance." *Organizational Research Methods* 13 (3): 540–561. doi:10.1177/1094428109335658.

Müller, J. M., O. Buliga, and K. I. Voigt. 2018. "Fortune Favors the Prepared: How SMEs Approach Business Model Innovations in Industry 4.0." *Technological Forecasting and Social Change* 132: 2–17. doi:10.1016/j.techfore.2017.12.019.

Osborn, E. (2015). "Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs." *CDT Technical Paper 01/15*. University of Oxford.

Pérez-González, D., S. Preciado, and P. Solana-Gonzalez. 2019. "Organizational Practices as Antecedents of the Information Security Management Performance: An Empirical Investigation." *Information Technology & People* 32 (5): 1262–1275. doi:10.1108/ITP-06-2018-0261.

Pirounias, S., D. Mermigas, and C. Patsakis. 2014. "The Relation between Information Security Events and Firm Market Value, Empirical Evidence on Recent Disclosures: An Extension of the GLZ Study." *Journal of Information Security and Applications* 19 (4–5): 257–271. doi:10.1016/j.jisa.2014.07.001.

Podsakoff, P. M., S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies." *Journal of Applied Psychology* 88 (5): 879–903. doi:10.1037/0021-9010.88.5.879.

Ponsard, C., J. Grandclaudon, and G. Dallons (2018). "*Towards A Cyber Security Label for SMEs: A European Perspectiv*e." In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), pages 426–431. Funchal - Madeira, Portugal : Science and Technology Publications

Posey, C., T. L. Roberts, and P. B. Lowry. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets." *Journal of Management Information Systems* 32 (4): 179–214. doi:10.1080/07421222.2015.1138374.

Sahoo, S. R., and S. B. Gupta. 2019. "Classification of Various Attacks and Their Defence Mechanism in Online Social Networks: A Survey." *Enterprise Information Systems* 13 (6): 832–864. doi:10.1080/17517575.2019.1605542.

Sangani, N. K., and B. Vijayakumar. 2012. "Cyber Security Scenarios and Control for Small and Medium Enterprises." *Informatica Economica* 16 (2): 58–71.

Seibold, C., W. Samek, A. Hilsmann, and P. Eisert. 2020. "Accurate and Robust Neural Networks for Face Morphing Attack Detection." *Journal of Information Security and Applications* 53: 102526. doi:10.1016/j.jisa.2020.102526.

Somers, M. J., and J. C. Casal. 2009. "Using Artificial Neural Networks to Model Nonlinearity: The Case of the Job Satisfaction—job Performance Relationship." *Organizational Research Methods* 12 (3): 403–417. doi:10.1177/1094428107309326.

Srinidhi, B., J. Yan, and G. K. Tayi. 2015. "Allocation of Resources to Cyber-security: The Effect of Misalignment of Interest between Managers and Investors." *Decision Support Systems* 75: 49–62. doi:10.1016/j.dss.2015.04.011.

Sung, S., Y. Kim, and H. Chang. 2018. "Improving Collaboration between Large and Small-medium Enterprises in Automobile Production." *Enterprise Information Systems* 12 (1): 19–35. doi:10.1080/17517575.2016.1161242.

Valli, C., I. C. Martinus, and M. N. Johnstone (2014). "*Small to Medium Enterprise Cyber Security Awareness: An Initial Survey of Western Australian Business*." Proceedings of International Conference on Security and Management. (pp. 71–75). Las Vegas, USA. CSREA Press.

Wang, L., and Y. Zhang. 2020. "Linear Approximation Fuzzy Model for Fault Detection in Cyber-physical System for Supply Chain Management." *Enterprise Information Systems* 1–18. doi:10.1080/17517575.2020.1791361.

Wang, Q. 2007. "Artificial Neural Networks as Cost Engineering Methods in a Collaborative Manufacturing Environment." *International Journal of Production Economics* 109 (1): 53–64. doi:10.1016/j.ijpe.2006.11.006.

Wright, R. T., M. L. Jensen, J. B. Thatcher, M. Dinger, and K. Marett. 2014. "Research Note—influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance." *Information Systems Research* 25 (2): 385–400. doi:10.1287/isre.2014.0522.