

# Information security investment prioritization using best-worst method for small and medium enterprises

Alva Hendi Muhammad<sup>1</sup>, Joko Dwi Santoso<sup>2</sup>, Ananda Fikri Ijlal Akbar<sup>2</sup>

<sup>1</sup>Department of Informatics, Post Graduate Program, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia

<sup>2</sup>Department of Computer Engineering, Faculty of Computer Science, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia

## Article Info

### Article history:

Received Sep 21, 2022

Revised Feb 15, 2023

Accepted Feb 20, 2023

### Keywords:

Best-worst method

Cybersecurity operation

Information security

MCDM

Security investment

## ABSTRACT

In recent years, cyber security has become an increasingly important aspect of the decision-making process of corporations. It is essential to make investments in cybersecurity at this point to guard against the frequent disruption of business operations posed by cyberattacks. In the context of small and medium-sized organizations, this study recommends using a multi-criteria decision-making technique to evaluate information security aspects. The information security index is derived as the foundation for every one of these features. The best-worst method is carried out to establish the best and worst possible security investments. In order to validate these findings, a survey was distributed to a variety of professionals and business decision-makers. The criteria for selection are laid forth in the form of categories labeled technology and organization, respectively. The findings are presented in a rating system with three tiers, with the highest level representing the absolute best of the results. In the final section of the study, we will examine potential future possibilities for research and policy.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Alva Hendi Muhammad

Department of Informatics, Post Graduate Program, Universitas Amikom Yogyakarta

Jl. Ring Road Utara, Ngringin, Condongcatur, Depok, Sleman, D. I. Yogyakarta, 55281, Indonesia

Email: [alva@amikom.ac.id](mailto:alva@amikom.ac.id)

## 1. INTRODUCTION

Information security investment refers to the action or process of investing funds and resources in all activities, including controls, programs, and technology, with the goal of minimizing risks and improving the company's safety against cybercrime activity. With the increased use of information and technology, an organization is expected to be constantly ready to identify, respond, and recover from security threats at any moment. This condition has led to a greater demand for cybersecurity efforts by implementing strategy, policy, technology, controls, and procedures at various levels of the organization for a strong security posture. The decision to take investment has long been a question in top level-management and is often handed over to a security manager (CSO). Since security investment is often ridden with problems, many CSOs are pressured to prioritize funds while also expected to achieve more significant return on investment (ROI) on existing programs [1], [2]. As a matter of fact, the CSO is required to maximize the security investments and also measure the budget cost-effectiveness. These conditions may be due to some organizations having a limited budget for information security costs. Therefore, security managers need a mechanism to identify gaps in security controls that can prioritize with limited funds and resources but could achieve the most significant security impact.

The studies that associated with information security investment have been a challenging topic for years, and there are two main challenges faced by many researchers [3]. The first problem is associated with the characteristic of information security as a multi-discipline area. Every organization or industry has different

resources, risks, technologies, and even organizational needs and structures. For example, the business and financial system tend to minimize operational risks by strengthening protection, monitoring, and mitigation response [4]. Thus, the most needed investments are in the most reliable hardware, software, data encryption systems, firewalls, cyber surveillance, risk detection systems, and information technology (IT) training [5]. This requirement differs for small and medium enterprises (SMEs) with small assets. In this case, they commonly take cloud storage backup and web server logging as the primary cybersecurity investment [6]. The government and military institutions also have different priorities. Since their priority is mostly on compliance with internal regulations and policies, the suitable investment will be for education and training to improve user compliance with institutional policies and necessary security checks [7].

The second challenge faced by researchers is how to tackle the dynamic growth of information technology that is constantly evolving. Technology changes every time at a rapid pace. Cloud computing, machine learning, the internet of things, and other technological advances hold the promise of making efficient and effective systems. Every organization will adopt those new advanced technologies and find ways to improve their productivity. As a result, the advanced adoption will pose new challenges and risks that may be more difficult to handle [8]. In their recent report, Verizon claims that even the attacker also invests in software or content development, using actors and facilities for targeting and distributing tools to compromise the targets [9]. Even though most incidents are related to basic web application attack and denial of services, the number of complex system intrusion attack that leverage malware and hacking are increasing. The report suggests that the trend of attacks and incidents will continue to rise, although organizations have significantly increased their security investment [9].

Our review of the literature concluded that the most critical factors that influence information security investment have been recognized. However, the priority and importance of each factor vary significantly between organizations. These factors are generally affected by technological adoption (products and devices) and organizational context (risk, culture, and structure) [10]. Furthermore, the research in information security investment suggested two approaches to address this situation: implementing a decision-making strategy or using an economic model [3]. Previous studies largely dealt with specific objectives, goals, and missions that define the organizations' purposes or problems. For example, the decision-making in [11] simulates a cyber risk profile and provides several scenarios to highlight the effect of different decision-making strategies; [12] focuses on solving the investment priority of information security resources for the industrial control system operation using the analytic hierarchy process (AHP); and studies Weishäupl *et al.* [13] using grounded-theory models to reveals empirical results from several case studies that help to understand external and internal factors in selecting best investment attribute. In economic models, most of the study have generally been restricted to the analysis of a model in a specific environment. For instance, several game theories models were proposed to estimate optimal amount of investment by considering some constrains, like considering the threat and vulnerability [14], [15], attack probability [16], or multiple propagations of security breaches in the network [17]. The economic model in [18], [19] utilizes return on security investments (ROSI) for estimating future information security investments. Mayadunne and Park [20] using the expected utility model to analyze information security investment decisions in small and medium enterprises (SMEs).

Previous studies have demonstrated significant results of decision-making and economic model to assist the decision-maker in the organization by considering all available options. Moreover, the main issue confronted in this paper relates to investment priority for public organizations and government agencies with limited security budgets. This paper proposes several factors related to technology adoption and organizational system. These factors were derived from up-to-date conceptual models and frameworks from the literature that represents the attributes in reality. The information was gathered from potential experts and stakeholders through an online survey study. A best-worst method (BWM) as a decision-making model is applied in this research. The results are compared to AHP and decision making trial and evaluation laboratory (DEMATEL) to enhance our understanding of the organization's information security.

The rest of the article is organized as shown in: Section 2 describes the context of the study, data collection, and explains how and why the proposed method can handle the challenge of information security investments. Section 3 describes the results derived from the models and discusses the findings, including the impact from theoretical concepts to practical. Finally, section 4 summarizes this paper, including conclusions and recommendations for future work.

## 2. RESEARCH METHOD

### 2.1. Context of the study

We highlighted the question of what is the suitable security priority for a company with a certain limited budget as analogous to a complex decision-making problem. Scholars have long debated the best cybersecurity strategies for firms. Fedele and Roner [21], there are four streams that have been proposed in the

literature. The early stream suggested that a company should invest in a single cybersecurity framework and neglect all forms of interdependence that can arise among firms. Following this basis, the second stream suggested interdependent security among multi-firm initiatives. The third stream focuses on the strategy where a firm should operate non-interconnected computer systems from competitors. The last stream suggested investing in cybersecurity of firms that use a common computer network that is similar to the competitors. Nevertheless, the total budget for cybersecurity programs is often influenced by at least two factors. In general, the size of the company will affect the investment capability, even though many still believe a high cybersecurity budget is still insufficient to prevent a breach [22]. Moreover, the second factor that affects the budget is the type of risk and the likelihood of incidents. A firm that provides open public services requires high connectivity, which increases the likelihood of risks [5].

In the context of this study, we focused on addressing the challenges of prioritizing information security programs by identifying the circumstances in Indonesia's organization. The increasing number of data breach attacks on Indonesian public firms and agencies has also driven this research. The massive attack began in 2019 when the two biggest marketplaces in Indonesia, Bukalapak, and Tokopedia, were hacked and affected the data of more than 104 million users and 70 million merchants [23]. This trend is still continuing in 2022 and affecting several Indonesian agencies and ministries. Regardless of the concerns over personal data protection in Indonesia, the reality is that these incidents occur in big corporations and government institutions is a distressing situation. In fact, around 99% of businesses in Indonesia are categorized as small and medium enterprises with limited financial services [24]. Even more worrisome is that SMEs are three times more likely to be targeted by cybercriminals than larger companies [25].

The Indonesian government has provided various ways to improve security awareness in organizations. One of the interesting efforts is a simple information security assessment tool named information security index (KAMI) [26] that was developed by National Cyber and Crypto Agency (<https://bssn.go.id>). Despite its simplicity, the tool can examine and evaluate the completeness and maturity of information security based on ISO/IEC 27001 standards. As shown in Figure 1, KAMI consists of five dimensions: governance, risk management, security framework, asset management, and security technology. Although the tool is not for evaluating the viability or efficacy of existing security forms, it provides a rapid overview of the preparedness and readiness of the information security rank for the company. Using the control objectives for information and related technology (COBIT) or capability maturity model integration (CMMI) maturity level (<https://www.isaca.org>) as a reference, the assessment results may be utilized to map and rate the company's information security.

Despite the fact that KAMI is based on current standards and best practices for businesses, it should still be adapted by each sector to meet their circumstances and requirements better. Since organizations will continue to face their own particular risks, threats, and vulnerabilities, the ways in which they implement KAMI practices to achieve positive outcomes will vary. KAMI should not be applied as a one-size-fits-all strategy for all enterprises that manage critical infrastructure. For this reason, the current research focused on exploring the information security attributes extracted from KAMI to assist SMEs in better managing their cybersecurity risks.



Figure 1. KAMI's five dimensions

## 2.2. Research design

The study involves complex decision-making from several attributes (alternatives) in KAMI. Thus, the multi-criteria decision making (MCDM) method is utilized to prioritize the most important activities in KAMI and help SMEs maximize the impact of every investment spent on cybersecurity operations. Overall, the design of the study has three phases:

### 2.2.1. Analysis and extract the core knowledge of KAMI

This phase involves a knowledge acquisition process by identifying objects, attributes, and values from a knowledge source. The primary knowledge developed in this study was constructed from KAMI's framework [26], where the secondary knowledge was obtained from related literature [1], [10], [13], [27], [28]. The latest version of KAMI (version 4.2) consists of seven parts, where the first part is used to decide the level or category of the electronic system used in the organization. The following five parts are the main dimensions that contain 131 checklist questions. The latest part is called a supplement and consists of 53 checklist questions. Since this step aims to understand the core knowledge of KAMI, we analyzed the knowledge code structure of questions to define the entities that represent the questions. To understand the process, Table 1 shows the example of questions from domain 2, Information Security Governance. We manually highlighted and extracted similar entities from the four presented questions as 'head of the team' or 'person in charge' for information security management.

Table 1. The example of KAMI's checklist questions (domain 2)

No.	Questions	Similar Entities
2.1	Is the head of your agency/company in principle and officially responsible for implementing the information security program (for example, listed in the ITSP), including enforcing related policies?	'head of ... agency ... responsible for ... information security'
2.15	Does the person in charge of information security management report the condition, performance/effectiveness and compliance of the information security program to the head of the agency/company regularly and officially?	'person in charge of information security management'
2.17	Does the head of the work unit in your agency/company implement a special program to comply with information security compliance goals and objectives, especially those covering information assets that are their responsibility?	'head of the work unit ... implement ... information security ...'
2.20	Has your agency/company implemented information security management targets and objectives for various relevant areas, evaluated their achievements regularly, and implemented corrective steps to achieve existing targets, including reporting on status to the head of the agency/company?	'head of the agency'

### 2.2.2. Build a list of attributes from previously gathered entities

In this step, candidate lists of attributes were collected with various names. Moreover, we eliminated similar names and classified similar mining into a group. Then, a general name will be used to label the attribute. To illustrate the process, we continue the example from Table 1. The similar entities from the highlighted questions are 'head of the agency' or 'person in charge of information security'. Since those entities have different names for the same purpose, we labelled the entities with the most recognized name in this category: Chief security officer. The proposed name is aligned with other models and references, such as in [10], [29]-[31]. Therefore, the term chief security officer was listed in the final list of attributes. By performing similar steps, a total of 18 attributes have been obtained as information security operations from the KAMI.

The final step includes the classification of the results based on their function. The approach to classify the attributes was adopted from Govender's taxonomy, which distinguishes two broad categories, that is social and technical factors [10]. After considering the general purpose of KAMI, the name of the criteria proposed for the main classification are technology and organization. The classification of attributes based on their criteria in this study is shown in Table 2.

### 2.2.3. Identify and apply a BWM decision-making technique

The final stage is determining the best strategy for selecting attributes based on context. Due to the fact that all of the criteria are qualitative and more difficult to quantify, we have refined the method that is appropriate for selection. Given this combination of relatively diverse criteria, we give a comparison of the 18 qualities' competitiveness at a high level using multiple-criteria evaluation (MCDM). MCDM encompasses a broad family of quantitative approaches that employ several factors for decision-making. Rezaei's best-worst method (BWM) is one of the most recently established MCDM approaches [32]. BWM is a multi-criteria decision-making approach in which the criteria weights are determined via pairwise comparisons. However, before examining the multiple alternatives and preferences, BWM provides the decision-maker with a list of the most important and least important variables to consider. All of the criteria are evaluated using pairwise comparisons, including both of these (best and worst) and the other criteria. To establish how much weight should be assigned to each condition, it is necessary to define and solve a maximin problem. The relative weights of the various alternatives are determined using the same method, and the outcomes depend on various factors. The optimal option is calculated by summing the points assigned to each alternative on a scale from 1 to 10 and then picking the option with the greatest total score. A consistency ratio has been developed for the BWM to determine whether the comparisons are reliable.

Table 2. The final attributes of information security operation

Main criteria	Sub-criteria	Code
Technology	Anti virus and anti malware	T1
	Data and system encryption	T2
	Network protection	T3
	Physical security	T4
	System backup and recovery	T5
	Asset and risk management system	T6
	User and password management system	T7
	System monitoring and log	T8
	Software management (update/patch)	T9
Organization	Vendor partnership	O1
	Chief security officer	O2
	Security operating procedure	O3
	Information security officer	O4
	Security insurance	O5
	Security audit	O6
	Risk mitigation plan	O7
	Awareness training	O8
	Skills and competency improvement	O9

BWM generally derives weights for a set of decision criteria by comparing pairwise the “best” (i.e., the most important and wanted) and “worst” (i.e., the least important and least desired) criteria with the other criteria in the set. This section compares the “best” and “worst” criteria with the other criteria. Several characteristics of BWM contribute to its higher resilience when compared to other MCDM approaches [33]-[35]. In contrast to AHP, the vector-based method allowed BWM to reduce the number of pairwise matrix comparisons. Depending on the conditions, this essential characteristic may make it easier and less time-consuming for decision-makers or specialists to evaluate the essential criteria [36]. In addition, it may be more viable for studies that require the participation of respondents with limited Internet access. Moreover, the conclusions BWM draws from its comparisons are highly reliable and consistent. Lastly, BWM alone or in conjunction with other MCDM methodologies can be used to determine weights.

This approach is used to evaluate the investment choice for information security, as BWM offers the previously mentioned benefits. After deciding on the list of attributes for selection, the following steps are used to apply the BWM:

- Step 1: Select the most significant and the least significant criteria. Respondents in this study are required to identify the most significant and the least significant attributes among the set of factors.
- Step 2: Conduct a pairwise comparison between the most significant and the other criteria. After selecting the most significant attribute, the respondents are asked to compare it with the rest of the criteria. A 1-to-9 scale is used to indicate the degree of importance between two factors. The value 1 indicates both criteria are equally important, while 9 indicates the most significant criteria than the other. This process resulting the most significant criteria-to-others (TB) vector, which is:

$$T_B = (t_{b1}, t_{b2}, \dots, t_{bn}), \tag{1}$$

where  $t_{bi}$  represents the preference of most significant criteria  $t$  over the criterion  $i$ .  $b$  indicates the most significant criteria selected by a respondent. In this study,  $i$  (1, 2, ...,  $n$ ) indicates the number of nine criteria of information security related to technology.

- Step 3: Conduct a pairwise comparison between the other criteria and the least significant. Similarly, the respondent is asked to rate the importance of other criteria in the set over the least significant criteria using a scale of 1-to-9. The result is a vector others-to-worst (TW) in the technology dimension:

$$T_W = (t_{1w}, t_{2w}, \dots, t_{nw}), \tag{2}$$

where  $t_{iw}$  represents the preference of other criteria  $i$  over the worst criteria  $w$ .  $w$  is the least significant criterion selected by a respondent.  $i$  (1, 2, ...,  $n$ ) indicates the number of nine criteria of information security related to technology.

- Step 4: Estimate the optimal weights. This step is finding the optimal weights of criteria by minimizing the absolute difference ( $|wb-t_{biw}|, |wi-tw_{iww}|$ ) for all  $i$ . Taking into consideration the non-negativity and sum condition for the weights in (3) using liner programming will result in the following:

$$\begin{aligned}
 & \min \xi^L \\
 & |w_b - t_{bi} w_i| \leq \xi^L, \text{ for all } i \\
 & |w_i - t_{iw} w_w| \leq \xi^L, \text{ for all } i \\
 & \sum_i w_i = 1 \\
 & w_i \geq 0, \text{ for all } i
 \end{aligned} \tag{3}$$

It is common practice when conducting surveys to enquire about respondents' thoughts on the significance of both organizations and technologies. To answer the question, the respondents should rank the considerations from most significant to least significant. The BWM technique will be explained as a decision-making process in the following section, followed by an application evaluating the importance of the aspects in reducing the cost of information security. After this, there will be a description of the data collection procedure.

### 2.3. Data collection

Multiple polls and surveys were performed to identify which cybersecurity investments should be made first. The level of significance was determined using a scale from 1 to 9. The report is organized into three sections: an introduction, a section on technology, and an organization section.

Purposive sampling was utilized to acquire the relevant information for the investigation. Participants were chosen based on their prior participation in information security emergency response teams, cybersecurity, and data protection. Because we have a network of Indonesian institutions with experts in numerous sectors, we were able to identify the respondents with the most pertinent experience. A crucial element in their selection was their extensive knowledge of data and network security. We anticipated that while assessing the provided criteria, industry professionals would take into account a wide range of SME-relevant contextual factors. In addition to being distributed in person, the survey was also emailed to our respondents.

In order to achieve data saturation, the great majority of published MCDM research uses a sample size of between 4 and 10 observations [37]. The process in MCDM is fully analytic and require no statistical inference. In analytical approaches, the precision of the observations and the data quality is given precedence over the quantity of observations or data points. As part of this study, fifty working professionals were contacted for a period of twenty-one days. As a result, we have received 41 responses, but only 31 of which are complete and valid. Thus, it represents approximately a 62% audience response rate. The information background of our respondents is presented in Figure 2. The pie chart in Figure 2(a) shows the levels of expertise in IT security. Meanwhile, the years of experience and preferences between the main criteria are shown in Figure 2(b) and Figure 2(c), respectively. According to the results, there is sufficient variety in the respondents' subject matter competence.

Since the research evaluates two groups of criteria related to technology and organization, the process above is performed twice. In our survey, the respondents are needed to finish the technology category first, followed by the organization. The next section presents the findings of the results, followed by the discussion.

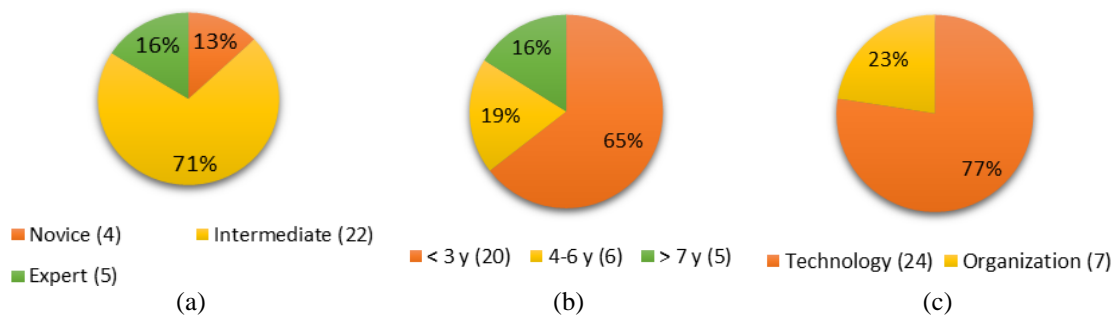


Figure 2. Background information of respondents; (a) level of expertise, (b) years of experience, and (c) preference between technology and organization

### 3. RESULTS AND DISCUSSION

The goal of our research is to prioritize the information security operation to be invested in by SMEs. The BWM analysis operationalized in this study identifies the most and the least essential information security operation derived from KAMI. Since the implementation of KAMI's information security program is still

debatable, this study delineates a holistic view of information security features when operated in SMEs where the investment budget is often limited. It is evident that the multi-dimension characteristics of recent cyber systems have increased the security challenges. However, this study has analyzed the priority using the multi-criteria decision method. The notion can be further justified by observing the global weights of the sub-criteria to understand the process.

In this research, the aggregation of judgment is expected from the individual respondent and not from a group or team. Therefore, the study applied geometric means to get the aggregation of individual priorities and not judgments as a team. The excel solver linear for the BWM model is used to calculate aggregated priorities. The outcomes of the results are displayed in Tables 3 and 4, respectively. As illustrates in Table 3 below, the best information security feature related to technology is network protection (T3), while anti virus and anti malware (T1) is the last. From the organization criteria (Table 4), the highest rank is skills and competency improvement (O9), while the security insurance (O5) program is the latest.

Table 3. The optimal weight of technology criteria

Attributes	Anti virus and anti malware (T1)	Data and system encryption (T2)	Network protection (T3)	Physical security (T4)	System backup and recovery (T5)	Asset and risk management system (T6)	User and password management system (T7)	System monitoring and log (T8)	Software management (T9)
Final Weight	0.0754	0.1086	0.1990	0.0805	0.1248	0.1015	0.1021	0.1063	0.1018
Ranks	9	3	1	8	2	7	5	4	6

Table 4. The optimal weight of organization criteria

Attributes	Vendor partnership (O1)	Chief security officer (O2)	Security operating procedure (O3)	Information security officer (O4)	Security insurance (O5)	Security audit (O6)	Risk mitigation plan (O7)	Awareness training (O8)	Skills and competency improvement (O9)
Final Weight	0.0866	0.1252	0.1029	0.1152	0.0669	0.0891	0.0823	0.0945	0.2372
Ranks	7	2	4	3	9	6	8	5	1

What is interesting about the results is that the BWM can easily determine the best and worst criteria. However, the final weight data in the tables above reveals that the outcomes for various attributes are quite similar. For instance, in Table 3 the weight for positions 3 (0.1086) through 7 (0.1015) are on the same levels. Similarly, the results of organizational criteria between ranks 6 (O6) to 8 (O7) also fall within comparable ranges, which is around 0.08. Even if just a few small difference numbers can be used to determine the rank, in practical this will result in a significant impact for SMEs. For the SMEs that have already invested in data and system encryption (T2), should they also invest in system monitoring and log (T8)?

This study introduces using class tier to present the results rather than ranking the outcome from the best to the worst criteria. For this purpose, it will be necessary to determine the number of clusters and identify the greatest common factor between the highest and lowest ultimate weight. In our technological case, the number of specified clusters is 3, while the highest weight is 0.1990 and the lowest is 0.0754. Thus, the closest highest value that might be divided by 3 is 0.21. By assigning this number, the resulting cluster will be 0-0.7, 0.8-0.14, and 0.15-0.21. However, the first cluster will be empty using the produced cluster since no weight belongs in the range. This condition suggests the next factor, which is 0.27. After plotting the final ranking according to their tier, the final results can be seen in Figure 3. Moreover, the final result for technological criteria is presented in Figure 3(a). By using a similar step, the result from organization criteria is shown in Figure 3(b).

The image above shows the final tier of information security features for SMEs based on BWM. Only one feature of both categories belongs to the first tier: network protection (T3) for the technology; Skills and competency improvement (O9) for the organization. The second tier shows almost a balance level for technology criteria. These findings have raised an important point about whether SMEs should use their funds to invest in multiple features within the same tier. Unfortunately, these problems are rather difficult to interpret by using current results. However, this is an important issue for future research. On the surface, BWM might work well to identify ranking among candidates. Still, under the hood, the position among some criteria might overlap, and there should be an effort to correlate or combine between criteria.

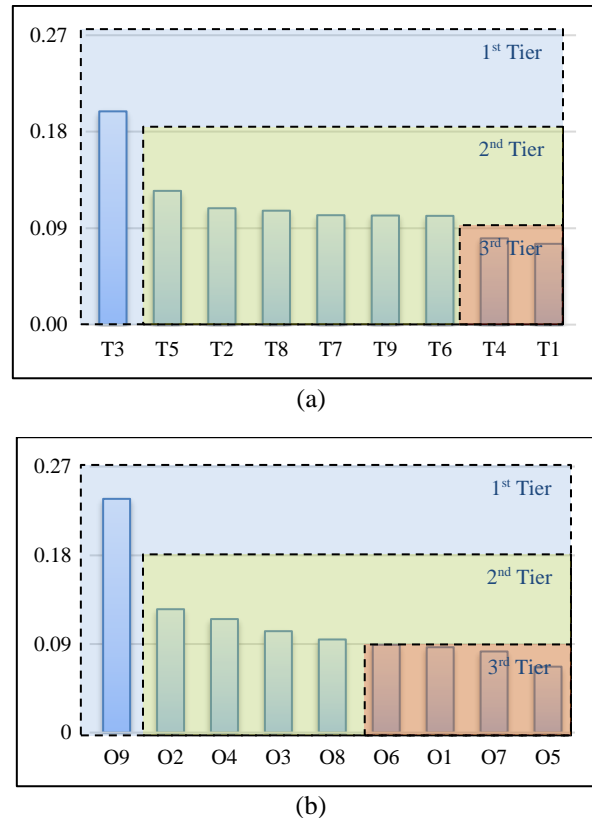


Figure 3. The final tier of information security features for SMEs; (a) technological and (b) organizational

#### 4. CONCLUSION

The significance of decision-making processes in cyber security has progressively increased over the past several years. The study has suggested that it is crucial to invest in a proper cybersecurity program to safeguard a firm from cyberattacks, which offer a threat of frequent interruptions to commercial operations. In the context of small and medium-sized organizations, this study advises the best operation to be invested in by using a decision-making method that considers several considerations when evaluating various information security features. The KAMI's information security index serves as the base and foundation for each of these qualities. The optimal and ideally risky security investments are determined by examining the best and worst features named BWM. In order to determine the dependability of these results, a survey was distributed to a variety of professionals and business decision-makers. The selection criteria are classified into technological and organization-specific categories. The findings are then presented using a three-tiered grading system, with the highest level representing the findings deemed to be the best overall.

#### ACKNOWLEDGEMENTS

This study was funded by Internal of Excellence Research Grant, Research Department of Universitas Amikom Yogyakarta, Indonesia, number: 001/KONTRAK-LPPM/AMIKOM/XII/2021, December 27<sup>th</sup>, 2021.




#### REFERENCES

- [1] D. Schatz and R. Bashroush, "Economic valuation for information security investment: a systematic literature review," *Information Systems Frontiers*, vol. 19, no. 5, pp. 1205–1228, Oct. 2017, doi: 10.1007/s10796-016-9648-8.
- [2] Y. Miaoui and N. Boudriga, "Enterprise security investment through time when facing different types of vulnerabilities," *Information Systems Frontiers*, vol. 21, no. 2, pp. 261–300, Apr. 2019, doi: 10.1007/s10796-017-9745-3.
- [3] D. Dor and Y. Elovici, "A model of the information security investment decision-making process," *Computers and Security*, vol. 63, pp. 1–13, Nov. 2016, doi: 10.1016/j.cose.2016.09.006.
- [4] L. J. Mester, "Cybersecurity and Financial Stability," 2019, [Online]. Available: <https://www.clevelandfed.org/newsroom-and-events/speeches/sp-20191121-cybersecurity-and-financial-stability>.
- [5] M. H. Uddin, M. H. Ali, and M. K. Hassan, "Cybersecurity Hazards and Financial System Vulnerability: A Synthesis of Literature," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3689162.






- [6] S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," *Journal of Organizational Computing and Electronic Commerce*, vol. 28, no. 3, pp. 269–282, Jul. 2018, doi: 10.1080/10919392.2018.1484598.
- [7] C. Solar, "Cybersecurity and cyber defence in the emerging democracies," *Journal of Cyber Policy*, vol. 5, no. 3, pp. 392–412, Sep. 2020, doi: 10.1080/23738871.2020.1820546.
- [8] M. Calvo and M. Beltrán, "A Model For risk-Based adaptive security controls," *Computers and Security*, vol. 115, p. 102612, Apr. 2022, doi: 10.1016/j.cose.2022.102612.
- [9] Verizon, "Data Breach Investigation Report," 2014. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>.
- [10] S. G. Govender, E. Kritzing, and M. Look, "A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture," *Personal and Ubiquitous Computing*, vol. 25, no. 5, pp. 927–940, Oct. 2021, doi: 10.1007/s00779-021-01549-w.
- [11] S. Armenia, M. Angelini, F. Nonino, G. Palombi, and M. F. Schlitzer, "A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs," *Decision Support Systems*, vol. 147, p. 113580, Aug. 2021, doi: 10.1016/j.dss.2021.113580.
- [12] J. Shin, I. You, and J. T. Seo, "Investment Priority Analysis of ICS Information Security Resources in Smart Mobile IoT Network Environment Using the Analytic Hierarchy Process," *Mobile Information Systems*, vol. 2020, pp. 1–11, Nov. 2020, doi: 10.1155/2020/8878088.
- [13] E. Weishäupl, E. Yasasin, and G. Schryen, "Information security investments: An exploratory multiple case study on decision-making, evaluation and learning," *Computers and Security*, vol. 77, pp. 807–823, Aug. 2018, doi: 10.1016/j.cose.2018.02.001.
- [14] R. Safi, G. J. Browne, and A. J. Naini, "Mis-spending on information security measures: Theory and experimental evidence," *International Journal of Information Management*, vol. 57, p. 102291, Apr. 2021, doi: 10.1016/j.ijinfomgt.2020.102291.
- [15] Y. Wu, G. Feng, N. Wang, and H. Liang, "Game of information security investment: Impact of attack types and network vulnerability," *Expert Systems with Applications*, vol. 42, no. 15–16, pp. 6132–6146, Sep. 2015, doi: 10.1016/j.eswa.2015.03.033.
- [16] X. Li, "Decision making of optimal investment in information security for complementary enterprises based on game theory," *Technology Analysis and Strategic Management*, vol. 33, no. 7, pp. 755–769, Jul. 2021, doi: 10.1080/09537325.2020.1841158.
- [17] X. Qian, X. Liu, J. Pei, P. M. Pardalos, and L. Liu, "A game-theoretic analysis of information security investment for multiple firms in a network," *Journal of the Operational Research Society*, vol. 68, no. 10, pp. 1290–1305, Oct. 2017, doi: 10.1057/s41274-016-0134-y.
- [18] T. Yaqoob, A. Arshad, H. Abbas, M. F. Amjad, and N. Shafiqat, "Framework for Calculating Return on Security Investment (ROSI) for Security-Oriented Organizations," *Future Generation Computer Systems*, vol. 95, pp. 754–763, Jun. 2019, doi: 10.1016/j.future.2018.12.033.
- [19] H. S. B. Herath and T. C. Herath, "Post-audits for managing cyber security investments: Bayesian post-audit using Markov Chain Monte Carlo (MCMC) simulation," *Journal of Accounting and Public Policy*, vol. 37, no. 6, pp. 545–563, Nov. 2018, doi: 10.1016/j.jaccpubpol.2018.10.005.
- [20] S. Mayadunne and S. Park, "An economic model to evaluate information security investment of risk-taking small and medium enterprises," *International Journal of Production Economics*, vol. 182, pp. 519–530, Dec. 2016, doi: 10.1016/j.ijpe.2016.09.018.
- [21] A. Fedele and C. Roner, "Dangerous games: A literature review on cybersecurity investments," *Journal of Economic Surveys*, vol. 36, no. 1, pp. 157–187, Feb. 2022, doi: 10.1111/joes.12456.
- [22] T. Kissoon, "Optimum spending on cybersecurity measures," *Transforming Government: People, Process and Policy*, vol. 14, no. 3, pp. 417–431, May 2020, doi: 10.1108/TG-11-2019-0112.
- [23] Zico Law, "Data Leaks in Heavy Cyberattack Season: Increasing Concerns Over Personal Data Protection in Indonesia," 2022. [Online]. Available: [https://www.zicolaw.com/wp-content/uploads/2022/02/ZICO\\_1010\\_Data-Leaks-in-Heavy-Cyberattack-Season\\_-Feb-2022.pdf](https://www.zicolaw.com/wp-content/uploads/2022/02/ZICO_1010_Data-Leaks-in-Heavy-Cyberattack-Season_-Feb-2022.pdf).
- [24] ILO, "Financing Small Businesses in Indonesia: Challenges and Opportunities," 2019. [Online]. Available: [www.ilo.org/publns](http://www.ilo.org/publns).
- [25] B. Practices and E. Attacks, "Spear Phishing: Top Threats and Trends," *Barracuda*, 2019. <https://www.barracuda.com/reports/spear-phishing-report-7>.
- [26] Indeks Keamanan Informasi (KAMI) Versi 4.2, "Indeks Keamanan Informasi (KAMI)," 2021. [Online]. Available: <https://bssn.go.id/indeks-kami/>.
- [27] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egy.2021.08.126.
- [28] G. Wangen, C. Hallstensen, and E. Snekkenes, "A framework for estimating information security risk assessment method completeness," *International Journal of Information Security*, vol. 17, no. 6, pp. 681–699, Nov. 2018, doi: 10.1007/s10207-017-0382-0.
- [29] NIST Cybersecurity Framework Team, "Framework for Improving Critical Infrastructure Cybersecurity," in *Proceedings of the Annual ISA Analysis Division Symposium*, 2018, vol. 535, pp. 9–25, [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
- [30] Australian Prudential Regulation Authority (APRA), "Prudential practice guide: CPG 234 information security," 2019. [Online]. Available: [http://www.apra.gov.au/adi/Documents/cfdocs/PPG511\\_REM\\_revised-Dec-09.pdf](http://www.apra.gov.au/adi/Documents/cfdocs/PPG511_REM_revised-Dec-09.pdf).
- [31] J. M. Borky and T. H. Bradley, "Protecting Information with Cybersecurity," in *Effective Model-Based Systems Engineering*, Cham: Springer International Publishing, 2019, pp. 345–404.
- [32] J. Rezaei, "Best-worst multi-criteria decision-making method," *Omega*, vol. 53, pp. 49–57, Jun. 2015, doi: 10.1016/j.omega.2014.11.009.
- [33] S. J. H. Dehshiri, M. S. M. M. Emamat, and M. Amiri, "A novel group BWM approach to evaluate the implementation criteria of blockchain technology in the automotive industry supply chain," *Expert Systems with Applications*, vol. 198, p. 116826, Jul. 2022, doi: 10.1016/j.eswa.2022.116826.
- [34] X. Mi, M. Tang, H. Liao, W. Shen, and B. Lev, "The state-of-the-art survey on integrations and applications of the best worst method in decision making: Why, what, what for and what's next?," *Omega*, vol. 87, pp. 205–225, Sep. 2019, doi: 10.1016/j.omega.2019.01.009.
- [35] Z. H. Munim, H. Sornn-Friese, and M. Dushenko, "Identifying the appropriate governance model for green port management: Applying Analytic Network Process and Best-Worst methods to ports in the Indian Ocean Rim," *Journal of Cleaner Production*, vol. 268, p. 122156, Sep. 2020, doi: 10.1016/j.jclepro.2020.122156.
- [36] J. Rezaei, "Best-worst multi-criteria decision-making method: Some properties and a linear model," *Omega (United Kingdom)*, vol. 64, pp. 126–130, Oct. 2016, doi: 10.1016/j.omega.2015.12.001.
- [37] C. Bai, S. Kusi-Sarpong, H. B. Ahmadi, and J. Sarkis, "Social sustainable supplier evaluation and selection: a group decision-support approach," *International Journal of Production Research*, vol. 57, no. 22, pp. 7046–7067, Nov. 2019, doi: 10.1080/00207543.2019.1574042.




**BIOGRAPHIES OF AUTHORS**

**Alva Hendi Muhammad**    received his Ph.D. in Information System Modelling from University of Technology Sydney, Australia. He is currently working in Postgraduate Program at Universitas Amikom Yogyakarta, Indonesia. He has more than 10 years of teaching experience at the undergraduate and postgraduate levels. He published a few papers in journals and conferences. His research interests are modeling decision and expert systems, artificial intelligence applied to engineering and educational technologies, and information security. He can be contacted at email: [alva@amikom.ac.id](mailto:alva@amikom.ac.id).



**Joko Dwi Santoso**    received his Master's degree in Informatics Engineering from Universitas Amikom Yogyakarta, Indonesia. He also works as a lecturer at Universitas Amikom Yogyakarta, Indonesia. He has been teaching for more than 10 years in the field of network security and analyst, networking, security pentest, web security, and cyber forensic and investigation. He has various competency licenses from CISCO Networking Academy, EC-Council, and OSCP-PWK. He can be contacted at email: [joko@amikom.ac.id](mailto:joko@amikom.ac.id).



**Ananda Fikri Ijlal Akbar**    is a bachelor's student at the Computer Engineering Department, Universitas Amikom Yogyakarta, Indonesia. He is interested in infrastructure and blue team scope in cyber security. He is currently studying Infrastructure (DevOps) and Security incident response analysis. He was also a member of the blue team in the National Capture the Flags (Cyber Security) competition (GEMASTIK XIV) in 2021. His working experience includes being an English tutor and DevOps Engineer at Practical DevSecOps Singapore. He can be contacted at email: [ananda.akbar@students.amikom.ac.id](mailto:ananda.akbar@students.amikom.ac.id).