DOI: 10.1111/risa.13761

Assessing the risk of robbery in bank branches to reduce impact on personnel

María Pilar de la Cruz López,[1] Juan José Cartelle Barros,[2,*] Alfredo del Caño Gochi,[1] María Concepción Garaboa Fernández,[3] and Jesús Blanco Leis[3]

According to existing literature, bank robberies can have a considerable impact on the people involved (employees, customers, and police officers), even if the direct economic losses are negligible. Consequently, this article presents a model to assess the risk of bank robbery, with the aim of reducing the impact on the people and prioritizing the investments in security measures. It is based on the MIVES (Spanish acronym for the Integrated Value Model for Sustainability Assessment) method and it was combined with Monte Carlo simulation as a way of taking into account the uncertainty. Correlations were also modeled, for simulation purposes. Indicators for addressing issues related to security features, employees, operational procedures, and physical and social environment were defined. The model was applied to two fictitious but realistic sets of cases. The first simulation provides a quick overview of the risk level of a fictitious bank, before collecting the full set of data from hundreds or thousands of branches. The second simulation analyzes the risk variation of a specific bank branch over time. The model was also used to assess the risk index of 636 real branches belonging to a Spanish bank. All the results are presented and discussed in depth. The model allows the user to identify the weak points of a branch, so that corrective measures can be taken.

KEY WORDS: Commercial bank branches; MCDM method; Monte Carlo; risk analysis; robbery risk

1. INTRODUCTION: LITERATURE REVIEW AND MAIN OBJECTIVES

In recent years, the amount of money stolen during bank robberies in developed countries has decreased. This conclusion may be reached by looking at historical data from banks or scientific publications (European Banking Federation [EBF], 2010, 2011; Gill, 2000; Reilly, Rickman, & Witt, 2012). This is due, among other things, to the fact that banks have made a great effort to improve their anti-theft systems (EBF, 2010, 2011). For example, money storage devices are becoming increasingly safer with mechanisms for hindering robberies, such as delayed opening (Dugato, 2014). On the other hand, electronic payment systems, e-banking services, and Automated Teller Machines (ATMs) have become more commonplace (Dugato, 2014; EBF, 2010, 2011). Consequently, bank offices do not currently need to have large amounts of cash. Thus, in a considerable number of bank robberies, no cash is actually taken and, in almost all the remaining cases, the amount of money stolen is minimal. Furthermore, convicted bank robbers fare badly in a harsh penal system and,

[1] Departamento de Ingeniería Civil, Escuela Politécnica Superior (EPS), Universidade da Coruña (UDC), Campus de Esteiro, C/Mendizábal s/n, Ferrol (A Coruña), Ferrol, 15403, Spain.

[2] Escuela Politécnica Superior (EPS), Universidade da Coruña (UDC), Campus de Esteiro, C/Mendizábal s/n, Ferrol (A Coruña), Ferrol, 15403, Spain.

[3] ABANCA Corporación Bancaria S.A., C/ Olmos 26, Coruña, A Coruña, 15003, Spain.

[*] Address correspondence to Juan José Cartelle Barros, Escuela Politécnica Superior (EPS), Universidade da Coruña (UDC), Campus de Esteiro, C/Mendizábal s/n, 15403, Ferrol (A Coruña), Spain; juan.cartelle1@udc.es

in most developed countries, police forces usually solve 60–70% of these cases. As the risk–benefit ratio is not favorable (Dugato, 2014), professional criminal activity is moving toward less risky objectives with greater opportunities (Dugato, 2014; EBF, 2010, 2011; Haran & Martin, 1977). In this sense, cyber bank robberies are becoming more frequent, which has attracted the attention of a considerable number of researchers such as Hole, Moen and Tjostheim (2006), Lesk (2011), Sood and Enbody (2013), Gorton (2014) or Damenu and Beaumont (2017), among others.

Despite the displacement effect that has taken place, many robbers are still willing to take the risk of robbing a bank branch even if the financial benefits are reduced (Morrison & O'Donnell, 1996). On the other hand, the impact that bank robberies can have on everyone involved—employees, customers, and police officers—can be very severe, or even fatal. While direct economic losses may be negligible, people can sustain serious psychological after-effects, physical injuries, and even death. The possible psychological after-effects have been studied by a range of authors; in general, directly experiencing a bank robbery often has dire consequences (Converso & Viotti, 2014; Fichera et al., 2015; Frans, Åhs, Bihre, & Åhs, 2018; Giorgi, Fiz Perez, et al., 2015; Giorgi, Leon Perez, Montani, Courcy, & Arcangeli, 2015; Hansen, Armour, & Elklit, 2012; Hansen, Armour, Shevlin, & Elklit, 2014; Hansen & Elklit, 2013; Hansen, Hyland, & Armour, 2016; Hansen, Lasgaard, & Elklit, 2013; Johnston, 1978; Jones, 2002; Jones & Jones, 1998; Kamphuis & Emmelkamp, 1998; Leymann, 1985, 1988; Miller-Burke, Attridge, & Fass, 1999; Mucci, Giorgi, Perez, Iavicoli, & Arcangeli, 2015; Paes-Machado & Nascimento, 2006). Similar impacts occur when other establishments, such as pharmacies (Fichera, Sartori, & Costa, 2009), supermarkets, jewelry shops, or tobacconists (Setti et al., 2018), are targeted by robbers.

Despite the fact that there is a considerable body of literature addressing the psychological consequences of bank robberies, the number of studies analyzing the risk of robbery in banking is limited. Dugato (2014) says that academia has not paid enough attention to this issue, and that most of the existing studies use out-of-date information, adopting a descriptive approach instead of an analytical one.

Some publications deal with factors that may influence robbers' decisions (Dugato, 2014; Hochstetler, 2001; Levine, 2007; Morrison & O'Donnell, 1996; Samavati, 2006). These include, among other aspects, gun availability, motivation group dynamics of robbers, social issues, bank procedures, location of the branch, escape routes, or previous bank robberies (once a bank branch has been robbed, the evidence suggests that the probability of repetition increases up to a certain number of times).

Other authors examine robbery typology, modus operandi, criminals' characteristics, or even the moment at which the crimes were committed (Abraham & Baldassaro, 2001; Borzycki, 2003; EBF, 2010, 2011; Federal Bureau of Investigation [FBI], 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018; Samavati, 2004). These studies refer to a city, a region or, at most, a country, but there is no study on Spain.

Some works analyze the differences that exist between different cities or countries (Dugato, 2014; Levine, 2007; Matthews, Pease, & Pease, 2001; Samavati, 2006; Wang, 2002). Security measures also receive attention in the literature, although many works are quite old and outdated (Ozenne, 1974). However, some of them are useful to get an idea of the security devices that robbers have been most concerned about (Büchler & Leineweber, 1991; Hannan, 1982; Kube, 1988; Nugent, Burns, Wilson, & Chappell, 1989).

Other research is on the security measures themselves, with the aim of improving them or developing new ones. Szczodrak and Szwoch (2013) propose using thermal camera images for bank robbery detection. Similarly, Khera and Verma (2014) look at an autonomous control system for bank vaults to detect and record suspicious movements. Kotus, Łopatka, Czyżewski and Bogdanis (2016) propose a new control system capable of distinguishing between normal sounds and the ones—like shots and screams—caused by threatening circumstances. By simulating a dangerous situation in a real bank branch, the authors tested their system. Similarly, Gupta, Kumar and Malhotra (2015) develop a hand gesture recognition method for bank employees during a robbery.

In relatively recent times, one study looks at the robbery procedures used in Italy (De Leo, Volpini, & De Gregorio, 2006). The authors highlight the most relevant security measures to prevent robberies and how people must act during such crimes to diminish the possible harmful effects. Weisel (2007) and Braga (2008) carry out similar studies in the United States on a comparable scale. All of these studies have a common thread: the effectiveness of the security measures is analyzed in a qualitative way based on the authors' opinions or interviews with criminals.

To the best of the authors' knowledge, there is only one quantitative model to manage the risk of robbery in bank branches: Guazzoni and Ronsivalle (2009). It uses an Artificial Neural Network (ANN), which takes into account both endogenous (concerning the bank office and its security systems) and exogenous (associated with the geographic location, population density, and the crime rate) factors. Both come into play when a Global Robbery Risk Index (GRRI) is being estimated for each bank branch. The authors rely on all the available historical data of bank robberies in Italy to train and validate the ANN. Consequently, if the ANN is employed to estimate the GRRI of the bank branches located in a different country, the associated historical data must be collected to train the model first. This can be a time-consuming and cost-extensive activity, especially if there are no available databases. Furthermore, it may be impossible to collect certain data. If this is the case, the ANN training cannot be successfully executed, and the results would be untrustworthy.

In view of the above, the main objective of this article is to present an up-to-date model that makes it possible to quantitatively assess the risk of robbery in bank branches. The model is based on the MIVES method (Spanish Acronym of Integrated Value Model for Sustainability Assessment method). To deal with uncertainty, it was combined with Monte Carlo simulation. Correlations between risk indicators were also taken into account. The assessment model does not need historical data for its application, although certain historical information was considered during its conception. The results can be used to identify the weak points of a branch. Consequently, investments to increase security can be made. This serves to reduce both the risk of robbery and also the possible impacts on people. To the best of the authors' knowledge, there is no model like the one presented here in the existing literature.

The characteristics, advantages, and disadvantages of a total of 15 methods that could have been applied to this work were analyzed. It was concluded that MIVES was the best suited to the bank's needs. In particular, for example, the traditional method of estimating the level of risk as a function of threat, vulnerability, and consequences, has several problems. One is the nonadditivity of the risks estimated by this method. On the other hand, this technique is not suitable for adequately allocating the new security measures that an office needs to achieve an adequate level of risk. Further problems with this method can be found in Cox (2008) (subjectivity and ambiguity in estimating threat, vulnerability, and consequence figures; problems with correlations, among others).

Three security staff members of a Spanish bank (ABANCA Corporación Bancaria S.A., from now on ABANCA, or the bank), with extensive experience in security and safety issues, have participated in creating the model. In terms of bank robbery-related matters, their combined experience is over 60 years. One is a criminology expert with 37 years of experience. Moreover, other experts were consulted, one of whom was a former police inspector with over a decade of security experience in the banking sector. Trade unions health and safety representatives were also involved.

On the one hand, through two Monte Carlo simulations, the model was used to generate a wide range of fictitious case studies. On the other, ABANCA performed a deterministic risk assessment of its entire network of bank branches, carrying out improvement projects until all the bank branches complied with management's requirements. For obvious reasons, it is not possible to reproduce real data associated with a specific office here, but the general results derived from using the complete model to assess all the ABANCA branches are presented and discussed.

The reader should bear in mind that the model goes beyond the national legislation in terms of banks' security issues.

This article is organized as follows. In Section 2, the methodology is explained, while the final model is presented in Section 3. The simulation case studies are included in Section 4. Results are presented and discussed in Section 5. Finally, the main conclusions are outlined in Section 6.

2. MATERIALS AND METHODS

2.1. Multi-Criteria Decision Making (MCDM) Methods: MIVES

Most of the decisions to be taken in real life are of a multicriteria nature, and assessing the risk of robbery in bank branches is not an exception. Multi-Criteria Decision Making (MCDM) methods are of great help at the time of facing multi-criteria problems.

A wide range of MCDM methods exist such as the analytic hierarchy process (AHP) (Saaty, 1980,

Table I. Some Recent Studies Using MIVES Method for Solving Problems in a Wide Range of Fields

Field of Application	Source
Energy sector	(Cartelle Barros et al., 2015; Cartelle Barros, Lara Coira, de la Cruz López, & del Caño Gochi, 2016; Cartelle Barros, Lara Coira, de la Cruz López, del Caño Gochi, & Soares, 2020)
Construction sector	(Casanovas-rubio et al., 2019; Habibi, Pons Valladares, & Peña, 2020; Josa, de la Fuente, Casanovas-Rubio, Armengou, & Aguado, 2021; Zubizarreta et al., 2019)
University education	(Pons, Franquesa, & Hosseini, 2019)
Industrial sector	(Cartelle Barros, Lara Coira, de la Cruz López, & del Caño Gochi, 2018)
Prioritization of investments in public services	(Pardo-Bosch, Aguado, & Pino, 2019; Pujadas, Pardo-Bosch, Aguado-Renter, & Aguado, 2017)
Natural disasters and extreme events	(Gandini, Garmendia, Prieto, Alvarez, & San-José, 2020)
Emergency and post-disaster problems	(Hosseini, Pons, & de la Fuente, 2018; Hosseini, Yazdani, & de la Fuente, 2020)
Project management	(Zubizarreta, Ganzarain, Cuadrado, & Lizarralde, 2021)

2006); the analytic network process (ANP) (Saaty & Vargas, 2006) or MIVES (Cartelle Barros, Lara Coira, de la Cruz López, & del Caño Gochi, 2015; Casanovas-rubio, Pujadas, Pardo-bosch, Blanco, & Aguado, 2019; de la Cruz, Castro, del Caño, Gómez, Lara, & Cartelle, 2014; Zubizarreta, Cuadrado, Orbe, & García, 2019), among others. The reader can find in Hajkowicz & Collins (2007) and in Shao et al. (2020) additional information about some of these and other MCDM methods used in the scientific literature.

The results provided by different MCDM methods are similar (Zamani-Sabzi, King, Gard, & Abudu, 2016), at least at the time of selecting the best alternatives (Chitsaz & Banihabib, 2015). In fact, the discrepancies that do exist are mostly related to the weights of the model, which can be corrected (Kou, Lu, Peng, & Shi, 2012). However, not all the MCDM methods present exactly the same advantages. MIVES is one of the alternatives with the best complexity-performance ratio (Cartelle Barros et al., 2015). By way of example, MIVES makes it possible to consider potential nonlinearities in the assessment of both quantitative (continuous) and qualitative (discrete) indicators. If necessary, it also integrates AHP for establishing weights (Cartelle Barros et al., 2015). Moreover, it can be easily combined with the Monte Carlo simulation (de la Cruz, Castro, del Caño, Gómez, Lara, & Cartelle, 2014) or fuzzy arithmetic (de la Cruz, Castro, del Caño, Gómez, Lara, & Gradaille, 2014) in order to consider uncertainty. MIVES is a flexible method that can be used to solve problems in a wide range of fields. In fact, to date, more than 60 articles on MIVES have been published in scientific journals. The reader can find in Table I some of the most recent studies using this method. The reasons summarized here, along with other discussed throughout this article, have led to the use of MIVES in this work. MIVES uses requirement trees and value functions.

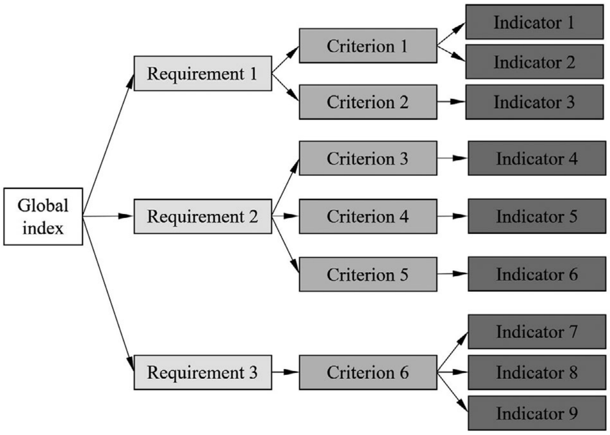

Fig 1. Example of a theoretical requirement tree.

A requirement tree is a scheme that usually consists of an overall index with three breakdown levels: requirements, criteria, and indicators. The first two levels facilitate the understanding of the problem to be solved, and the calculations to be made. The indicators are the quantitative or qualitative aspects that are going to be assessed through the use of value functions. The overall index is used to make an assessment that takes into account all the indicators of the model, as an aid to decision making. Fig. 1 shows an example of a theoretical requirement tree with three requirements, six criteria, and nine indicators. The requirement tree conceived in this work is shown in Table II.

Value functions are mathematical tools that serve to transform the different units for the

Table II. Requirement Tree for the Model with the Weights for the Requirements (α_{ind}), Criteria (β_{ind}) and Indicators (γ_{ind}). The Input Values of the Qualitative Indicators as well as their Corresponding Levels of Risk (V_{ind}) are Also Included

	α_{ind}	Requirements	β_{ind}	Criteria	γ_{ind}	Indicators[b]
RI[a]	26%	1. Branch security features	10%	1.1. Alarm reception	100%	1.1.1. Communication channels: • One channel (PSTN), $V_{\mathrm{ind}} = 1$ • One channel (IP), $V_{\mathrm{ind}} = 0.85$ • Two channels (PSTN/GSM), $V_{\mathrm{ind}} = 0.5$ • Two channels (one of them IP), $V_{\mathrm{ind}} = 0.4$ • Three channels (IP, PSTN, GSM), $V_{\mathrm{ind}} = 0$
			40%	1.2. Storage device location	50%	1.2.1. Safes: • Visible and located in the main service area, $V_{\mathrm{ind}} = 1$ • Not visible and located in the main service area, $V_{\mathrm{ind}} = 0.25$ • Located in the archive, $V_{\mathrm{ind}} = 0.05$
					50%	1.2.2. Cash box: • Visible from the main service area, $V_{\mathrm{ind}} = 1$ • Not visible from the main service area, $V_{\mathrm{ind}} = 0$
			50%	1.3. Security devices	75%	1.3.1. Devices for cash storing and handling: • One safe and one cash box, $V_{\mathrm{ind}} = 1$ • One safe and one cash dispenser, or cash recycler, $V_{\mathrm{ind}} = 0.83$ • One safe, one cash dispenser or cash recycler, and one cash box, $V_{\mathrm{ind}} = 0.66$ • Two safes and one cash box, $V_{\mathrm{ind}} = 0.5$ • Two safes and one cash dispenser, or cash recycler, $V_{\mathrm{ind}} = 0.33$ • Two safes, one cash dispenser or cash recycler and one cash box, $V_{\mathrm{ind}} = 0.16$ • Two safes, more than one cash dispenser or cash recycler, and one cash box, $V_{\mathrm{ind}} = 0$
					25%	1.3.2. Security cameras: • Main entrance, $V_{\mathrm{ind}} = 1$ • Main entrance and cashier desks, $V_{\mathrm{ind}} = 0.8$ • Main entrance, cashier desks, and main service area $V_{\mathrm{ind}} = 0.4$ • The previous three options and the archive, $V_{\mathrm{ind}} = 0.15$ • The previous four options and out of the branch, $V_{\mathrm{ind}} = 0$
	21%	2. Branch employees	60%	2.1. Deterrent capacity	100%	2.1.1. Number of employees[c]: • $P_{\mathrm{ind,min}} = 8$ • $P_{\mathrm{ind,max}} = 0$ • $n_{\mathrm{ind}} = 4$ • $m_{\mathrm{ind}} = 0.5$ • $A_{\mathrm{ind}} = 3$

(*Continued*)

Table II. (Continued)

α_{ind}	Requirements	β_{ind}	Criteria	γ_{ind}	Indicators[b]
		40%	2.2. Response capacity	30%	2.2.1. Staff composition: • Combination of personnel with more and less of two years of experience, $V_{\text{ind}} = 1$ • Only personnel with more than two years of experience, $V_{\text{ind}} = 0.20$
				70%	2.2.2. Training: • At least one worker without training, $V_{\text{ind}} = 1$ • All personnel with training but one of them with only online training, $V_{\text{ind}} = 0.4$ • All personnel with classroom training, $V_{\text{ind}} = 0.12$ • All personnel with classroom and online training, $V_{\text{ind}} = 0.05$
26%	3. Operational procedures	30%	3.1. Cash storing during noncommercial hours	100%	3.1.1. Cash storing during noncommercial hours: • Out of storing locking-devices, $V_{\text{ind}} = 1$ • In one locking device, $V_{\text{ind}} = 0.66$ • In two locking devices, $V_{\text{ind}} = 0.33$ • In more than two locking devices, $V_{\text{ind}} = 0$
		70%	3.2. Cash handling during commercial hours	95%	3.2.1. Cash handling during commercial hours: • Bunker, $V_{\text{ind}} = 1$ • Security lock, $V_{\text{ind}} = 0.95$ • Cash box, $V_{\text{ind}} = 0.9$ • Cash dispenser or cash recycler, $V_{\text{ind}} = 0.2$ • Other, $V_{\text{ind}} = 0$
				5%	3.2.2. Amount of money: • Level 3 (less than 100,000 €), $V_{\text{ind}} = 0$ • Level 2 (between 100,000 and 200,000 €), $V_{\text{ind}} = 0.5$ • Level 1 (more than 200,000 €), $V_{\text{ind}} = 1$
12%	4. Physical environment	100%	4.1. Physical environment	45%	4.1.1. Location: • Rural area (less than 10,000 inhabitants), $V_{\text{ind}} = 1$ • Urban area, $V_{\text{ind}} = 0.95$ • Suburbs, $V_{\text{ind}} = 0.9$ • Others, $V_{\text{ind}} = 0.5$
				35%	4.1.2. Surrounding buildings: • Abandoned building, upper, or lower floor, $V_{\text{ind}} = 1$ • Uninhabited building, upper or lower floor; or garage and basement, $V_{\text{ind}} = 0.95$ • There are no surrounding buildings or floors, $V_{\text{ind}} = 0.5$ • Without information about the surrounding buildings, $V_{\text{ind}} = 0.3$ • Inhabited surrounding-building, upper floor, or lower floor, $V_{\text{ind}} = 0.05$
				20%	4.1.3. Escape route: • Easy and close to the branch (vehicle), $V_{\text{ind}} = 1$ • Easy and close to the branch (on foot), $V_{\text{ind}} = 0.9$ • Difficult but close to the branch, $V_{\text{ind}} = 0.25$ • Difficult and distant to the branch, $V_{\text{ind}} = 0.1$

(*Continued*)

Table II. (Continued)

α_{ind}	Requirements	β_{ind}	Criteria	γ_{ind}	Indicators[b]
15%	5. Social environment	70%	5.1. Potential of conflict	50%	5.1.1. Number of robberies in the province: • Level 3 (more than 10), $V_{\text{ind}} = 1$ • Level 2 (between 5 and 10), $V_{\text{ind}} = 0.4$ • Level 1 (less than 5), $V_{\text{ind}} = 0.1$
				50%	5.1.2. Number of robberies in the branch (5 years): • More than 3, $V_{\text{ind}} = 1$ • Between 1 and 3, $V_{\text{ind}} = 0.7$ • Less than 1, $V_{\text{ind}} = 0.2$
		30%	5.2. Police operations	100%	5.2.1. Response time • More than 30 minutes, $V_{\text{ind}} = 1$ • Between 10 and 30 minutes, $V_{\text{ind}} = 0.8$ • Less than 10 minutes, $V_{\text{ind}} = 0.1$

[a] RI is the risk index. It falls within the interval [0,1], being 0 and 1 the maximum and minimum levels of satisfaction (or the minimum and maximum levels of risk), respectively.

[b] The possible input values (answers) that the qualitative (discrete) indicators can take are listed below their names. The number that follows each input value is the level of risk (V_{ind}). Once again, this number falls within the interval [0,1], being 0 and 1 the maximum and minimum levels of satisfaction (or the minimum and maximum levels of risk), respectively.

[c] This indicator can be treated as a quantitative (continuous) one. The values that take the different value function parameters are indicated below its name. These are the same parameters that appear in Equation (2). It could also have been possible to treat this indicator as a discrete one.

indicators into a common and dimensionless parameter called value (V_{ind}). In this work, this parameter will be related to the risk level. The performance of each indicator is assessed through a value function that allows the user to consider possible nonlinearities. MIVES also allows the establishment of filters to cancel the evaluation if an indicator does not reach a minimum level. More details about the MIVES model presented here, including the requirement tree and the corresponding value functions, are discussed in Section 3.1. Moreover, the reader can find more information about the MIVES method in Cartelle Barros et al. (2015) and in de la Cruz, Castro, del Caño, Gómez, Lara and Cartelle (2014).

2.2. General Methodology

The followed methodology entailed these main steps, listed chronologically:

- A preliminary proposal was made for a requirement tree with all the indicators that had to be considered to assess the risk of robbery in bank branches. Both academia and security staff from the bank were involved in this first task. The group (from now on, the project team) included three ABANCA employees with 37, 14, and 10 years of experience in bank robbery risk, and three university researchers with more than 25, 20, and seven years of experience in the fields of risk assessment and management, and decision support methods.
- Meetings were held for the project team to discuss how to assess each indicator included in the preliminary MIVES model.
- An inquiry form was used to collect real information from the bank branches. The objective of this step was to determine the extent to which real information could feed the preliminary model. Furthermore, the bank branches were asked to provide comments on the preliminary model so that modifications could be made.
- Statistical data related to robberies that occurred in the bank were gathered. The available historical data were taken into account at the time of creating the model. Nevertheless, as previously stated, the user does not need to collect historical information for using the model presented here.
- Extensive consultations were made with the trade unions. They could also make comments on and suggestions about the preliminary

model. This and the two previous steps were conducted simultaneously.

- With the information collected in the previous two phases, the preliminary model was amended. After this step, the final model, with 24 indicators, was thoroughly defined and ready to use.
- The final model was implemented to assess the risk of robbery of the bank branches.
- The results obtained were used to create a prioritized list of investment projects for improving security systems.
- A final phase was carried out by the authors: a sensitivity analysis on the 24-indicator-model was performed. With this step, it was possible to reduce the number of indicators in the model, eliminating those that did not generate significant differences in the results. Thus, a second, final model with 17 indicators was defined. Correlations were also established between the indicators. The latter model is the one presented in Section 3.1 and used in the two simulation cases for this work.

3. MODEL

3.1. MIVES Model

Table II presents the requirement tree, with its corresponding weights, from the final model mentioned above. It consists of 17 indicators grouped into five thematic blocks or requirements. The first block relates to branch security features; it takes into account five different indicators. Three of them belong to the second block in which the consequences that the branch employees have on the risk of robbery are assessed. The branch operational procedures were evaluated by the use of three indicators included in the third requirement. Finally, another set of three indicators was used to assess the physical and social environment.

A glossary of terms was included as Supplementary material.

As previously indicated, requirement trees usually consists of three levels: requirements, criteria, and indicators. There can be trees with less than three levels, for very simple problems in which it is not necessary to assess a great number of indicators. Similarly, there can be very complex problems that may need more than three levels, although it is not common. The case here studied is sufficiently intricate for using three levels.

The number of requirements, criteria, and indicators is not established beforehand. It is the result of the reflection process undertaken for creating the model. In this work, the requirements and criteria were selected during brainstorming meetings aimed at compiling all aspects that can influence the risk of robbery. At those moments, requirements and criteria served, among other things, (i) to better understand the problem and its specific topics; (ii) to group the generated ideas in an orderly manner, including in a single criterion all indicators belonging to a specific topic, and then doing the same with criteria and requirements; and (iii) to identify and eliminate repetitions.

On the other hand, if only two breakdown levels (requirements and indicators) are considered, or even if only one level is defined (all the indicators belonging to the same block), some problems may arise at the time of establishing the weights. For example, if the model in Table II consisted of only one level with the 17 indicators, their weights would have to be defined by comparing 17 very uneven parameters. In this way, it is easy to lose sight of the overall picture, and the resulting weights are not always consistent. The problem increases when employing 24 indicators. Even when using AHP there could be problems. By employing requirements and criteria, the model developers only have to compare the importance of a limited number of parameters, in each tree branch. Moreover, the requirement tree allows the generation of subindexes, or partial indexes, which can be very useful. In this work, it allows to evaluate not only the office as a whole, but also its different aspects (employees, operating procedures, social environment, etc.). In the same way, for instance, subindexes of environmental, social, and economic sustainability can be calculated when assessing sustainability employing life-cycle analysis and the MIVES method (Cartelle Barros et al., 2015).

All the indicators included in Table II are qualitative (discrete), with only one exception: indicator 2.1.1 (Number of employees). Each qualitative indicator presents some possible input values (listed below its name in Table II), or answers to a specific question. Each input value or answer is a semantic label associated with a specific level of risk (V_{ind}). This number falls within the interval [0,1], being 0 and 1 the minimum and maximum levels of risk, respectively (or the maximum and minimum levels of satisfaction). The risk (V_{ind}) associated with each of

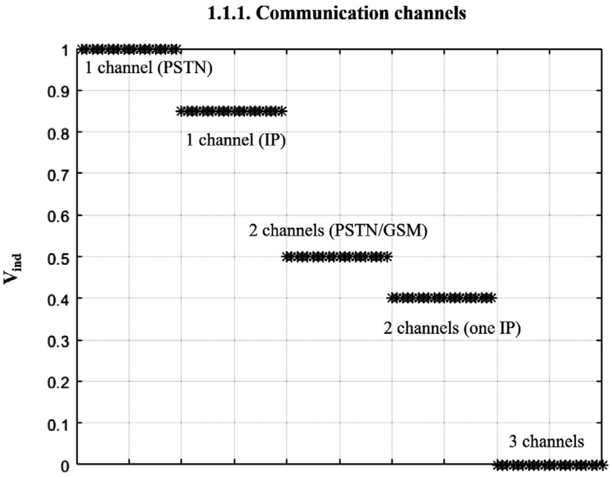

Fig 2. Example of qualitative value function: indicator 1.1.1. (Communication channels).

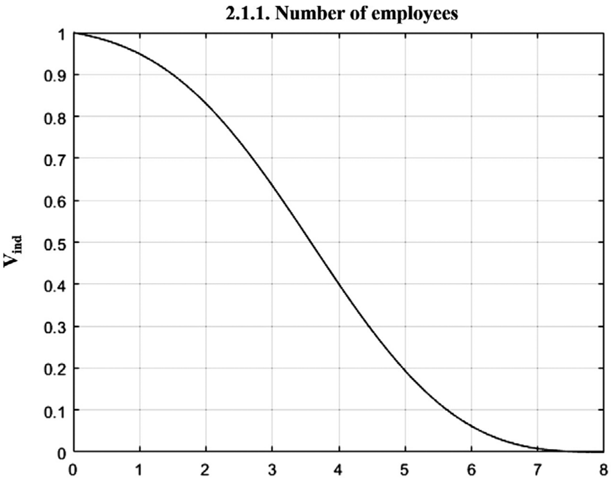

Fig 3. Value function related to the indicator 2.1.1. (Number of employees).

the potential values taken by an indicator was established by the project team, taking into account all the available information mentioned earlier. These can be found in Table II. Fig. 2 includes an example of qualitative value function, in particular, for the indicator related to communication channels. It should be noted that this value function is slightly nonlinear. On the other hand, this indicator presents five possible input values with their corresponding levels of risk (V_{ind}). For example, as can be deducted from Fig. 2, the input value “1 channel (PSTN)” is the worst option, since it is linked to the maximum level of risk ($V_{ind} = 1$).

The level of risk (V_{ind}) associated with the continuous indicator 2.1.1. (Number of employees) is calculated using the following equation:

$$V_{\text{ind}} = \frac{1 - \exp\left(-m_{\text{ind}} \cdot \left(\frac{|P_{\text{ind}} - P_{\text{ind,min}}|}{n_{ind}}\right)^{A_{\text{ind}}}\right)}{1 - \exp\left(-m_{ind} \cdot \left(\frac{|P_{\text{ind,max}} - P_{\text{ind,min}}|}{n_{\text{ind}}}\right)^{A_{\text{ind}}}\right)}, \quad (1)$$

where P_{ind} is the input value to the value function of the alternative under assessment. $P_{\text{ind,min}}$ is the input value that returns the minimum level of risk ($V_{\text{ind}} = 0$). Similarly, $P_{\text{ind,max}}$ is the input value that generates the maximum level of risk ($V_{\text{ind}} = 1$). A_{ind}, m_{ind}, and n_{ind} are shape parameters used to generate different geometries. The values that these parameters adopt are included in Table II. They generate the nonlinear geometry shown in Fig. 3. Equation (1) makes it possible to generate linear, concave, convex, and S-shaped geometries both for decreasing and increasing value functions. Moreover, throughout the use of this equation, the geometry of a value function can be adapted for being more or less demanding at the time of assessing a specific indicator (more or less concave, for instance). Consequently, Equation (1) is usually adequate for the majority of MIVES models, allowing the user to define many different geometries. Nevertheless, there can be specific cases in which the use of Equation (1) is not valid. For example, value functions for thermal comfort can have parabolic geometries, among other options (Alarcon, Aguado, Manga, & Josa, 2011). However, Equation (1) is suitable for the case presented in this study.

As can be seen in Fig. 3, the influence on risk of the number of employees present in the branch is assessed through a decreasing value function in which a higher input value presents a lower level of risk. In other words, a large number of employees will normally be considered as a deterrent by the robber. By way of example, if a specific bank branch has four employees, the level of risk (V_{ind}) will take a value close to 0.4 as can be deduced from Fig. 3. The reader can obtain this value by introducing in Equation (1) the corresponding values for all the parameters.

Using the model presented in Table II, it is possible to obtain the Risk Index (RI). It is a number that falls within the interval [0,1], the maximum and minimum levels of satisfaction (or the minimum and maximum levels of risk), respectively. The RI is calculated from Equation (2):

$$\text{RI} = \sum_{\text{ind}=1}^{17} \alpha_{\text{ind}} \cdot \beta_{\text{ind}} \cdot \gamma_{\text{ind}} \cdot V_{\text{ind}} \,, \quad (2)$$

where α_{ind}, β_{ind}, and γ_{ind} are the weights for the requirements, criteria, and indicators, respectively. The sum of the weights of all the elements belonging to a certain branch of the requirement tree must be equal to 100 %. For example, the first requirement (1. Branch security features) consists of three criteria: 1.1. Alarm reception, 1.2. Storage device location, and 1.3. Security devices. The sum of their weights (10%, 40% and 50%, respectively) gets a value of 100%.

There are different options for establishing the weights for the requirements, criteria, and indicators. The simplest alternative is direct allocation. As its name suggests, it involves using numerical values directly established by experts in the field. Its use is appropriate when a reduced number of elements have to be weighted (normally, between 2 and 4), as long as there are no significant discrepancies among the experts. The proportional method is another option. In this case, one of the elements that must be weighted is selected as reference, and a relative importance is assigned to it (for example 100). The weights for the remaining elements that belong to the same branch of the tree are established by direct comparison with the reference requirement, criteria, or indicator. The process ends with a normalization stage, so that the sum of the weights gets a value of 100%. This method can be appropriate when the number of variables to be weighted varies between three and seven. It is also useful when there is some discrepancy among the people involved in the weighting process, even if the number of parameters is below five. If there are significant discrepancies among the experts or if the number of parameters to be weighted exceeds seven, the use of AHP is recommended (Saaty, 1980, 2006). The weights included in Table II were defined with the help of these three methods, in several meetings with all the members of the project team. The final proposal was reviewed and approved by the key staff of the bank and its branches, and by the trade unions.

It should be noted that RI is not the probability of robbery that each bank branch faces. In fact, any branch, irrespective of its security systems, can be targeted by criminals. Therefore, an RI of 0 is not equivalent to a zero probability in terms of being robbed. It must be understood as a minimum level of risk, corresponding to an excellent office, taking into account the available statistical data and the opinions of the experts that participated in the project. In the same line, an RI equal to 1 suggests that the branch satisfies national regulations, although there is great room for improvement.

3.2. Sensitivity Analysis

The final model employed by the bank was made up of 24 indicators. However, it is not desirable to handle a large number of indicators. Each additional parameter to be assessed requires information as well as extra mathematical operations. Obtaining information can be a complex, even impossible, task. Therefore, whenever possible, a sensitivity analysis must be performed to remove unnecessary indicators. These indicators are the ones that hardly cause major changes in the results (*RI*), regardless of the value adopted. There can be indicators that always assume the same value (or a similar one) for all the alternatives. In such a case, those indicators can also be eliminated.

One of the strengths of the MIVES method is that it uses value functions. As previously indicated in Section 2.1, they make it possible to consider nonlinearities when assessing with both continuous and discrete indicators (please see Figs. 2 and 3). Thus, a sensitivity analysis should be carried out under different situations. Four different scenarios were considered in this analysis. In the first one, all the indicators adopted the input value associated with the minimum level of satisfaction (maximum risk) as a reference. The second case was the opposite of the first one. In the third scenario all the indicators took the input value closest to the medium level of risk (0.5). If two input values were at the same distance from a 0.5 risk level, the worst one, or higher risk, was chosen. If an indicator could only adopt two values, the worst one was selected unless the best one looked very close to a 0.5 risk level. The last case was similar to the third one with two differences. Now, if two input values were at the same distance from the medium level of risk, the best one (lower risk) was selected. Furthermore, if there were only two possible input values, the best one was used, unless the worst one adopted a value very close to 0.5.

For the four scenarios, the same process was carried out. The RI was calculated with all the indicators adopting the reference value. After that, the value adopted for each one of the indicators was modified separately, from the best to the worst possible input value, while all the other indicators continued to have the same reference value. The maximum and minimum RIs were calculated and compared with the initial one. This provided a vision of how each indicator could affect the RI. This process was repeated for all the indicators independently. After that, the indicators with less influence on the RI were identified and removed, obtaining a final MIVES model with 17 indicators (Table II).

By way of example, indicators such as the number of panic buttons or the number of different police forces were removed. In the first case, if people's safety is considered paramount, as is the case here, the general idea is to avoid using the panic button, since this could lead to a violent situation. Consequently, the number of panic buttons during a robbery is irrelevant. In the second one, police forces work in a coordinated way. Thus, the response time is the determining factor. The other indicators that were removed after the sensitivity analysis are: security level of the premises regarding reception of alarms (Levels I or II; very soon after the model was completed, all the branches were at Level II); mandatory security measures, required by legislation (this was merely a compliance check indicator; the bank had always gone far beyond such measures); custody of the branch keys and procedures for opening the heavy security devices during noncommercial hours (the corresponding weights were very low); and type of branch (regular, temporary or stand for specific events, among others; very low weight).

3.3. Correlations between Indicators

Probabilistic MIVES models very often present whatever type of relation between two or more indicators. In other words, there can be indicators that cannot adopt an independent random input value. If the input value of one indicator depends on the one adopted by other indicator, it is possible to say that these two indicators are correlated. Correlations can be covered in different ways. In this work, an analytical approach was taken.

Correlations were only needed when a probabilistic case was analyzed. In other words, they were only taken into account for the two fictitious simulation cases presented in Section 4. Nevertheless, if a real branch had been studied at a particular moment, correlations and simulations would not have been required, since the user of the model would have needed to introduce only one input value for each indicator, in particular, the one linked to the real bank branch.

A correlation was established between indicators 1.3.1. (Devices for cash storing and handling) and 3.1.1. (Cash storing during noncommercial hours). The relation between these two aspects is clear. It is not possible to put the cash into two locking-devices if the office only has one. Nevertheless, the opposite can happen: that is, cash can be stored out of locking-devices even if there are two or more of those devices. This last case can be linked to an inadvisable practice by employees. Therefore, during the Monte Carlo simulation, if indicator 1.3.1. adopted the third, fourth, fifth, sixth, or seventh input values of Table II, indicator 3.1.1. could adopt any of the possible input values. Nevertheless, if indicator 1.3.1. adopted the first or the second values, indicator 3.1.1. had to adopt one of the first three input values.

There was also a correlation between indicators 1.3.1. (Devices for cash storing and handling) and 3.2.1. (Cash handling during commercial hours). In this case, the correlation was imposed by the existence or nonexistence of a cash box, cash dispenser, or cash recycler. In other words, if indicator 1.3.1. adopted the first or fourth input values of Table II, all the possible input values are valid for indicator 3.2.1. with the exception of the fourth one. If indicator 1.3.1. took the second or the fifth input value, indicator 3.2.1. could not adopt the third input value. In all other cases, indicator 3.2.1. could take any input value.

A correlation was also modeled between indicators 2.1.1. (Number of employees) and 3.2.2. (Amount of money). The number of employees was assumed to be an integer number. A noninteger number of employees could be valid, if one or more of the workers had part-time contracts. Nevertheless, this assumption was not considered here. On the other hand, it was reasonable to assume that a higher number of employees was linked to a higher level of activity (payment transactions, bill collection) and, as a result, to the need to have more cash in the office. If the number of employees was less than or equal to two, indicator 3.2.2. adopted the first input value (Level 3) of Table II. If it was higher than 8, the amount of money was over 200,000 € (Level 1). Level 2 was the input value adopted in the remaining cases.

4. SIMULATION STUDIES

Two different simulation cases were studied in this manuscript. The goal of the first one is to provide a quick overview of the risk level of a whole bank; in this case, a fictitious one. Before collecting the full set of data from hundreds or thousands of branches, a simulation can be made to give a general idea of the bank's situation. To do this, the bank's security staff, who are well aware of the condition of most agencies, will set up distribution functions for the model's indicators. Here, a probability was assigned to each one of the possible input values for the qualitative (discrete) indicators (Table III, Simulation 1). Despite the fact that the considered commercial bank did not exist, those values were established with the help of the main ABANCA experts, taking into account real situations in different Spanish banks. The sum of the probabilities for the different answers must be equal to 1, as can be deduced from Table III. For the number of employees (indicator 2.1.1), a closed triangular distribution was defined (Table IV). As previously mentioned, the number that the triangular distribution provides in each iteration was rounded to the nearest integer.

Therefore, results of Simulation 1 provide quick, preliminary information about the real level of risk that the different bank branches can have. From these results, after analyzing the most unfavorable cases, the security specialists can quickly identify the real offices with the highest risk of robbery, in order to make immediate decisions. For instance, investing more in training employees, changing the storage devices' locations, replacing the current devices with safer ones or increasing the number of safety devices, among many other options.

The reader should bear in mind that, as a result of the Monte Carlo simulation, the number of possible situations (that is, the number of *RIs*) can be higher than the number of bank branches that a commercial bank can have. Nevertheless, real bank branches are dynamic, since the staff and number of employees are not always the same. People go on holiday, take time off, or are even moved to another branch. They also carry out work-related tasks out of the office or go out to have a break. The bank office can be refurbished to modernize facilities. Even migratory movements can have an impact on certain indicators, such as the amount of money (indicator 3.2.2). This can be the case of a community that has undergone a population loss due to an economic crisis. With a reduced number of inhabitants, less money is needed for fewer economic transactions. The opposite can also happen.

As real bank branches were dynamic, the authors found it necessary to carry out a second simulation, to examine how uncertainty can affect a specific bank branch. Simulation 2 provided probabilistic information about a fictitious one. In this case, the term "dynamic" was associated with staff. In other words, possible reforms of the office were not taken into account. Consequently, only the indicators linked to employees (indicators 2.1.1., 2.2.1., 2.2.2., 3.1.1., and 3.2.1.) were defined as probabilistic. The remaining indicators were considered deterministic, adopting only one possible input value (probability equal to 1 in Table III). The reasons for treating certain indicators as probabilistic are the same as those mentioned in Simulation 1. Furthermore, the reader should bear in mind that offenders usually perpetrate a robbery when the benefit is supposed to be higher or when, according to their perception, the risk is lower (Morrison & O'Donnell, 1996). With these ideas linked, the time of day in which the number of employees is at its lowest—with fewer witnesses and possible heroes to interfere—can be perceived by the robber as the best moment to act.

In Simulation 2, all the indicators were defined as qualitative. Therefore, the number of employees (indicator 2.1.1.) was transformed into a discrete parameter with only three possible input values: (i) two employees, (ii) three employees, and (iii) four employees. A probability was defined for each possible answer (Table V). This is still consistent with the continuous value function displayed in Fig. 3. In other words, the levels of risk (V_{ind}) for the three possible answers were obtained by using the continuous value function. Their values are 0.8302, 0.6350, and 0.4008, respectively.

Indicator 3.2.2. (Amount of money) is not included in Table III. Defining the probabilities for the different input values of this parameter is not necessary, since it is correlated with the number of employees (indicator 2.1.1.).

5. RESULTS AND DISCUSSION

This section is divided into two different subsections. In the first, the results for the two simulation case studies are presented and discussed. Section 5.2 summarizes the general results obtained once the 24-indicator model to the ABANCA branches was applied.

5.1. Results for the Simulation Case Studies

Table VI includes the statistical parameters of the RI for the two simulation case studies, after the Monte Carlo method was applied. Fig. 4 contains the cumulative probability curve as well as the frequency histogram for Simulation 1. Fig. 5 provides analogous information for Simulation 2.

Table III. Probabilities Associated with the Different Input Values of the Qualitative (Discrete) Indicators for the Two Simulations

Indicators	Simulations	
	Simulation 1 Probability[a]	Simulation 2 Probability[a]
1.1.1. Communication channels:		
• One channel (PSTN)	0.06	0
• One channel (IP)	0.12	0
• Two channels (PSTN/GSM)	0.17	0
• Two channels (one of them IP)	0.59	1
• Three channels (IP, PSTN, GSM)	0.06	0
1.2.1. Safes:		
• Visible and located in the main service area	0.06	0
• Not visible and located in the main service area	0.47	1
• Located in the archive	0.47	0
1.2.2 Cash box:		
• Visible from the main service area	0.09	0
• Not visible from the main service area	0.91	1
1.3.1. Devices for cash storing and handling:		
• One safe and one cash box	0.04	0
• One safe and one cash dispenser or cash recycler	0.04	0
• One safe, one cash dispenser or cash recycler and one cash box	0.46	1
• Two safes and one cash box	0.04	0
• Two safes and one cash dispenser or cash recycler	0.04	0
• Two safes, one cash dispenser or cash recycler and one cash box	0.36	0
• Two safes, more than one cash dispenser or cash recycler and one cash box	0.02	0
1.3.2. Security cameras:		
• Main entrance	0.05	0
• Main entrance and cashier desks	0.49	1
• Main entrance, cashier desks, and main service area	0.39	0
• The previous three options and the archive	0.05	0
• The previous four options and out of the branch	0.02	0
2.2.1. Staff composition:		
• Combination of personnel with more and less of two years of experience	0.71	0.10
• Only personnel with more than two years of experience	0.29	0.90
2.2.2. Training:		
• At least one worker without training	0.06	0
• All personnel with training but one of them with only online training	0.65	0.91
• All personnel with classroom training	0.26	0.09
• All personnel with classroom and online training	0.03	0
3.1.1. Cash storing during noncommercial hours:		
• Out of storing locking devices	0.01	0
• In one locking device	0.14	0
• In two locking devices	0.52	0.70
• In more than two locking devices	0.33	0.30

(*Continued*)

Table III. (Continued)

Indicators	Simulations	
	Simulation 1 Probability[a]	Simulation 2 Probability[a]
3.2.1. Cash handling during commercial hours:		
• Bunker	0.02	0
• Security lock	0.02	0
• Cash box	0.31	0.23
• Cash dispenser or cash recycler	0.63	0.77
• Other	0.02	0
4.1.1. Location:		
• Rural area (less than 10,000 inhabitants)	0.39	0
• Urban area	0.39	1
• Suburbs	0.20	0
• Others	0.02	0
4.1.2. Surrounding buildings:		
• Abandoned building, upper or lower floor	0.02	0
• Uninhabited building, upper, or lower floor; or garage and basement	0.04	0
• There are no surrounding buildings or floors	0.02	0
• Without information about the surrounding buildings	0.30	0
• Inhabited surrounding building, upper floor, or lower floor	0.62	1
4.1.3. Escape route:		
• Easy and close to the branch (vehicle)	0.48	1
• Easy and close to the branch (on foot)	0.18	0
• Difficult but close to the branch	0.24	0
• Difficult and distant to the branch	0.10	0
5.1.1. Number of robberies in the province:		
• Level 3 (more than 10)	0.07	0
• Level 2 (between 5 and 10)	0.26	0
• Level 1 (less than 5)	0.67	1
5.1.2. Number of robberies in the branch (5 years):		
• More than 3	0.04	0
• Between 1 and 3	0.22	0
• Fewer than 1	0.74	1
5.2.1. Response time		
• More than 30 minutes	0.03	0
• Between 10 and 30 minutes	0.69	1
• Less than 10 minutes	0.28	0

[a] The sum of the probabilities of all the possible input values for an indicator is equal to 1.

Unfortunately, the results obtained in this work cannot be compared with other from the existing literature. As explained in previous sections, there are no similar or comparable pieces of research. As indicated in Section 4, Simulation 1 can provide a quick overview of the risk level of a whole bank, without the need for collecting information from all branches. Consequently, it seems reasonable to obtain a significant difference between the minimum and maximum levels of risk, as is the case in this study (0.1556 and 0.7508, first row of Table VI). A commercial bank can have modern branches equipped with the

Table IV. Model Input Values for Indicator 2.1.1. (Number of employees) for Simulation 1

Simulation	Distribution Function	Distribution Parameters		
		Minimum	Mode	Maximum
Simul. 1	Closed triangular[a]	1	3	10

[a] In Simulation 1, a closed triangular distribution function was used during the Monte Carlo simulation for indicator 2.1.1.

Table V. Probability Values for Indicator 2.1.1. (Number of Employees) for Simulation 2

Simulation	Distribution Function	Distribution input Values and their Probabilities[a]		
		2 Employees	3 Employees	4 Employees
Simul. 2	Discrete	0.3	0.4	0.3

[a] In Simulation 2, indicator 2.1.1. was treated as a discrete indicator with three possible input values: (i) two employees, (ii) three employees, and (iii) four employees. The level of risk associated to each one of the input values was obtained by using Equation (2) with the parameters defined in Table II and being P_{ind} equal to 2, 3, and 4. The levels of risk are 0.8302, 0.6350, and 0.4008, respectively.

Table VI. Statistical Parameters of the RI for the Two Simulation Cases

Simulation	Statistical parameters					
	Minimum	Maximum	Mean	Modal Interval (MI)	Frequency of MI	*SD*
Simul. 1	0.1556	0.7508	0.4180	[0.3,0.4)	37.32%	0.087
Simul. 2	0.3446	0.5776	0.4315	[0.4,0.5)	47.57%	0.056

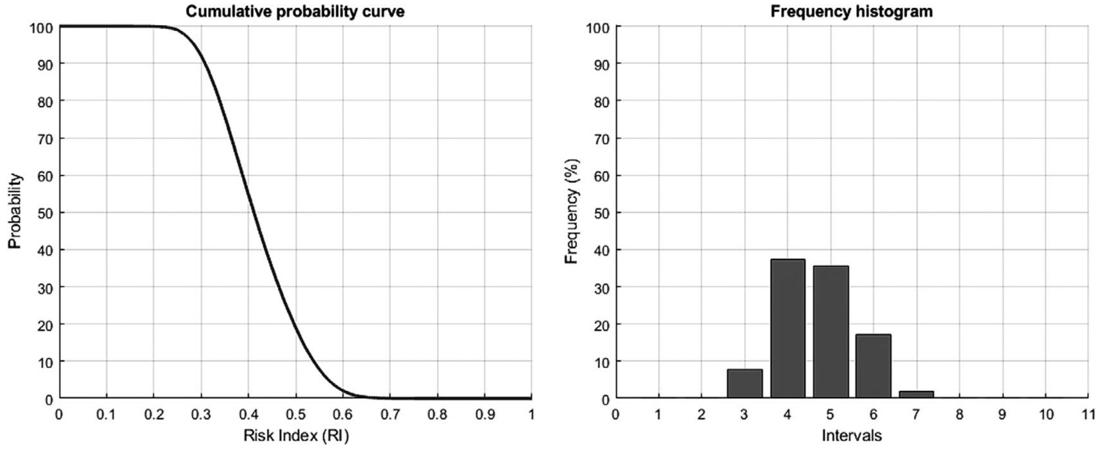

Fig 4. Cumulative probability curve and frequency histogram for the RI of the first simulation analysis. Interval 1 corresponds with (0.0, 0.1). The range for each interval is equal to 0.1.

best security features, located in nonconflictive areas, with a considerable number of experienced and well-trained employees. Nevertheless, the opposite can also happen, at least in terms of its location. However, if the reader analyzes the results as a whole, he or she realizes that both the more probable level of risk (between 0.3 and 0.4, the longest bar in the frequency histogram of Fig. 4) and the mean value (0.4180 in Table VI) are far from this latter scenario of high risk level. This is because commercial banks in developed countries go beyond the security legislation. The reader should bear in mind that it is not

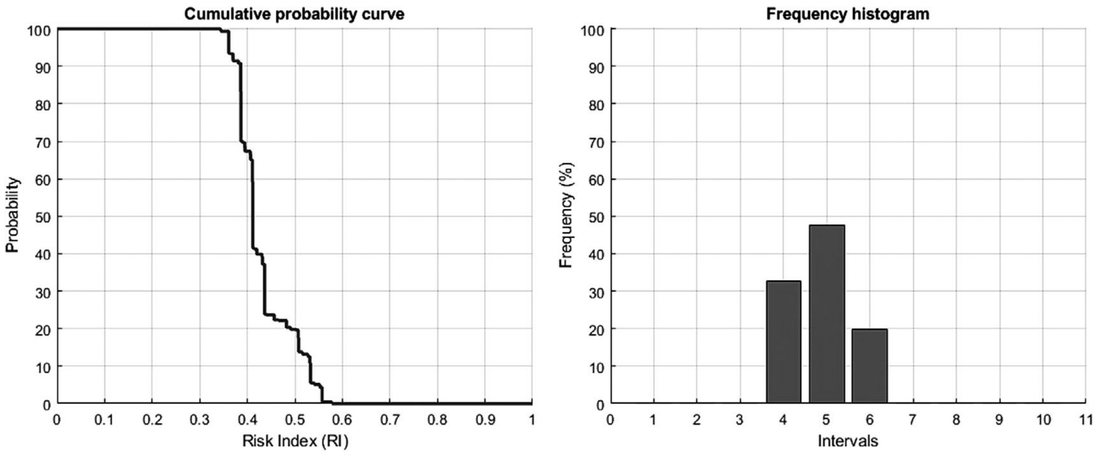

Fig 5. Cumulative probability curve and frequency histogram for the RI of the second simulation study. Interval 1 corresponds with (0.0, 0.1). The range for each interval is equal to 0.1.

possible to obtain a level of risk equal to zero, since even the best branch from a security point of view can be the target of a robbery. Nonetheless, a level of risk below 0.5 can be considered a high-performing result, especially taking into account that the model presented here is quite demanding. The percentage of branches with a RI over 0.5 is under 20% as can be deducted from the cumulative probability curve in Fig. 4. In cases such as these, the bank staff from the security department must study the specific characteristic of each one of the branches separately, to detect and correct weak points.

Possible corrective measures may entail: (i) improving branch security features by, for instance, replacing current devices with safer ones, or increasing the number of safety devices; (ii) promoting training courses on security issues for the employees, and (iii) establishing control procedures for ensuring that the staff follow guidelines in terms of cash handling and storing, among many others. On the other hand, some indicators that can contribute to an increased level of risk, in particular the ones linked to requirements 4 and 5 (physical and social environment, respectively), are less readily corrected. Where an unacceptable level of risk has been achieved, the commercial bank must consider the option of closing the branch and opening a new one that can meet the needs of the same population group but, this time, with a lower RI. In other words, at the time of opening the new branch, it is important to find a space with no abandoned or uninhabited surrounding buildings, located in an area that police response is swift and, at the same time, is not conducive to the robbers' easy escape.

In addition to the issues related to the previous simulation (Simulation 1), it is also interesting to understand how the level of risk of a specific branch can vary over time (Simulation 2). This is particularly true when changes are more likely to happen in the short term, that is, the ones linked to the staff. This is discussed in the second simulation (Simulation 2). Before talking about it, a brief comparison can be made between its results with those for Simulation 1.

The variability affecting a specific branch (Simulation 2) is lower than the one affecting all the branches of a commercial bank (aspect related to Simulation 1). Consequently, in the second simulation, a smaller number of indicators are defined as probabilistic, as explained in Section 4. Obviously, the greater the variability (uncertainty) affecting the inputs to the model, the greater the variability affecting its results. This is the reason why the difference between the maximum (0.5776, Table VI) and minimum (0.3446, Table VI) levels of risk in this second simulation is lower than in the first one (maximum and minimum values of 0.7508 and 0.1556, respectively, Table VI). This is also the case when frequency histograms from Figs. 4 and 5 are compared. The frequency histogram for the second simulation (Fig. 5) presents RIs in a smaller number of intervals. That is, the branch in Simulation 2 obtained RIs belonging to [0.3,0.4), [0.4,0.5), and [0.5,0.6) (Fig. 5), while in Simulation 1, the results fall within the following intervals: [0.1,0.2), [0.2,0.3), [0.3,0.4), [0.4,0.5), [0.5,0.6), [0.6,0.7), and [0.7,0.8) (Fig. 4).

Taking these factors into account, it seems reasonable to say that, in Simulation 2, there is a reduced number of "possible real snapshots" in comparison with the first one. On the other hand, in Simulation 2, the RI function leaps as can be seen in Fig. 5. This is due to the fact that only a limited number of qualitative indicators were treated as probabilistic.

Regarding the results of this second simulation, it can be concluded that the level of risk is acceptable, with a mean value under 0.5 (0.4315, Table VI). Nevertheless, it should be noted that the level of risk of a specific branch can vary considerably (from 0.34 to 0.58, minimum and maximum values in Table VI) depending on the number of employees and their level of training, as well as on whether or not they follow guidelines for cash handling and storing. The reader should not forget that professional robbers normally study their targets with great care. Consequently, if the employees of a specific branch do not respect the bank's procedures by, for instance, failing to place cash in the storage devices, the robber will see that branch as a more attractive target. In the same vein, if robbers realize that there are specific moments in the day when the number of employees is reduced, they will take advantage of this situation.

5.2. General Results for a Real Bank

The security personnel of the bank used the 24-indicator model by means of a software developed by researchers from the Technical University of Catalonia and the University of A Coruña (Technical University of Catalonia, 2016). Once the model is defined in the corresponding software, assessing the robbery risk of a specific bank branch is a simple process. The user only has to collect the real information related to the model indicators. These data are then introduced into the MIVES software, which automatically provides the risk index of the branch under consideration. A beta version of the MIVES software as well as its user manual can be downloaded from the website of the Technical University of Catalonia (Technical University of Catalonia, 2016). Deterministic models can be implemented on electronic spreadsheets, but this is not possible when probabilistic analysis is needed (in this case additional software is required).

The results obtained with the 24-indicator model must be similar to the ones that the final 17-indicator-model can provide, as explained in Section 3.2. Nevertheless, the bank or any commercial bank may find it useful to employ the complete model, even if doing so only has a slight impact on the results. Stated another way, the complete model provides a more comprehensive definition of each real branch.

The 24-indicator model was used to estimate, in a deterministic way, the RI of 636 real bank branches belonging to ABANCA. They were classified into three groups depending on the level of risk: (i) low risk ($RI \leq 0.5$), (ii) medium risk ($0.5 < RI \leq 0.65$), and (iii) high risk ($RI > 0.65$). A medium or high-risk branch means that the office is far from security excellence, although it fulfils national legislation in terms of bank security issues. 567 branches obtained a RI equal to or under 0.5 (low risk), while 54 and 15 branches obtained RIs belonging to the medium and high-risk levels, respectively. An action plan with preventive and corrective measures was designed for the 69 branches with medium and high-risk levels. These measures were classified into four groups depending on different priority levels. The aim was to take steps in the short term with the branches with the highest RIs. Consequently, in the six months following the assessment, 18 branches reduced their RI considerably. Among the measures carried out were relocating storage devices, increasing the number of devices for cash storing, and handling, improving, or changing communication channels and installing new security cameras.

At the time of preparing this manuscript, all the branches that have been assessed now present a low or medium level of risk. In fact, the corrective measures implemented in some branches meant that they could go from a high level to a low level of risk. As previously indicated, an RI between 0.4 and 0.5 is linked to a high-performing branch for risk of robbery.

On the other hand, it has been found that the investment made to improve the branches with highest RIs did manage to hinder robberies. In fact, since the improvement plan was carried out, the number of raids and attempted robberies has dropped considerably. Furthermore, the model also helped promote a safety and security culture among bank employees; they know about and respect the security procedures. Their perception has also changed. They are now aware that ABANCA's priority is to protect people. Since the implementation of the improvement plan, no sick leave related to robberies has been taken. Consequently, the trade unions supported this model, which has had a positive impact on this commercial bank.

The application of the model to a real bank served to confirm its usefulness at the time of classifying a branch according to its risk of robbery. The bank security personnel compared all the results with the real situation in the different bank branches, and found no contradictory results. This served to validate the model. This work also served to identify quickly and accurately the measures that most reduce the risk index. This allows the bank to manage more efficiently the money spent on improving the security of its branches. As previously indicated, after adopting the corrective measures identified with the help of the model here presented, the number of attempted robberies has decreased significantly.

6. CONCLUSIONS

In this article, a model for assessing the risk of bank robberies was presented with the aim of reducing the risk, the impact on people and prioritizing investment to improve security. The model consists of a wide range of indicators in which the following issues are addressed: (i) security features, (ii) employees, (iii) operational procedures, (iv) physical environment, and (v) social environment. The model is based on the MIVES method and it was combined with the Monte Carlo simulation to take uncertainty into account. Correlations between indicators were also established. Two fictitious but possible sets of real cases were considered, employing the Monte Carlo simulation method. The model was also used to assess, in a deterministic way, the risk of 636 real bank branches belonging to a Spanish commercial bank (ABANCA). The most important conclusions of this work are:

- The model provides valuable results, easy for bank employees to understand. It allows the user to identify the weak points of a branch.
- Uncertainty and variability can play a key role. The level of risk for a specific branch can significantly vary over time, even if the office is not renovated.
- Considerable levels of risk can be achieved if employees do not respect the internal guidelines for cash handling and storing.
- The model was validated through its application to the previously alluded bank. It served to identify the bank branches with medium or high levels of risk.
- Steps like relocating storage devices, installing new security cameras and using devices for cash storing and handling, among others, were taken in the short term (six months after the assessment) to reduce the RI of 18 of the 636 branches.
- This kind of model is useful in fostering a security and safety culture among employees. It also serves to change the perception of the employees in terms of bank's priorities.

This model should be regularly updated to take into account new legal requirements as well as security devices. Despite the fact that this model was designed for a specific commercial bank, it can be applied to other banks, at least in the same country. In some specific cases, minor changes may be necessary. Furthermore, both the methodology and a part of the model can also be used to assess the risk of robbery for different types of commercial establishments if the corresponding modifications are introduced.

Regarding future applications, the model could be used to assess the risk of other commercial banks, both in Spain and in other countries. This would allow comparisons to be made. Furthermore, it could also be modified so that it can be applied to other commercial establishments.

ACKNOWLEDGMENTS

The present research work was supported and funded by ABANCA Corporación Bancaria S.A. Funding for open access charge: Universidade da Coruña/CISUG. The authors would also like to thank Prof. Antonio Aguado (Technical University of Catalonia, Spain) as well as the anonymous reviewers for some interesting comments that served to improve the article. Two of the authors are employees of the bank (ABANCA).

REFERENCES

Abraham, B. R., & Baldassaro, P. J. (2001). Leaving robbers barren. *Security Management*, *45*(2), 42–46.

Alarcon, B., Aguado, A., Manga, R., & Josa, A. (2011). A value function for assessing sustainability: Application to industrial buildings. *Sustainability*, *3*, 35–50. https://doi.org/10.3390/su3010035

Borzycki, M. (2003). Bank robbery in Australia. *Australian Institute of Criminology*, *253*, 1–6.

Braga, A. A. (2008). *Problem-oriented policing and crime prevention* (2nd edition). New York: Criminal Justice Press.

Büchler, H., & Leineweber, H. (1991). The escape behavior of bank robbers and circular blockade operations by the police. In E. Kube & H. U. Störzer (Eds.), *Police Research in the Federal Republic of Germany* (pp. 199–208). Berlin, Germany: Springer. https://doi.org/10.1007/978-3-642-74176-0_16

Cartelle Barros, J. J., Lara Coira, M., de la Cruz López, M. P., & del Caño Gochi, A. (2015). Assessing the global sustainability of different electricity generation systems. *Energy*, *89*, 473–489. https://doi.org/10.1016/j.energy.2015.05.110

Cartelle Barros, J. J., Lara Coira, M., de la Cruz López, M. P., & del Caño Gochi, A. (2016). Probabilistic life-cycle cost analysis for renewable and non-renewable power plants. *Energy*, *112*, 774–787. https://doi.org/10.1016/j.energy.2016.06.098

Cartelle Barros, J. J., Lara Coira, M., de la Cruz López, M. P., & del Caño Gochi, A. (2018). Sustainability optimisation of shell and tube heat exchanger, using a new integrated methodology. *Journal of Cleaner Production*, *200*, 552–567. https://doi.org/10.1016/j.jclepro.2018.07.266

Cartelle Barros, J. J., Lara Coira, M., de la Cruz López, M. P., & del Caño Gochi, A., & Soares, I. (2020). Probabilistic multicriteria environmental assessment of power plants: A global approach. *Applied Energy*, *260*, 114344. https://doi.org/10.1016/j.apenergy.2019.114344

Casanovas-rubio, M., Pujadas, P., Pardo-bosch, F., Blanco, A., & Aguado, A. (2019). Sustainability assessment of trenches including the new eco-trench : a multi-criteria decision-making tool. *Journal of Cleaner Production*, *238*, 117957. https://doi.org/10.1016/j.jclepro.2019.117957

Chitsaz, N., & Banihabib, M. E. (2015). Comparison of different multi criteria decision-making models in prioritizing flood management alternatives. *Water Resources Management*, *29*, 2503–2525. https://doi.org/10.1007/s11269-015-0954-6

Converso, D., & Viotti, S. (2014). Post-traumatic stress reaction in a sample of bank employees victims of robbery in the workplace: The role of pre-trauma and peri-trauma factors. *Medicina Del Lavoro*, *105*(4), 243–254.

Cox, L. A. (2008). Some limitations of " risk = threat × vulnerability × consequence " for risk analysis of terrorist attacks. *Risk Analysis*, *28*(6), 1749–1761. https://doi.org/10.1111/j.1539-6924.2008.01142.x

Damenu, T. K., & Beaumont, C. (2017). Analysing information security in a bank using soft systems methodology. *Information and Computer Security*, *25*(3), 240–258. https://doi.org/10.1108/ICS-07-2016-0053.

de la Cruz, M. P., Castro, A., del Caño, A., Gómez, D., Lara, M., & Cartelle, J. J. (2014). Comprehensive methods for dealing with uncertainty in assessing sustainability part 1: The MIVES-Monte Carlo method. In M. S. García-Cascales, J. M. Sánchez-Lozano, A. D. Masegosa, & C. Cruz-Corona (Eds.), *Soft computing applications for renewable energy and energy efficiency* (pp. 69–106). Hershey, PA: IGI Global.

de la Cruz, M. P., Castro, A., del Caño, A., Gómez, D., Lara, M., & Gradaille, G. (2014). Comprehensive methods for dealing with uncertainty in assessing sustainability part 2. In M. S. García-Cascales, J. M. Sánchez-Lozano, A. D. Masegosa, & C. Cruz-Corona (Eds.), *Soft computing applications for renewable energy and energy efficiency* (pp. 107–140). Hershey, PA: IGI Global.

De Leo, G., Volpini, L., & De Gregorio, E. (2006). La rapina in banca aspetti criminologici, problemi di sicurezza e prospettive di prevenzione.pdf. *Rassegna Penitenziaria e Criminologica*, 2, 105–119.

Dugato, M. (2014). Analyzing bank robbery in Italy. In S. Caneppele & F. Calderoni (Eds.), *Organized crime, corruption and crime prevention* (pp. 115–125). Berlin, Germany: Springer.

European Banking Federation (EBF). (2010). *18th report on bank robberies & other raid types*. Brussels, Belgium: EBF.

European Banking Federation (EBF). (2011). *19th report on bank robberies & other raid types*. Brussels, Belgium: EBF.

Federal Bureau of Investigation (FBI). (2003). *Special report: Bank robbery in the United States*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2004). *Bank crime statistics 2004*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2005). *Bank crime statistics 2005*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2006). *Bank crime statistics 2006*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2007). *Bank crime statistics 2007*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2008). *Bank crime statistics 2008*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2009). *Bank crime statistics 2009*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2010). *Bank crime statistics 2010*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2011). *Bank crime statistics 2011*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2012). *Bank crime statistics 2012*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2013). *Bank crime statistics 2013*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2014). *Bank crime statistics 2014*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2015). *Bank crime statistics 2015*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2016). *Bank crime statistics 2016*. Washington, DC: FBI.

Federal Bureau of Investigation (FBI). (2017). *Bank crime statistics 2017*. Washington, DC: FBI

Federal Bureau of Investigation (FBI). (2018). *Bank crime statistics 2018*. Washington, DC: FBI.

Fichera, G. P., Fattori, A., Neri, L., Musti, M., Coggiola, M., & Costa, G. (2015). Post-traumatic stress disorder among bank employee victims of robbery. *Occupational Medicine*, *65*, 283–289. https://doi.org/10.1093/occmed/kqu180

Fichera, G. P., Sartori, S., & Costa, G. (2009). Post-traumatic Stress Disorder following robbery at the workplace: A pilot study on 136 pharmacy workers. *Medicina Del Lavoro*, *100*(2), 97–108.

Frans, Ö., Åhs, J., Bihre, E., & Åhs, F. (2018). Distance to threat and risk of acute and posttraumatic stress disorder following bank robbery: a longitudinal study. *Psychiatry Research*, *267*, 461–466. https://doi.org/10.1016/j.psychres.2018.06.050

Gandini, A., Garmendia, L., Prieto, I., Alvarez, I., & San-José, J.-T. (2020). A holistic and multi-stakeholder methodology for vulnerability assessment of cities to flooding and extreme precipitation events. *Sustainable Cities and Society*, *63*, 102437. https://doi.org/10.1016/j.scs.2020.102437

Gill, M. (2000). *Commercial robbery*. London, UK: Perpetuity Press.

Giorgi, G., Leon Perez, J. M., Montani, F., Courcy, F., & Arcangeli, G. (2015). Distress and job satisfaction after robbery assaults: a longitudinal study. *Occupational Medicine*, *65*, 290–295. https://doi.org/10.1093/occmed/kqv051

Giorgi, G., Fiz Perez, F. S., D ' Antonio, A. C., Mucci, N., Ferrero, C., Cupelli, V., & Arcangeli, G. (2015). Psychometric properties of the impact of event scale-6 in a sample of victims of bank robbery. *Psychology Research and Behavior Management*, *2015*(8), 99–104. https://doi.org/10.2147/PRBM.S73901

Gorton, D. (2014). Using incident response trees as a tool for risk management of online financial services. *Risk Analysis*, *34*(9), 1763–1774. https://doi.org/10.1111/risa.12195

Guazzoni, C., & Ronsivalle, G. B. (2009). An artificial neural network for bank robbery risk management: The OS.SI.F web online tool of the ABI anti-crime department. In E. Corchado, R. Zunino, P. Gastaldo, & A. Herrero (Eds.), *Proceedings of the international workshop on computational intelligence in security for information systems CISIS'08* (Vol. *53*, pp. 1–10). Berlin, Germany: Springer. https://doi.org/10.1007/978-3-540-88181-0_1

Gupta, A., Kumar, Y., & Malhotra, S. (2015). Banking security system using hand gesture recognition. *Paper presented in 2015 International Conference on Recent Developments in Control, Automation and Power Engineering (RDCAPE)* (pp. 243–246). Noida, India: IEEE. https://doi.org/10.1109/RDCAPE.2015.7281403

Habibi, S., Pons Valladares, O., & Peña, D. (2020). New sustainability assessment model for Intelligent Façade Layers when applied to refurbish school buildings skins. *Sustainable Energy Technologies and Assessments*, *42*, 100839. https://doi.org/10.1016/j.seta.2020.100839

Hajkowicz, S., & Collins, K. (2007). A review of multiple criteria analysis for water resource planning and Management, *Water Resources Management*, *21*, 1553–1566. https://doi.org/10.1007/s11269-006-9112-5

Hannan, T. H. (1982). Bank robberies and bank security precautions. *The Journal of Legal Studies*, *11*(1), 83–92. https://doi.org/10.1086/467693

Hansen, M., Armour, C., & Elklit, A. (2012). Assessing a dysphoric arousal model of acute stress disorder symptoms in a clinical sample of rape and bank robbery victims. *European Journal of Psychotraumatology*, *3*, 1–10. https://doi.org/10.3402/ejpt.v3i0.18201

Hansen, M., Armour, C., Shevlin, M., & Elklit, A. (2014). Investigating the psychological impact of bank robbery: a cohort study. *Journal of Anxiety Disorders*, *28*, 454–459. https://doi.org/10.1016/j.janxdis.2014.04.005

Hansen, M., & Elklit, A. (2013). Does acute stress disorder predict posttraumatic stress disorder following bank robbery? *Journal of Interpersonal Violence*, *28*(1), 25–44. https://doi.org/10.1177/0886260512448848

Hansen, M., Hyland, P., & Armour, C. (2016). Does highly symptomatic class membership in the acute phase predict highly symptomatic classification in victims 6 months after traumatic exposure? *Journal of Anxiety Disorders*, *40*, 44–51. https://doi.org/10.1016/j.janxdis.2016.04.008

Hansen, M., Lasgaard, M., & Elklit, A. (2013). The latent factor structure of acute stress disorder following bank robbery: testing alternative models in light of the pending DSM-5. *British Journal of Clinical Psychology*, *52*, 82–91. https://doi.org/10.1111/bjc.12002

Haran, J. F., & Martin, J. M. (1977). The imprisonment of bank robbers: The issue of deterrence. *Federal Probation*, *41*(3), 27–30.

Hochstetler, A. (2001). Opportunities and decisions: Interactional dynamics in robbery and burglary groups. *Criminology*, *39*(3), 737–764. https://doi.org/10.1111/j.1745-9125.2001.tb00939.x

Hole, K. J., Moen, V., & Tjostheim, T. (2006). Case study: Online banking security. *IEEE Security & Privacy*, *4*(2), 14–20. https://doi.org/10.1109/MSP.2006.36

Hosseini, S. M. A., Pons, O., & de la Fuente, A. (2018). A combination of the Knapsack algorithm and MIVES for choosing optimal temporary housing site locations: a case study in Tehran. *International Journal of Disaster Risk Reduction*, *27*, 265–277. https://doi.org/10.1016/j.ijdrr.2017.10.013

Hosseini, S. M. A., Yazdani, R., & de la Fuente, A. (2020). Multiobjective interior design optimization method based on sustainability concepts for post-disaster temporary housing units. *Building and Environment*, *173*, 106742. https://doi.org/10.1016/j.buildenv.2020.106742

Johnston, D. A. (1978). Psychological observations of bank robbery. *American Journal of Psychiatry*, *135*(11), 1377–1379. https://doi.org/10.1176/ajp.135.11.1377

Jones, C. A. (2002). Victim perspective of bank robbery trauma and recovery. *Traumatology*, *8*(4), 191–204. https://doi.org/10.1177/153476560200800402

Jones, I. H., & Jones, A. L. (1998). Psychological consequences of armed hold up. *Australian Family Physician*, *17*(6), 447–450.

Josa, I., de la Fuente, A., Casanovas-Rubio, M. del M., Armengou, J., & Aguado, A. (2021). Sustainability-oriented model to decide on concrete pipeline reinforcement. *Sustainability*, *13*, 3026. https://doi.org/10.3390/su13063026

Kamphuis, J. H., & Emmelkamp, P. M. G. (1998). Crime-related trauma: Psychological distress in victims of bank robbery. *Journal of Anxiety Disorders*, *12*(3), 199–208. https://doi.org/10.1016/S0887-6185(98)00009-7

Khera, N., & Verma, A. (2014). Development of an intelligent system for bank security. *Paper presented at 5th International Conference on Confluence 2014: the Next Generation Information Technology Summit* (pp. 319–322). Noida, India: IEEE. https://doi.org/10.1109/CONFLUENCE.2014.6949339

Kotus, J., Łopatka, K., Czyżewski, A., & Bogdanis, G. (2016). Processing of acoustical data in a multimodal bank operating room surveillance system. *Multimedia Tools and Applications*, *75*, 10787–10805. https://doi.org/10.1007/s11042-014-2264-z

Kou, G., Lu, Y., Peng, Y., & Shi, Y. (2012). Evaluation of classification algorithms using MCDM and rank correlation. *International Journal of Information Technology and Decision Making*, *11*(1), 197–225. https://doi.org/10.1142/S0219622012500095

Kube, E. (1988). Preventing bank robbery: Lessons from interviewing robbers. *Journal of Security Administration*, *11*(2), 78–83.

Lesk, M. (2011). Cybersecurity and economics. *IEEE Security and Privacy Magazine*, *9*(6), 76–79. https://doi.org/10.1109/MSP.2011.160

Levine, N. (2007). Crime travel demand and bank robberies: Using CrimeStat III to model bank robbery trips. *Social Science Computer Review*, *25*(2), 239–258. https://doi.org/10.1177/0894439306298923

Leymann, H. (1985). Somatic and psychological symptoms after the experience of life threatening events: A profile analysis. *Victimology*, *10*(1–4), 512–538.

Leymann, H. (1988). Stress reactions after bank robberies: psychological and psychosomatic reaction patterns. *Work and Stress*, *2*, 123–132. https://doi.org/10.1080/02678378808259156

Matthews, R., Pease, C., & Pease, K. (2001). Repeated bank robbery: theme and variations. In G. Farrell & K. Pease (Eds.), *Repeat victimization, crime prevention studies* (Vol. *12*, pp. 153–164). Monsey, NY: Criminal Justice Press.

Miller-Burke, J., Attridge, M., & Fass, P. M. (1999). Impact of traumatic events and organizational response: A study of bank robberies. *Journal of Occupational and Environmental Medicine*, *41*(2), 73–83. https://doi.org/10.1097/00043764-199902000-00001

Morrison, S. A., & O'Donnell, I. (1996). An analysis of the decision-making practices of armed robbers. *National Criminal Justice*, *167532*, 1–30.

Mucci, N., Giorgi, G., Perez, J. F., Iavicoli, I., & Arcangeli, G. (2015). Predictors of trauma in bank employee robbery victims. *Neuropsychiatric Disease and Treatment*, *11*, 2605–2612. https://doi.org/10.2147/NDT.S88836

Nugent, S., Burns, D., Wilson, P., & Chappell, D. (1989). *Armed robbery from an offender' s perspective: Implications for prevention*. Canberra, Australia: Australian Institute of Criminology.

Ozenne, T. (1974). The economics of bank robbery. *The Journal of Legal Studies*, *3*(1), 19–51.

Paes-Machado, E., & Nascimento, A. M. (2006). Bank money shields: work-related victimisation, moral dilemmas and crisis in the bank profession. *International Review of Victimology*, *13*, 1–25. https://doi.org/10.1177/026975800601300101

Pardo-Bosch, F., Aguado, A., & Pino, M. (2019). Holistic model to analyze and prioritize urban sustainable buildings for public services. *Sustainable Cities and Society*, *44*, 227–236. https://doi.org/10.1016/j.scs.2018.09.028

Pons, O., Franquesa, J., & Hosseini, S. M. A. (2019). Integrated value model to assess the sustainability of active learning activities and strategies in architecture lectures for large groups. *Sustainability*, *11*, 2917. https://doi.org/10.3390/su11102917

Pujadas, P., Pardo-Bosch, F., Aguado-Renter, A., & Aguado, A. (2017). MIVES multi-criteria approach for the evaluation, prioritization, and selection of public investment projects. A case study in the city of Barcelona. *Land Use Policy*, *64*, 29–37. https://doi.org/10.1016/j.landusepol.2017.02.014

Reilly, B., Rickman, N., & Witt, R. (2012). Robbing banks: crime does pay - but not very much. *Significance*, *9*(3), 17–21. https://doi.org/10.1111/j.1740-9713.2012.00570.x

Saaty, T. L. (1980). *The analytic hierarchy process*. New York: McGraw Hill.

Saaty, T. L. (2006). *Fundamentals of decision making and priority theory with the analytic hierarchy process*. Pittsburg, PA: RWS Publications.

Saaty, T. L., & Vargas, L. G. (2006). *Decision making with the analytic network process* (1st ed.). Berlin, Germany: Springer.

Samavati, H. (2004). Bank robbers' blues. *Business Horizons*, *47*(1), 59–63. https://doi.org/10.1016/j.bushor.2003.11.009

Samavati, H. (2006). Economics of crime: panel data analysis of bank robbery in the United States. *Atlantic Economic Journal*, *34*, 455–466. https://doi.org/10.1007/s11293-006-9033-y

Setti, I., van der Velden, P. G., Sommovigo, V., Ferretti, M. S., Giorgi, G., O'Shea, D., & Argentero, P. (2018). Well-being and functioning at work following thefts and robberies: a comparative study. *Frontiers in Psychology*, *9*, 1–13. https://doi.org/10.3389/fpsyg.2018.00168

Shao, M., Han, Z., Sun, J., Xiao, C., Zhang, S., & Zhao, Y. (2020). A review of multi-criteria decision making applications for renewable energy site selection. *Renewable Energy*, *157*, 377–403. https://doi.org/10.1016/j.renene.2020.04.137

Sood, A. K., & Enbody, R. J. (2013). The art of cyber bank robbery: stealing your money through insidious attacks. *CrossTalk*, 9–16.

Szczodrak, M., & Szwoch, G. (2013). An approach to the detection of bank robbery acts employing thermal image analysis. In *Signal processing—Algorithms, architectures, arrangements, and applications (SPA)* (pp. 297–301). Poznan, Poland: IEEE.

Technical University of Catalonia. (2016). MIVES tool: Methodology, downloading, error collection procedure and models. Retrieved from https://deca.upc.edu/es/proyectos/mives/herramientas

Wang, J. Z. (2002). Bank robberies by an Asian gang: an assessment of the routine activities theory. *International Journal of Offender Therapy and Comparative Criminology*, *46*(5), 555–568. https://doi.org/10.1177/030662402236740

Weisel, D. L. (2007). *Bank robbery. Problem-oriented guides for police*. Washington, DC: Center for Problem Oriented Policing.

Zamani-Sabzi, H., King, J. P., Gard, C. C., & Abudu, S. (2016). Statistical and analytical comparison of multi-criteria decision-making techniques under fuzzy environment. *Operations Research Perspectives*, *3*, 92–117. https://doi.org/10.1016/j.orp.2016.11.001

Zubizarreta, M., Cuadrado, J., Orbe, A., & García, H. (2019). Modeling the environmental sustainability of timber structures: a case study. *Environmental Impact Assessment Review*, *78*, 106286. https://doi.org/10.1016/j.eiar.2019.106286

Zubizarreta, M., Ganzarain, J., Cuadrado, J., & Lizarralde, R. (2021). Evaluating disruptive innovation project management capabilities. *Sustainability*, *13*, 1–22. https://doi.org/10.3390/su13010001

SUPPORTING INFORMATION

Additional supporting information may be found online in the Supporting Information section at the end of the article.

Supplementary Material