Computers & Security 124 (2022) 102954

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019

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

[a] WMG Cyber Security Centre, University of Warwick, Coventry, United Kingdom
[b] Data Services, Commercial Banking, Lloyds Banking Group, London, United Kingdom
[c] Greenwich Business School, University of Greenwich, London, United Kingdom
[d] Essex Business School, University of Essex, Colchester CO4 3SQ, United Kingdom

ARTICLE INFO

Article history:
Received 19 June 2021
Revised 19 September 2022
Accepted 11 October 2022
Available online 17 October 2022

Keywords:
Cybersecurity capabilities
Cyber-attacks
Organizations' strategy
Cybersecurity investment
Cybersecurity systems
Machine learning

ABSTRACT

Our study explores how cyber-capabilities and cyber-attacks drive investment in cybersecurity systems. We assume that cybersecurity investment is a strategic decision in the organizations. To analyze this research question, we make use of the Cyber Security Breaches Survey data, with a sample consisting of 4,163 UK organizations in the periods 2018 to 2019, and employ machine learning techniques (ANN and K-mean cluster). The study extends the current literature on cybersecurity systems and improves our understanding of it in several ways. First, it provides evidence for how the cybersecurity systems are developed in organizations. Second, regarding what factors affect investment in cybersecurity systems, it shows that organizations invest in cybersecurity based on their cybersecurity capabilities and the experienced cyber-attacks. Third, from a managerial point of view, the paper contributes to understanding cybersecurity within the management of the organization.

1. Introduction

Cybersecurity has become a key factor that determines the success or failure of organizations (Karjalainen et al., 2019; Jeong et al., 2019; Chronopoulos et al., 2017; Wolff, 2016; Cavusoglu et al., 2015; Bose and Luo, 2014; Bulgurcu et al., 2010). One of the greatest challenges that organizations face nowadays is determining the level of investment in cybersecurity systems that provides an adequate level of protection (Shao et al., 2020; Jalali et al., 2019; Nagurney and Shukla, 2017; Fielder et al., 2016; Heitzenrater and Simpson, 2016; Srinidhi et al., 2015; Bose and Luo, 2014). This decision is referred to as the *cybersecurity investment challenge* (Fielder et al., 2016, p. 13), where the range and scope of the attacks are unknown and the decision process is complex[1] and involves both the IT department and the organization's management (Cavusoglu et al., 2015; Choo, 2011). Therefore, determining what factors influence the decision to invest in cybersecurity in organizations has become a key issue for research (Shao et al., 2020; Jalali et al., 2019; Bose and Luo, 2014).

Traditionally, the analysis of the factors that impact investment in cybersecurity has been approached from different perspectives. The first line of research has taken financial and game theory perspectives (Jalali et al., 2019; Qian et al., 2018; Mayadunne and Park, 2016; Srinidhi et al., 2015), emphasizing the economic value of the investment. This approach considers the investment's decision to be determined by the economic profitability of the investment in terms of the level of protection. Huang et al. (2008) indicate that each company should consider the threats and vulnerabilities, aiming for an equilibrium between protection and investment that result in an acceptable risk level. The second line of research takes the point of view of the decision of the IT manager[2] and addresses the factors (drivers) that motivate the IT manager to invest in cybersecurity. Internal factors such as attitude, self-efficacy, experience, and habits, or exter-

* Corresponding author.
E-mail address: jcfern@essex.ac.uk (J.C. Fernandez de Arroyabe).

[1] Following Arranz and Fernandez de Arroyabe (2009), the word "complex" refers to the multiple levels and the heterogeneity of agents.

[2] This approach to the cybersecurity investment decision has been made from different theoretical lenses (see Table 1) such as Protection Motivation Theory (Menard et al., 2017; Zhao et al., 2016; Ifinedo, 2012; Vance et al., 2012), Planned Behavioural Theory (Ifinedo, 2012) or Habit Theory (Vance et al., 2012).

https://doi.org/10.1016/j.cose.2022.102954

Table 1
The conceptualization of organizational and cybersecurity capability.

Organizational Capability: *the power or ability to generate an outcome in the* organization.	**Cyber Capability:** *the power or ability to protect and avoid the threats and attacks in the* organization.
Definition	***Definition***
• Amit and Schoemaker (1993): organizations' capacity to deploy resources, using organizational processes, to effect a desired end. • Eisenhardt and Martin (2000): specific and identifiable processes, through which the organization manages its resource, to obtain the success of the company. • Ulrich and Lake (1990): businesses' ability to establish internal structures and processes that influence its members to create organization-specific competencies and thus enable the business to adapt to changing customer and strategic needs.	***Cyber Capabilities*** • Woon et al. (2005): the ability to handle threats and avoid losses or damages that might derive from these threats. • ISO 27000 (ISO/IEC 27001:2013, 2013): a dynamic process in which resources, competencies and routines interact in the development of cybersecurity systems. ***Cyber Dynamic capabilities*** • Kosutic and Pigni, (2021): permitting the development of cyber-resistance and security innovation
Key elements • *Organizationa*l resources: all assets, organization attributes, information, knowledge, etc. controlled by a organization that enables the organization to conceive and implement strategies that improve its efficiency and effectiveness. • Organizational procedures: specific methods employed to express policies in action in the day-to-day operations of the organization. • Organizational rules: interaction patterns that are pertinent to the coordination of organizational activities and differentiate them from actions that are preceded by decision making.	***Key elements*** (Kosutic and Pigni, 2021; Ifinedo, 2012) • Cybersecurity resources: resource management that provides strategic direction for security activities, ensuring the cybersecurity objectives. For example a cybersecurity board. • Cybersecurity procedures: the specific methods employed, to identify, analyze and prioritise the risks and threats of IT systems. For example an internal audit, any business-as-usual health checks. • Cybersecurity rules: the interactions patterns of the organization to ensure the cybersecurity objectives, For example, up-to-date malware protection, access rights to specific users, encrypting and security controls.

nal factors such as the severity of the attack, have been the main factors analyzed (see Table 1). However, both approaches have been recently criticised as they do not provide a satisfactory explanation of which factors determine the decision of organizations to invest in cybersecurity systems (Shao et al., 2020; Pérez-González et al., 2019; Weishäupl et al., 2018; Fielder et al., 2016; Mallinder and Drabwell, 2014; Caldwell, 2013; Weber, 2012; Choo, 2011). Jalali et al. (2019), and Bose and Luo (2014) have pointed out the difficulties that entail achieving equilibrium between risks and investment. In general, organizations have problems in determining the severity of the attacks and the implications in terms of costs, disruption time, loss of data, and the cost of additional personnel derived from the attacks (Shao et al., 2020). Moreover, criticism also esteems from the decision processes in organizations, where both the IT department and the senior-managers of the organizations take part in the decision to invest in cybersecurity systems (Moore et al., 2015; Ifinedo, 2012). As indicated by Cyber Security Breaches Survey (CSBS) (2019), over 33% of the managers do not receive updates over the cybersecurity or they do it once per year, with only 21% of senior managers receiving information on a daily or weekly basis. In fact, the traditional structure of organizations does not involve senior managers in the cybersecurity processes as it relegates cybersecurity to an operational rather than strategic function concentrated in the IT department (Moore et al., 2015) .[3] All of these contribute to myopia at the management level when it refers to investment in cybersecurity systems. For instance, 80% of CISOs claim not to have a sufficient budget (Deloitte, 2016), and 81% of CISOs are not confident that their companies can effectively address a cybersecurity incident (ServiceNow, 2017; Jalali et al., 2019).

To understand the shortcomings, firstly, we assume that cybersecurity should be a strategic function in the organizations (Adesemowo, 2021 [4]; Chronopoulos et al., 2017). In this line, Chronopoulos et al., 12,175) point out that *cybersecurity is not only a defensive manoeuvre but also a strategic decision that may increase the competitive advantage of an organization over potential rivals*. Therefore, this will imply that the investment in cybersecurity is a decision of the organization, in which all levels of the company are involved, with the senior managers of the company having an important weight in the decision (S. Okae et al., 2019). Secondly, in this paper, the theoretical approach is dynamic capabilities theory (Eisenhart and Martin, 2000). Jalali et al. (2019) point out that effective investments in IT, and information security in particular, require allocating resources to cybersecurity capabilities. From a dynamic capabilities perspective, the possession of resources affects the capabilities, through the development of competencies, increasing the control of activities, and, finally, creating organizational routines (Anzola-Román et al., 2018; Jalali and Kaiser, 2018; Adesemowo, 2021). That is, managers can not only effectively reduce potential losses due to cyberattacks, but also improve the overall performance of their operations.

In this context, our research model considers that the cybersecurity investment, as a strategic decision, will be influenced by internal (cyber-capabilities) and external factors (threats and attacks of the cyber-environment). The investment in cybersecurity is related to the capabilities of the organizations in this area, which reflects the resources, competencies and organizational routines that determine propensity of organizations to develop cybersecurity protection activities (Bulgurcu et al., 2010; Posey et al., 2015; Lee et al., 2018). In this paper, we assume the conceptualization de cybersecurity investment from CSBS (2019, 2018), which defines cybersecurity as the set of organization' expenditures, which aim to develop activities or projects targeted at preventing or identifying cybersecurity breaches or attacks.[5] Therefore, the investment in cybersecurity is conditioned by the organizations' perception of the digital environment of the organization. When companies are attacked, this means not only economic costs for organizations but also legal and reputational costs (Shin et al., 2018; Bulgurcu et al., 2010). Thus, companies will decide to invest in cybersecurity systems as a way to anticipate and protect from future threats and attacks, and to guarantee the operability of the information systems.

[3] Okae et al. (2019) find a greater presence of IT managers on company boards.

[4] Adesemowo (2021) point out that '*Frameworks such as COBIT 2019 (ISACA, 2018), King IV (Institute of Directors in Southern Africa, 2016), Enterprise risk management/internal controls frameworks by Committee of Sponsoring Organizations of the Treadway Commission's (COSO, 2013; 2017), and literature (Ahmad et al., 2014; Goosen and Rudman, 2013; Kim et al., 2018) concurred that IT is strategic*'.

[5] These expenditures include software, hardware, staff, salaries, outsourcing and training-related expenses.

Hence, we pose a research question: *how do attacks on the cyber-environment and the cyber-capabilities of the companies will affect the investment in cybersecurity systems?*

For this, our study uses the Cyber Security Breaches Survey (2019, 2018). As compared to previous studies that have focused on organizations' case studies, we make use of a sample of the 4168 UK organizations since 2019 and 2018, which allows reflecting on the investment of cybersecurity in enterprises, getting an overall picture of the behavioral pattern of organizations and being able to generalize the results. Moreover, as an instrumental approach, we use Machine Learning techniques (ML). In particular, our analysis uses Artificial Neural Networks (ANNs) and K-mean clusters, which are a type of Machine Learning (ML) methods that allows analyzing the complex problems. Compared to conventional regression methods, which have important concerns (Ciurana et al., 2008; Somers and Casal, 2009), ML permits a good pattern recognition and modelling of multivariate non-linear relationships and of datasets with problems of missing data. This is especially relevant in cybersecurity, since obtaining quantitative information on the type of attacks and their frequency is an important concern (Holland, 2017; Arranz et al., 2021).

2. Conceptual framework and research model

2.1. Dynamic capabilities approach: cyber-capabilities

Dynamic capabilities consist of a set of higher-level activities that allow organizations to orientate their activities to high-payoff endeavours (Faridian and Neubaum, 2020; Fainshmidt et al., 2016; Teece, 2014). This requires managing and coordinating organizational' resources to address rapidly changing business environments (Teece, 2014). Dynamic capabilities encompass two important elements: capabilities and dynamic (Bitencourt et al., 2020). The term "capabilities" refers to the capacity of organizations to deploy resources, using organizational processes to achieve an objective (Barreto, 2010; Fainshmidt et al., 2016). Organizations' capabilities result from learning, organizational resources and organizational histories (Suddaby et al., 2020; Teece, 2014). The term "dynamic" refers to the changing nature of the environment and the ability of organizations to change their capabilities, (Zahra et al., 2006).

Regarding IT systems, Bharadwaj (2000) consider IT as an organizational capability. Similarly, Jalali et al. (2019) introduce cybersecurity capabilities as an organizational capability and focus on the challenges to develop them within organizations. Woon et al. (2005) define the cybersecurity capabilities of an organization (cyber-capabilities) as the ability to handle threats and avoid losses or damages that might derive from these threats. Organizations build up cybersecurity capabilities in a dynamic process in which resources, procedures, and routines interact in developing the cybersecurity systems (Burns et al., 2019; Jeong et al., 2019; Rai and Tang, 2010; ISO 27000, 2007; Ravichandran et al., 2005). Firstly, cybersecurity capabilities involve the management of cybersecurity resources (see Table 2). The existence of a cybersecurity board together with employees designated for cybersecurity tasks, or an outsourced provider in charge of managing the organizations' cybersecurity, are the resources that organizations usually deploy for risk management. Secondly, cybersecurity capabilities imply the development of procedures for cybersecurity risk management. For example, it is well known that companies use cybersecurity procedures as internal audits, and any business-as-usual health checks, either undertaken regularly or ad-hoc, etc. (see, for example, ISO 27000, 2007). Moreover, the existence of organizational routines, such as up-to-date malware protection, access rights to specific users, encrypting and security controls, are the most frequent routines employed by organizations.

Table 2
The main theoretical approach to the IT decisions.

Planned Behavioral Theory (PBT) (see, for example, Ajzen, 1991; Krueger y Brazeal, 1994; Kolvereid, 1996; Rise et al., 2003)
- PBT studies the individual's intention to develop an action.
- PBT postulates that individual behavior is influenced by attitude, subjective norms and perceived behavioral control.

Perceived behavioral control (PBC) (see, for example, Ajzen, 2002; Conner and Armitage, 1998).
- PBC stresses that the behavioral decision to develop a strategy is conditional on the degree to which the manager applies control to the behavior of interest, his or her self-efficacy, and the strategy's perceived feasibility.
- Conner and Armitage (1998) suggest that control comes in two forms: internal control, based on factors that come from within the individual (e.g., self-efficacy, motivation), and external control, based on factors that come from outside the individual (e.g., task difficulty, access to necessary resources). Thus, the perceived difficulty implicitly takes into account both internal and external control factors.

Protect motivation theory (**PMT**) (see, for example, Rogers, 1983; Woon et al., 2005; Herath y Rao, 2009; Vance et al., 2012; Ifinedo, 2012; Zhao et al., 2016; Menard et al., 2017)
- PMT explains how people are motivated to respond to threats or dangerous behaviors.
- PMT points out that the motivation for protection arises both from the evaluation of threats and from the evaluation of the capacity of the response.
- PMT postulates that individual behavior is influenced by perceived vulnerability, perceived severity, self-efficacy, response effectiveness, and response cost.

Self-Determination Theory (SDT) (see, for example, Ryan and Deci, 2000; Deci and Ryan, 2002; Grant and Ashford, 2008).
- SDT proposes that individuals are proactive with their potential and master their internal forces, such as drives and emotions (Deci and Ryan, 2002).
- SDT assumes that people are active organisms, with tendencies toward growing, mastering ambient challenges, and integrating new experiences, taking an active role in their work. This is in contrast to a more passive and reactive behavior pattern. Proactive people actively seek information and opportunities to improve things; they do not passively wait for information and opportunities to go to them.

Theory of habits (TH) (see, for example, Vance et al., 2012; Ifinedo, 2012; Fielder et al., 2016).
- TH suggests that many actions occur without a conscious decision to act and are performed because individuals are accustomed to performing them (Vance et al., 2012). Thus, the behavior is often more controlled by situational signals than by conscious decision making.
- TH points out that the beginning of a new behavior requires a conscious decision (Vance et al., 2012). This new behavior is done gradually until after the time it becomes automatic.

2.2. The cybersecurity in the organization: a strategic position

In Table 2, we show the main approaches that have been used in the literature to explain the manager's decision in the context of IT systems. These previous approaches have been criticized by the literature because they do not adequately explain companies' decisions to invest in cybersecurity systems. Easttom (2012), and Fielder et al. (2016) point out that in the face of these individual decisions within the company, the decisions in the company must be analyzed as a whole, considering the factors that influence them. Harrison (1996) already established a series of criteria to differentiate the individual decision from the decision of the organization.[6] Organizations' decisions must consider the organiza-

[6] Following Harrison (1996), there are five criteria for identifying and making a strategic decision:• The decision must be directed towards defining the organization's relationship to its environment.• The decision must take the organization as a whole as the unit of analysis.• The decision must encompass all of the major func-

tion as a unit of analysis, given that decisions are based on the organization's relationship to its environment.

Recent studies have highlighted the strategic nature of cybersecurity (Adesemowo, 2021; S. Okae et al., 2019), emphasising its importance for the correct functioning of organizations and reputation. In addition, an adequate cybersecurity investment enables organizations to fulfil the requirements of an information system (ISO/IEC 27001:2013; ISO/IEC 27002:2022; CLUSIF, 2008), which in the case of non-compliance usually entails operational problems, economic loss, and legal responsibility for the organization (Warkentin et al., 2016; Hamid et al., 2006). To guarantee the security of information systems(IS), organizations should include all members of the organization, introducing solutions that are complex, up-to-date and proven and that ensure faster and more effective actions against cyber-attacks (Lee et al., 2018; CLUSIF, 2008). This is only possible if organizations adopt a position in which cybersecurity is part of the organizations' strategy (Choo, 2011; ISO/IEC 27000, 2009; CLUSIF, 2008).

2.3. Research model: organizations' investment in cybersecurity systems

Our research model considers that organizations' investment in cybersecurity systems is a strategic decision, derived from the importance it has for its operation and performance, as well as the responsibilities that may arise from the incorrect operation. Literature suggests that cybersecurity investment decisions involve a complex decisional process, which is not without difficulty for organizations (Moore et al., 2015; Hamid et al., 2006), being the senior manager who rationally coordinates the organization's decisions. Moreover, the literature suggests that organizations' decision is the result of the reflection of the organization, and their decisions are based on their capabilities, and influences on the social environment (Teece, 2007; Eisenhardt and Martin, 2000).

First, cyber-capabilities allow organizations handling threats and avoiding losses or damages that might derive from these threats, in a dynamic process in which resources, procedures, and routines interact in developing the cybersecurity systems (Kosutic and Pigni, 2021). Second, cybersecurity investment decisions not only rely on the cyber-capabilities of the organization but also on external threats and attacks. Contech and Schimick (2016) point out that more and more attacks on the vulnerabilities of organizations are intensifying, diversifying and sophisticating, which makes it difficult to estimate the impact and outcomes. How cyber-attacks occur are varied, depending on the typology and frequency of the attacks. In this sense, organizations evaluate the likelihood of being attacked and the potential impact on the organization (Feng et al., 2019; Shin et al., 2018; Benaroch, 2018; Conteh and Schmick, 2016; Wright et al., 2014; Cybenko et al., 2002), Thus, a higher level of the potential severity of cyber-attacks increases the probability of organizations' investing in cybersecurity systems.

In Fig. 1, we can see the research model where the investment in cybersecurity will be determined by factors such as *the capabilities of cybersecurity and the attacks on the cyber-environment.*

3. Methodology

3.1. Unit of analysis and target study population

In this study, the data is collected from the Cyber Security Breaches Survey. The Cyber Security Breaches Survey is a survey of UK organizations, 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 survey was designed to collect information about a range of topics related to cybersecurity. First, the survey asked about organizations' the perception of cybersecurity; e.g.: how organizations approach the management of cybersecurity risks; what is the level of awareness and the attitude of organizations toward cybersecurity; what is the perception of organizations on the information and guidance available on cybersecurity; and reasons why managers thought cybersecurity was important. Second, the survey covered topics related to organizations' own experiences with cybersecurity; e.g.: organizations' previous experiences with cybersecurity breaches; the impact and nature of these breaches; and organizations' managerial approach and expenditures on cybersecurity.

The unit of analysis is the organization, and for this study, we use two samples, for the years 2019 and 2018. The samples were obtained using the Government's Inter-Departmental Business Register (IDBR), which includes UK organizations across all sectors. The Cyber Security Breaches Survey 2019 and 2018 comprised two quantitative random probability telephone surveys, carried out from 10 October 2018 to 20 December 2018, and from 9 October 2017 to 14 December 2017, respectively.

The Cyber Security Breaches Survey is statistically representative of UK businesses both in all sizes and sectors. The Cyber Security Breaches Surveys (2019 and 2018) use random-probability sampling to avoid selection bias, and the second includes micro and small businesses, which ensures that the respective findings are not skewed towards larger organizations.

The two samples were treated separately, analyzing the data with SPSS, both for the year 2018 and 2019. The same analyses were performed on each of the two samples, permitting to compare them. After a revision to clean the databases, it was only necessary to recode the various missing values, being able to fully use both databases. Thus, the first sample (2019) contains the cybersecurity information from 2080 UK companies, and the second sample (2018) includes the information about 2088 UK companies.

3.2. Measures

3.2.1. Dependant variable

The dependant variable for this analysis is the organizations' *investment* in cybersecurity. The survey includes a question on organizations' expenditures prevision in activities or projects aimed at preventing or identifying cybersecurity breaches or attacks. These expenditures include software, hardware, staff, salaries, outsourcing and training-related expenses. The dependant variable is measured as an ordinal scale, determined by cybersecurity investment intervals. Table 8 shows the various investment steps and the distribution of the companies based on these expenses.

3.2.2. Independent variables

For explaining organizations' investment in cybersecurity, we define two sets of explanatory variables. The first set of variables corresponds to organizations' cyber-capabilities. The second set of variables refers to the threats and attacks of UK organizations.

The first independent variable is *cybersecurity resources*. With this variable, the survey aims to capture the different cybersecurity management resources used by organizations in the last 12 months. The survey defines five items that measure the management resources in the organization: i) Board members with responsibility for cybersecurity; ii) An outsourced provider that man-

tions performed in the organization.• The decision must provide constrained guidance for all of the administrative and operational activities of the organization.• The decision must be critically important to the long-term success of the total organization.

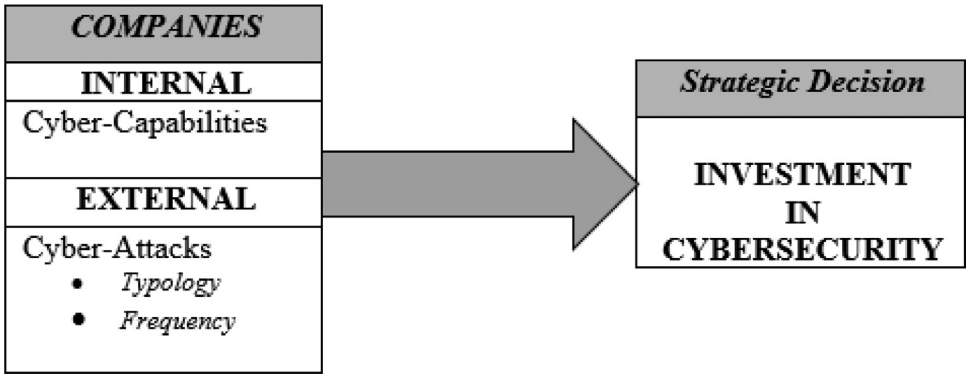


Fig. 1. Research model.

ages your cybersecurity; iii) A formal policy or policies in place covering cybersecurity risks; iv) A Business Continuity Plan; and v) Staff members whose job role includes information security or governance (RESOURCES). In line with Costantini et al. (2017), and Arranz et al. (2021), the dependant variable was formed as a cumulative index of the five items. This method has advantages over other methods such as factor analysis, in that we have no loss of variance, it maintains the typology of the measuring scale and it allows us to measure resources in all their breadth, both in diversity and intensity. Methodologically, there are two requirements: first, a high level of reliability between variables (Cronbach's Alpha (2018): 0.672; Cronbach's Alpha (2019): 0.671) ,[7] and second, that the scales of the variables are consistent with each other.

The second independent variable is the *cybersecurity procedures* that organizations have conducted in the last 12 months. The survey provides five items: i) An internal audit; ii) An external audit; iii) Any business-as-usual health checks that are undertaken regularly; iv) Ad-hoc health checks or reviews beyond your regular processes; v) A risk assessment covering cyber security risks; and vi) Invested in threat intelligence Following the same method that in the above variable, we have grouped the six items into one variable (PROCEDURES) as a cumulative index (Cronbach's Alpha (2018): 0.662; Cronbach's Alpha (2019): 0.653).

The third independent variable refers to the *cybersecurity rules* used by the organization in the last 12 months. The survey contains a set of eleven possible rules: i) Applying software updates when they are available; ii) Up-to-date malware protection; iii) Firewalls with the appropriate configuration; iv) Restricting IT admin and access rights to specific users; v) Any monitoring of user activity; vi) Security controls on company-owned devices (e.g. laptops); vii) Only allowing access via company-owned devices; viii) A segregated guest wireless network; ix) Backing up data securely via a cloud service, and x) Backing up data securely via other means. Also, the new variable (RULES) is created as a cumulative index (Cronbach's Alpha (2018): 0.744; Cronbach's Alpha (2019): 0.686).

Regarding the second set of independent variables, the first variable in this set is the *typology of attacks.* The survey presents a set of nine items: i) Computers becoming infected with ransomware; ii) Computers becoming infected with other viruses, spyware or malware; iii) Attacks that try to take down your website or online services; iv) Hacking or attempted hacking of online bank accounts; v) People impersonating your organization in emails or online; vi) Staff receiving fraudulent emails or being directed to fraudulent websites; vii) Unauthorised use of computers, networks or servers by staff, even if accidental; and viii) Unauthorised use or hacking of computers, networks or servers by people outside your organization. The variable TYPOLOGY of ATTACK has been created as a cumulative index (Cronbach's Alpha (2018): 0.664; Cronbach's Alpha (2019): 0.654).

The last variable refers to the *frequency of the attacks* (FREQUENCY). The variable is measured with a Likert scale with values 1 to 6. A value of 1 corresponds to a one-time event; a value of 2 is more than once but less than once a month; 3 when the frequency is roughly once a month; 4 for attacks that occur roughly once a week; 5 for attacks occurring roughly once a day; and 6 for attacks that take place more than once per day.

3.2.3. Robustness of survey

In our empirical analysis, we have also checked the robustness of the survey, testing the common method variance (CMV), to avoid bias in the estimation of the covariance between variables. Podsakoff et al. (2012) pointed out that the problem can arise in cross-sectional studies, where independent variables and dependant variables are collected simultaneously with a similar format (for example, the use of consistent Likert-type scales). This may produce an error as a consequence of introducing a systematic variance in the responses, which may affect the reliability and validity of the measures. Podsakoff et al. (2003) propose a testing method, applying factor analysis,[8] which is fundamentally based on detecting the non-existence of highly correlated variables. Thus, we proceed to introduce all the variables in the factor analysis. The existence of CMV is determined by the number of new variables or constructs created by factor analysis. Thus, if the number of constructs is low, and there are factors with high variance (> 50%), there is a probability of bias and therefore the existence of CMV (Podsakoff et al., 2012).

[7] Cronbach's alpha is a way to assess reliability by comparing the amount of shared variance, or covariance, between the items that make up an instrument to the amount of overall variance. The idea is that if the instrument is reliable, there should be a lot of covariance between the items relative to the variance. Cronbach's alpha is equivalent to taking the average of all possible reliabilities divided in half. Pallant (2001) states that the Alpha Cronbach value above 0.6 is considered highly reliable and an acceptable index. The formula for the Cronbach's alpha is: $\alpha = \frac{N\bar{c}}{\bar{v}+(N-1)\bar{c}}$ where N is equal to the number of items, $\bar{c}$ is the average inter-item covariance among the items and $\bar{v}$ equals the average variance.The MathML code is : \alpha = \frac{N \bar{c}}{\bar{v} + (N-1) \bar{c}};

[8] Factor analysis is a statistical technique that reduces the amount of data by means of correlation among variables. Factor analysis is used when there is a set of variables, which are highly correlated, and it is desired to reduce them to a new variable (called construct) that jointly explains all the variables.The variables are modelled as linear combinations of factors. To test the validity and reliability of the analysis, various tests are implemented: (1) the significance of the model, (2) KMO test, and (3) the explained variance.The first one determines whether a construct is significant (sig. <0.05).The KMO test takes values between 1, meaning that the constructs explains and perfectly adjust to the initial variables, and 0, where the construct does not explain the model.The explained variance shows the percentage of variation accounted for by the new construct (range: 0% to 100%).

3.3. Methodology

As indicated in the introduction, the paper utilises Machine Learning (ML) techniques as the methodological and instrumental framework. ML is framed as a subfield of artificial intelligence, which is characterised as the capability of a machine to mimic intelligent human behavior (Alpaydin, 2021). Hence, machine-learning algorithms are computational methods utilised to learn or uncover hidden patterns rooted in the data, which allows a machine to learn automatically from previous data without having to programme it explicitly. Moreover, machine learning encompasses a set of computational algorithms that by learning from existing data can perform pattern identification, classification, and prediction (Alpaydin, 2021011).

Regarding the study of business, most of the problems of companies are based on decision-making. These decisions involve the interaction of various variables through a dependency relationship. These types of problems are solved via traditional methods of regression, looking for the relationship between dependant and independent variables. Thus, linear regression, logistic regression (Logit, Probit, Tobit), etc., are conventionally used, supplemented with methods of Structural Equations Models (SEM). Each method has its own restrictions such as collinearity, endogeneity, etc. (Hair, 2006). Moreover, in many cases, the decisions of the companies involve non-linearity, not a direct causality, and multiple interactions (for example, Arranz and Fernandez de Arroyabe, 2009; Arranz et al., 2021). All of this means that the explanatory capacity of the classical models is reduced (Hair, 2006; Asteriou and Hall, 2015). In this context, Fernandez de Arroyabe and Fernandez de Arroyabe (2021) point out that ML has the capacity to give an adequate answer to complex problems, where interactions between variables, non-linearity, and collinearity problems are present.

In this paper, we estimate the research models, using an artificial neural network (ANN), which considers the interaction and interdependence between input variables. 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.

Regarding the typology of ANN, for this application, we have used a multilayer perceptron (MLP) (Fig. 2). This architecture is known as a supervised network in the sense that the predicted results can be compared against known values of the dependant variables. The network architecture of an MLP has an input layer, hidden layers, and an output layer. The hidden and output layers' neurons, with their associated weights, are connected, which allows for analyzing the interaction between input variables.

To design the ANN-MLP architecture, we follow Wang (2007), and Arranz and Fernandez de Arroyabe (2010), see Table 3. In the procedure of design of the ANN-MLP architecture, we can distinguish two key points: i) the choice of the number and size of the hidden layers, and ii) the choice of the learning algorithm. First, 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 are determined by testing several combinations of the number of hidden layers and the number of neurons, using a *trial* and *error approach* (Ciurana et al., 2008; Mohrotra, 1997; Master, 1999). That is, the selected architectures are tested with diverse activations functions, finding that the best architecture is one that minimizes the error. We have established

Table 3
Steps of the ANN 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 the efficiency are dependant 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 choice of an appropriate number of hidden neurons is extremely important; if few are used, few resources would be available to solve the adjustment problem and the use of too many neurons would increase the training time in addition to causing an overfit. Ciurana et al. (2008) and Mohrotra (1997) point out that for function approximation a two-layer neural network is usually sufficient to accurately model. Regarding the number of neurons in each hidden layer, Hegazy et al. (1994) proposed that the number of neurons should be 0.75m or m, where m is the number of input neurons. Master (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 (Master, 1993; Bishop, 1995).
- The types of activation functions, typically, can be:
- For the hidden layer, we can use sigmoid logistic (values from 0 to 1) and a hyperbolic tangent (−1 to 1),
- For the output layer: softmax (identity) function.

3. The learning algorithm
Backpropagation. This learning algorithm determines the connection weights of each neuron, readjusting the weights and minimizing the error.
The backpropagation algorithm (Rojas, 1996) works as follows: an input is set as a stimulus for the first layer of neurons in the network, this stimulus spreads through all the layers until it generates an output. The result obtained in the output neurons is compared with the actual output and an error value is calculated for each output neuron. These errors are then transmitted backwards, starting from the output layer, to all the neurons in the intermediate layer that contribute directly to the output, receiving the approximate error percentage of the participation of the intermediate neuron in the original output. Based on the value of the error received, the connection weights of each neuron are readjusted. This process is critical for network optimization and error minimization.

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.

the following model considering the input and output variables.

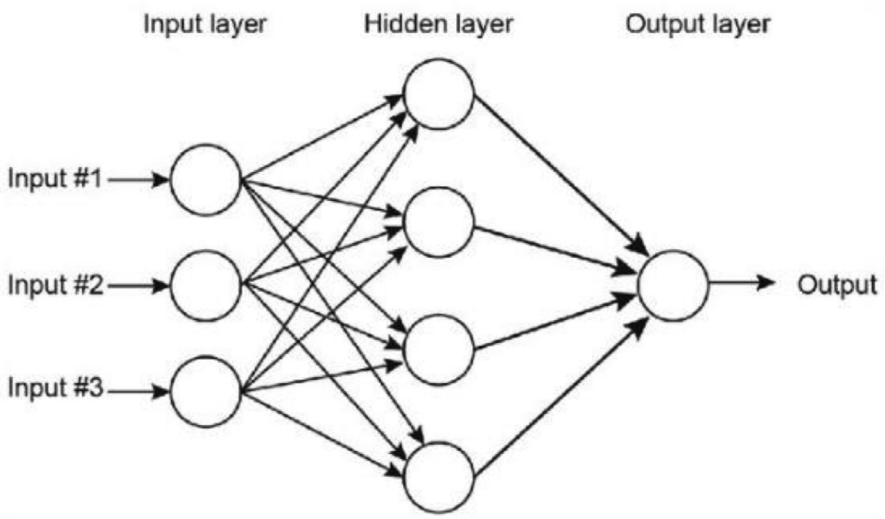
$$\text{Model}: Investment = f(RULES;\ PROCEDURE;\ RESOURCES;\ TYPOLOGY\ ATTACKS;\ FREQUENCY\ ATTACKS)$$

Second, regarding the choice of the learning algorithm, we use a backpropagation algorithm. This learning algorithm determines the connection weights of each neuron, readjusting the weights and minimizing the error. The equation for modifying the algorithm weights is shown below:

$$\Delta wji(n+1) = \Delta \cdot \mu_{pi} \cdot x_{pi} + \beta \Delta w_{ji}(n)$$

where,

w_{ji}= weight neuron i and j



Source: Manning et al. (2014)

Fig. 2. ANN Multilayer Perceptron (MLP) architecture. Source: Manning et al. (2014).

Table 4
ANN-MLP architecture for investment in cybersecurity analysis.

Model	Output variable	Imputvariables	ANN architecture	Activation Functions	Error Function
Model Year 2018	Investment	RESOURCES PROCEDURES RULES ATTACKS FREQUENCY	5–4-12	• Hyperbolic tangent • Identity (Sofmax)	Cross-entropy
Model 2 the Year 2019	Investment	RESOURCES PROCEDURES RULES ATTACKS FREQUENCY	5–7-12	• Hyperbolic tangent • Identity (Softmax)	Cross-Entropy

n= number of interactions
$\mathcal{E}$= learning rate
μ_{pi}= neuron j error for pattern p
x_{pi}= output of neuron i for pattern p
β=momentum

From the equation, we can see that there are three critical variables: the *number of interactions*, the *learning rate*, and the *moment*. Regarding the number of interactions (n), we have used 10,000.[9] As for the value of the learning rate (β), it controls the size of the change of the weights in each iteration,[10] a value of the learning rate is usually between 0.05 and 0.5. Finally, the moment factor (α) accelerates the convergence of the weights. Hassoun (1995), and Yegnanarayana (2009) point out that a value close to 1, for example, 0.9, is a good value.

The results of the architecture for the model are shown in Table 4. The structure for 2018 is 5–4–12,[11] which means that there are 5, 4, and 12 neurons in the input, hidden and output layers respectively.[12] In the case of the hidden layer, the activation function used was the hyperbolic tangent and the softmax function for the output layer.

Fig. 3

The analytical equation of our simulation with ANN-MLP takes the following form:

Regarding the robustness of the analysis, we have developed a second test, using cluster analysis. In fact, we analyze the existence of different behaviors/groups of companies depending on the investment in cybersecurity. For this, we use a statistical model K-means cluster, which allows us to obtain different groups of companies. As classification variables, we use the investment variable. Table 5 describes the K-means cluster analysis, and the procedure.

4. Analysis and results

Before analyzing the results, we have performed checks of the survey to verify our data quality, following Podsakoff et al's method (2003). This analysis reveals twelve distinct latent constructs that account for 54.05% of the variance for 2019. The first factor accounts for 12.99% of the variance, which is below the recommended limit of 50 percent. Along these same lines, the results of the analysis for 2018 show seven variables, which explain 47.29% of the variance. This result suggests CMV and CMB are not a concern in our results. Moreover, the sample is composed of a

[9] Normally the number of iterations ranges from 1000 to 10,000, and a trial and error process is recommended (Cabaneros et al. 2019; Yegnanarayana, 2009).

[10] Two extremes should be avoided: too little of a learning rate can cause a significant decrease in the speed of convergence and the possibility of ending up trapped in a local minimum; instead, too high of a learning rate can lead to instabilities in the error function, which will prevent convergence from occurring because jumps around the minimum will be made without reaching it. Therefore, it is recommended to choose a learning rate as large as possible without causing large oscillations (Hassoun, 1995).

[11] The output variable is investment in cybersecurity with a 12 Likert scale range.

[12] To obtain these results, the 70.3% of observations were used in the training, 19.7% in the testing and 10.0% in the holdout phases.

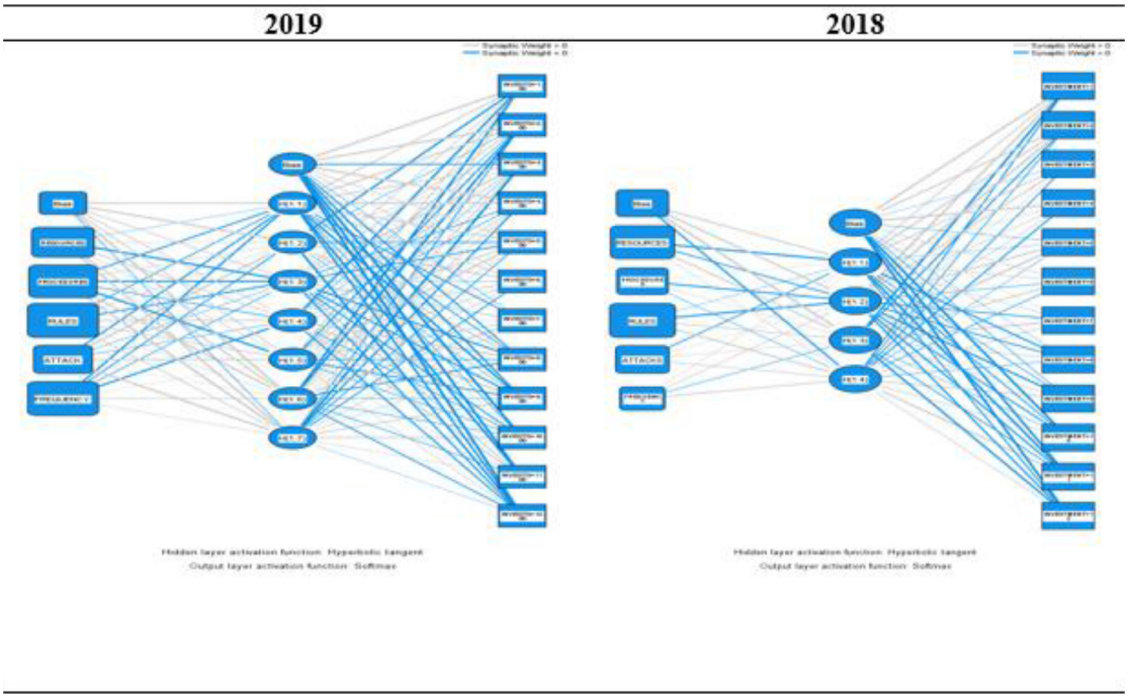


Fig. 3. AMM-MLP architecture and topology.

$$Investment = h\left[\sum_{k=1}^{k} \alpha_k \cdot g\left(\sum_{j=1}^{j} \beta_{jk} \cdot X_j\right)\right]$$

with X_j being the input variables;
j the number of input variables;
$h(.)$ and $g(.)$ the hyperbolic tangent and softmax activation functions;
α_k and β_{jk} the input and hidden network weights, respectively;
k the number of hidden layers.

Table 5
Cluster analysis: K-mean cluster.

Description
Cluster analysis is a set of data reduction techniques which are designed to group similar observations in a dataset, such that observations in the same group are as similar to each other as possible, and similarly, observations in different groups are as different to each other as possible. *K-means* is one method of cluster analysis that groups observations by minimizing Euclidean distances between them.
Procedure
To perform k-means clustering, the algorithm randomly assigns k initial centres (k specified by the user), either by randomly choosing points in the "Euclidean space" defined by all n variables, or by sampling k points of all available observations to serve as initial centres. It then iteratively assigns each observation to the nearest centre. Next, it calculates the new centre for each cluster as the centroid means of the clustering variables for each cluster's new set of observations. K-means re-iterates this process, assigning observations to the nearest centre (some observations will change cluster). This process repeats until a new iteration no longer re-assigns any observations to a new cluster. At this point, the algorithm is considered to have converged, and the final cluster assignments constitute the clustering solution.
The standard algorithm is the Hartigan-Wong algorithm, which aims to minimize the Euclidean distances of all points with their nearest cluster centres, by minimizing the within-cluster sum of squared errors (SSE).

balanced sample of companies by their size, both micro, small, medium and large companies, as we see in the distribution of Table 6.

Tables 7 to 10 display the descriptive analysis. Regarding the integration of IT systems in the organizations in our sample, around 80% of the organizations integrate from three to five online services as well as the use of email, websites, online bank payments and social networks (see Table 8). Table 7 shows the perception and the attitude of the UK organizations in cybersecurity where we observe a high degree of priority, with 80% of the organizations considering cybersecurity a high or very high priority. Regarding the updates that managers have on cybersecurity issues, we observe a low level of communication between the IT department and the senior managers of the organization. In a nutshell, our descriptive statistics reveal that organizations consider cybersecurity a priority, but with a poor information level amongst senior managers on cybersecurity topics.

Regarding the management of cybersecurity, around 70% of the sample spend less than £10,000 on cybersecurity (Table 8). In particular, for the cybersecurity resources management, about 50% of the organizations use Business Continuity Plans, and cybersecurity policies and have employees that are specifically assigned to information security or have externalized the cybersecurity of the organization (see Table 9). Regarding the cybersecurity procedures, (Table 9), around 40.0% of the organizations claimed to have conducted business-as-usual checks, and the organization's internal audit procedures, and 30%, approximately, non-regular checks. When it comes to the cybersecurity rules employed by the sampled organizations, the results show the prevalence, over 90%, of malware protection, firewalls, and software updates (Table 9). Organizations also resort to restrictions on IT rights as well as the security control of organizations' devices.

Table 10 displays the frequency of occurrence of the attacks and breaches experienced by the sample organizations. As seen in the table, the majority of the organizations report having suffered attacks either only once or less than once per month at most. Moreover, the survey also collects information on the output and the

Table 6
Size of the companies of the sample.

Size	2019 Total	%	2018 Total	%
< 10 employees	871	41.9%	786	37.6%
10 to 49 employees	530	25.5%	600	28.7%
50 to 249 employees	417	20.0%	384	18.4%
≤ 250 employees	258	12.4%	315	15.1%
Missing	4	2%	3	1%
Total	2080	100.0%	2088	100.0%

Table 7
Cybersecurity in the companies.

Online Services	2019 Total	%	2018 Total	%
Emails	1907	91.7%	1945	93.2%
Website or Blog	1748	85.8%	1808	86.6%
Social Media Sites	1352	65.0%	1396	66.9%
Order, Book or Pay services	611	29.4%	595	28.5%
Pay Bank Account	1492	71.7%	1444	69.2%
Industrial Control System	58	2.8%	90	4.3%
Number of Online Services				
1.00	111	5.3%	96	4.6%
2.00	253	12.2%	248	11.9%
3.00	553	26.6%	576	27.6%
4.00	734	35.3%	725	34.7%
5.00	388	18.0	378	18.1%
6.00	9	0.4%	28	1.3%
Priority				
Missing values	32	1.5%	26	1.2%
Very high	991	47.6%	821	39.3%
Fairly high	760	36.5%	800	38.3%
Fairly Low	220	10.6%	279	13.4%
Very Low	77	3.7%	162	7.8%
Update				
Missing	110	5.3%	105	5%
Never	258	12.4%	360	17.2%
Less than once a year	107	5.1%	148	7.1%
Annually	242	11.6%	246	11.8%
Quarterly	464	22.3%	438	21.0%
Monthly	446	21.4%	415	19.9%
Weekly	177	8.5%	163	7.8%
Daily	174	8.4%	120	5.7%
Each time there is a breach or attack	102	4.9%	93	4.5%

Table 8
Investment in cybersecurity in the companies.

Investment		2019 Total	%	2018 Total	%
	Don't invest anything	538	25.9%	523	32.4%
	Less than £500	322	15.5%	325	20.1%
	£500 to less than £1000	112	5.4%	110	6.8%
	£1000 to less than £5000	302	14.5%	249	15.4%
	£5000 to less than £10,000	97	4.7%	107	6.6%
	£10,000 to less than £20,000	111	5.3%	107	6.6%
	£20,000 to less than £50,000	86	4.1%	77	4.8%
	£50,000 to less than £100,000	51	2.5%	53	3.3%
	£100,000 to less than £500,000	57	2.7%	42	2.6%
	£500,000 to less than £1 million	9	0.4%	6	0.4%
	£1 million to less than £5 million	8	0.4%	12	0.7%
	£5 million to less than £10 million	3	0.1%	2	0.1%
	Total	1696	100.0%	1613	100.0%
	Missing	384		475	
Total		2080		2088	

impact of the attack on sampled organizations. Table 10 shows the typology of the attack, e.g. damage to software or systems, destruction or alteration of data, money being stolen, etc. In general, the results show very low-frequency rates of positive answers to any of the possible outcomes of the cyber-attack.

Regarding the research question, which analyses how both cyber-attacks and a company's cyber-capabilities affect its likelihood of investing in cybersecurity, Table 4 shows the results of the ANN-MLP analysis. Previously, we test the robustness of the analysis, and we can point out that the robustness of the simulation is high, considering the various tests performed. First, we have tested the fitting of the ANN-MLP design, performing a level of the fitting upper to 70%. Second, we have analysed the correlation of the actual output variable and predicted output variable, getting a

Table 9
Cybersecurity capabilities in the companies.

Cybersecurity governance resources	2019		2018	
	Total	%	Total	%
Board members with responsibility for cybersecurity	843	40.5%	752	36.0%
An outsourced provider that manages your cybersecurity	1029	49.5%	989	47.4%
A formal policy or policies in place covering cybersecurity risks	1008	48.5%	862	41.3%
A Business Continuity Plan	1119	53.8%	1071	51.3%
Staff members whose job role includes information security or governance	1175	56.5%	1064	51.0%
Cybersecurity procedures				
An internal audit	854	41.1%	680	32.6%
Any business-as-usual health checks that are undertaken regularly	957	46.0%	920	44.1%
Ad-hoc health checks or reviews beyond your regular processes	678	32.6%	601	28.8%
A risk assessment covering cybersecurity risks	886	42.6%	731	35.0%
Investment in threat intelligence	319	15.3%	278	13.3%
Cybersecurity rules				
Applying software updates when they are available	1907	91.7%	1896	90.8%
Up-to-date malware protection	1890	90.9%	1871	89.6%
Firewalls with appropriate configuration	1879	90.3%	1853	88.7%
Restricting IT admin and access rights to specific users	1792	86.2%	1755	84.1%
Any monitoring of user activity	1060	51.0%	1023	49.0%
Security controls on company-owned devices	1559	75.0%	1485	71.1%
Only allowing access via company-owned devices	1352	65.0%	1292	61.9%
A segregated guest wireless network	996	47.9%	961	46.0%
Backing up data securely via a cloud service	1325	63.7%	1220	58.4%
Backing up data securely via other means	1394	67.0%	1462	70.0%

Table 10
Attack frequency and typology in the companies.

Attack frequency	2019		2018	
Total	Total	%	Total	%
Once only	185	22.3%	269	27.6%
More than once but less than once a month	224	27.0%	299	30.6%
Roughly once a month	175	21.1%	172	17.6%
Roughly once a week	108	13.0%	115	11.8%
Roughly once a day	60	7.2%	57	5.8%
Several times a day	52	6.3%	64	6.6%
Typology of Attack				
Computers becoming infected with ransomware	94	4.5%	165	7.9%
Computers become infected with other viruses, spyware or malware	189	9.1%	303	14.5%
Attacks that try to take down your website or online services	104	5.0%	132	6.3%
Hacking or attempted hacking of online bank accounts	61	2.9%	64	3.1%
People impersonating your organization in emails or online	336	16.2%	414	19.8%
Staff receiving fraudulent emails or being directed to fraudulent websites	698	33.6%	787	37.7%
Unauthorised use of computers, networks or servers by staff, even if accidental	56	2.7%	93	4.5%
Unauthorised use or hacking of computers, networks or servers by people outside your organization.	89	4.3%	124	5.9%

high correlation (The year 2018: 0.611; the year 2019: 0.633). Last, we have checked the predictability of our models, using the ROC curve,[13] which is a figure of sensitivity versus specificity, showing the classification performance (Woods and Bowyer, 1997). That is, if the curve moves away from the 45-degree, the accuracy of the model is higher. In our case, the ROC curve shows that the chosen architecture can predict more than 70% of the values of the output variable (Figs. 4 and 5).

Focusing on the results of the simulation of the impact of cyber-capabilities and cyber-attacks on investment in cybersecurity, Fig. 6 shows the normalized importance of each input variable in the output variable.[14] We observe that all cyber-capabilities have a positive and significant impact on the investment in cybersecurity, but with a differential impact. In the 2018 results there are two levels of impact, the first and highest corresponds to the cyber-capabilities (RULES: 0.305, 100% normalized value; RESOURCES: 0.302; 98.9% normalized value; PROCEDURES: 0.159, 52.5% normalized value), and with less importance and therefore less effect on investment in cybersecurity, the cyber-environment (FREQUENCY: 0.092, 30.2% normalized value; ATTACK: 0.142, 46.6% normalized value). For the 2019 results, the difference between cyber-capabilities and cyber-attacks disappears, with both factors having a similar impact in the level of investment in cybersecurity. In particular, RULES (0.222; 100% normalized value), FREQUENCY (0.221; 99.7% normalized value) and PROCEDURES (0.209; 94.4% normalized value) have high a positive effect in the investment. At a second level of importance are RESOURCES (0.182; 82.2% normalized value) and ATTACK (0.165; 74.4% normalized value).

[13] The ROC (Receiver Operating Characteristics) curve is a figure of sensitivity versus specificity, showing the classification performance, i.e. if the curve moves away the 45-degree, the accurate of the model is higher.

[14] Ibrahim (2013) revises some methods for assessing the relative importance of input variables in artificial neural networks. These methods are based on Garson's algorithm (1991), which uses the absolute values of the final connection weights when calculating variable contributions. $RI_x = \sum_{x=1}^{n} \frac{|w_{xy}\ w_{yz}|}{\sum_{y=1}^{m} |w_{xy}\ w_{yz}|}$ where RI_x is the relative importance of neuron x. $\sum_{y=1}^{m} w_{xy}\ w_{yz}$ represents the sum of the product of the final weights connection from input neurons to hidden neurons with the connnections from hidden neurons to output neurons.

2019

Area	
Don't invest anything	.762
Less than £500	.789
£500 to less than £1,000	.788
£1,000 to less than £5,000	.658
£5,000 to less than £10,000	.647
£10,000 to less than £20,000	.672
£20,000 to less than £50,000	.775
£50,000 to less than £100,000	.786
£100,000 to less than £500,000	.838
£500,000 to less than £1 million	.860
£1 million to less than £5 million	.815
£5 million to less than £10 million	.955

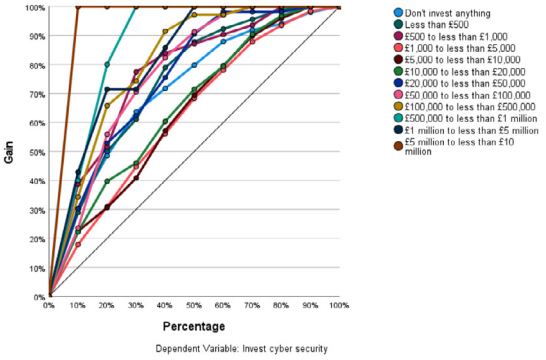


Fig. 4. The ROC curve (2019 and 2018).

2018

Area	
Don't invest anything	.784
Less than £500	.775
£500 to less than £1,000	.679
£1,000 to less than £5,000	.581
£5,000 to less than £10,000	.681
£10,000 to less than £20,000	.669
£20,000 to less than £50,000	.773
£50,000 to less than £100,000	.774
£100,000 to less than £500,000	.841
£500,000 to less than £1 million	.832
£1 million to less than £5 million	.970
£5 million to less than £10 million	.767

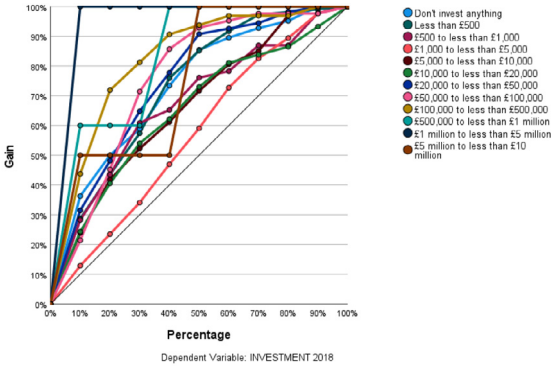


Fig. 5. The ROC curve (2018).

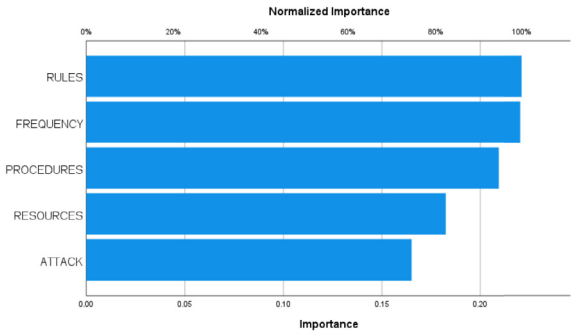
In addition, we have performed a cluster analysis to test the robustness of the analysis with ANN-MLP. In this case, the results of applying the K-mean cluster algorithm in the years 2018 and 2019, give us a solution of the three groups of companies (clusters), showing significant differences between the companies of each group in terms of investment in cybersecurity. In the tables in Fig. 7, we see the distribution of each cluster based on the number of companies included. To graphically illustrate the differences between the three clusters, both for the year 2018 and 2019, Fig. 7 represents the mean values of each cluster, both for the variable investment, resources, procedures, rules, attacks, and their frequency. Thus, we observe in the two years of analysis, that both the resources, procedures, rules and attacks, follow parallelism with the investment. In more detail, we see that in 2019, Cluster 3 (128 companies), has a higher average value of investment in cybersecurity than Cluster 2 (294 companies) and this in turn than Cluster 1 (1274 companies) and observing this same trend in the variables input, cyber-capabilities and cyber-attacks. The year 2018 follows the same pattern of behavior as the year 2019. Thus, Cluster 1 (192 companies) has a higher level of investment than Cluster 2 (463 companies) and Cluster 3 (958 companies), and the same occurs with the medium level of cyber-capabilities and cyber-attacks. Therefore, we can corroborate the results of the ANN-MLP analysis, that the greater the cyber-capabilities and the greater the cyber-attacks, the greater organizations' investment in cybersecurity. However, the FREQUENCY variable does not have this behavior, contradicting the ANN-MLP result, in which in both years of analysis the FREQUENCY variable has a positive effect on investment.

To find an explanation for this inconsistency, we must consider that while ANN-MLP considers the indirect effect or interaction effect of the input variables on the output variable, the cluster analysis analyses the direct effect (without interaction of the input variables). To delve into this issue, we have analyzed the direct effect of each input variable on investment, through an Ordinal Logit Regression model.[15] As shown in Table 11, Model 1 shows us the direct effect of FREQUENCY on the investment acting individually and Model 2 shows us the direct effect of all the variables. In

[15] The dependent variable (investment in cybersecurity) is an ordinal scale.

2019

	Importance	Normalized Importance
RESOURCES	.182	82.2%
PROCEDURES	.209	94.4%
RULES	.222	100.0%
ATTACK	.165	74.4%
FREQUENCY	.221	99.7%



2018

	Importance	Normalized Importance
RESOURCES	.302	98.9%
PROCEDURES	.159	52.2%
RULES	.305	100.0%
ATTACKS	.142	46.6%
FREQUENCY	.092	30.2%

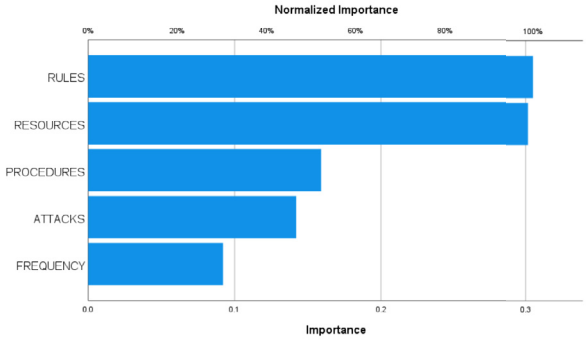


Fig. 6. ANN-MLP results (2019 and 2018).

Table 11
Ordinal logit regression analysis.

Variables	2019				VIF	2018				VIF
	Estimate	Std. Error	Estimate	Std. Error		Estimate	Std. Error	Estimate	Std. Error	
RESOURCES			.330***	.060	1.543			.404***	.057	1.758
PROCEDURES			.352***	.057	1.571			.346***	.055	1.794
RULES			.250***	.054	1.413			.215***	.044	1.673
ATTACK			.271***	.059	1.074			.255***	.053	1.126
FREQUENCY	.058	.042	.024	.047	1.018	−0.007	.012	.025	.043	1.019
−2 Log-Likelihood	282.956		2414.409			279.023		2781.302		
Chi-Square	1.902		277.099			.256		399.353		
Df	1		5			1		5		
Sig.	.000		.000			.613		.000		
Cox and Snell	.002		.345			.000		.407		
Nagelkerke	.003		.350			.000		.412		
McFadden	.001		.098			.000		.120		

*** $p<0.001$, ** $p<0.005$, * $p<0.01$.Durbin-Watson (2019): 1.879; Durbin-Watson (2018): 1.783.

both cases, we see that the FREQUENCY variable is not significant. Therefore we can conclude that the FREQUENCY variable has no direct effect on investment; however, in interaction with ATTACKS, and with CYBER-CAPABILITIES, it affects investment in cybersecurity.

5. Discussion and conclusion

This paper shows how cyber capabilities and cyber-attacks influence the cybersecurity investment in organizations. In our study we have used the Cyber Security Breaches Surveys database for the years 2019 and 2018, consisting of two random samples of more than 4000 organizations.

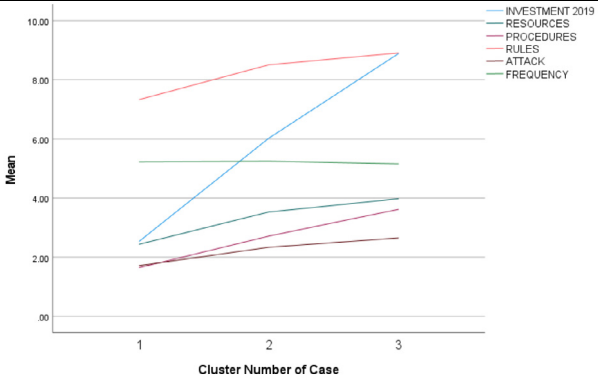
5.1. Discussion of ANN methodology accuracy

Previously to the discussion of the results, we analyze the robustness of the study, analyzing both the research question and the analysis methodology used. First, regarding the research question and in line with previous works (Adesemowo, 2021; S. Okae et al., 2019; Chronopoulos et al., 2017) which indicate that cybersecurity is a strategic function of organizations, the results adequately cor-

2019

Number of organizations in each Cluster

Cluster	1	1274
	2	294.000
	3	128.000
Valid		1696.000
Missing		384.000



2018

Number of organizations in each Cluster

Cluster	1	192.000
	2	463.000
	3	958.000
Valid		1613.000
Missing		475.000

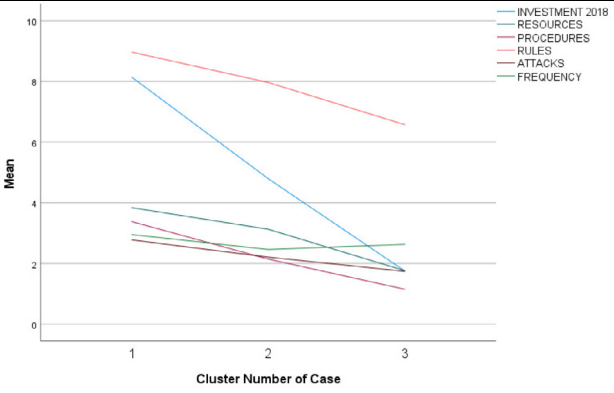


Fig. 7. Cluster analysis and results.

roborate the strategic approach to cybersecurity. Second, from this approach, and in line with Teece (2007), and Eisenhardt and Martin (2000), strategic decisions are supported by the analysis of the capabilities of companies, and the analysis of the environment of organizations. In this sense, our results show a positive and significant effect of both aspects, both cyber-capabilities and cyber-attacks, which validates the question raised.

Second, regarding the robustness of the analysis, we have opted for the use of machine learning techniques. First, we reached a high level of robustness in our analysis with ANN, showing a level of explained variance of over 70%, much higher than the classic statistical models (Arranz et al., 2021). Moreover, with ANN, we have been able to analyze the interaction effect of the input variables, which is more realistic. This is, the senior manager in the decision's process, need a complete overview of the situation, considering all both internal and external variables. Also, using ANN, we have been able to eliminate the bias produced by the existence of missing observations in the sample, as it is produced by the lack of information on the attacks, as well as any problems derived from collinearity, homoscedasticity and endogeneity, typical of the classic regression models. Second, we have analyzed the direct effect of the input variables on the output variable, using the K-mean cluster. This analysis allows us to explore various groups of organizations based on their behavior pattern, relating them to the input and output variables. In this way, through the K-mean cluster, we eliminate possible bias from cross-sectional studies, avoiding endogeneity problems between input and output variables. Finally, we have tested our analysis, with the use of an ordinary logit regression, which shows us the direct effect of the input variables on the output variable. Fig. 8 shows the types of effects analyzed in our paper between the input variables (cyber-attacks and cyber-capabilities) and the output variable (investment in cybersecurity).

5.2. Discussion of results

Regarding the exploratory analysis, the results of both years do not show significant differ in terms of investment (t: 0.081; df: 1302; significance: 0.963). We can point out that the average investment corresponds to the interval between 1000 and 5000 pounds (for example, the mean on 2018 was, £3580), with significant variability depending on the size of the company, from an average investment for micro and small companies of £3490, up to an average value of £277,000 for large companies. These results reinforce previous studies showing that size is a significant variable in cybersecurity investment. The literature indicates that one of the reasons is that small and medium-sized enterprises (SMEs) do not perceive threaten by cybersecurity attacks (Osborn, 2015; Fernandez de Arroyabe and Fernandez de Arroyabe, 2021), although in reality approximately 72% of breaches occur in SMEs (Fielder et al., 2016). Moreover, Ponsard et al. (2018), Osborn (2015) and Sangani and Vijayakumar (2012) point out that SMEs feel that IS security is not their primary concern, which is reflected on their small an-

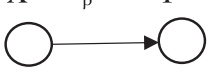
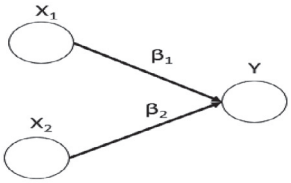
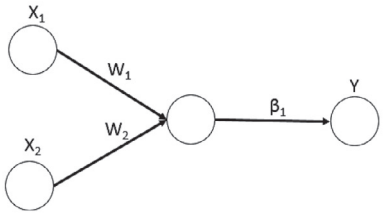
Direct Effect (Individually)	Direct Effect (Combined)	Interaction Effect
		
$Y=\beta_0+\beta_1.X_1$	$Y=\beta_0+\beta_1.X_1+\beta_2.X_2+e$	Y=f(X1,X2) i) Interaction of variables X1 and X2: $Y=\beta_0+f(w_1.X_1+w_2.X_2)+e=\beta_0+\beta_1(w_1.X_1+w_2.X_2)+e$ where, w_i, the weight of variable i in the interaction.

Fig. 8. Direct and Interaction effect.

nual cybersecurity budgets (Osborn, 2015). This is because SMEs managers evaluate that the level of risk (looking at the likelihood and the motivation) is very low as compared with large companies, therefore having a false sense of security (Osborn, 2015; Walli et al., 2014).

Second, regarding the degree of integration for organizations in the use of online services, the results are consistent for both years, as it shows that there are no significant differences in the results. Moreover, the results show a high degree of integration of services, with the use of email, websites, online bank payments and social network sites being the most common. As in the previous question, the degree of integration is also not homogeneous, with significant differences depending on size. Finally, regarding the perception and attitude of the organizations in the use of cybersecurity, as in previous variables, there are no significant differences in the two years of study. While organizations consider cybersecurity as an important priority in the organization; cybersecurity is not considered part of the core of the business, as can be seen from the disconnection between the organizations' senior managers/direction and the organizations' internal developments in cybersecurity. These results are in line with previous investigations that show the low level of information that organizations' managers have about cybersecurity (Choo, 2011; Fernandez de Arroyabe and Fernandez de Arroyabe, 2021), and confirming that cybersecurity mostly has an operational nature in the organization (S. Okae et al., 2019; Chronopoulos et al., 2017; Srinidhi et al., 2015).

Regarding the research question, the results confirm that investment in cybersecurity is a strategic decision in the company. First, the organizations' decisions are conditioned by the level of capability in the development of these tasks (Teece, 2007; Eisenhardt and Martin, 2000). Thus, an organization' cybersecurity decision depends on their cybersecurity capabilities. Organizations perceive the high ease or difficulty of taking and implementing these investment decisions that are likely to impact their predisposition to support their decisions in cybersecurity. Therefore, from these results, we can infer that having developed procedures, rules and governance resources in the organization, which represent organizations' cyber-capabilities, has a positive impact on the investment in cybersecurity systems. In line with previous works, we corroborate the work of Jalali et al. (2019) and Woon et al. (2005), showing that investment in cybersecurity systems depends on the organizations' cybersecurity capabilities. Moreover, the results show a high level of integration of resources, procedures, and rules in organizations. In this sense, Jalali et al. (2019) have highlighted that organizations are adopting an active role in implementing cybersecurity processes and take the initiative for building up a suitable cybersecurity strategy, for example, by pursuing the ISO 2700 and 27001 or other widely accepted certification of assurance of cyber security controls, policies and requirements (such as SOC2 readiness report), and by exploiting internal capabilities or by coping with threats. Jalali et al. (2019) and Fernandez de Arroyabe and Fernandez de Arroyabe (2021) highlight that a proactive positioning in the use of cyber-capabilities is consistent with a competitive cybersecurity strategy, in which the organization not only aims at achieving an adequate cybersecurity system but also aims at improving organizations' image, competitive position or undertaking an active cybersecurity policy.

Second, an organization's strategic decisions not only rely on the capabilities of the organization but also the interaction with the environment. In this sense, organizations evaluate the likelihood of being attacked and the potential impact on the organization (e.g. cost of damaged, additional personnel, customer relationship, legal, fines and continuity of the organization) (Feng et al., 2019; Shin et al., 2018; Benaroch, 2018; Conteh and Schmick, 2016; Wright et al., 2014; Cybenko et al., 2002). Thus, a higher level of cyber-attacks increases the probability of organizations' investing in cybersecurity systems. From our results, we can confirm that organizations 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 organization's assets. 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 organization's personnel of cybersecurity policies (Ponsard et al., 2018). Moreover, in line with previous work, malware attacks are important in organizations (Valli et al., 2014; Sangani and Vijayakumar, 2012). Sangani and Vijayakumar (2012) and Osborn (2015) highlighted the lack of adequate protection of the IS in organizations, either due to the diversity of devices (also, with the introduction of Internet of Things/IoT devices) or the lack of knowledge in their cybersecurity management, which are an important source of vulnerabilities in organizations. Moreover, the results show a low frequency of attacks, which may explain the *null* direct effect that this variable has on investment in cybersecurity. Previous literature indicates that the frequency of attacks increases the concerns over the proper functioning of organizations, perceiving the frequency of attacks as a threat to the organization, which will affect the decision to invest in cybersecurity.

However, previous studies point out that attacks that occur less frequently have a greater impact on organizations (Jensen et al., 2017; Hamid et al., 2006). Moreover, the low level of information and updates that senior managers receive in the area of cybersecurity provides evidence of the disconnection between business administration and IT departments (Kim and Salomon, 2012). Thus, our results show an increase in the importance of attacks and their frequency in the investment in cybersecurity. These results confirm previous works (Conteh and Schmick, 2016; Hamid et al., 2006), which highlight that managers are becoming aware of the problems of a cyber-offender, both from the operational, economic and commercial point of view as well as from a reputational perspective.

5.3. Conclusion

Our study extends the current literature on cybersecurity in organizations and improves our understanding of it. First, we contribute by explaining the drivers of investment in cybersecurity systems, complementing previous studies from financial and games theory literature, or taking an individual perspective. Unlike other studies that take the point of view of the decision-maker, this study addresses the topic taking as a unit of analysis the organization, which allows us to avoid personal bias, showing how the investment in cybersecurity systems fits into the decisional system of organizations. This implies that we consider the important role that the senior managers of the organization have in this decision. Moreover, our contribution points out that the decision to invest in cybersecurity systems is a strategic decision of the organization. The strategic nature of cybersecurity investment is not only shown by its importance for the performance of the organization, but also by the decisional factors that influence investment, which follow the patterns of strategic decisions. In line with the strategic perspective of organizations, we highlight that the investment decision in cybersecurity systems is conditioned by the capabilities, competencies and attacks of organizations. As compared to previous studies, organizations' possession of cyber-capabilities has a positive effect on the investment in cybersecurity, where organizations can take from a more proactive to a more reactive position. Moreover, the severity of the threats affects the investment in cybersecurity, which diverges from the mainstream strategy that states that organizations need to adapt and anticipate the changes in the cyber environment.

The second contribution is framed from a methodological point of view. We consider that the use of machine learning techniques allows us to identify the cause-effect relationships between attacks and capabilities and their investment in organizations. Firstly, the use of statistical techniques and adequate surveys allows us to characterise the behavior 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.

Lastly, our study also informs policy-makers. Traditionally, cybersecurity systems were considered an operational rather than strategic element of organizations; however, our results show the strategic nature of the cybersecurity investment decisions. Moreover, the behavior of enterprises towards cybersecurity is characterized by reactivity, contrasting the strategic decisions of organizations in which the prospective, the proactivity and anticipation capacity are determinants of the behavior. Our results suggest a set of activities to be implemented at the organizational level. First, it is necessary that organizations involve all levels of decision to update on cybersecurity. For example, organizations should emphasize the importance of developing information channels, as well as training programs for the management of the company, having as the goal to involve the senior managers of the company in the cybersecurity management. Second, organizations should develop prospective systems on the cyber environment, to identify threats and attacks, as well as the vulnerabilities of the company. This will transform the reactive position of the organization to a more proactive one in accordance with the organization's strategic decisions.

Credit author statement

All authors contributed equally.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Ignacio Fernandez De Arroyabe: Conceptualization, Writing – original draft, Investigation, Visualization. **Carlos F.A. Arranz:** Data curation, Formal analysis, Methodology. **Marta F. Arroyabe:** Supervision, Data curation, Formal analysis, Resources, Writing – review & editing. **Juan Carlos Fernandez de Arroyabe:** Supervision, Methodology, Writing – review & editing.

Data Availability

Data will be made available on request.

References

Adesemowo, A.K., 2021. Towards a conceptual definition for IT assets through interrogating their nature and epistemic uncertainty. Comput. Secur. 105, 102131.
Ajzen, I., 1991. The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50 (2), 179–211.
Ajzen, I., 2002. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. J. Appl. Soc. Psychol. 32 (4), 665–683.
Amit, R., Schoemaker, P.J., 1993. Strategic assets and organizational rent. Strateg. Manag. J. 14 (1), 33–46.
Alpaydin, E., 2021. Machine Learning. MIT Press.
Arranz, N., Fernandez de Arroyabe, J.C., 2009. Complex joint R&D projects: from empirical evidence to managerial implications. Complexity 15 (1), 61–70.
Arranz, N., Fernandez de Arroyabe, J.C., 2010. Efficiency in technological networks, an approach from Artificial Neural Networks (ANN). International Journal of Management Science and Engineering Management 5, 453–460.
Arranz, N., Arguello, N.L., Fernandez de Arroyabe, J.C., 2021. How do internal, market and institutional factors affect the development of eco-innovation in firms? J. Clean. Prod. 297, 126692.
Asteriou, D., Hall, S.G., 2015. Applied Econometrics. Macmillan International Higher Education.
Benaroch, M., 2018. Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. Inf. Syst. Res. 29 (2), 315–340.
Bitencourt, C.C., de Oliveira Santini, F., Ladeira, W.J., Santos, A.C., Teixeira, E.K., 2020. The extended dynamic capabilities model: A meta-analysis. European Management Journal 38 (1), 108–120.
Bose, R., Luo, X., 2014. Investigating security investment impact on firm performance. Int. J. Account. Inf. Manag. 22 (3), 194–208.
Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 34 (3), 523–548.
Burns, A.J., Roberts, T.L., Posey, C., Lowry, P.B., 2019. The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. Inf. Syst. Res. 30 (4), 1228–1247.
Caldwell, T., 2013. Plugging the cyber-security skills gap. Comput. Fraud Secur. (7) 5–10 2013.
Cavusoglu, H., Cavusoglu, H., Son, J.Y., Benbasat, I., 2015. Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources. Inf. Manag. 52 (4), 385–400.
Choo, K.R., 2011. The cyber threat landscape: challenges and future research directions. Comput. Secur. 30 (8), 719–731.
Chronopoulos, M., Panaousis, E., Grossklags, J., 2017. An options approach to cybersecurity investment. IEEE Access 6, 12175–12186.

Barreto, I., 2010. Dynamic capabilities: A review of past research and an agenda for the future. Journal of management 36 (1), 256–280.
Ciurana, J., Quintana, G., Garcia-Romeu, M.L., 2008. Estimating the cost of vertical high-speed machining centres, a comparison between multiple regression analysis and the neural networks approach. International Journal of Production Economics 115 (1), 171–178.
CLUSIF, 2008. Risk Management. Concepts and Methods. Club de la Securite Infomatique, Paris.
Conner, M., Armitage, C.J., 1998. Extending the theory of planned behavior: a review and avenues for further research. J. Appl. Soc. Psychol. 28 (15), 1429–1464.
Conteh, N.Y., Schmick, P.J., 2016. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. Int. J. Adv. Comput. Res. 6 (23), 31–43.
Cybenko, G., Giani, A., Thompson, P., 2002. Cognitive hacking and the value of information. In: Workshop on Economics and Information Security, pp. 16–17.
Cyber Security Breaches Survey, 2018. Official Statistics. Cyber Security Breaches Survey 2018. Culture, Media & Sport. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018 .
Cyber Security Breaches Survey, 2019. Official Statistics.Cyber Security Breaches Survey2019. Department for Digital, Culture, Media & Sport https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019.
Deci, E.L., Ryan, R.M., 2002. Overview of self-determination theory: an organismic dialectical perspective. In: Handbook of Self-Determination Research, pp. 3–33.
Easttom, 2012. Computer Security Fundamentals. Pearson, Indianapolis.
Eisenhardt, K.M., Martin, J.A., 2000. Dynamic capabilities: what are they? Strateg. Manag. J. 21 (10–11), 1105–1121.
Eisenhardt, K.M., Martin, J.A., 2000. Dynamic capabilities: what are they? Strategic Management Journal 21 (10-11), 1105–1121.
Fainshmidt, S., Pezeshkan, A., Lance Frazier, M., Nair, A., Markowski, E., 2016. Dynamic capabilities and organizational performance: a meta-analytic evaluation and extension. Journal of Management Studies 53 (8), 1348–1380.
Faridian, P.H., Neubaum, D.O., 2021. Ambidexterity in the age of asset sharing: Development of dynamic capabilities in open source ecosystems. Technovation 99, 102125.
Feng, N., Chen, Y., Feng, H., Li, D., Li, M., 2019. To outsource or not: the impact of information leakage risk on information security strategy. Inf. Manag., 103215 doi:10.1016/j.im.2019.103215.
Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F., 2016. Decision support approaches for cyber security investment. Decis. Support Syst. 86, 13–23.
Hair, J.F., 2006. Multivariate Data Analysis. Pearson Education.
Hamid, M., Boudriga, N., Obaidat, M.S., 2006. Security policy guidelines. In: Bidgoli, H. (Ed.), Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management. Wiley, New Jersey, pp. 945–958.
Harrison, E.F., 1996. A process perspective on strategic decision making. Manag. Decis. 34 (1), 46–53.
Heitzenrater, C., Simpson, A., 2016. Software security investment: the right amount of a good thing. In: IEEE Cybersecurity Development (SecDev). IEEE, pp. 53–59.
Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organizations. Eur. J. Inf. Syst. 18 (2), 106–125.
Holland, S.J., Shore, D.B., Cortina, J.M, 2017. Review and recommendations for integrating mediation and moderation. Organizational Research Methods 20, 686–720.
Huang, C.D., Hu, Q., Behara, R.S., 2008. An economic analysis of the optimal information security investment in the case of a risk-averse firm. Int. J. Prod. Econ. 114 (2), 793–804.
Ifinedo, P., 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31 (1), 83–95.
ISO 27000, 2007. The ISO27001 Certification Process. The ISO 27000 Directory. ISO/IEC http://www.27000.org/ismsprocess.htm.
ISO/IEC 27000, 2009. Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary (ISO/IEC 27000:2009). ISO/IEC, Geneva, Switzerland F8B5 06E4 A169 4E46.
ISO/IEC 27002:2022, 2022. Information Security, Cybersecurity and Privacy Protection—Information Security Controls. ISO/IEC, Geneva.
Jalali, M.S., Kaiser, J.P., 2018. Cybersecurity in hospitals: a systematic, organizational perspective. J. Med. Internet Res. 20 (5), e10059.
Jalali, M.S., Siegel, M., Madnick, S., 2019. Decision-making and biases in cybersecurity capability development: evidence from a simulation game experiment. J. Strateg. Inf. Syst. 28 (1), 66–82.
Jensen, M.L., Dinger, M., Wright, R.T., Thatcher, J.B., 2017. Training to mitigate phishing attacks using mindfulness techniques. J. Manag. Inf. Syst. 34 (2), 597–626.
Jeong, C.Y., Lee, S.Y.T., Lim, J.H., 2019. Information security breaches and IT security investments: impacts on competitors. Inf. Manag. 56 (5), 681–695.
Karjalainen, M., Sarker, S., Siponen, M., 2019. Toward a theory of information systems security behaviors of organizational employees: a dialectical process perspective. Inf. Syst. Res. 30 (2), 687–704.
Kim, D., Salomon, M.G., 2012. Fundamentals of Information System Security. Jones & Bartlett Learning International, N.J..
Kolvereid, L., 1996. Prediction of employment status choice intentions. Entrep. Theory Pract. 21 (1), 47–58.
Krueger Jr, N.F., Brazeal, D.V, 1994. Entrepreneurial potential and potential entrepreneurs. Entrep. Theory Pract. 18 (3), 91–104.
Lee, Jae Kyu, Cho, Daegon;, Lim, Gyoo Gun, 2018. Design and validation of the bright internet. J. Assoc. Inf. Syst. 19 (2), 63–85.
Mallinder, J., Drabwell, P., 2014. Cyber security: a critical examination of information sharing versus data sensitivity issues for organizations at risk of cyber-attack. J. Bus. Contin. Emerg. Plan. 7 (2), 103–111.
Mayadunne, S., Park, S., 2016. An economic model to evaluate information security investment of risk-taking small and medium enterprises. Int. J. Prod. Econ. 182, 519–530.
Menard, P., Bott, G.J., Crossler, R.E., 2017. User motivations in protecting information security: protection motivation theory versus self-determination theory. J. Manag. Inf. Syst. 34 (4), 1203–1230.
Moore, T., Dynes, S., Chang, F.R., 2015. Identifying How Firms Manage Cybersecurity Investment. Southern Methodist University http://blog.smu.edu/research/files/2015/10/SMU-IBM.
Mohrotra, K., 1994. Elements of artificial neural networks. MIT Press, Cambridge, MA.
Masters, T., 1993. Practical neural network recipes in C++. Academic Press Professional, Inc.
Nagurney, A., Shukla, S., 2017. Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. Eur. J. Oper. Res. 260, 588–600.
Okae, S., Andoh-Baidoo, F.K., & Ayaburi, E. (2019). Antecedents of optimal information security investment: IT governance mechanism and organizational digital maturity. In Y. Dwivedi, E. Ayaburi, R. Boateng, & J. Effah (Eds.), IFIP AICT: ICT Unbounded, Social Impact of Bright ICT Adoption, 558, 442–453. Springer, Cham.
Osborn, E., Simpson, A., 2015. Small-scale cyber security. In: 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing. IEEE, pp. 247–252.
Pérez-González, D., Preciado, S., Solana-Gonzalez, P., 2019. Organizational practices as antecedents of the information security management performance: an empirical investigation. Inf. Technol. People 32 (5), 1262–1275.
Podsakoff, P.M., MacKenzie, S.B., Podsakoff, N.P., 2012. Sources of method bias in social science research and recommendations on how to control it. Annual review of psychology 63 (1), 539–569.
Podsakoff, N.P., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of applied psychology 88 (5), 879–903.
Posey, C., Roberts, T.L., Lowry, P.B., 2015. The impact of organizational commitment on insiders' motivation to protect organizational information assets. J. Manag. Inf. Syst. 32 (4), 179–214.
Ponsard, C., Deprez, J.C., 2018, May. Helping SMEs to better develop software: experience report and challenges ahead. In: 2018 IEEE/ACM 40th International Conference on Software Engineering: Software Engineering in Practice Track (ICSE–SEIP). IEEE, pp. 213–214.
Qian, X, Liu, X, Pei, J, Pardalos, P.M., 2018. A new game of information sharing and security investment between two allied firms. Int. J. Prod. Res. 56 (12), 4069–4086.
Rai, A., Tang, X., 2010. Leveraging IT capabilities and competitive process capabilities for the management of interorganizational relationship portfolios. Inf. Syst. Res. 21 (3), 516–542.
Ravichandran, T., Lertwongsatien, C., Lertwongsatien, C., 2005. Effect of information systems resources and capabilities on firm performance: a resource-based perspective. J. Manag. Inf. Syst. 21 (4), 237–276.
Rise, J., Thompson, M., Verplanken, B., 2003. Measuring implementation intentions in the context of the theory of planned behavior. Scand. J. Psychol. 44 (2), 87–89.
Rogers, R., 1983. Cognitive and physiological processes in fear-based attitude change: a revised theory of protection motivation. In: Social Psychophysiology: a Sourcebook. Guilford Press, New York, pp. 153–176.
Ryan, R.M., Deci, E.L., 2000. Intrinsic and extrinsic motivations: classic definitions and new directions. Contemp. Educ. Psychol. 25 (1), 54–67.
Sangani, N.K., Vijayakumar, B., 2012. Cyber security scenarios and control for small and medium enterprises. Informatica Economica 16 (2), 58–63.
ServiceNow (2017). How Leading Organizations Respond to Security Threats and Keep Data Safe. https://theboardinstitute.com/leading-organizations-respond-security-threats-keep-data-safe.
Shao, X., Siponen, M., Liu, F., 2020. Shall we follow? Impact of reputation concern on information security managers' investment decisions. Comput. Secur. 97, 101961.
Shin, Y.Y., Lee, J.K., Kim, M., 2018. Preventing state-led cyberattacks using the bright internet and internet peace principles. J. Assoc. Inf. Syst. 19 (3), 152–181.
Somers, M.J., Casal, J.C., 2009. Using artificial neural networks to model nonlinearity: The case of the job satisfaction—job performance relationship. Organizational Research Methods 12 (3), 403–417.
Srinidhi, B., Yan, J., Tayi, G.K., 2015. Allocation of resources to cyber-security: the effect of misalignment of interest between managers and investors. Decis. Support Syst. 75, 49–62.
Suddaby, R., Coraiola, D., Harvey, C., Foster, W., 2020. History and the micro-foundations of dynamic capabilities. Strategic Management Journal 41 (3), 530–556.
Teece, D.J., 2007. Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. Strateg. Manag. J. 28 (13), 1319–1350.
Teece, D.J., 2014. The foundations of enterprise performance: Dynamic and ordinary capabilities in an (economic) theory of firms. Academy of management perspectives 28 (4), 328–352.
Ulrich, D., Lake, D.G., 1990. Organizational Capability: Competing from the Inside Out. John Wiley & Sons.
Vance, A., Siponen, M., Pahnila, S., 2012. Motivating IS security compliance: insights from habit and protection motivation theory. Inf. Manag. 49 (3–4), 190–198.
Wali, A, Chun, SA, Geller, J, 2014. A bootstrapping approach for developing a cybersecurity ontology using textbook index terms. In: Guerrero, J.E. (Ed.), Proceedings of the 2013 International Conference on Availability, Reliability, and Secu-

rity. IEEE Computer Society, Washington, pp. 569–576. doi:10.1109/ARES.2013.75.
Warkentin, M., Johnston, A.C., Walden, E., Straub, D.W., 2016. Neural correlates of protection motivation for secure IT behaviors: an fMRI examination. J. Assoc. Inf. Syst. 17 (3), 194–211.
Weber, R., 2012. Evaluating and developing theories in the information systems discipline. J. Assoc. Inf. Syst. 13 (1), 1–13.
Weishäupl, E., Yasasin, E., Schryen, G., 2018. Information security investments: an exploratory multiple case study on decision-making, evaluation and learning. Comput. Secur. 77, 807–823.
Wolff, J., 2016. Perverse effects in defense of computer systems: when more is less. J. Manag. Inf. Syst. 33 (2), 597–620.
Woon, I.M., Low, R.T., Tan, G.W., 2005. A protection motivation theory approach to home wireless security. International Conference on Information Systems.
Wright, R.T., Jensen, M.L., Thatcher, J.B., Dinger, M., Marett, K., 2014. Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. Inf. Syst. Res. 25 (2), 385–400.
Zahra, S.A., Sapienza, H.J., Davidsson, P., 2006. Entrepreneurship and dynamic capabilities: A review, model and research agenda. Journal of Management studies 43 (4), 917–955.
Zhao, L., Detlor, B., Connelly, C.E., 2016. Sharing knowledge in social Q&A sites: the unintended consequences of extrinsic motivation. J. Manag. Inf. Syst. 33 (1), 70–100.

Ignacio Fernandez de Arroyabe is Cyber Risk Manager in Lloyds Bank Commercial Banking (UK). He has worked in cybersecurity in Jaguar Land Rover in the UK. His-research interests are in cybersecurity risk management in the firms. He is a PhD candidate in cybersecurity at Warwick Manufacturing Group (Warwick University).

Carlos F.A. Arranz is a Lecturer in Business Operations at the University of Greenwich. His-main research interest centres on the application of Machine Learning methods to the analysis of business, particularly on the implementation of Circular Economy Models. He holds a PhD in Business Analytics from Essex Business School (University of Essex), an MRes in International Political Economy from the London School of Economics and Political Science (LSE), and an MRes in Economics and Finance from the Université du Luxembourg. Before that, he received a BSc in Economics and Business Economics (International Economics Studies Specialisation) from Maastricht University.

Marta F. Arroyabe is a senior lecturer at Essex Business School. She is also associate editor of the Journal of Entrepreneurship in Emerging Economies. Marta's research focuses on four primary areas: innovation, environmental management, digitalisation & cybersecurity, and entrepreneurship. In the area of innovation, her research aims at understanding the development and implementation of innovation in firms, and explores firms' innovation decisions and strategies. In the area of environmental management, she primarily focuses on two topics, eco-innovation and circular economy, where she studies business responses to improving environmental performance and to increasing societal concerns for the environment. Her research explores the development of eco-innovation and circular economy business models in firms and the impact of these on firms' performance. In the area of digitalisation and cybersecurity, her research investigates the drivers behind firms' implementation of and investment in cybersecurity, and the role of cybersecurity in firms' decision-making process in the implementation of new digital technologies. Finally, in the area of entrepreneurship, her research primarily focuses on entrepreneurial education and entrepreneurial intention. Her work aims at understanding to which extent entrepreneurial education in higher education institutions (such as universities) spurs the entrepreneurial intention of students and fosters entrepreneurial activity. She has published her work in "Journal of Business Research", "R&D Management", "Technovation", "Studies in Higher Education", "British Journal of Management", "European Journal of Innovation Management", "Technology Analysis and Strategic Management", "Journal of Cleaner Production", "Technological Forecasting and Social Change", and "Scandinavian Journal of Hospitality and Tourism".

Juan Carlos. Fernandez de Arroyabe is a Professor in Essex Business School (University of Essex). His-research interests include joint R&D projects, R&D networks, and complex technological systems. He is author or co-author of numerous papers published in the *British Journal of Management, IEEE Transaction Engineering Management, the Complexity, Technovation, Studies in Higher Education, Journal Cleaner Production, Business Strategy and The Environment, Journal Business Research; Emergence: Organization and Complexity, Technological Forecasting Social Change, Journal of Enterprise Information Management, International Small Business Journal, European Journal of Work and Organizational Psychology, Scandinavian Journal of Tourism, and Industry Higher Education*. Also, he is Associate Editor of the Journal of Entrepreneurship in Emerging Economies and member of Editorial Board of Technological Forecasting Social Change.