TOPSIS-based framework for evaluating employee cybersecurity risk

Katarina Kostelić[1,*],

[1] *Faculty of Informatics, Juraj Dobrila University of Pula, Negrijeva ulica 6, 52100 Pula, Croatia*
E-mail: ⟨katarina.kostelic@unipu.hr⟩

Abstract. This paper presents the development and initial validation of a TOPSIS-based framework for evaluating employee cybersecurity risk (TFEECR). The framework offers a structured and objective approach to assessing multiple dimensions of employee behavior and attitudes toward cybersecurity. It integrates the Technique for Order of Preference by Similarity to the Ideal Solution (TOPSIS) with Saaty's criteria weighting, enabling a comprehensive evaluation across five criteria: knowledge, compliance, risky behaviors, attitudes, and training. The framework is validated using simulated data, and it showed robustness in differentiating between high- and low-risk employees. Such results are useful for organizations that want to implement targeted interventions. A sensitivity analysis highlights the framework's adaptability to various settings. This conceptual framework lays the groundwork for future empirical validation and practical application in enhancing organizational cybersecurity.

Keywords: cybersecurity risk assessment, employee behavior, MCDM, risk management, TOPSIS framework

Received: July 14, 2024; accepted: October 14, 2024; available online: February 4, 2025

DOI: 10.17535/crorr.2025.0003

Original scientific paper.

1. Introduction

Managing cybersecurity risks is becoming more important for organizations to operate successfully in the digital era. Cyber threats are becoming more sophisticated, meaning that companies need to continuously monitor and develop their security posture and a resilient cybersecurity framework. Since employees are integral to these frameworks, it is mandatory to assess and reduce the risks related to human behavior. Employees who lack knowledge and skillsets are seen as a susceptible threat vector for cyber attacks, making them vulnerable targets for attackers [7]. The increased vulnerability of organizations during extreme events, as observed in 2020-21, underscores the importance of robust knowledge risk strategies, including proper knowledge identification and guidelines for online behavior, to mitigate the heightened employee-related cybersecurity risks [1, 14], ever more important in ongoing digitalization processes.

Conventional risk assessment methods often overlook the human factor or do not consider all variables or different evaluation criteria related to human behavior. Even if they do consider them, evaluations are often complicated by the subjective nature of human reporting and the complexity of integrating qualitative and quantitative data in comprehensive assessments. The evaluation of employee-related cybersecurity risks is a complex process that considers a number of variables [4, 11, 29]. The evaluation is usually conducted through data collection, measuring scale, and analysis [12]. However, using only subjective measurements from self-assessment questionnaires adds a subjective element that may be harmful to the evaluation procedure [12].

*Corresponding author.

Moreover, the importance of employing multi-criteria optimization methods in cybersecurity and information security tasks is emphasized to overcome these limitations and ensure accurate decision-making [13]. That points to a gap and a need for a systematic approach to evaluating multiple criteria that affect an employee's cybersecurity risk profile. Therefore, developing a more objective evaluation process of employee-related cybersecurity risks is a promising research direction.

The goal of this paper is to present the framework for evaluating employee-related cybersecurity risk, which offers a systematic way to evaluate and rank employees according to their degrees of cybersecurity risk, which can be further tested in future research. In order to achieve a comprehensive approach, multiple factors – knowledge, compliance, risky behaviors, attitudes, and training – will be considered, in combination with a Multi-Criteria Decision-Making (MCDM) technique, the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). This combination creates a TOPSIS-based Framework for Evaluating Employee Cybersecurity Risk, or TFEECR for short. In such a way, the aim is to provide a conceptual framework that can provide organizations with a holistic, objective, and scalable approach to improve their entire cybersecurity posture and direct future empirical research for further validation.

This paper advances the cybersecurity risk assessment literature by presenting a TOPSIS-based framework for evaluating employee-related cybersecurity risks. The proposed framework integrates multiple criteria, and enables the assessment of employees based on their cybersecurity risk levels, which allows organizations to implement targeted measures to reduce these risks. This systematic approach offers a scalable and customizable framework that can be tailored to various organizational needs, thereby enhancing the overall cybersecurity posture. The research contributes to filling the noted gap in the literature regarding the use of quantitative methods in cybersecurity risk evaluations and provides a basis for subsequent empirical investigations and practical implementation in organizational contexts.

The subsequent sections of the paper are structured as follows: the second section presents an overview of the methodologies employed, encompassing the combination of the TOPSIS framework with Saaty's criteria weighting. The third section delineates the analysis and outcomes of the framework applied to simulated employee data. The fourth section examines the ramifications of the findings and their practical utilization. The conclusion encapsulates the primary contributions and proposes avenues for future research.

2. Methods

Cybersecurity risk management involves complex decision-making processes, which require considering multiple criteria. So, simpler, single-criterion models cannot capture the versatile nature of cybersecurity threats and related human behavior, which involves various desirable and undesirable traits and behaviors that can be identified. According to Khoroshko et al. [13], using multi-criteria optimization methods in cybersecurity and information security tasks can overcome these limitations, leading to the enhanced correctness of decision-making. The importance of quantitative methods in developing practical applications and filling in research gaps is also stressed by the bibliometric study of cybersecurity threats [16]. Quantitative methods enable continuous improvement and self-assessment in companies, which allows them to improve their security posture by making informed and cost-effective decisions [8].

According to Saaty's criteria for MCDM methods [21], TOPSIS is particularly advantageous when the decision problem involves ranking alternatives based on multiple conflicting criteria and there is a need for simplicity and computational efficiency. Moreover, TOPSIS is highly versatile when it comes to data types and scenarios. It works best with numeric data and is suited to handling criteria with different metrics and scales, where it handles variability in the data quite effectively. Since TOPSIS focuses on identifying the best alternative based on the

relative closeness to an ideal solution, it makes it suitable and "intuitive" for HR decisions where scoring is relative to an "ideal employee".

While preferred for its simplicity and versatility, TOPSIS can be outperformed by other methods in some scenarios. For example, PROMETHEE is a better choice in any situation where nuanced or non-linear human preferences, non-compensatory trade-offs, or complex outlier handling are needed because it handles them with flexible preference functions and allows for visual interpretability. In some cases, TOPSIS and PROMETHEE can both be suitable and produce similar results, although the output will be sensitive to the criteria used [19]. PROMETHEE is deemed more appropriate for partial ranking and decision-making in situations where, for example, environmental issues or sustainability considerations require more tailored judgments [23]. However, it can become complicated in terms of requiring expert input and adjusting the preference threshold, whereas TOPSIS stands out for its simplicity and uses distance-based measures to rank alternatives, making it more suitable when a clear numerical assessment is possible. Furthermore, ELECTRE is more complex than TOPSIS and is particularly suitable for handling ambiguous, non-compensatory criteria. However, it is used for exclusion-based ranking rather than optimality-based ranking like TOPSIS. VIKOR is similar to TOPSIS in its simplicity but focuses more on maximizing group utility and minimizing regret. However, VIKOR is more complex than TOPSIS and will not be a first choice in scenarios where straightforward ranking is needed. Another commonly applied method, SMART, is a very straightforward, simple, and intuitive method where criteria are weighted, and alternatives are scored based on a weighted sum of criteria values. However, the downside is that SMART assumes linear trade-offs between criteria and does not account for the distances between alternatives and ideal points, as TOPSIS does. In addition, AHP is one of the most frequently applied methods, which allows pairwise comparisons to determine the relative importance of each criterion and provides a structured framework for decision-making. Still, it cannot deal with conflicting criteria. Considering the goal – to develop a framework for evaluating employee-related cybersecurity risk – where numerical input is expected, with different metrics and scales, along with the conflicting criteria, TOPSIS is the simplest method that is effective and versatile enough to handle such demands.

TOPSIS is one of the MCDM methods, introduced in 1981 [10] and has been widely applied since. It has been successfully applied to assess cybersecurity risks in multiple sectors [30, 31, 33]. The method has proved to be useful in complex, practical domains [3, 19, 23].

TOPSIS is primarily developed to identify the best alternative among a set of options based on their relative closeness to an ideal solution [10]. That is achieved by first determining the best and worst solutions in the data and then ranking the alternatives based on their relative closeness to these ideal solutions. But, in doing so, it also ranks all the alternatives, which broadens its possible application. It fully utilizes attribute information, offers a cardinal ranking of alternatives, and does not require the independence of attribute preferences [3]. The technique can handle multiple, often conflicting, criteria and provide actionable rankings. Additionally, it supports the integration of both qualitative and quantitative data, allowing for a comprehensive evaluation. The technique uses a simple and effective approach to data normalization, distance calculation, and ranking, which enhances the ease of implementation and encourages its wide use [3].

In the context of employee-related cybersecurity risk, an important TOPSIS characteristic is that it integrates both beneficial and non-beneficial criteria, thus allowing the evaluation to be based on desirable and non-desirable attributes simultaneously. For example, while knowledge is a beneficial criterion and desirable behavior, risky behavior is not a desirable behavior and represents a non-beneficial criterion.

In addition, some evaluations can be made using validated questionnaires and tests, but they can be measured on different scales and result in different score intervals. On the other hand, some evaluations, such as observed behavior, can be conveyed as qualitative information

and then coded. Moreover, the values can differ in measurement units, where the knowledge can be a test result measured in points, and training can be measured in hours. Normalization, which is the first step of this method, allows for comparison of such data.

These characteristics show the technique's flexibility and allow for application to various (complex) settings. It can be argued that this technique is particularly appropriate for assessing employee-related cybersecurity risks because it upholds a combination of possibly conflicting criteria, both quantitative and qualitative data, and computationally efficient calculations. The method application unfolds as follows.

To apply the TOPSIS method effectively, it is important to determine the weights that reflect the relative importance of each criterion in assessing employee-related cybersecurity risks. Saaty's criteria for MCDM [21] highlight the importance of structured frameworks for prioritizing criteria and assigning weights. One commonly used method for determining these weights is Saaty's pairwise comparison, which is used at the beginning of the Analytic Hierarchy Process (AHP). It involves comparing each criterion against others to establish their relative importance verbally and then translating them into numerical values using a scale of one to nine [22]. These comparisons are organized into a matrix, which is then normalized, and the eigenvector is calculated to determine the weights for each criterion. This process ensures that the criteria weights reflect their significance in evaluating employee-related cybersecurity risks while maintaining consistency in judgments.

While this consideration clearly shows that not all criteria are equally important in an employee profile, TOPSIS's classical approach to weighting alternatives stems from the variation in the data rather than utilizing the practical meaning of the criteria. However, borrowing from the Saaty criteria weighting can help to deal with the importance of criteria. At the same time, AHP does not support the non-beneficial criteria in the ranking, so it is not appropriate for the entire process. Nevertheless, there is no obstacle in combining the weights derived by pairwise comparison on the Saaty scale and TOPSIS, as has been shown by previous research, where this approach of using Saaty criteria weighting to determine criterion weights and TOPSIS to rank alternatives based on closeness to the ideal solution. It is referred to as the AHP-TOPSIS method or the AHP-TOPSIS method combination [23, 24].

2.1. Goal definition

The goal is to define and test the framework to assess employee-related cybersecurity risks within an organization using the TOPSIS method. By systematically evaluating individual employees based on multiple relevant criteria, the framework aims to identify best-behaving and high-risk individuals to enable the implementation of targeted interventions to mitigate these risks. This proactive approach helps strengthen the organization's overall security posture, ensuring that all employees contribute to a safer digital environment.

2.2. Criteria identification

Evaluating employee-related cybersecurity risks requires a comprehensive approach that considers multiple dimensions of knowledge and behavior. The assessment of employees as cybersecurity risk is proposed to be based on several key traits in different combinations, such as knowledge, attitudes, skills, and behavioral intentions [29].

Knowledge of cybersecurity threats and best practices is foundational, as it directly influences employees' ability to recognize and respond to potential risks [17]. It involves employee's understanding of fundamental security principles, protocols, and practices. This includes awareness of common cyber threats and knowledge of protective measures like strong passwords, multi-factor authentication, and encryption. Studies show that security knowledge positively impacts both security compliance and participation, with threat appraisal (severity and sus-

ceptibility) further strengthening these effects [6]. The role of knowledge is further underscored by the findings that employees familiar with their company's cybersecurity policies are better equipped to handle related tasks, suggesting that organizational environments fostering cybersecurity awareness positively impact employee behavior [28]. Yet, data breaches persist due to insider actions, highlighting the need for a more nuanced understanding of security knowledge breadth, depth, and finesse [26].

Compliance with cybersecurity policies is another critical factor that involves the adherence to established security policies, procedures, and regulatory requirements within an organization. It consists of following guidelines related to data protection, password management, access controls, and incident reporting [17]. Compliance ensures that all members of the organization are aligned with best practices and legal mandates, reducing vulnerabilities and preventing security breaches. For instance, cybersecurity awareness programs that enhance knowledge and attitudes toward compliance can lead to better adherence to information security policies and protective behaviors [27]. The assessment of employees as cybersecurity risk is proposed through the components of compliance and participation in cybersecurity behavior [6]. Bélanger et al. [4] suggested that organizations implement holistic employee compliance programs that include repeated exposure to security and privacy news to improve employees' information protective behaviors.

Attitudes toward cybersecurity encompass employees' perceptions, beliefs, and mindsets regarding the importance and impact of security measures [5, 17]. Positive attitudes, such as recognizing the value of security protocols and feeling responsible for protecting sensitive information, contribute to a more proactive and vigilant security culture. Employees' attitudes toward cybersecurity risks were found to have a significant impact on their engagement in risky online behaviors [9]. Cultivating a positive security mindset through education and communication is vital for fostering a culture of security awareness and accountability.

Training is the process of educating employees about cybersecurity best practices, potential threats, and appropriate responses to security incidents. Regular, comprehensive training sessions help reinforce good security habits, update employees on emerging threats, and ensure that security protocols are understood and followed. Effective training methods, such as text-based and game-based formats, have been shown to significantly influence employees' attitudes and behaviors toward cybersecurity [2]. Additionally, periodic training and awareness programs are recommended to counteract the inherent risks in cyberspace and ensure employees are prepared for potential cyber threats [18, 28]. The training is suggested to include characteristics of cyberspace risk and specific guidelines for employees to enhance their awareness and preparedness in dealing with potential cyber threats [18]. Nevertheless, research by Renaud and Goucher [20] suggests that employees, even those with the required knowledge, sometimes compromise the security of an organization's systems and information by behaving insecurely, emphasizing the need to understand how employees are expected to assist in keeping the organization's information secure.

Risky behaviors, such as neglecting password management or mishandling information, may be a result of insufficient knowledge and poor attitudes toward cybersecurity and increase the likelihood of security breaches. Examples include using weak or reused passwords, clicking on suspicious links, downloading unverified software, neglecting to update systems and software, and a lack of active cyber defense measures while working from home [14, 25]. Identifying and mitigating these behaviors is crucial, as they can create significant security gaps that cybercriminals may exploit [11]. It is suggested that by promoting awareness and encouraging safer practices, organizations can reduce the risk posed by such behaviors and strengthen their overall security defenses.

The relevant criteria for evaluating employee-related cybersecurity risks are encompassed by the umbrella terms of knowledge, compliance, risky behaviors, attitudes, and training (Table 1). These criteria capture the multifaceted nature of employee cybersecurity behavior outlined

in Ali et al.'s [1] systematic review of information security policy compliance. By considering these diverse criteria, the framework provides a comprehensive assessment of an employee's cybersecurity risk profile.

Objective	Criteria	Description	Common measures	References
Minimize risky behaviors	Risky behavior	actions that increase vulnerability to cyber threats	questionnaire, Behavioral-Cognitive Internet Security Questionnaire (BCISQ)	[1, 14, 20, 25]
Increase cybersecurity knowledge	Knowledge	understanding of fundamental cybersecurity principles and threats	questionnaire, Human Aspects of Information Security Questionnaire (HAIS-Q)	[1, 6, 17, 29]
Enhance compliance with policies	Compliance	adherence to established security policies and procedures	questionnaire, Human Aspects of Information Security Questionnaire (HAIS-Q)	[1, 4, 6, 17, 27, 29]
Improve attitudes toward security	Attitudes	perceptions and mindsets toward cybersecurity policies and measures	questionnaire, Security Attitude Inventory (SA-13), Human Aspects of Information Security Questionnaire (HAIS-Q)	[1, 5, 17, 29]
Promote sufficient training participation	Training	participation in cybersecurity education programs	attended or not; level of training; hours of training	[1, 2, 4, 6, 27, 28]

Table 1: *Criteria for employees' overall cybersecurity behavior.*

So, the approach to the pairwise comparison is based on the deduction from the theoretical framework (Table 2), and more detailed reasoning for the comparisons can be found in the Supplementary file. The table was constructed using the Saaty scale. Risky behaviors are identified as the most critical factor in cybersecurity risks because they can directly lead to incidents like data breaches and malware infections, regardless of an employee's knowledge level [4, 20]. Whereas risky behavior may be understood as a habitual version of non-compliance due to bad habits, or carelessness, compliance refers to behaving in line with the security rules. However, being compliant does not automatically mean that risky behaviors are entirely avoided, so they will not have equal weight, with Risky behavior being slightly more important. Compliance ensures adherence to security protocols [4], applying the gained Knowledge so they are interconnected and evaluated as equally important. Attitudes toward cybersecurity influence the overall security culture and employees' motivation to follow best practices. Still, without Knowledge, Compliance, and the absence of Risky Behaviors, they cannot lead to the desired behavior. At the same time, training, though essential, depends on the proper integration of knowledge, compliance, and attitudes to be effective [9]. Training per se is a requirement, but it is not sufficient without the other criteria and thus least relevant.

Criteria	Risky Behaviors	Knowledge	Compliance	Attitudes	Training
Risky Behaviors	1	2	2	3	5
Knowledge	1/2	1	1	2	4
Compliance	1/2	1	1	2	3
Attitudes	1/3	1/2	1/2	1	2
Training	1/5	1/3	1/3	1/2	1

Table 2: *Pairwise comparison.*

This resulted in the following priorities, that will further be used as weights: $w_{RB} = 0.38$, $w_K = 0.22$, $w_C = 0.21$, $w_A = 0.12$, and $w_T = 0.07$. The consistency ratio of these criteria is 0.0055, which indicates that the pairwise comparisons made using the Saaty scale are highly consistent, thus ensuring the reliability of the derived weights and minimizing the risk of random or biased judgments in the comparison process.

2.3. Simulated data

The data is simulated and involves generating synthetic employee data across five cybersecurity risk-related criteria: Risky Behavior, Knowledge, Compliance, Attitudes, and Training. Target means, standard deviations, and correlations are derived from real-world studies such as the Behavioral-Cognitive Internet Security Questionnaire (BCISQ) [25], the Human Aspects of Information Security Questionnaire (HAIS-Q) [15, 17], and the Security Attitude Inventory (SA-13) [5]. These data are used to generate distributions, which are then refined iteratively to match the statistical properties of the target dataset. The questions, metrics from previous surveys, data generation, and procedure are available in the Supplementary files.

Statistics	Knowledge	Compliance	Risky behaviors	Attitudes	Training
Minimum	65	66	3.984	31	0
Q1	76.75	79	6.332	40.75	0
Median	81.5	85	7.42	46	1.474
Mean	81.34	84.9	7.41	45.83	1.538
Q3	86	90.25	8.643	50	2.276
Maximum	97	103	11.105	60	6.959

Table 3: *Insight into the simulated data.*

The dataset's (Table 3) diversity in metrics, scales, ranges, and variation highlights the advantages of using TOPSIS. Or, the other way around, the method's ability to handle different variations, ranges, metrics, and scales, as well as both benefit and cost criteria, confirms it is particularly well-suited for the analysis of such data. While using simulated data in multi-criteria decision-making (MCDM) methods, such as TOPSIS, is not typical, it is not an uncommon approach to assess a method's applicability or to compare methods [32]. Simulated data enables a conceptual demonstration of the framework before it undergoes empirical testing. This approach allows for the evaluation of its applicability, potential (dis)advantages, and requirements, offering valuable insights before exposing respondents to extensive questionnaires.

2.4. Analysis and results

After the goal definition, criteria are determined, and data is generated, the next step is to construct a decision matrix. Each element in the matrix represents the performance score of

an alternative with respect to a criterion. Suppose there are m alternatives and n criteria; the decision matrix D can be represented as: $D = [x_{ij}]$ for $i = 1, \ldots, m$, and $j = 1, \ldots, n$, where x_{ij} is the score of the i-th alternative with respect to the j-th criterion. The next step is normalization. In TOPSIS, the normalization method typically uses vector normalization, which transforms the various criteria dimensions into non-dimensional criteria, allowing for comparisons across different scales. The normalized value r_{ij} is calculated as:

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}}, \tag{1}$$

which ensures that all criteria have equal importance in subsequent calculations.

The box plots of the normalized data indicate that the distribution of values across the criteria has been effectively transformed to a comparable scale (available in the Supplementary file, Figure 3). The variability within each criterion is evident from the length of the boxes and the range of the whiskers, highlighting the diversity in employee scores across the different cybersecurity-related attributes. Next, each criterion is assigned a weight w_i reflecting its relative importance. The weighted normalized value v_{ij} is computed as:

$$v_{ij} = w_j \cdot r_{ij}, \tag{2}$$

where $\sum_{j=1}^{n} w_j = 1$. The results of the implementation of weights can be observed in Figure 1.

Figure 1: *Box plots of the weighted normalized values.*

This is followed by the calculation of the positive ideal solution (A^*) and the negative ideal solution (A^-). A^* and A^- are determined based on the weighted normalized decision matrix. For beneficial criteria (higher values are better), and are defined as:

$$A^* = \{v_1^*, v_2^*, \ldots, v_n^*\} = \left\{\max_i v_{ij}\right\} \tag{3}$$

$$A^- = \{v_1^-, v_2^-, \ldots, v_n^-\} = \left\{\min_i v_{ij}\right\} \tag{4}$$

For non-beneficial criteria (lower values are better), the values are reversed:

$$A^* = \{v_1^*, v_2^*, \ldots, v_n^*\} = \left\{\min_i v_{ij}\right\} \tag{5}$$

$$A^- = \{v_1^-, v_2^-, \ldots, v_n^-\} = \left\{\max_i v_{ij}\right\} \tag{6}$$

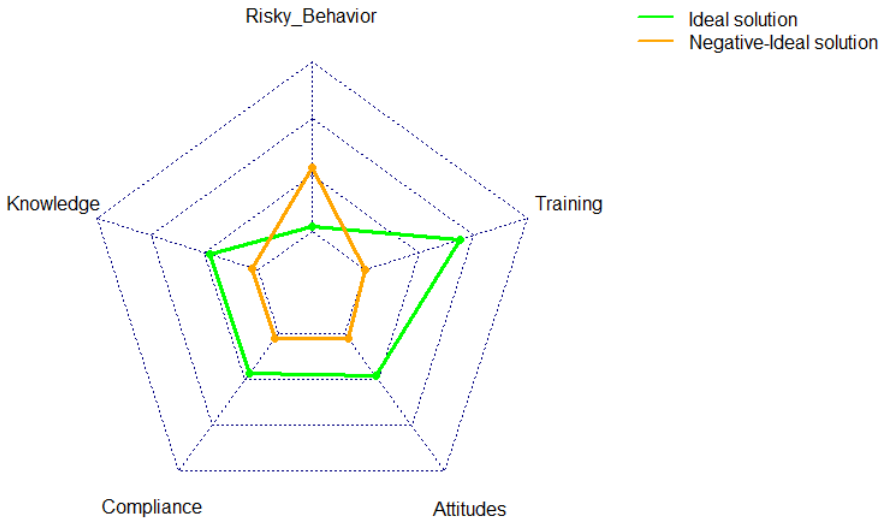

Figure 2: *Ideal vs negative ideal solution.*

The ideal and negative ideal solutions in TOPSIS are determined by evaluating the criteria based on their benefit or cost nature (Figure 2). The difference between the ideal and negative ideal solutions depends on the data's distribution and the criteria values. If the criteria values are relatively close to each other after normalization and weighting, the ideal and negative ideal solutions might not show a large difference.

Risky behaviors are identified as the most critical factor, and they obtained the highest weight. As they directly undermine cybersecurity efforts, risky behaviors are considered non-beneficial criteria in the TOPSIS framework. This means that lower values of risky behaviors are more desirable, and thus, the goal is to minimize these behaviors to reduce overall cybersecurity risk. This ensures that the ideal solution represents the most favorable conditions, and the negative ideal solution represents the least favorable conditions for each criterion.

The separation measures, calculated in the next step, are the Euclidean distances of each alternative from the positive and negative ideal solution. The separation from A^* is S_i^* and from A^- is S_i^-, and are calculated as:

$$s_i^* = \sqrt{\sum_{j=1}^{n}(v_{ij} - v_j^*)^2} \tag{7}$$

$$s_i^- = \sqrt{\sum_{j=1}^{n}(v_{ij} - v_j^-)^2} \tag{8}$$

These separation distances are further used to compute the relative closeness of each employee to the ideal solution. The relative closeness of each alternative to the ideal solution C_i^* is computed as:

$$C_i^* = \frac{s_i^-}{s_i^* + s_i^-} \tag{9}$$

where $0 \leq C_i^* \leq 1$. The alternative with a C_i^* value closer to 1 is preferred, as it is nearer to the positive and farther from the negative ideal solution. The last step is to rank

employees based on their relative closeness scores, C^*. The alternative with the highest C_i^* value is considered the best choice, or in this case, the highest rank. Such ranking allows the identification of the best-performing and high-risk individuals and recommends interventions.

Empl.	**Risky Behavior**	**Knowledge**	**Compliance**	**Attitudes**	**Training**	**C***	**Rank**
Emp_96	0.034	0.035	0.044	0.035	0.063	0.678	1
Emp_56	0.056	0.045	0.040	0.036	0.087	0.668	2
Emp_16	0.054	0.036	0.039	0.036	0.082	0.653	3
Emp_41	0.027	0.021	0.024	0.024	0.076	0.650	4
Emp_51	0.047	0.037	0.042	0.046	0.054	0.604	5
...							
Emp_35	0.026	0.024	0.020	0.020	0.000	0.297	96
Emp_14	0.016	0.010	0.012	0.012	0.006	0.294	97
Emp_54	0.014	0.012	0.009	0.008	0.000	0.286	98
Emp_39	0.027	0.020	0.022	0.020	0.000	0.282	99
Emp_49	0.017	0.011	0.011	0.013	0.000	0.276	100

Table 4: *Bottom and top ranked employees.*

The rankings derived from the TOPSIS method reveal insights into employee cybersecurity risks (Table 4). The top-ranked employees exhibit high compliance, knowledge, attitudes, and training scores, coupled with low risky behavior scores, underscoring their adherence to security protocols and proactive security measures. Conversely, the bottom-ranked employees demonstrate significant gaps in these areas, highlighting the need for targeted awareness programs, training, and reinforcement to mitigate their potential risks. These findings emphasize the effectiveness of the TOPSIS-based framework in pinpointing specific areas for improvement and guiding strategic interventions to enhance the organization's cybersecurity resilience.

2.5. Evaluation

Several approaches were applied to evaluate the proposed framework. Through the examination of the separation distances from ideal and negative-ideal solutions, analysis of relative closeness scores and criteria, and examining the sensitivity of the framework to changes in criteria weights, the aim is to demonstrate the framework's ability to differentiate between employees and validate its robustness.

The variations in the distances from both the ideal and negative ideal solutions across employees indicate that the method captures differences in their performance (Figure 6 in the Supplementary file). If the lines were flat or showed little variability, it would suggest the method is not distinguishing well between the employees. In addition, the plot shows that some employees are closer to the ideal solution while others are closer to the negative ideal solution. This range of performance reflects the method's ability to differentiate between high and low performers. While the green and orange lines come very close together for some employees, which indicates the method is struggling to differentiate effectively in these cases. However, the plot shows sufficient separation overall, so it can be concluded that the framework is differentiating employees fairly well.

The relationship between the results, that is, relative closeness scores, to initial employees' values per each criterion (Figures 8-10 in the Supplementary file) reveals that values for any criterion observed alone cannot lead to the prediction of the final scores. That can be observed

in similar spreads of C* scores, where no criterion has a very strong correlation (either positive or negative) compared to the others. That additionally emphasizes the holistic and intertwined evaluation based on the beneficial and non-beneficial criteria applied to the data with high variability.

However, criteria still have a meaningful impact on C*, meaning that the overall framework is sensitive enough to differentiate between employees based on all the criteria. The points in the scatter plot are sufficiently spread out, which indicates that the method successfully differentiates between employees.

Sensitivity analysis in TOPSIS typically involves examining how changes in input data, such as criteria weights, affect the final assessment outcomes. Additional analysis of changes in the weights was conducted to examine the effect of varying each criterion's weight across a range of values (from 0.01 to 0.45, increasing by 0.01) while proportionally adjusting the other criteria weights. This allows for the assessment of the sensitivity of final rankings to changes in criteria weights, which are essential parts of the framework.

The systematically varied criteria weights were used to calculate the employee rankings, and then they were compared with the original rankings using Spearman's rank correlation coefficient (the complete analysis is available in the Supplementary file). A threshold of 0.7 for the correlation coefficient was selected based on Chaddock's scale, denoting the boundary between moderate and strong correlations, and further used to identify criteria weight sets that produced closely aligned rankings. For these selected weight sets, the minimum and maximum values of each criterion were determined, representing the range of weights that resulted in similar rankings. These wide ranges of criteria weights (Table 5) demonstrate the framework's stability. Since there is a low sensitivity to variations in criteria weights within this range, this indicates that the model produces relatively consistent outcomes despite moderate changes in the weighting scheme.

Criteria	**min**	**max**
Risky Behavior	0.22	0.4884
Knowledge	0.01	0.40
Compliance	0.01	0.38
Attitudes	0.01	0.31
Training	0.01	0.26

Table 5: *Range of weights for different criteria.*

Further specific examples of changes in criteria weights were demonstrated in Supplementary files. They show that whereas the framework has a low sensitivity to changes in the criteria weights within the ranges, its ability to discern ideal from negatively ideal solutions effectively diminishes for uniformly distributed criteria. In addition, while there is no meaningful reason to treat Risky Behavior as a beneficial factor (as such an approach would substantially deviate from the proposed framework if it were attempted), it would result in significantly different rankings.

The comparison of the TOPSIS results to the PROMETHEE-derived results (available in the Supplementary file) shows a strong agreement in identifying the lowest-performing employees, demonstrating that the framework is highly reliable in assessing poor performance, which is particularly important in the context of cybersecurity risk evaluation. A Spearman's correlation coefficient of 0.6768 between PROMETHEE and TOPSIS's rankings suggests a moderate to strong positive relationship between the results of the two methods. It indicates that the framework is fairly robust, with both methods agreeing on a substantial portion of the rankings.

3. Discussion

The results indicate that the TOPSIS-based framework for evaluating employee cybersecurity risk (TFEECR) effectively distinguishes between high-risk and low-risk employees by evaluating multiple criteria: knowledge, compliance, risky behaviors, attitudes, and training. This approach addresses the limitations of traditional single-criterion models, which often fail to capture the complexity and variability of human behavior in cybersecurity contexts.

In line with previous studies, the utility of multi-criteria decision-making (MCDM) methods in cybersecurity is reaffirmed [8, 13, 16]. For instance, Khoroshko et al. [13] highlighted the importance of incorporating multiple factors in security evaluations to provide more comprehensive and accurate assessments. Our study extends this line of research by focusing specifically on employee-related risks, emphasizing the critical role that human factors play in organizational cybersecurity.

A relevant finding is the identifiable impact of risky behaviors on an employee's cybersecurity risk profile. This aligns with the literature emphasizing the importance of mitigating human errors and non-compliant behaviors [4, 11, 14]. The strong influence of risky behaviors suggests that targeted interventions aimed at reducing such behaviors could substantially enhance organizational security.

Whereas TOPSIS itself is not a new methodology, its integration into a structured framework for the evaluation of employee-related cybersecurity risk provides originality. In addition, the study also sheds light on the practical application of TOPSIS in evaluating cybersecurity risks, demonstrating its ability to handle different criteria and provide clear, actionable rankings. This aligns with prior research that utilized TOPSIS in other security-related assessments [30, 31].

4. Conclusion

The TOPSIS-based framework for evaluating employee cybersecurity risk (TFEECR) presents a flexible, robust, and comprehensive method for assessing employee-related cybersecurity risks. It is adaptive and scalable in terms that it can be further refined to satisfy the specific needs of a research goal or organization performance with the adjustable number of examined employees. By integrating multiple criteria, such as knowledge, compliance, risky behaviors, attitudes, and training, the framework offers a holistic evaluation that addresses the complexity and variability of human factors in cybersecurity. The proposed framework bridges the gap between risk assessment and risk management, allowing an analyst to ensure a structured and transparent process of selecting risk management alternatives.

This study contributes to the growing body of research advocating for multi-criteria decision-making methods in cybersecurity evaluations. The conceptual application of TOPSIS demonstrated in this study underscores its utility in providing a more objective assessment and actionable insights, enabling organizations to identify high-risk individuals and implement targeted risk mitigation strategies.

Given the inevitable limitations of using simulated data, future research should focus on empirical validation of the TFEECR framework using real-world data to establish its effectiveness and generalizability further. Additionally, exploring the integration of other MCDM methods and enhancing the framework to include dynamic and adaptive criteria based on evolving cybersecurity threats could provide even more robust and comprehensive risk assessments.

Supplementary materials

Supplementary materials are available at:
https://doi.org/10.17605/OSF.IO/TFMXB

References

[1] Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M. and Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. Applied Sciences, 11(8), 3383. doi: 10.3390/app11083383

[2] Alkhazi, B., Alshaikh, M., Alkhezi, S. and Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. IEEE Access, 10, 132132–132143. doi: 10.1109/ACCESS.2022.3230286

[3] Behzadian, M., Otaghsara, S. K., Yazdani, M. and Ignatius, J. (2012). A state-of the-art survey of TOPSIS applications. Expert Systems with applications, 39(17), 13051–13069. doi: 10.1016/j.eswa.2012.05.056

[4] Bélanger, F., Maier, J. and Maier, M. (2022). A longitudinal study on improving employee information protective knowledge and behaviors. Computers and Security, 116, 102641. doi: 10.1016/j.cose.2022.102641

[5] Faklaris, C., Dabbish, L. and Hong, J. I. (2022). Do They Accept or Resist Cybersecurity Measures? Development and Validation of the 13-Item Security Attitude Inventory (SA-13). ArXiv Cs, (April 2022), 248006293. doi: 10.48550/ARXIV.2204.03114

[6] Gerdenitsch, C., Wurhofer, D. and Tscheligi, M. (2023). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. Cyberpsychology, 17(4), 7. doi: 10.5817/CP2023-4-7

[7] Goode, J., Levy, Y., Hovav, A. and Smith, J. (2018). Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. The Online Journal of Applied Knowledge Management, 6(1), 67–80. doi: 10.36965/OJAKM.2018.6(1)67-80

[8] Görkan Evre, Ö. and CiYlan, B. (2023). Measurement of the Cybersecurity Strategy Effectiveness with a Scorecard Based On Risk Analysis. Gazi University Journal of Science Part C: Design and Technology, 11(4), 1116–1130. doi: 10.29109/gujsc.1345984

[9] Hadlington, L. (2018). Employees Attitude Towards Cyber Security And Risky Online Behaviours: An Empirical Assessment In The United Kingdom. International Journal of Cyber Criminology, 12(1), 269-281. doi: 10.5281/ZENODO.1467909

[10] Hwang, C.-L., Yoon, K., Hwang, C.-L. and Yoon, K. (1981). Methods for multiple attribute decision making. In Hwang C.-L. and Yoon, K. (Eds.) Multiple attribute decision making: methods and applications a state-of-the-art survey (58–191). Springer Nature.

[11] Ifinedo, P. (2023). Effects of Security Knowledge, Self-Control, and Countermeasures on Cybersecurity Behaviors. Journal of Computer Information Systems, 63(2), 380–396. doi: 10.1080/08874417.2022.2065553

[12] Kannelønning, K. and Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. Information and Computer Security, 31(4), 463–477. doi: 10.1108/ICS-08-2022-0139

[13] Khoroshko, V., Brailovskyi, M. and Kapustian, M. (2023). Multi-criteria assesment of the correctness of decision-making in information security tasks. Computer systems and information technologies, 4, 81–86. doi: 10.31891/csit-2023-4-11

[14] Klein, G. and Zwilling, M. (2024). The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home. Journal of Computer Information Systems, 64(3), 408–422. doi: 10.1080/08874417.2023.2221200

[15] McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M. and Pattinson, M. (2016). Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q) In: *ACIS 2016 Proceedings*, 56. url: aisel.aisnet.org/acis2016/56 [Accessed 21/11/2024]

[16] Nobanee, H., Alodat, A., Bajodah, R., Al-Ali, M. and Al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. Journal of Financial Crime, 30(6), 1736–1754. doi: 10.1108/JFC-11-2022-0287

[17] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies.

Computers and Security, 66, 40–51. doi: 10.1016/j.cose.2017.01.004

[18] Pieczywok, A. (2022). Training employees on risks in the area of cybersecurity. Cybersecurity and Law, 7(1), 261–271. doi: 10.35467/cal/151832

[19] Podrug, D. and Kovač, D. (2023). Improving portfolio liquidity: MCDM approach to share selection on the Zagreb Stock Exchange. Croatian Operational Research Review, 14(1), 29–39. doi: 10.17535/crorr.2023.0003

[20] Renaud, K. and Goucher, W. (2014). The Curious Incidence of Security Breaches by Knowledgeable Employees and the Pivotal Role of Security Culture. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (361–372). url: springer.com/chapter/10.1007/978-3-319-07620-1$_3$2 [Accessed 23/11/2024]

[21] Saaty, T. L. and Ergu, D. (2015). When is a decision-making method trustworthy? Criteria for evaluating multi-criteria decision-making methods. International Journal of Information Technology and Decision Making, 14(6), 1171–1187. doi: 10.1142/S021962201550025X

[22] Saaty, T. L. and Vargas, L. G. (2012). The seven pillars of the analytic hierarchy process. In Saaty, T. L. and Vargas, L. G. (Eds.) Models, methods, concepts and applications of the analytic hierarchy process (23–40). Springer Nature. url: springer.com/book/10.1007/978-1-4614-3597-6 [Accessed 23/11/2024]

[23] Shaktawat, A. and Vadhera, S. (2021). Ranking of hydropower projects based on sustainability criteria in India using multicriteria decision making methods. Croatian Operational Research Review, 12(1), 75–90. doi: 10.17535/crorr.2021.0007

[24] Sharma, D., Sridhar, S. and Claudio, D. (2020). Comparison of AHP-TOPSIS and AHP-AHP methods in multi-criteria decision-making problems. International Journal of Industrial and Systems Engineering, 34(2), 203-223. doi: 10.1504/IJISE.2020.105291

[25] Solic, K., Velki, T. and Galba, T. (2015). Empirical study on ICT system's users' risky behavior and security awareness, In: *38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, (1356–1359). doi: 10.1109/MIPRO.2015.7160485

[26] Strang, K. D. (2024). Cybercrime Risk Found in Employee Behavior Big Data Using Semi-Supervised Machine Learning with Personality Theories. Big Data and Cognitive Computing, 8(4), 37. doi: 10.3390/bdcc8040037

[27] Tran, D. V., Nguyen, P. V., Le, L. P. and Nguyen, S. T. N. (2024). From awareness to behaviour: Understanding cybersecurity compliance in Vietnam. International Journal of Organizational Analysis, Ahead of print, doi: 10.1108/IJOA-12-2023-4147

[28] Tripathy, S., Rao, C. L., Kumar, V., Adity, P. H., Kumar, D. and Jindal, M. (2023). Investigating How Employees' Cybersecurity Behaviour is Affected by Their Knowledge of Cybersecurity Policy. In: *2023 IEEE International Conference on ICT in Business Industry and Government (ICTBIG)* (1–6). url: ieeexplore.ieee.org/document/10456050 [Accessed 21/11/2024]

[29] Van Steen, T. (2023). Measuring Behavioural Cybersecurity: An Overview of Options. In: Schmorrow, D.D. and Fidopiastis, C.M. (Eds.) Augmented Cognition, Lecture Notes in Computer Science (460–471). Springer Nature doi: 10.1007/978-3-031-35017-7_29

[30] Wang, T. J. (2019). The Information System Security Assessment Model Based on TOPSIS Method and Linguistic Variable. In: *2019 IEEE 5th International Conference on Computer and Communications (ICCC)* (1617–1620). doi: 10.1109/ICCC47050.2019.9064245

[31] Wu, X., Shen, Y., Zhang, G. and Zhi, H. (2016). Information security risk assessment based on D-S evidence theory and improved TOPSIS. In: *2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)* (153–156) doi: 10.1109/ICSESS.2016.7883037

[32] Zanakis, S. H., Solomon, A., Wishart, N. and Dublish, S. (1998). Multi-attribute decision making: A simulation comparison of select methods. European Journal of Operational Research, 107(3), 507–529. doi: 10.1016/S0377-2217(97)00147-1

[33] Zhang, Z., Liu, Z., Yang, L., Zhe, T. and Wu, J. (2023). Security Risk Assessment of Image Classification Model Based on ANP-TOPSIS. In: *2023 International Conference on Networking and Network Applications (NaNA)* (300–306). doi: 10.1109/NaNA60121.2023.00057