*electronics*

MDPI

*Article*

# Modeling Cybersecurity Risk: The Integration of Decision Theory and Pivot Pairwise Relative Criteria Importance Assessment with Scale for Cybersecurity Threat Evaluation

**Aleksandar Šijan [1], Dejan Viduka [2], Luka Ilić [1], Bratislav Predić [1] and Darjan Karabašević [2,3,*]**

[1] Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, 18000 Niš, Serbia; aleksandar@mef.edu.rs (A.Š.); luka.ilic@mef.edu.rs (L.I.); bratislav.predic@elfak.ni.ac.rs (B.P.)
[2] Faculty of Applied Management, Economics and Finance, University Business Academy in Novi Sad, Jevrejska 24, 11000 Belgrade, Serbia; dejan.viduka@mef.edu.rs
[3] College of Global Business, Korea University, Sejong 30019, Republic of Korea
* Correspondence: darjankarabasevic@korea.ac.kr

**Abstract:** This paper presents a comprehensive model for cyber security risk assessment using the PIPRECIA-S method within decision theory, which enables organizations to systematically identify, assess and prioritize key cyber threats. The study focuses on the evaluation of malware, ransomware, phishing and DDoS attacks, using criteria such as severity of impact, financial losses, ease of detection and prevention, impact on reputation and system recovery. This approach facilitates decision making, as it enables the flexible adaptation of the risk assessment to the specific needs of an organization. The PIPRECIA-S model has proven to be useful for identifying the most critical threats, with a special emphasis on ransomware and DDoS attacks, which represent the most significant risks to businesses. This model provides a framework for making informed and strategic decisions to reduce risk and strengthen cyber security, which are critical in a digital environment where threats become more and more sophisticated.

**Keywords:** cybersecurity risk; decision theory; PIPRECIA-S; threat evaluation; risk assessment model



**Citation:** Šijan, A.; Viduka, D.; Ilić, L.; Predić, B.; Karabašević, D. Modeling Cybersecurity Risk: The Integration of Decision Theory and Pivot Pairwise Relative Criteria Importance Assessment with Scale for Cybersecurity Threat Evaluation. *Electronics* **2024**, *13*, 4209. https://doi.org/10.3390/electronics13214209

Academic Editor: Aryya Gangopadhyay

Received: 29 September 2024
Revised: 20 October 2024
Accepted: 25 October 2024
Published: 27 October 2024



## 1. Introduction

The rapid advancement of digital technologies has brought numerous benefits to industries around the world, but it has also led to significant cybersecurity risks [1]. With increasing reliance on interconnected systems, the potential for cyberattacks has grown exponentially [2,3]. These attacks, such as malware, ransomware, phishing and Distributed Denial of Service (DDoS), threaten not only data integrity but also the operational stability of organizations. As industries strive to protect sensitive information and maintain business continuity, robust cybersecurity strategies have become critical [2,4,5]. Cybersecurity risk assessment is a fundamental aspect of defending against these attacks [6,7]. This includes the identification, analysis and assessment of risks that could potentially affect information systems and networks. However, the complexity of modern cyberattacks require more sophisticated and structured approaches to effectively assess and mitigate these risks. Decision theory offers a valuable framework for addressing such challenges by providing systematic methods for evaluating multiple criteria in complex environments. In response to these challenges, multi-objective optimization frameworks have proven to be highly effective in balancing conflicting criteria, such as security, performance, and cost. Studies such as those on energy efficiency [8] and renewable energy optimization [9] demonstrate the power of such frameworks in diverse fields, highlighting the importance of multi-criteria decision making in tackling complex problems. In the context of cybersecurity, decision theory can be applied to assess and prioritize cybersecurity threats based on various factors [10] such as severity of impact, financial losses, ease of detection and

prevention, impact on reputation and system recovery. These criteria play a vital role in understanding which threats pose the greatest risk and how they can be effectively addressed. The PIPRECIA-S model (Pivot Pairwise Relative Criteria Importance Assessment with Scale) has emerged as a valuable tool for this purpose. It enables a detailed, structured assessment of the relative importance of different criteria in cybersecurity threat assessment. By applying the PIPRECIA-S model to decision making, cybersecurity professionals can develop a comprehensive risk assessment model that not only assesses existing threats but also assists in the strategic planning of defense mechanisms [11]. The aim of this study is to develop a cyberattack risk assessment model by integrating decision theory and the PIPRECIA-S method. Through a detailed analysis of cybersecurity threats and relevant criteria, this research aims to provide a structured approach to identifying, assessing and prioritizing cybersecurity risks. The proposed model will guide organizations in implementing more effective and targeted cybersecurity strategies, providing improved protection against modern cybersecurity threats.

Motivation for Research:

The increasing sophistication of cyber threats demands a more structured and comprehensive approach to cybersecurity risk assessment. Existing models often lack the ability to adapt to the specific needs of organizations or fail to prioritize threats effectively.

Risk Mitigation Strategies:

In addition to risk assessment, it is essential to consider the risk mitigation strategies that are available for organizations to implement. For instance, Cyber Insurance and Cyber Liability Insurance are increasingly recognized as effective tools for managing the financial risks associated with cyber incidents. These insurance policies can provide organizations with financial protection against losses resulting from data breaches, ransomware attacks and other cyber threats. Incorporating such strategies into a comprehensive cybersecurity framework not only helps in risk reduction but also supports organizations in recovery efforts post-incident.

Research Contributions:

- Development of a comprehensive cybersecurity risk assessment model that integrates decision theory with the PIPRECIA-S method, allowing organizations to systematically identify and prioritize key threats.
- Detailed evaluation of specific threats, including malware, ransomware, phishing, and DDoS attacks, using criteria such as severity of impact, financial losses, ease of detection and prevention, impact on reputation and system recovery.
- Provision of a strategic framework that assists organizations in making informed decisions to strengthen their cybersecurity posture, particularly against the most critical threats.

This study aims to enhance our understanding of cybersecurity risks and facilitate more effective and targeted strategies for defending against modern cyber threats.

## 2. The Need for Assessing Cybersecurity Challenges

Cybersecurity has become a critical element in modern society, due to the significant development of information technologies and their ubiquity in everyday life [12]. The development of the Internet and other networks enabled a faster flow of information [13] and facilitated business processes, but at the same time opened the door to an increasing number of cybersecurity threats [14]. Threats, such as malware, ransomware, phishing attacks and DDoS, are becoming increasingly sophisticated and difficult to detect [15–19]. These attacks can not only cause financial losses, but can also lead to the compromise of private and sensitive data, which can result in long-term consequences for the reputation of organizations.

Given the complexity and severity of cybersecurity threats, the question is how to effectively assess these challenges and develop strategies that will minimize the risks [20,21]. The need to assess security risks is significant, in order to identify weaknesses in systems, prioritize their potential impact, and direct resources to effective defense strategies [22,23].

The risk assessment process allows organizations to better understand the vulnerabilities of their systems, as well as to implement measures that will reduce the possibility of successful attacks [24–26].

### *2.1. Types of Cybersecurity Threats*

Cybersecurity threats are constantly evolving and becoming increasingly difficult to detect [27–29]. In light of the numerous threats in cyberspace, we have focused our research on the four most common types of attacks:

- Malware (malicious software), which can be any malicious software, e.g., viruses, worms, trojans, aims to compromise computer systems in order to access confidential data or damage user data.
- Ransomware attacks are a form of malware in which attackers lock or encrypt user data and demand a ransom for its return.
- Phishing attacks rely on social engineering to trick users into revealing sensitive information, such as passwords or credit card numbers.
- DDoS attacks (Distributed Denial of Service) flood the network or server with a large number of requests, making it difficult or impossible for the system to function normally.

These attacks can cause serious consequences for businesses, including financial losses and losses of reputation and user trust, as well as legal consequences for violating data protection regulations.

### *2.2. Cybersecurity Assessment Challenges*

One of the key challenges organizations face is cybersecurity risk assessment [30,31]. The assessment process includes the identification of threats and vulnerabilities, but also the quantification of potential losses [32] that may occur as a result of an attack. Organizations often have to balance investment in security systems against the costs these systems require, with limited resources being another challenge [33].

The assessment of security risks is complex, as it involves multiple variables, from evaluating the level of system vulnerability [34], through the potential impact of threats on business operations, to the organization's capacity to adequately defend against attacks. One of the key factors is the timely identification of new types of threats that are constantly changing and becoming more sophisticated [35]. In addition, digitization and the introduction of technologies such as the Internet of Things (IoT) create additional challenges in the context of cybersecurity [36], as they increase the number of vulnerabilities that attackers can exploit.

### *2.3. The Need for Cybersecurity Risk Assessment*

Due to the increasing frequency and sophistication of cyberattacks, a comprehensive assessment of security risks is necessary, which enables strategic decisions to be made regarding the allocation of resources and protective measures [37]. This process involves the use of various methods and tools to quantify risk, assess the severity of the attack, and the impact of the attack on the business. Without adequate risk assessment, organizations are unable to effectively respond to attacks and optimize their security strategies [38,39].

The PIPRECIA-S model, as part of decision theory, provides a systematic framework for evaluating criteria [40,41] that are key to assessing security risks. This method allows threats to be ranked according to their relative importance, thus facilitating the process of prioritizing security measures. PIPRECIA-S was selected despite its lack of consistency checks due to its simplicity and adaptability, which are crucial in cybersecurity risk assessments. Compared to models like AHP, which offer complex consistency checks, PIPRECIA-S enables faster and more efficient evaluations without significant losses in accuracy. PIPRECIA-S is very suitable when collecting the attitudes of respondents that are not familiar with MCDM methods and that are not prepared in advance for its usage [40]. This is particularly important in cybersecurity, where quick decision making is often required due to rapidly evolving threats. While the lack of consistency checks is a limitation, it can

be mitigated by combining PIPRECIA-S with other methods in future studies to enhance the reliability of the assessments.

The goal of this research is to highlight the importance of risk assessment in cybersecurity and to present a model that can help organizations to better understand threats, identify the most critical vulnerabilities and develop effective defense strategies.

## 3. Previous Research

### 3.1. An Overview of Decision Making Theories in Cybersecurity Risk Assessment

The rise in sophisticated cybersecurity threats has required the development of robust methodologies for assessing cybersecurity risks. Cyberattacks such as malware, ransomware, phishing and DDoS attacks are becoming increasingly complex and impactful, requiring organizations to adopt structured decision making processes to effectively mitigate these risks. Decision theories have proven invaluable in complex technical fields, offering frameworks for solving multifaceted problems involving multiple stakeholders and competing goals [42]. In cybersecurity, decision making frameworks help identify the most critical threats, ref. [43] allocate resources, and prioritize defense [39]. Over the years, various decision making models such as Analytic Hierarchy Process (AHP), Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) and VIKOR (Multicriteria Optimization and Compromise Solution) have become widely accepted in risk assessment processes [44–49]. These models allow organizations to assess multiple criteria, such as threat severity, financial losses and system vulnerability, helping them to determine the best course of action when there are multiple competing risks. For example, AHP and TOPSIS have been used to prioritize different types of cybersecurity threats [50–53] based on their potential impact and ease of prevention. This allows cybersecurity teams to allocate resources more efficiently and focus on the most pressing vulnerabilities.

### 3.2. Application of the PIPRECIA-S Model in Cybersecurity Risk Assessment

The PIPRECIA-S model has emerged as an effective tool for assessing and ranking various cybersecurity risks [54–56] based on the relative importance of multiple criteria. PIPRECIA-S offers a simplified yet powerful method for multi-criteria decision making [57], making it an ideal approach for cybersecurity risk assessment. By applying pairwise comparisons, the model allows for the weighting of criteria such as severity of impact, financial losses, ease of detection and prevention, impact on reputation and system recovery. This method has been applied in various industries, such as construction, manufacturing, and information technology, where it helps determine the most critical factors that influence decision outcomes [57–62]. In the context of cybersecurity, PIPRECIA-S enables a structured threat assessment, helping organizations to prioritize risks and develop effective mitigation strategies. However, its application in cybersecurity is still relatively new, indicating the need for further research to explore its full potential.

### 3.3. Application of Decision Making Theories in Cybersecurity Threat Assessment

Decision making theories have been successfully applied in the field of cybersecurity to address cybersecurity threat evaluation [63]. AHP, TOPSIS, and similar models have been used to prioritize cyberattacks based on factors such as potential financial damage, ease of exploitation, and impact on operations [64]. For example, AHP has been used to evaluate different types of malware based on their potential to cause disruption [65], while TOPSIS has been used to evaluate phishing and ransomware attacks by comparing their likelihood of occurrence and impact on data security [66]. Integrating decision makig theories into cybersecurity risk management processes provides organizations with a robust framework for threat assessment [67]. These methods enable a comprehensive assessment of threats by weighing various criteria, such as severity and financial impact, thus helping decision makers to choose the most appropriate risk mitigation strategies. This approach ensures that defense is focused on the most critical vulnerabilities and that resources are deployed efficiently.

### *3.4. Importance of Further Research*

Although decision making theories such as AHP and TOPSIS are extensively applied in cybersecurity [68], the use of the PIPRECIA-S model in this domain remains limited. This paper seeks to bridge that gap by applying the PIPRECIA-S model for cybersecurity risk assessment, focusing on key criteria such as severity of impact, financial losses, ease of detection and prevention, impact on reputation and system recovery. Further research into the application of the PIPRECIA-S model in cybersecurity may lead to the development of more sophisticated risk assessment frameworks, contributing to improved protection against evolving cybersecurity threats. By expanding the use of decision making models such as PIPRECIA-S, future research can provide valuable insights into improving cybersecurity, enabling organizations to respond more effectively to the growing complexity of cyberattacks. This study aims to inspire further research on the application of decision making theories in cybersecurity, ultimately contributing to the broader development of resilient and secure systems.

## 4. Methodology and Materials

### *4.1. Simplified Method for Assessing the Relative Importance of Criteria (PIPRECIA-S)*

The PIPRECIA-S method was selected to facilitate the determination of criteria weight coefficients. Unlike the original PIPRECIA method, in the PIPRECIA-S method, the importance of each criterion is compared to the importance of the first criterion. The main advantage of the PIPRECIA-S method is its simplicity and ease of application in group decision making processes. However, unlike the extended PIPRECIA method (PIPRECIA-E) [69] and the AHP method [70], PIPRECIA-S does not include a consistency check, which can be mentioned as a limitation.

The procedure for determining the weight coefficients of criteria using the PIPRECIA-S method consists of five steps, which are outlined below [71].

Step 1. Selection of evaluation criteria $C_j$. This step involves defining the criteria $C_j, j = 1, \ldots, n$ where $n$ is the number of criteria taken into account when solving the problem. Criteria can be determined using the literature and/or with the help of expert opinions.

Step 2. Determining the relative importance of criteria $s_j$. First, the criterion is established ($C_1$) which is used as a basis for comparison. Starting with the second criterion, to each criterion, $C_j$, the relative importance of the criterion $s_j$ is assigned based on Equation (1). So, every criterion $C_j$ is compared with the reference criterion $C_1$.

$$s_j = \begin{cases} 1, C_j > C_1 \\ 1, C_j = C_1 \\ 1, C_j < C_1 \end{cases} \tag{1}$$

If the criterion $C_j$ more important than the criteria $C_1$ it is assigned a value $s_j$ which is greater than 1. In the case that the criterion $C_j$ is less important than the criteria $C_1$, it is assigned a value less than 1. In the case that the criteria $C_1$ and $C_j$ are equally important, then both criteria have an importance value of 1. Values $s_j$ belong to the interval [0.6, 1.4]. Value $s_1$ is always 1 and represents the assessment of the importance of the reference criterion $C_1$.

Step 3. The value of the coefficient $k_j$ is calculated based on Equation (2).

$$k_j = \begin{cases} 1, j = 1 \\ 2 - s_j, j > 1 \end{cases} \tag{2}$$

Step 4. The value of the coefficient $q_j$ is calculated based on Equation (3).

$$q_j = \begin{cases} 1, j = 1 \\ \frac{q_{j-1}}{k_j}, j > 1 \end{cases} \tag{3}$$

Step 5. Calculating the relative weight $w_j$ of the criteria. Based on Equation (4), the relative weight of criteria is calculated $w_j$, where $0 \leq w_j \leq 1$ and $\sum_{k=1}^{n} w_k = 1$.

$$w_j = \frac{q_j}{\sum_{k=1}^{n} q_k} \tag{4}$$

After this step, the process of determining the weight values of the criteria is completed.

### *4.2. Evaluation Criteria*

In the context of cybersecurity risk assessment, the PIPRECIA-S method is used to define key criteria for evaluating different types of threats, allowing experts to express their opinions and more easily assess the importance of each criterion. This method, similar to the AHP method, is based on comparative evaluations, but in a simpler way, it allows decisions to be made about priorities. In order to define the criteria for evaluating threats such as malware, ransomware, phishing and DDoS attacks, data from the literature and the opinions of cybersecurity experts were used.

The following five criteria are key to evaluating threats:

- Severity of impact—this criterion evaluates how seriously a single threat can affect the organization's operations and systems. This includes potential data loss and business interruptions, as well as long-term consequences for the organization's reputation.
- Financial losses—this criterion focuses on the financial consequences of the threat, including the cost of remediation and restoring the system to function, as well as the potential loss of income due to interruption of work.
- Ease of detection and prevention—this criterion evaluates how easy it is to detect and prevent a certain type of threat. For example, phishing attacks often rely on human error and can be difficult to detect, while DDoS attacks are often easier to detect but more difficult to prevent.
- Impact on reputation—this criterion refers to how much the threat can damage the organization's reputation. Attacks such as ransomware or the leakage of confidential information due to phishing can significantly undermine the trust of users and business partners, which can have long-term consequences for a business.
- System recovery—This criterion assesses how quickly an organization can recover from an attack. Some attacks, such as malware, can be remedied relatively quickly, while ransomware or DDoS attacks can require a lengthy recovery process, especially if data are encrypted or systems are overloaded.

Using the PIPRECIA-S model, these five criteria enable a systematic and structured threat assessment, helping organizations prioritize which threats pose the greatest risk and how to allocate resources. This approach enables not only better protection of the system, but also an improvement of strategic planning and decision making in the field of cybersecurity. It should be noted that different organizations, such as financial institutions, healthcare facilities and educational institutions, may prioritize cybersecurity threats in different ways, depending on industry-specific risks and regulations. This approach indicates that the variability of the cybersecurity threat assessment model and criteria can significantly depend on the sector in which organizations operate, as well as the specific challenges and regulations that define them.

### *4.3. Ranking Scale*

For each of the above criteria, a ranking scale will be used to enable an objective and consistent evaluation of cybersecurity risks. The proposed scale is shown in Table 1.

The PIPRECIA-S method uses a specific rating scale to determine the relative importance of criteria. According to the PIPRECIA-S method, the values usually range from 0.6 to 1.4, using the scale shown in Table 2.

**Table 1.** Ranking scale.

| Description | Rating | PIPRECIA-S Scale |
|---|---|---|
| Very bad | 1 | 0.60 |
| Bad | 2 | 0.80 |
| Satisfying | 3 | 1.00 |
| Good | 4 | 1.20 |
| Excellent | 5 | 1.40 |

**Table 2.** PIPRECIA-S grading values.

| Criterion Value | Description of the Importance of Criteria |
|---|---|
| 0.6 | The criterion is much less important than the reference one |
| 0.8 | The criterion is somewhat less important than the reference one |
| 1.0 | The criterion has the same importance as the reference criterion (neutral value) |
| 1.2 | The criterion is somewhat more important than the reference one |
| 1.4 | The criterion is much more important than the reference one |

Values less than 1.0 indicate reduced importance in relation to the reference criterion, while values greater than 1.0 indicate increased importance. In order to relate the rating scale from 1 to 5 to the PIPRECIA scale from 0.6 to 1.4, it is possible to carry out a recalculation that will allow the use of the known rating scale while maintaining the principles of the PIPRECIA method as shown in Table 1. This scale has been adapted for ease of use during evaluation by experts who are not familiar with the PIPRECIA-S decision making method.

### *4.4. Setting Priorities in Criteria*

Prioritizing criteria such as severity of impact, financial losses, ease of detection and prevention, impact on reputation and system recovery is key to assessing cybersecurity threats. This process is of critical importance for decision makers in organizations, as it allows them to identify which threats pose the greatest risk and where resources should be directed to protect the system. In accordance with the organization's specific needs, technical requirements and available resources, priorities are determined to best match the organization's cybersecurity strategy.

The main objective is to enable the organization to systematically determine the weighted coefficients for each criterion through a simple process of comparing the importance between the criteria. This facilitates decision making on priorities in protection against cybersecurity threats, aligning technical aspects of security systems with business objectives. This process ensures that the solution is efficient, reliable and long-lasting.

When determining the weighting coefficients for the criteria, expert feedback was crucial in achieving the most accurate results. To avoid bias in the evaluations, an iterative consensus-building process was applied. In the initial phase, experts individually ranked the criteria, and then the results were aggregated. In subsequent rounds, participants had the opportunity to adjust their ratings based on the aggregated results, allowing for the alignment of different perspectives. Additionally, anonymous evaluations were used to reduce the influence of authority or group bias, ensuring that the ratings reflect genuine priorities in the context of cybersecurity threat assessment. This approach enabled a fairer and more objective distribution of the weighting coefficients.

Table 3 shows a possible example of ranking criteria by importance in the cybersecurity threat assessment process. The criteria were ranked by a carefully selected group of experts in the fields of cybersecurity, finance and management, taking into account the unique challenges in each of those fields. These experts were chosen based on their qualifications,

including relevant certifications and extensive experience in cybersecurity analysis and threat management. Each expert independently evaluated the criteria according to their importance for the decision making process in their field.

**Table 3.** Relative importance of weighting criteria for the selection of security risks.

| Notation | Criteria | Grades |
|---|---|---|
| $C_1$ | Severity of impact | 5 (1.40) |
| $C_2$ | Financial losses | 4 (1.20) |
| $C_3$ | Ease of detection and prevention | 3 (1.00) |
| $C_4$ | Impact on reputation | 2 (0.80) |
| $C_5$ | System recovery | 1 (0.60) |

To minimize bias during this process, structured guidelines were provided, outlining the objectives and expectations for the experts. Additionally, the Delphi method was employed to facilitate anonymous feedback and to ensure a systematic approach to achieving consensus. In the initial evaluation, experts ranked the criteria individually, and the results were aggregated. In subsequent rounds, participants had the opportunity to adjust their ratings based on the aggregated results, allowing for the alignment of different perspectives.

After the initial evaluation, the results were used as input to the PIPRECIA-S method, where criteria weights were further adjusted through this iterative process until consensus was reached. This methodology ensured a comprehensive and balanced evaluation of the criteria, reflecting the multidisciplinary nature of the decision making process in cybersecurity threat assessment. It is important to recognize the limitation of relying on expert opinions, particularly regarding their applicability across all industries.

In the initial phase, each expert ranked the criteria on a scale of 1 to 5, with 1 being the lowest priority and 5 being the highest. The ranking results were then aggregated, and the average scores were used as initial weights in the PIPRECIA-S method. Participants had the opportunity to adjust their ratings based on the results of the aggregation in the next step, thus allowing the alignment of different perspectives. The final weightings of the criteria, which are the result of this process, represent a consensus that reflects a multidisciplinary approach to research and decision making.

Although the priorities in the table are defined based on the specific needs of this study, it is important to note that the ranking of these criteria may differ depending on the specific requirements, context and goals of each individual case. Accordingly, the ranking should be adapted to suit the specific needs and specifics of the project.

This ranking allows organizations to clearly identify which threats should be addressed first, thereby optimizing the allocation of resources and defense strategies.

## 5. Research Results

Table 4 shows the relative importance of the considered cybersecurity threats (malware, ransomware, phishing, DDoS) in terms of the severity of impact criterion on the basis of which the following conclusions can be drawn:

- Malware is rated 3 (Medium) for severity, meaning it can cause data theft and system corruption, but usually does not lead to catastrophic consequences.
- Ransomware achieves a rating of 5 (Very High) because it can block entire systems and demand a ransom, resulting in serious consequences.
- Phishing is also rated 4 (High), as it can lead to the theft of sensitive information, but mostly affects individuals rather than entire systems.
- DDoS is rated 4 (High), indicating that it can disrupt services on a large scale, but recovery is generally faster than ransomware attacks.

**Table 4.** Research results based on severity of impact.

| Criterion | Malware | Ransomware | Phishing | DDoS |
|---|---|---|---|---|
| Grade | 3 (1.00) | 5 (1.40) | 4 (1.20) | 4 (1.20) |

Source: Author's research.

Table 5 shows the relative importance of these threats in terms of financial losses:

- Malware is rated 3 (Medium) for financial losses due to system repair costs and potential downtime.
- Ransomware receives the highest rating of 5 (Very High), because paying the ransom and restoring the system can lead to significant financial losses.
- Phishing is rated 4 (High), because stealing financial data or hacking accounts can lead to large but limited losses.
- DDoS also receives a rating of 4 (High), because service interruptions can cause major financial consequences, especially in e-commerce and online services.

**Table 5.** Research results based on financial losses.

| Criterion | Malware | Ransomware | Phishing | DDoS |
|---|---|---|---|---|
| Grade | 3 (1.00) | 5 (1.40) | 4 (1.20) | 4 (1.20) |

Source: Author's research.

Table 6 rates the ease of detection and prevention for these threats:

- Malware is rated 3 (Medium) because it can often be detected by anti-virus tools, although sophisticated malware can go unnoticed.
- Ransomware is rated 2 (Low) because it is difficult to prevent once a system has been compromised.
- Phishing is also rated 2 (Low) because it relies on human error and is difficult to detect without user training.
- DDoS scores 3 (Medium) because it is relatively easy to detect but more difficult to prevent in real time.

**Table 6.** Research results based on ease of detection and prevention.

| Criterion | Malware | Ransomware | Phishing | DDoS |
|---|---|---|---|---|
| Grade | 3 (1.00) | 2 (0.80) | 2 (0.80) | 3 (1.00) |

Source: Author's research.

Table 7 gives the ranking according to the impact on reputation criterion:

- Malware is rated 2 (Low) because the reputational impact is usually minor, unless there is a significant data breach.
- Ransomware receives a 5 (Very High), because publicly paying a ransom or locking up data can seriously damage an organization's reputation.
- Phishing receives a score of 4 (High), especially when the target of the attack is high-ranking employees, which can lead to public scandals.
- DDoS also receives a rating of 4 (High), as prolonged downtime can erode user confidence and damage brand image.

**Table 7.** Impact on reputation research results.

| Criterion | Malware | Ransomware | Phishing | DDoS |
|---|---|---|---|---|
| Grade | 2 (0.80) | 5 (1.40) | 4 (1.20) | 4 (1.20) |

Source: Author's research.

Finally, Table 8 shows the system recovery:

- Malware is rated 4 (High) because systems can usually be restored relatively quickly after malware removal.
- Ransomware is rated 2 (Low) because recovery can be slow and expensive without backups.
- Phishing is rated 3 (Medium), where recovery is possible, but the damage caused by data theft can have long-term consequences.
- DDoS achieves a score of 3 (Medium), where recovery is usually fast after the attack stops.

**Table 8.** Research results based on system recovery.

| Criterion | Malware | Ransomware | Phishing | DDoS |
|---|---|---|---|---|
| Grade | 4 (1.20) | 2 (0.80) | 3 (1.00) | 3 (1.00) |

Source: Author's research.

The tables above show how different cybersecurity threats rank against key criteria. Ransomware generally presents the most severe impact across several criteria, including financial loss and reputational damage. DDoS and Phishing also score high, especially in terms of financial and reputational consequences. Malware, while dangerous, ranks lower on several criteria, but still poses a significant risk.

These results can help organizations prioritize their defense strategies and allocate resources to protect against the most critical threats.

## 6. Discussion

Using the PIPRECIA-S evaluation method, the researchers concluded that ransomware and DDoS attacks (Figure 1) represent the greatest threats to organizations in terms of key criteria such as severity of impact, financial losses, ease of detection and prevention, impact on reputation and system recovery. These two threats stand out because of their ability to cause serious damage to both organizations and users. Ransomware attacks, given their ability to block access to critical systems and demand a ransom, cause significant financial losses and threaten reputation in the long term. On the other hand, DDoS attacks, although they do not require a ransom, disrupt the provision of services and can lead to large losses in e-commerce, also damaging the reputation of companies.

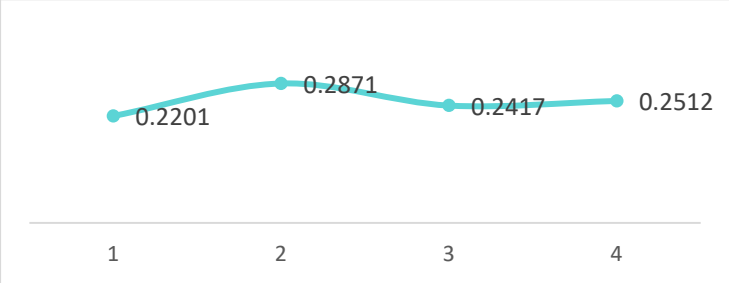


**Figure 1.** Final research results (1. Malware, 2. Ransomware, 3. Phishing, 4. DDoS).

Malware, although a serious risk, scores lower compared to ransomware and DDoS attacks, especially when it comes to financial damage and reputational impact. However, malware remains a significant problem due to its ability to cause data theft and system corruption. Phishing attacks, although often individually targeted, can lead to the theft of confidential information and, in the case of a successful attack, seriously damage the reputation of organizations.

In the context of system recoverability, malware attacks are relatively easier to remediate compared to ransomware, where recovery can be significantly prolonged if the organization does not have data backups. Phishing attacks can be solved by educating employees and strengthening protections, while DDoS attacks can be quickly recovered after the attack ends, but additional resources are needed to prevent future incidents.

Given the results of this analysis, it is recommended that organizations first focus resources on preventing ransomware and DDoS attacks, as they represent the most critical threat in terms of consequences and financial losses. Special attention should also be paid to employee education in order to reduce the risk of phishing attacks and strengthen security systems for malware prevention.

The use of decision theory, in this context, has proven to be a key tool for systematically assessing different types of cyber threats according to relevant criteria. Given the complexity of cybersecurity challenges, the PIPRECIA-S method enabled a detailed analysis and comparison of various threats, thereby identifying the optimal protection strategy. This research confirms the importance of decision theory in the domain of cybersecurity, where it is necessary to balance between several factors in order to achieve an optimal level of protection. As shown in recent studies, decision making frameworks such as the PIPRECIA-S model can effectively address the complexities of cyber threats, emphasizing the need for a structured approach to risk management [68]. Additionally, the application of dynamic behavior analysis and model checking can enhance understanding of threat behaviors, making it crucial for organizations to adapt their strategies accordingly [72]. The findings also underline the necessity of integrating innovative decision making processes for evaluating risks like ransomware, which continues to pose significant challenges [73]. Furthermore, educating employees about cybersecurity risks is fundamental, as it directly impacts the likelihood of successful phishing attempts [74].

## 7. Conclusions

Cybersecurity threat assessment plays a key role in keeping organizations safe in an increasingly complex digital environment. Research that included threats such as malware, ransomware, phishing and DDoS attacks showed that each of these threats has its own advantages and disadvantages when analyzed according to criteria such as severity of impact, financial losses, ease of detection and prevention, impact on reputation and system recovery.

Ransomware and DDoS attacks stand out as the most dangerous threats because of the serious consequences they cause, especially in terms of financial losses and reputational impact. Phishing and malware, although dangerous, have a lower threat level compared to ransomware and DDoS attacks, but still pose a significant risk.

This study does not attempt to provide a universal answer to the question of which threat is the most dangerous in each context, but to set up a model for risk assessment using the PIPRECIA-S method, which allows flexibility in decision making. The results of this analysis will always depend on organizations and decision making in terms of ranking and evaluating criteria or specific threats they face. The model developed here provides a framework that allows organizations to tailor risk assessment to their specific needs and priorities, thereby enabling strategic planning in the cybersecurity domain.

For decision makers, the results of this research provide important guidelines for identifying the threats that pose the greatest risk to their business. A focus on ransomware and DDoS attacks is crucial for organizations that want to minimize financial losses and protect their image. Ultimately, the successful implementation of these recommendations will depend on the ability of organizations to properly assess the relevant criteria and threats that are most critical to their business model.

**Author Contributions:** Conceptualization, A.Š. and L.I.; methodology, D.K. and D.V.; software, B.P.; validation, D.V. and D.K.; formal analysis, A.Š.; investigation, A.Š.; writing—original draft preparation, A.Š and L.I.; writing—review and editing, B.P. and D.K.; visualization, B.P. and L.I.; supervision, D.V. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was partially supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia [grant number 451-03-65/2024-03/200102].

**Data Availability Statement:** The data supporting the reported results in this study are contained within the article itself.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References


1. Ustundag, A.; Cevikcan, E.; Ervural, B.C.; Ervural, B. Overview of cyber security in the industry 4.0 era. *Ind. 4.0 Manag. Digit. Transform.* **2018**, *2018*, 267–284.
2. Djenna, A.; Harous, S.; Saidouni, D.E. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Appl. Sci.* **2021**, *11*, 4580. [CrossRef]
3. Amin, M. Toward secure and resilient interdependent infrastructures. *J. Infrastruct. Syst.* **2002**, *8*, 67–75. [CrossRef]
4. Corallo, A.; Lazoi, M.; Lezzi, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Comput. Ind.* **2020**, *114*, 103165. [CrossRef]
5. Rizwan, A.M.; Hu, Q.; Zeadally, S. Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Comput. Netw.* **2019**, *165*, 106946.
6. Süzen, A.A. A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. *Int. J. Comput. Netw. Inf. Secur.* **2020**, *14*, 1. [CrossRef]
7. Ganin, A.A.; Quach, P.; Panwar, M.; Collier, Z.A.; Keisler, J.M.; Marchese, D.; Linkov, I. Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Anal.* **2020**, *40*, 183–199. [CrossRef]
8. Guo, Y.; Guo, B. Enhancing Energy Efficiency in Telehealth IoT through MultiObjective Optimization on a Hybrid Fog/Cloud Computing Platform. *J. Biotechnol. Bioinform. Res.* **2024**, *6*, 1–12. [CrossRef]
9. Li, Y.; Wang, J.; Cao, Y. Multi-objective distributed robust cooperative optimization model of multiple integrated energy systems considering uncertainty of renewable energy and participation of electric vehicles. *Sustain. Cities Soc.* **2024**, *104*, 105308. [CrossRef]
10. Goel, R.; Kumar, A.; Haddow, J. PRISM: A strategic decision framework for cybersecurity risk assessment. *Inf. Comput. Secur.* **2020**, *28*, 591–625. [CrossRef]
11. Maček, D.; Magdalenić, I.; Redep, N.B. A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. *Int. J. Saf. Secur. Eng.* **2020**, *10*, 161–174. [CrossRef]
12. Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. *J. Comput. Syst. Sci.* **2014**, *80*, 973–993. [CrossRef]
13. Eric, Y. Information systems (in the Internet age). In *Practical Handbook of Internet Computing*; CRC: Boca Raton, FL, USA, 2004.
14. Evans, P.C.; Annunziata, M. Industrial internet: Pushing the boundaries. *Gen. Electr. Rep.* **2012**, 488–508. Available online: https://www.researchgate.net/profile/Marco-Annunziata/publication/271528854_Industrial_Internet_Pushing_the_Boundaries_of_Minds_and_Machines/links/566342e608ae418a786bb015/Industrial-Internet-Pushing-the-Boundaries-of-Minds-and-Machines.pdf (accessed on 1 September 2024).
15. Bonasera, W.; Chowdhury, M.M.; Latif, S. Denial of service: A growing underrated threat. In Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, East Africa, 7–8 October 2021; IEEE: Piscataway, NJ, USA, 2021.
16. Ferdous, J.; Islam, R.; Mahboubi, A.; Islam, M.Z. A State-of-the-Art Review of Malware Attack Trends and Defense Mechanism. *IEEE Access* **2023**, *11*, 121118–121141. [CrossRef]
17. Mishra, N.; Pandya, S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access* **2021**, *9*, 59353–59377. [CrossRef]
18. Falowo, O.I.; Ozer, M.; Li, C.; Abdo, J.B. Evolving Malware & DDoS Attacks: Decadal Longitudinal Study. *IEEE Access* **2024**, *12*, 39221–39237.
19. Ravichandran, N.; Tewaraja, T.; Rajasegaran, V.; Kumar, S.S.; Gunasekar, S.K.L.; Sindiramutty, S.R. Comprehensive Review Analysis and Countermeasures for Cybersecurity Threats: DDoS, Ransomware, and Trojan Horse Attacks. 2024. Available online: https://www.preprints.org/manuscript/202409.1369/v1 (accessed on 1 September 2024).
20. Ghadge, A.; Weiß, M.; Caldwell, N.D.; Wilding, R. Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Manag. Int. J.* **2020**, *25*, 223–240. [CrossRef]
21. Wang, W.; Lu, Z. Cyber security in the smart grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
22. Zografopoulos, I.; Ospina, J.; Liu, X.; Konstantinou, C. Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access* **2021**, *9*, 29775–29818. [CrossRef]
23. Moteff, J.D. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*; Congressional Research Service, The Library of Congress: Washington, DC, USA, 2007.
24. Cárdenas, A.A.; Amin, S.; Lin, Z.S.; Huang, Y.L.; Huang, C.Y.; Sastry, S. Attacks against process control systems: Risk assessment, detection, and response. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011.
25. Stoneburner, G.; Goguen, A.; Feringa, A. Risk management guide for information technology systems. *Nist Spec. Publ.* **2002**, *800*, 800-30.
26. Kure, I.H.; Islam, S.; Razzaque, M.A. An integrated cyber security risk management approach for a cyber-physical system. *Appl. Sci.* **2018**, *8*, 898. [CrossRef]
27. Fadziso, T.; Thaduri, U.R.; Dekkati, S.; Ballamudi, V.K.R.; Desamsetti, H. Evolution of the cyber security threat: An overview of the scale of cyber threat. *Digit. Sustain. Rev.* **2023**, *3*, 1–12.
28. Dillon, R.; Lothian, P.; Grewal, S.; Pereira, D. Cyber security: Evolving threats in an ever-changing world. In *Digital Transformation in a Post-COVID World*; CRC Press: Boca Raton, FL, USA, 2021; pp. 129–154.

29. Admass, S.W.; Munaye, Y.Y.; Diro, A. Cyber security: State of the art, challenges and future directions. *Cyber Secur. Appl.* **2023**, *2*, 100031. [CrossRef]
30. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. Inf. Secur.* **2020**, *2020*, 8. [CrossRef]
31. Amin, Z. A practical road map for assessing cyber risk. *J. Risk Res.* **2019**, *22*, 32–43. [CrossRef]
32. Mishra, S.; Anderson, K.; Miller, B.; Boyer, K.; Warren, A. Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. *Appl. Energy* **2020**, *264*, 114726. [CrossRef]
33. Weishäupl, E.; Yasasin, E.; Schryen, G. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Comput. Secur.* **2018**, *77*, 807–823. [CrossRef]
34. Akgun, I.; Kandakoglu, A.; Ozok, A.F. Fuzzy integrated vulnerability assessment model for critical facilities in combating the terrorism. *Expert Syst. Appl.* **2010**, *37*, 3561–3573. [CrossRef]
35. Galinec, D.; Luić, L. Design of conceptual model for raising awareness of digital threats. *WSEAS Trans. Environ. Dev.* **2020**, *16*, 493–504. [CrossRef]
36. Weber, R.H. Internet of Things–New security and privacy challenges. *Comput. Law Secur. Rev.* **2010**, *26*, 23–30. [CrossRef]
37. Dutta, A.; McCrohan, K. Management's role in information security in a cyber economy. *Calif. Manag. Rev.* **2002**, *45*, 67–87. [CrossRef]
38. Guikema, S.D.; Aven, T. Assessing risk from intelligent attacks: A perspective on approaches. *Reliab. Eng. Syst. Saf.* **2010**, *95*, 478–483. [CrossRef]
39. Ahmad, A.; Maynard, S.B.; Park, S. Information security strategies: Towards an organizational multi-strategy perspective. *J. Intell. Manuf.* **2014**, *25*, 357–370. [CrossRef]
40. Stanujkić, M.; Popović, G.; Karabašević, D.; Saračević, M.; Stanujkić, D.; Novaković, S. Approach to the personnel selection in a group decision-making environment based on the use of the MULTIMOORA and PIPRECIA-S methods. *BizInfo J. Econ. Manag. Inform.* **2024**, *15*, 19–26.
41. Hadad, S.H.; Metha, A.R.; Setiawansyah, S.; Sulistiani, H. Evaluation of Salesperson Performance in the Sales Allowance Decision Support System Using the MARCOS and PIPRECIA Methods. *J. Comput. Syst. Inform. (JoSYC)* **2024**, *5*, 477–486. [CrossRef]
42. Linkov, I.; Satterstrom, F.K.; Kiker, G.; Seager, T.P.; Bridges, T.; Gardner, K.H.; Rogers, S.H.; Belluck, D.A.; Meyer, A. Multicriteria decision analysis: A comprehensive decision approach for management of contaminated sediments. *Risk Anal. Int. J.* **2006**, *26*, 61–78. [CrossRef]
43. Bouramdane, A.-A. Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *J. Cybersecur. Priv.* **2023**, *3*, 662–705. [CrossRef]
44. Ramavandi, B.; Darabi, A.H.; Omidvar, M. Risk assessment of hot and humid environments through an integrated fuzzy AHP-VIKOR method. *Stoch. Environ. Res. Risk Assess.* **2021**, *35*, 2425–2438. [CrossRef]
45. Taylan, O.; Alamoudi, R.; Kabli, M.; AlJifri, A.; Ramzi, F.; Herrera-Viedma, E. Assessment of energy systems using extended fuzzy AHP, fuzzy VIKOR, and TOPSIS approaches to manage non-cooperative opinions. *Sustainability* **2020**, *12*, 2745. [CrossRef]
46. Bakioglu, G.; Atahan, A.O. AHP integrated TOPSIS and VIKOR methods with Pythagorean fuzzy sets to prioritize risks in self-driving vehicles. *Appl. Soft Comput.* **2021**, *99*, 106948. [CrossRef]
47. Zandi, P.; Rahmani, M.; Khanian, M.; Mosavi, A. Agricultural risk management using fuzzy TOPSIS analytical hierarchy process (AHP) and failure mode and effects analysis (FMEA). *Agriculture* **2020**, *10*, 504. [CrossRef]
48. Dincer, H.; Hacioglu, U. A comparative performance evaluation on bipolar risks in emerging capital markets using fuzzy AHP-TOPSIS and VIKOR approaches. *Eng. Econ.* **2015**, *26*, 118–129. [CrossRef]
49. Ak, M.F.; Gul, M. AHP–TOPSIS integration extended with Pythagorean fuzzy sets for information security risk analysis. *Complex Intell. Syst.* **2019**, *5*, 113–126. [CrossRef]
50. Hezer, S.; Gelmez, E.; Özceylan, E. Comparative analysis of TOPSIS, VIKOR and COPRAS methods for the COVID-19 Regional Safety Assessment. *J. Infect. Public Health* **2021**, *14*, 775–786. [CrossRef] [PubMed]
51. Putra, I.N.; Octavian, A.; Susilo, A.; Prabowo, A.R. A hybrid AHP-TOPSIS for risk analysis in maritime cybersecurity based on 3D models. *Decis. Sci. Lett.* **2023**, *12*, 759–772. [CrossRef]
52. Tamošaitienė, J.; Khosravi, M.; Cristofaro, M.; Chan, D.W.M.; Sarvari, H. Identification and prioritization of critical risk factors of commercial and recreational complex building projects: A Delphi study using the TOPSIS method. *Appl. Sci.* **2021**, *11*, 7906. [CrossRef]
53. Setiawansyah, S.; Sintaro, S.; Saputra, V.H.; Aldino, A.A. Combination of Grey Relational Analysis (GRA) and Simplified Pivot Pairwise Relative Criteria Importance Assessment (PIPRECIA-S) in Determining the Best Staff. *Bull. Inform. Data Sci.* **2024**, *2*, 57–66. [CrossRef]
54. Janošik, M.; Đukić, T.; Mladenović, M. Evaluating the Impact of Motivation Factors on Employee Organizational Behavior Using the PIPRECIA-S Method. *J. Process Manag. New Technol.* **2024**, *4*, 13–29. [CrossRef]
55. Setiawansyah, S.; Hadad, S.H.; Aldino, A.A.; Palupiningsih, P.; Laxmi, G.F.; Megawaty, D.A. Employing PIPRECIA-S weighting with MABAC: A strategy for identifying organizational leadership elections. *Bull. Electr. Eng. Inform.* **2024**, *13*, 4273–4284. [CrossRef]

56. Sarbat, I. A MCDM-based measurement proposal of job satisfaction comprising psychosocial risks. *Ergonomics* **2024**, 1–16. [CrossRef]
57. Stevic, Z.; Nunic, D.; Badi, I.; Karabasevic, D. Evaluation of dimensions of SERVQUAL model for determining quality of processes in reverse logistics using a Delphi–Fuzzy PIPRECIA model. *Rom. J. Econ. Forecast* **2022**, *25*, 139–159.
58. Arshad, W.M.; Setiawansyah, S.; Sintaro, S. Comparative Analysis of the Combination of MOORA and GRA with PIPRECIA Weighting in the Selection of Warehouse Heads. *BEES Bull. Electr. Electron. Eng.* **2024**, *4*, 112–122. [CrossRef]
59. Jaukovic Jocic, K.; Karabasevic, D.; Jocić, G. The use of the PIPRECIA method for assessing the quality of e-learning materials. *Ekonomika* **2020**, *66*, 37–45. [CrossRef]
60. Stanujkic, M.; Popovic, G.; Vukotic, S.; Karabasevic, D.; Stanujkic, D. Improvement of business decision-making in IT industry using the MCDM approach. *Industrija* **2023**, *51*, 73–88. [CrossRef]
61. Đukić, T.; Karabašević, D.; Popović, G. Evaluation of aspects of cognitive skills using the piprecia method. *Ekonomika* **2022**, *68*, 1–14. [CrossRef]
62. Aytekin, A. Determining criteria weights for vehicle tracking system selection using PIPRECIA-S. *J. Process Manag. New Technol.* **2022**, *10*, 115–124. [CrossRef]
63. Stević, Ž.; Stjepanović, Ž.; Božičković, Z.; Das, D.; Stanujkić, D. Assessment of conditions for implementing information technology in a warehouse system: A novel fuzzy PIPRECIA method. *Symmetry* **2018**, *10*, 586. [CrossRef]
64. Skinner, G.; Parrey, B. A literature review on effects of time pressure on decision making in a cyber security context. In *Journal of Physics: Conference Series*; IOP Publishing: Bristol, UK, 2019; Volume 1195.
65. Chen, Y.-S.; Chou, J.C.-L.; Lin, Y.-S.; Hung, Y.-H.; Chen, X.-H. Identification of SMEs in the Critical Factors of an IS Backup System Using a Three-Stage Advanced Hybrid MDM–AHP Model. *Sustainability* **2023**, *15*, 3516. [CrossRef]
66. Alhakami, W. Evaluating modern intrusion detection methods in the face of Gen V multi-vector attacks with fuzzy AHP-TOPSIS. *PLoS ONE* **2024**, *19*, e0302559. [CrossRef]
67. Jarjoui, S.; Murimi, R. A framework for enterprise cybersecurity risk management. In *Advances in Cybersecurity Management*; Springer International Publishing: Cham, Germany, 2021; pp. 139–161.
68. Zhu, T.; Li, X.; Zhang, W. Applying Markov Decision Processes to Evaluate Ransomware Data Theft Risks. 2023. Available online: https://www.researchsquare.com/article/rs-3736872/v1 (accessed on 1 September 2024).
69. Stanujkic, D.; Zavadskas, E.K.; Karabasevic, D.; Smarandache, F.; Turskis, Z. The use of the PIvot Pairwise RElative Criteria Importance Assessment method for determining the weights of criteria. *Rom. J. Econ. Forecast.* **2016**, *20*, 116–133.
70. Saaty, R.W. The analytic hierarchy process—What it is and how it is used. *Math. Model.* **1987**, *9*, 161–176. [CrossRef]
71. Stanujkic, D.; Karabasevic, D.; Popovic, G.; Sava, C. Simplified Pivot Pairwise Relative Criteria Importance Assessment (Piprecia-S) Method. *Rom. J. Econ. Forecast.* **2021**, *24*, 141–154.
72. AlSobeh, A. OSM: Leveraging Model Checking for Observing Dynamic 1 behaviors in Aspect-Oriented Applications. *arXiv* **2024**, arXiv:2403.01349. [CrossRef]
73. AlSobeh, A.M.R.; AlAzzam, I.; Shatnawi, A.M.J.; Khasawneh, I. Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online J. Commun. Media Technol.* **2004**, *13*, e202312. [CrossRef]
74. Zadeh, A.; Lavine, B.; Zolbanin, H.; Hopkins, D. A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. *Decis. Anal. J.* **2023**, *9*, 100328. [CrossRef]