A Multi-Criteria Decision-Making Framework for Cybersecurity Incident Severity Evaluation

Indre Grigaraviciute, Nikolaj Goranin

indre.grigaraviciute@vilniustech.lt, nikolaj.goranin@vilniustech.lt
Department of Information Systems, Vilnius Gediminas Technical University, Vilnius, Lithuania

Introduction

Cybersecurity incident severity evaluation is an important component of effective incident response and decision-making. It involves assessing the potential consequences of security incidents and determining their relative significance within an organizational context. Because incidents can differ in operational impact, information impact, affected assets, response urgency, and recovery requirements, their evaluation involves multiple and potentially conflicting criteria. Since these factors may differ in importance and influence an incident in different ways, a structured multi-criteria approach is required to integrate them into a consistent evaluation process.

This study proposes a Multi-Criteria Decision-Making (MCDM) framework for systematic cybersecurity incident severity evaluation. The framework considers five criteria: **Operational Impact, Data and Information Impact, Affected Asset Scope, Response Urgency, and Recovery Complexity.**

Expert judgments are incorporated through the **Analytic Hierarchy Process (AHP)** to determine the relative importance of these criteria. **VIKOR** and **PROMETHEE** are applied as complementary MCDM methods to evaluate and rank representative cybersecurity incident scenarios [1], [2]. The agreement between the resulting rankings is examined using Spearman's rank correlation, while sensitivity analysis is used to assess the robustness of the evaluation results under changes in criterion weights.

Problem relevance

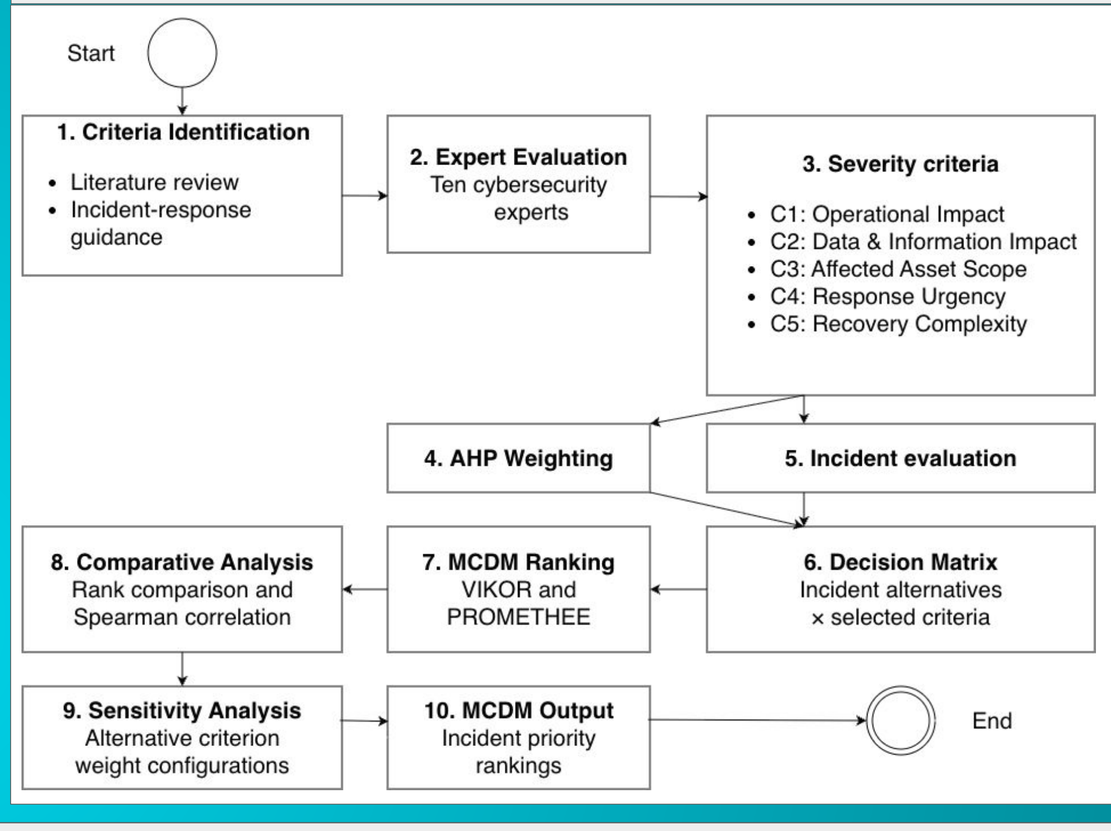
Increasing complexity:

- Cybersecurity incidents are becoming more frequent, complex, and potentially impactful.
- **Multiple incidents**: Organizations may face several incidents simultaneously across systems, information assets, users, and operational processes.
- **Multiple severity dimensions**: Incident severity depends on operational impact, information impact, affected asset scope, response urgency, and recovery requirements.
- **Limitations of conventional approaches**: Predefined categories, organizational rules, and expert judgment may provide limited transparency when multiple factors must be considered simultaneously.
- **Need for structured evaluation:** Incident-response guidance emphasizes factors such as scope, potential impact, time-criticality, and resource availability when assessing and prioritizing incidents [3], [4].
- **MCDM potential**: MCDM methods can integrate heterogeneous criteria and expert knowledge, yet their systematic application to cybersecurity incident severity evaluation remains comparatively limited.

Research Gap & Objective

Research Gap: MCDM methods have been widely applied to cybersecurity risk assessment, vulnerability prioritization, and security-related decision problems, but their systematic application to cybersecurity incident severity evaluation remains comparatively limited. Existing approaches also rarely distinguish between MCDM-based incident prioritization and independent expert severity assessment.
Objective: This study aims to develop an MCDM framework for systematic cybersecurity incident severity evaluation by integrating expert-based criteria weighting, complementary MCDM methods, and independent expert assessment for external validation.

MCDM Framework for Cybersecurity Incident Severity Evaluation

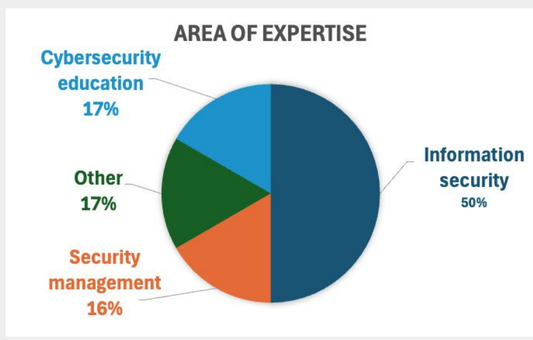


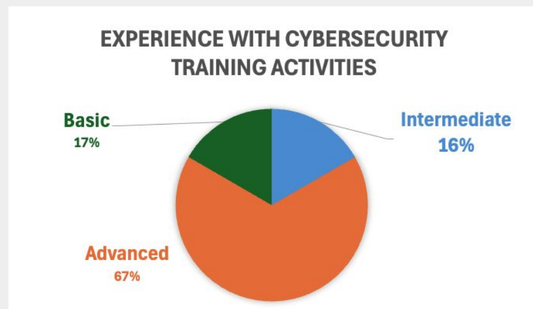
Results

AHP was used to determine the relative weights of five criteria for cybersecurity incident severity evaluation. The aggregated pairwise comparison matrix demonstrated acceptable consistency (CR = 0.0304).

The criteria weights were applied to five cybersecurity incident scenarios evaluated using VIKOR and PROMETHEE II. The resulting rankings enabled comparison of the scenarios and assessment of agreement between the two methods using Spearman's rank correlation.

Sensitivity analysis examined ranking stability under criterion weight variations of ±10% and ±20%. Spearman's rank correlation with baseline rankings ranged from 0.9 to 1.0, indicating high overall ranking consistency, although sensitivity varied across criteria and methods. The findings demonstrate the potential of the proposed framework to support structured, multi-criteria cybersecurity incident severity evaluation.





Scenario	VIKOR rank	PROMETHEE rank
A1 Phishing and Social Engineering	4	4
A2 Malware and Ransomware	1	1
A3 Data Breach and Information Disclosure	2	2
A4 Unauthorized Access and Account Compromise	5	5
A5 Insider Threat	3	3

Criterion	AHP weight
C1 Operational Impact	0,193
C2 Data and Information Impact	0,262
C3 Affected Asset Scope	0,126
C4 Response Urgency	0,311
C5 Recovery Complexity	0,107

Discussion

- The proposed MCDM framework provides a structured approach for **cybersecurity incident severity evaluation**, integrating multiple criteria with expert knowledge rather than relying on a single incident characteristic.
- **AHP** enables expert preferences to be incorporated into the evaluation by determining the relative importance of the selected severity criteria and providing explicit criterion weights.
- **VIKOR and PROMETHEE** provide complementary perspectives for evaluating and prioritizing the considered incident scenarios. The comparison of their results provides additional evidence regarding the consistency of the obtained rankings.
- The findings indicate that **incident severity and prioritization are related but not identical concepts**. Severity reflects the characteristics of an incident according to the defined criteria, whereas prioritization may also depend on the specific decision context and alternatives being considered.
- **Sensitivity analysis** supports the assessment of result robustness by examining how changes in criterion importance affect the evaluation and prioritization of incidents. It also helps identify criteria with greater influence on the results.
- Overall, the framework can support a more **transparent, systematic, and reproducible** approach to cybersecurity incident severity evaluation, while remaining adaptable to different incident types, criteria, and organizational contexts.

References

1. Opricovic, S. (1998). Multicriteria optimization of civil engineering systems [Doctoral dissertation]. Faculty of Civil Engineering, University of Belgrade.
2. Brans, J. P. (1982). L'ingénierie de la décision: Élaboration d'instruments d'aide à la décision. La méthode PROMETHEE. In R. Nadeau & M. Landry (Eds.), L'aide à la décision: Nature, instruments et perspectives d'avenir (pp. 183–214). Presses de l'Université Laval.
3. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2008). Computer security incident handling guide (NIST Special Publication 800-61 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r1
4. Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61 Revision 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

DATA ANALYSIS METHODS FOR SOFTWARE SYSTEMS

VILNIUS TECH