



A DATA-DRIVEN MULTI-CRITERIA DECISION FRAMEWORK FOR CYBERSECURITY INVESTMENT AND PROJECT PRIORITIZATION IN BANKING

Md. Sumsuzzaman ^{1*}, Masrufa Tasnim ², Md Abdullah Enayet ³, Rasel Hossain Babu ⁴, Mst Anupa Nasrin Khan ⁵, Tanaya Jakir ⁶, Shakila Sultana ⁷, Kabita Shamia Akter ⁸

¹ Master's of Business Administration, International American University, USA,
sumsuzzamanmd746@gmail.com

² Master of Business Administration (MBA) – Human Resource Management, University of Dhaka, Bangladesh, mtreema@gmail.com

³ Master of Science in Cybersecurity, Washington University of Science and Technology, USA,
menayet@student.wust.edu

⁴ MS in Cybersecurity (STEM), Bay Atlantic University, Washington, D.C., USA,
rbabu@stu.bau.edu

⁵ Master of Science in Zoology (Entomology Focus), The University of Rajshahi, Bangladesh,
anupa516@hotmail.com

⁶ PhD in Information Technology, University of the Cumberlands, USA, tanayajakir@gmail.com

⁷ Master's in Accounting (M.A.), National University, Bangladesh, sultanashakila6@gmail.com

⁸ Doctor of Business Administration, University of the Potomac, USA,
shamia.kabita@student.potomac.edu

*Corresponding Author: Md. Sumsuzzaman, Email: sumsuzzamanmd746@gmail.com

Abstract

Investments in cybersecurity prioritization by banks are usually determined based on expert judgement, which is hard to audit, reproduce and defend from regulators and boards of directors. We propose a hybrid, data-driven multi-criteria decision framework where two of the eight prioritization criteria (risk reduction and threat-likelihood coverage) are based on actual threat-intelligence data rather than opinion while keeping the other six transparent and analyst-editable. The data layer consists of a combination of 337,705 CVE records, Exploit Prediction Scoring System (EPSS) exploit-probability scores, Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities flags, and 893 banking-sector incidents identified over the use of VERIS Community Database (NAICS code 52). This data-driven severity ordering is held in a consistent feature-ordered sense across seven attack-type categories using a GPU-trained feed-forward deep neural network and is subsequently reweighted toward the specific banking threat landscape observable from the incident data. Next, twelve candidate security investments are ranked using five different independent methods such as Analytic Hierarchy Process (AHP), Shannon entropy weighting, TOPSIS, Fuzzy-TOPSIS and VIKOR. Pairwise Spearman correlation from 0.90 to 0.97 and strong cross-method agreement (Kendall's $W=0.944$), with the highest-ranked solution–vulnerability management platform—is stable across 232 weight-perturbation trials (rank-reversal rate=zero; mean full-ranking Spearman correlation against baseline ≥ 0.997). We present the framework, its validation method and limitations, including a data quality artifact in the KO given in the KEV field and that criteria derived from configurations are illustrative.

Keywords: Multi-criteria decision-making; cybersecurity investment; AHP; TOPSIS; VIKOR; deep learning; banking; CVE; EPSS



1. Introduction

The threat landscape, for banks meanwhile is large, fast moving and increasingly automated while bank budgets are tight and under heavy scrutiny. How much to fund, and in what order, security projects is thus a perennial high-stakes exercise. In practice these decisions are often made by expert panels that subjectively assign criteria values, and then apply a structured method (such as AHP or TOPSIS) on top of those values [1], [2], [3]. While the process looks procedurally rigorous, the inputs that are driving the output remain opinion; hard to audit, hard to replicate across analysts, and vulnerable when defending them with a regulator or informing an internal audit committee.

Coinciding with these efforts, an independent line of work has generated more and more data-driven indicators of cyber risk at the level of specific vulnerabilities. Common Vulnerability Scoring System (CVSS) [14] is a set of globally recognized systems for rating the severity of security vulnerabilities; Exploit Prediction Scoring System (EPSS) predicts if a vulnerability will be exploited in the wild [15], [16]; CISA Known Exploited Vulnerabilities catalog documents publicly known exploited vulnerabilities that have been addressed by vendors. These signals are linked to and extensively used for remediation triage, but rarely upward connected to the investment portfolio question of what security investments a bank should make.

This paper bridges that gap. Our paper proposes the framework in which two of the metrics that are most suitable for measurement, risk-reduction and threat-likelihood coverage are calculated using actual threat-intelligence data via a deep neural network trained to run on a GPU, while six of those metrics which really are institution-specific such as implementation cost, regulatory impact remain clear and editable configuration values. The framework does not look to eliminate human judgement. It quarantines judgment to the extent practicable, it makes that judgement visible, and the rest is anchored in data that can be audited.

Contribution. The contributions of this work are four-fold: First, we provide a reproducible pipeline that bases the risk-reduction and threat-coverage criteria upon real CVE, EPSS, and KEV data rather than pure expert opinion using a GPU-trained network. Second, we derive a prioritisation of threat exposure that is specific to the banking sector from incidents in the VERIS Community Database, such that threats are focused on those which threaten financial institutions. Thirdly, we verify the ranking from the advice through cross-validation using five distinct ranking methods and apply Kendall's coefficient of concordance and pairwise rank correlation as measurements for their agreement. Fourth, we present a sensitivity analysis assessing not only changes in the top alternative but also stability of the full ranking under both structured and random weight perturbation.

The remainder of the paper is organized as follows. Section 2 reviews related work. Section 3 describes the data. Section 4 presents the methodology. Section 5 reports results. Section 6 discusses the interpretation, Section 7 states limitations, and Section 8 concludes.

2. Related Work

MCDM for cybersecurity investment. Multi-criteria decision-making has a long history in the field of security spending. Gordon and Loeb cast information security expenditure as an economic optimization problem [1]. Decision support for cybersecurity risk planning under uncertainty was developed by Rees and colleagues [3], and approaches to decision-support methods for allocating a fixed security budget across controls were evaluated by Fielder and colleagues [2]. Ganin [4] et al. proposed a structured decision-analysis framework that quantifies threat, vulnerability, and consequence and Goel [5] et al. described a strategic decision framework for cybersecurity risk assessment. One common denominator of these studies is that values of the criteria are given by experts, which the present work attempts to decrease for two most measurable criteria.

Ranking methods. The Analytic Hierarchy Process uses pairwise comparisons (and the corresponding consistency check on those comparisons) to derive criteria weights [6], [7]. Specifically, the preference ranking organisation method for enrichment evaluation (TOPSIS) ranks alternatives according to their geometric distance to ideal and anti-ideal solutions [8]. In order to manage the uncertainty of expert-



elicited values, Chen utilized triangular fuzzy numbers in a fuzzy environment and extended TOPSIS [9]. VIKOR provides a compromise-ranking rationale based on group utility and individual regret, and was compared with TOPSIS [10]. Shannon entropy weighting, a member of the objective weighting methods family alongside correlation-based schemes [13], derive weights from the dispersion contained in decision matrix itself to provide an objective alternative for subjective weight generation [11], [12]. We use all of these methods intentionally, rather than picking one, to see if the recommended ranking is a property of the data or an artifact from just one aggregation rule.

Data-driven vulnerability signals. CVSS has continued to be the de facto standard of metric for severity [14] but explicitly states that the base score should not be interpreted as a measure of threat or exploitability. To predict exploitation in the wild, EPSS was introduced to address exactly that gap by modelling data-driven empirical prediction [15], [16]. Awareness about the vulnerability severity can also be obtained by applying machine learning techniques directly on vulnerabilities' descriptions and characteristics [17], [18]. We base our risk model on this work but uses the severity ordering learned as input to a portfolio-level decision, not an end in itself.

Incident data in financial services. For example, industry incident datasets such as those coded under the VERIS schema provides a characterization of actors, actions and assets in actual breaches [19]. We leverage the banking-sector subset of such incident data to reweight threat exposure toward the categories that over-index in breaches suffered by financial-sector entities.

3. Data and Materials

This framework is built upon three main data sources.

NVD CVE dataset. After filtering out records that contain missing targets, we are left with 337,705 CVE records, each described by seven binary attack-type flags (cross-site scripting, SQL injection, buffer overflow, remote code execution, privilege escalation,, denial of service and directory traversal), two text-derived features (word count and character length), the publication year (2010 to 2022) and the CVSS base score as regression target. EPSS and KEV enrichment. A second 360,836-row file of CVE records provides both EPSS exploit-probability scores as well as CISA KEV actively-exploited flags. It is then linked to its corresponding file in the CVE dataset using a common identifier known as CVE. VERIS Community Database. 10,047 incident records from the shallow clone of the VERIS Community Database. Of these, 893 correspond to a victim-industry prefix of 52 (NAICS grouping for banking, finance and insurance) that applies reweighting of threat-category exposure to the financial-sector threat landscape.

4. Methodology

4.1 Risk-scoring model (data-driven, GPU-trained)

It trains a feed-forward deep neural network (based on PyTorch + CUDA) on the seven attack-type flags together with their word count, character length and year of publication to regress the CVSS base score. It is a two hidden layer network of size 64 and 32 with ReLU activations, dropout p=0.2 on the hidden layers. Notes: They omit CVSS exploitability and impact sub-scores because those are near-deterministic components of the target, making the regression trivial. This indicates that feature normalization for continuous variables is now performed using statistics computed solely on the training split. Data is 70-10-20 training:validation:test and validated with early stopping on validation loss. We fully detail architectures (and hyperparameters) in Appendix A.

$$L_{MSE}(\theta) = \frac{1}{N} \sum_{i=1}^N (y_i - \hat{y}_i)^2, \hat{y}_i = f_{\theta}(x_i) \quad (1)$$

where x_i is the i -th CVE record input vector (which consists of seven binary attack-type flags, word count, character length and publication year), f_{θ} is feed-forward network with parameter θ , y_i is observed CVSS base score, $\hat{y}_i$ is predicted score and N is number of training records. This mean squared error on the training split is minimized in order to optimize network parameters, and that same loss evaluated on the validation split is used for early stopping.



After the training of this network, it is queried on 7 synthetic one-hot inputs representing each attack-type category, where continual features are fixed at their means in the training-set. This produces a predicted severity for each category and provides an ordering of categories that are consistently, data driven rather than dependent on any particular observed CVE.

4.2 Banking threat-exposure profile

Hence, EPSS and KEV are specified (with an extremely memory-efficient streamable accumulation process) to attack-type categories indexed by the common CVE key. The CVE dataset is paged through and running sums for each category accumulated instead of materialising the entire merged table into memory (peaking below 16 GB total working memory constraint). Average EPSS score and KEV rate are computed for each categories. from the table metaFlag+with a add-smoothing approachTo perform, we build seven attack-type categories + e.g. spam-run &phish &backdoor You can Mapping matrix for banking sector so, the code of this initial optimization to lookup it normalizes and smooths with in table. For each category, we are then taking a product of normalized predicted severity $N(p)$ (using the 2–5 MFE dataset), mean EPSS score $E(E(i))$, KEV-boost term TB and banking weight W_b followed by min-max normalization across the seven categories. The exact equations can be found in Appendix A.

$$w_k = \frac{n_k + \alpha}{\sum_{j=1}^K n_j + K\alpha}, \quad k = 1, \dots, K \quad (2)$$

where n_k is the number of VERIS incidents in banking-sector (NAICS 52) whose action varieties map to attack-type category k , $K = 7$ is the number of categories (see Table 1), and $\alpha > 0$ additive smoothing constant protecting a category with observed zeroed incidents from being assigned a weight of zero. w_k = the proportion of banking threat activity that can be attributed to category k .

$$E_k = \tilde{s}_k \cdot \bar{p}_k \cdot (1 + \kappa_k) \cdot w_k, \quad \tilde{E}_k = \frac{E_k - E_j}{E_j - E_j} \quad (3)$$

where $\tilde{s}_k$ is the normalized predicted severity of category k from the trained network, $\bar{p}_k$ is mean EPSS exploitation probability of CVEs in category k , κ_k is the fraction of those CVEs appearing in CISA KEV catalog (hence $1 + \kappa_k$ acting as posterior boost for KEVs) and w_k is banking weight from Eq. (2). Min-max normalization of raw exposure E_k to $\tilde{E}_k$ in $[0, 1]$ (the maximum category is valued with 1).

4.3 Decision matrix

A score is assigned to each of twelve candidate investments across eight criteria. Next, a mapping from investment A to relevance for each category (may be modified) computes requirement C1 according to the risk reduction principle and requirement C2 according to the threat-likelihood coverage. Transparent analyst-editable config values for item types include Purchase Order (PO), Software as a Service (SaaS) Subscription, Cloud Usage/License Analysis and C3 to C8 Criteria implementation cost, regulatory and compliance impact, operational resilience, feasibility and time to deployReturn on investment (ROI), strategic alignment. Table 2: Assembled matrix

$$S_i = \sum_{k=1}^K r_{ik} \tilde{E}_k, \quad C_{i1} = 10 \cdot \frac{S_i - S_l}{S_l - S_l} \quad (4)$$

where $r_{ik} \in [0, 1]$ is the adjustable relevance of investment alternative i for attach-type category k and are $\tilde{E}_k$ is the standardized banking exposure from Eq. (3) 2), S_i is the effective risk reduced by alternative i , and C_{i1} is its rescaled risk-reduction score (also normalized to a scale of $[0, 10]$) across the twelve alternatives. C_{i2} is also derived analogously except that the exposure term is now substituted with the likelihood component of category k (mean EPSS probability with the KEV boost), allowing both data-driven criteria to share a scale (0–1) with configuration-based criteria C3 to C8.

4.4 Ranking methods

AHP weights are calculated as the right normalized eigenvector of a pairwise comparison matrix on the Saaty scale, achieving a consistency ratio equal to 0.0085 much lower than the 0.10 threshold of



acceptability. Shannon entropy weights from decision matrix Its mean creates the fused weight vector employed within TOPSIS. Fuzzy-TOPSIS uses triangular fuzzy numbers for the configuration-based criteria and crisp for the data-driven criteria. Additionally, VIKOR is executed as an independent cross-check using a distinct aggregation logic relying on group utility and individual regret. All formulae are detailed in Appendix A.

4.5 Robustness and validation

Four checks are performed. Using 5-fold cross-validation, the network is evaluated against a linear regression baseline on matching features. Third, a multicollinearity diagnostic is inspected using a Pearson correlation matrix across the eight criteria. Lastly, the pairwise Spearman correlation/ Kendall's tau/ Kendall's coefficient of concordance rank agreement measures of all five ranking methods cross method were measured. Fourth, we conduct a sensitivity analysis for the criteria weights by perturbing them one-by-one within ± 10 and 20 percent of base case values and through 200 random multiplicative perturbations, reporting both rank-reversal rate of the top alternative as well as Spearman stability given baseline full ranking.

5. Results

5.1 Risk model

Its held-out split yields a test root-mean-square error of 2.246 (± 0.053), mean absolute error of 1.667 (± 0.0185) and coefficient of determination = 0.136 ($p < 2E-16$). It achieves an R-squared of 0.132 (standard deviation = 0.004) under 5-fold cross-validation, significantly outperforming the linear regression baseline (R-squared = 0.103, standard deviation = 0.002; Table 1 and Figures 1 and 2). Since seven binary technique flags and three text-derived features can explain only small amount of variance on the CVSS base score, so it is unsurprising that the absolute R-squared is modest. However, the goal of the model is to provide a consistent relative ranking of threat classes, not an exceedingly precise point estimate; the low variance across folds indicates that this relative ordering is stable.

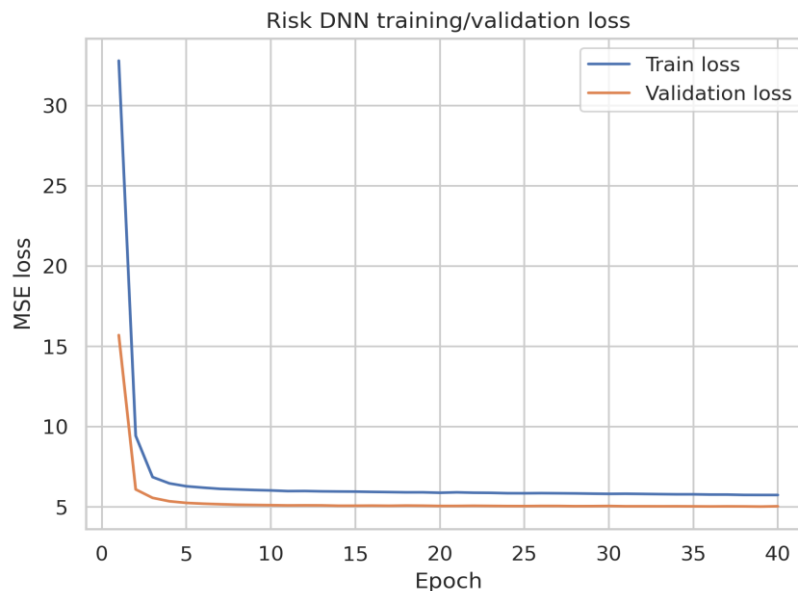


Figure 1: Training and validation loss of the risk-scoring network over 40 epochs, showing convergence without divergence between the two curves.

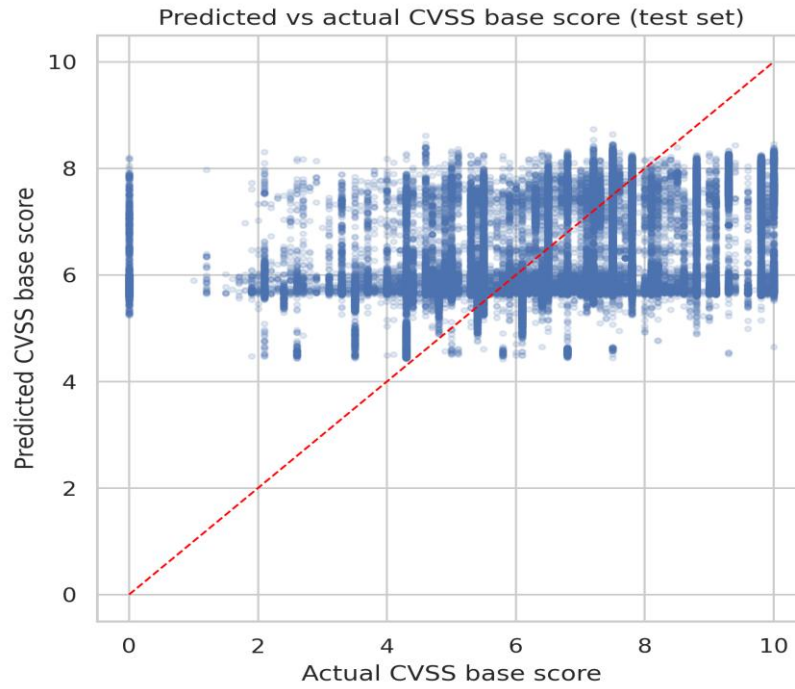


Figure 2: Predicted against actual CVSS base score on the held-out test set, with the identity line shown for reference.

Table 1: Risk-scoring network performance against a linear regression baseline on identical features, for CVSS base-score regression.

Model	Evaluation	RMSE	MAE	R-squared
Risk network	Held-out test split	2.246	1.667	0.136
Risk network	5-fold CV, mean (std)	2.254 (0.008)	1.677 (0.007)	0.132 (0.004)
Linear regression	5-fold CV, mean (std)	2.292 (0.007)	1.721 (0.005)	0.103 (0.002)

5.2 Threat exposure

With a normalized exposure of 1.00, remote code execution leads the banking-weighted profile, and is driven by the incident distribution of the banking sector--where remote-code-execution-mapped varieties have a bank weight (bWeight) of 0.713 for vulnerability exploitation, backdoors, command and control, ransomware. At all remaining categories (also lower than 0.02), privilege escalation follows with a mean of 0.102, and then goes on to name execution, detection avoidance, defense evasion etc. (Table S1 and Figure3). This focus is aligned with the finding that financial-sector incidents are predominantly those triggered by known vulnerabilities and ransomware.

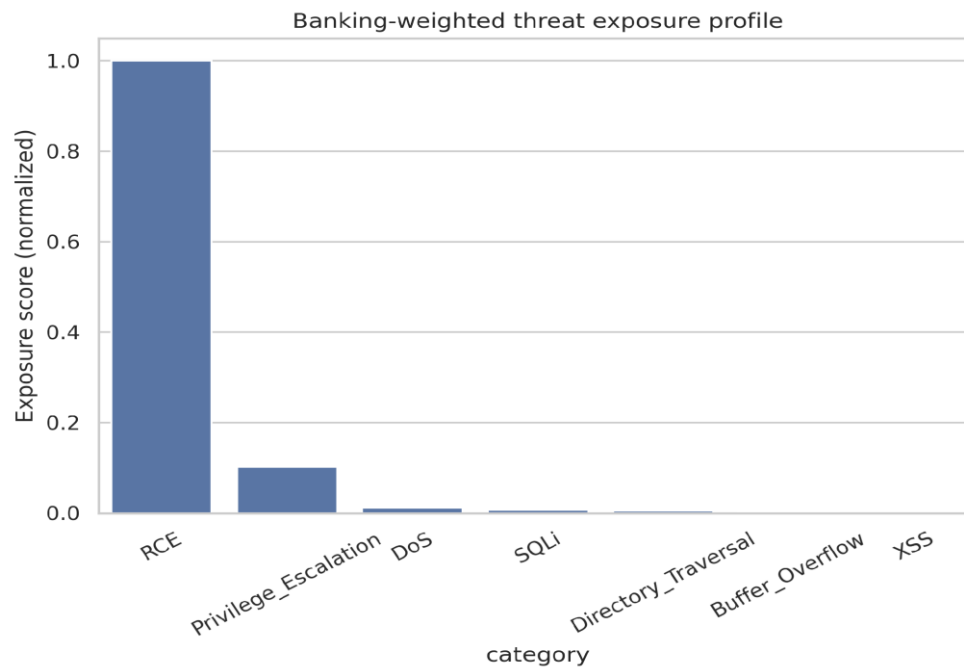


Figure 3: Banking-sector weighted threat-exposure profile across the seven attack-type categories, combining predicted severity, mean EPSS, KEV rate, and incident frequency.

5.3 Criteria weights

The two data-driven criteria, risk reduction (0.220) and threat-likelihood coverage (0.210), have been assigned the highest portion of the weight vector combined with implementation cost (0.163) and feasibility (0.133); The emphasis of comparison in AHP and entropy weightings is not surprising, the first being subjectively and the latter relies on matrix dispersion (Table 3, Figure 4), thus averaging them balances those two perspectives.

Table 3: Criteria weights from AHP, Shannon entropy, and their combined average. AHP consistency ratio equals 0.0085.

Criterion	Name	AHP	Entropy	Combined
C1	Risk reduction	0.213	0.226	0.220
C2	Threat-likelihood coverage	0.175	0.245	0.210
C3	Implementation cost	0.071	0.254	0.163
C4	Regulatory and compliance impact	0.198	0.012	0.105
C5	Operational resilience	0.122	0.030	0.076
C6	Feasibility and time to deploy	0.059	0.206	0.133
C7	ROI and ROSI	0.102	0.011	0.057
C8	Strategic alignment	0.059	0.016	0.038

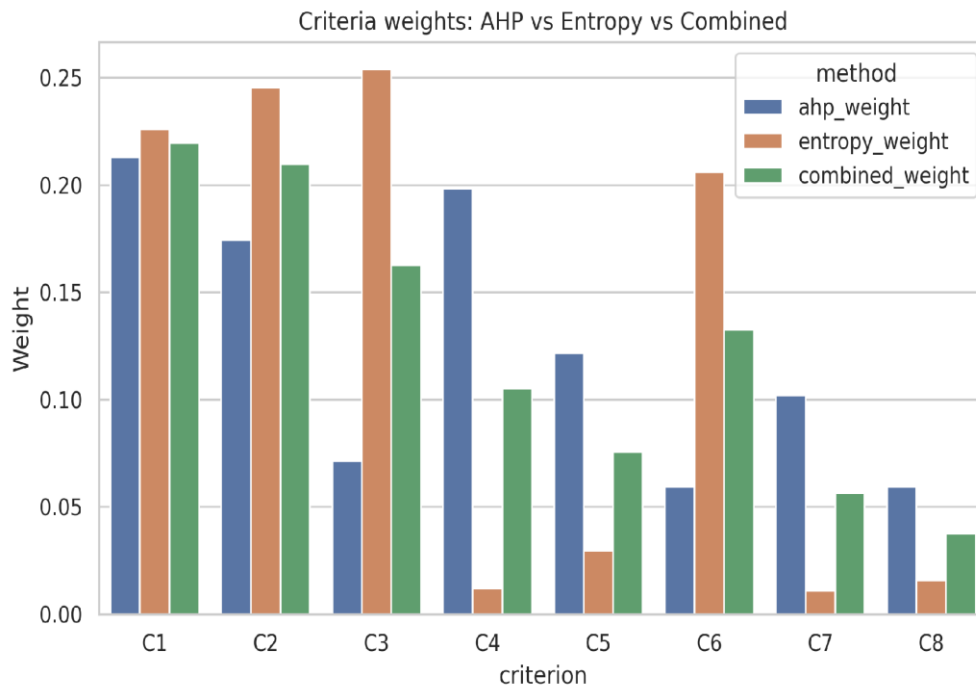


Figure 4: Criteria weights under AHP, Shannon entropy, and their combined average, for all eight decision criteria.

5.4 Decision matrix and ranking

Table 2: Assembled decision matrix of twelve candidate investments against eight criteria. C1 and C2 are data-driven; C3 through C8 are configuration-based. C3 (implementation cost) is a cost criterion where lower is better; the remaining criteria are benefit criteria.

Alternative	C1	C2	C3	C4	C5	C6	C7	C8
EDR/XDR deployment	6.60	10.00	7	7	8	6	8	8
SIEM upgrade	6.05	5.42	8	8	7	7	7	8
MFA rollout	2.52	2.43	3	9	6	3	9	8
Network segmentation	4.86	6.68	6	6	8	7	6	7
Security awareness training	1.22	1.25	2	7	5	2	7	6
Data encryption at rest and in transit	2.67	0.76	5	9	6	5	6	7
Penetration testing program	8.03	6.62	4	7	5	3	6	6
Zero-trust access	5.09	5.71	8	8	8	8	7	9
Vulnerability management platform	10.00	8.92	5	8	7	4	8	8
Cyber insurance	0.00	0.00	4	5	3	2	5	4
IAM/PAM	3.66	4.69	6	9	7	6	8	8
Backup and disaster recovery	1.48	2.73	5	7	9	4	7	7

The vulnerability management platform was scored as the top investment under each tested method (Table 4) using crisp TOPSIS with a closeness coefficient of 0.832, Fuzzy-TOPSIS with a closeness coefficient of 0.093 and VIKOR with an ideal distance of $Q = 0.035$ in satisfied compromise-solution conditions (Figures 6 and 7). The penetration testing program and the EDR/XDR deployment are second and third across methods, with a slight swap between the crisp and fuzzy versions. Under all three methods, cyber insurance consistently ranks worst, consistent with its role as a financial risk transfer, rather than a technical risk reduction.[20]

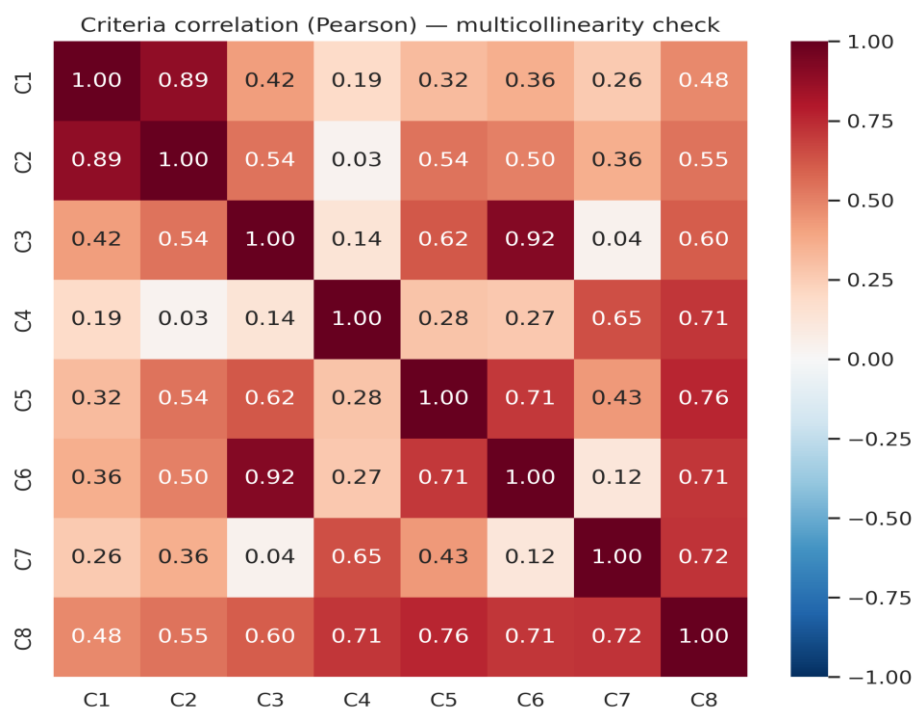


Figure 5: Pearson correlation matrix across the eight decision criteria, used as a multicollinearity diagnostic prior to weighting.

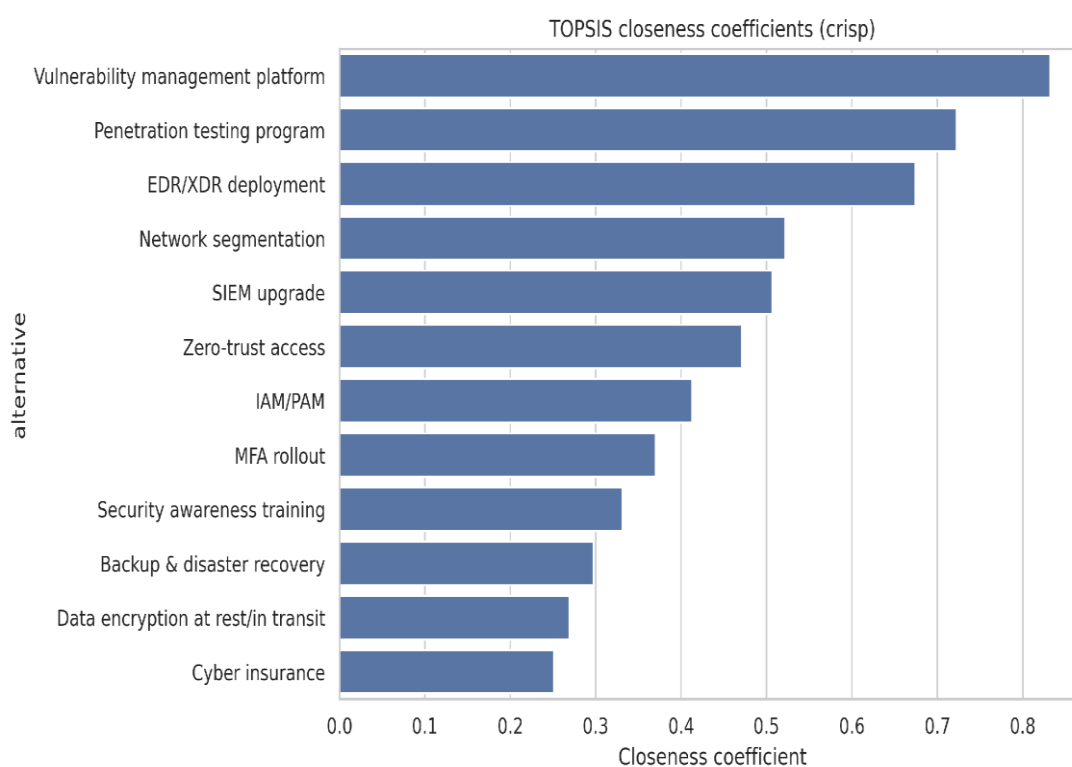


Figure 6: TOPSIS closeness coefficients for all twelve candidate investments under the combined weight vector.



Table 4: Final multi-method ranking. Ranks and scores under crisp TOPSIS, Fuzzy-TOPSIS, and VIKOR for all twelve alternatives.

Alternative	Crisp rank	Closeness	Fuzzy rank	Fuzzy closeness	VIKOR rank	Q
Vulnerability management platform	1	0.832	1	0.093	1	0.035
Penetration testing program	2	0.722	3	0.080	2	0.127
EDR/XDR deployment	3	0.674	2	0.081	3	0.370
Network segmentation	4	0.522	6	0.065	4	0.447
SIEM upgrade	5	0.507	4	0.066	7	0.608
Zero-trust access	6	0.471	5	0.065	8	0.624
IAM/PAM	7	0.413	9	0.062	5	0.484
MFA rollout	8	0.370	7	0.064	6	0.497
Security awareness training	9	0.331	8	0.062	9	0.698
Backup and disaster recovery	10	0.297	10	0.052	10	0.707
Data encryption at rest and in transit	11	0.269	11	0.048	11	0.764
Cyber insurance	12	0.251	12	0.039	12	1.000

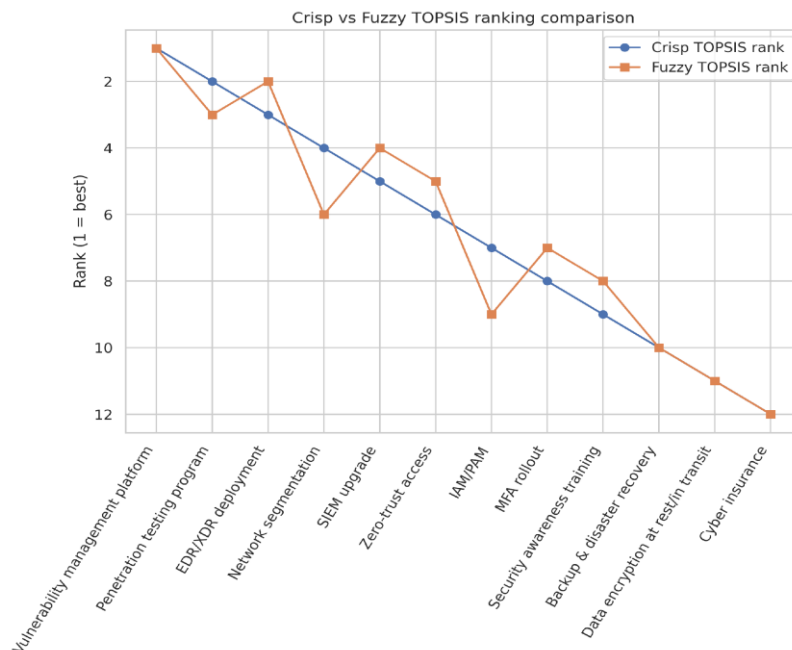


Figure 7: Rank comparison between crisp TOPSIS and Fuzzy-TOPSIS across all twelve alternatives.

5.5 Cross-method robustness

Kendall's coefficient of concordance across the five ranking methods is 0.944, with pairwise Spearman correlation ranging from 0.90 to 0.97 (Table 5, Figure 8). This very strong agreement indicates that the recommended ranking is not an artifact of any single method's aggregation logic.[21]



Table 5: Robustness and validation summary across the five ranking methods and the sensitivity analysis.

Metric	Value	Interpretation
Kendall's W across 5 ranking methods	0.944	Very strong concordance
Mean pairwise Spearman across methods	0.90 to 0.97	High correlation between every pair
Rank-reversal rate of top alternative (232 trials)	0.0	Top alternative never changes
Mean full-ranking Spearman vs baseline (one-at-a-time)	0.999	Ordering essentially unchanged
Mean full-ranking Spearman vs baseline (random)	0.997	Ordering essentially unchanged
Minimum Spearman observed across all trials	0.986	Worst case still near-identical
AHP consistency ratio	0.0085	Well below the 0.10 threshold

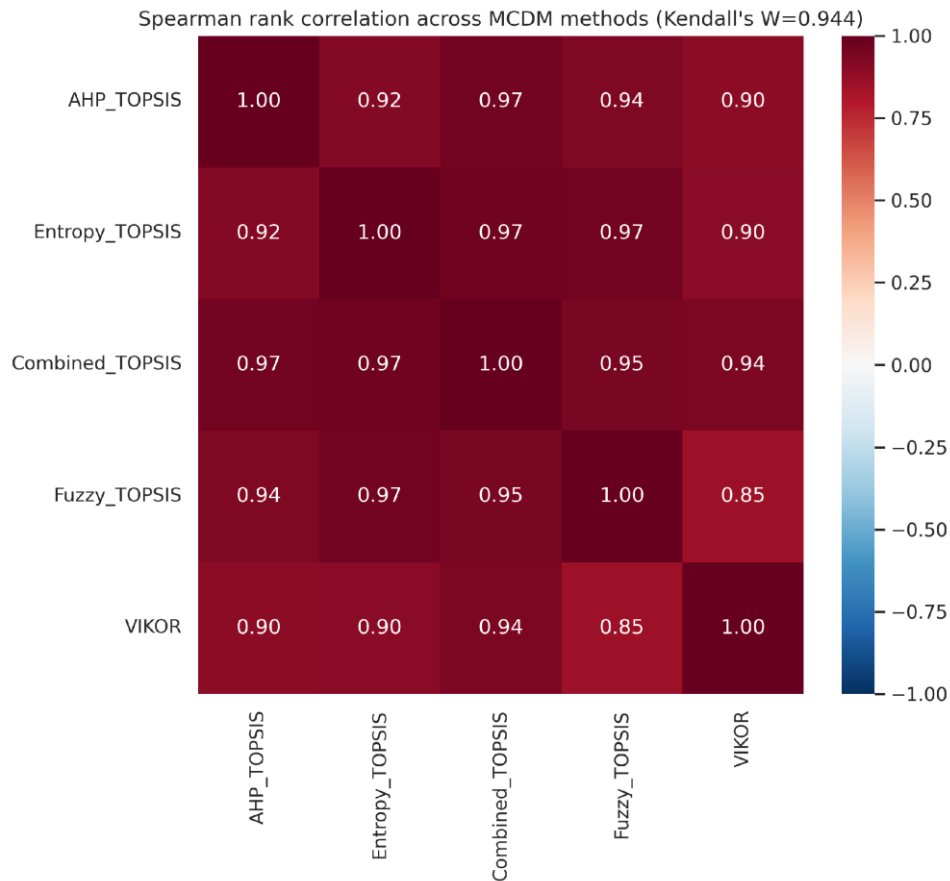


Figure 8: Spearman rank correlation across the five ranking methods, with Kendall's W of 0.944 annotated.

8. Conclusion

We provide a data-driven multi-criteria framework to prioritize cybersecurity investment in banking, which grounds its two most measurable criteria on real threat-intelligence data via a GPU-trained network, keeps the remaining criteria transparent and editable, and validates its recommended ranking across five independent methods and a widespread sensitivity analysis. The framework provides a robust ranking, headlined by a vulnerability management platform, that is stable to weighting and



aggregation choices for the data used here.[22] Rather than an autonomous decision-making entity, the framework is meant as a clear and audit-friendly foundation for investment discussion associated with configuration files; these are the vehicle through which a bank would translate its own numbers into something useful. In future work, we will populate the generic configuration with institution-specific data and augment the risk model with additional features, and produce a validation of our framework against realised security outcomes.

References

1. L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438-457, 2002.
2. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Systems*, vol. 86, pp. 13-23, 2016.
3. L. P. Rees, J. K. Deane, T. R. Rakes, and W. H. Baker, "Decision support for cybersecurity risk planning," *Decision Support Systems*, vol. 51, no. 3, pp. 493-505, 2011.
4. A. Ganin, P. Quach, M. Panwar, Z. A. Collier, J. M. Keisler, D. Marchese, and I. Linkov, "Multicriteria decision framework for cybersecurity risk assessment and management," *Risk Analysis*, vol. 40, no. 1, pp. 183-199, 2020.
5. R. Goel, A. Kumar, and J. Haddow, "PRISM: a strategic decision framework for cybersecurity risk assessment," *Information and Computer Security*, vol. 28, no. 4, pp. 591-625, 2020.
6. T. L. Saaty, *The Analytic Hierarchy Process*. New York, NY: McGraw-Hill, 1980.
7. T. L. Saaty, "How to make a decision: the analytic hierarchy process," *European Journal of Operational Research*, vol. 48, no. 1, pp. 9-26, 1990.
8. C. L. Hwang and K. Yoon, *Multiple Attribute Decision Making: Methods and Applications*. Berlin, Germany: Springer-Verlag, 1981.
9. C. T. Chen, "Extensions of the TOPSIS for group decision-making under fuzzy environment," *Fuzzy Sets and Systems*, vol. 114, no. 1, pp. 1-9, 2000.
10. S. Opricovic and G. H. Tzeng, "Compromise solution by MCDM methods: a comparative analysis of VIKOR and TOPSIS," *European Journal of Operational Research*, vol. 156, no. 2, pp. 445-455, 2004.
11. C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379-423, 1948.
12. M. Zeleny, *Multiple Criteria Decision Making*. New York, NY: McGraw-Hill, 1982.
13. D. Diakoulaki, G. Mavrotas, and L. Papayannakis, "Determining objective weights in multiple criteria problems: the CRITIC method," *Computers and Operations Research*, vol. 22, no. 7, pp. 763-770, 1995.
14. P. Mell, K. Scarfone, and S. Romanosky, "Common Vulnerability Scoring System," *IEEE Security and Privacy*, vol. 4, no. 6, pp. 85-89, 2006.
15. J. Jacobs, S. Romanosky, I. Adjerid, and W. Baker, "Improving vulnerability remediation through better exploit prediction," *Journal of Cybersecurity*, vol. 6, no. 1, tyaa015, 2020.
16. J. Jacobs, S. Romanosky, B. Edwards, I. Adjerid, and M. Roytman, "Exploit Prediction Scoring System (EPSS)," *Digital Threats: Research and Practice*, vol. 2, no. 3, article 20, 2021.
17. G. Spanos and L. Angelis, "A multi-target approach to estimate software vulnerability characteristics and severity scores," *Journal of Systems and Software*, vol. 146, pp. 152-166, 2018.
18. Z. Han, X. Li, Z. Xing, H. Liu, and Z. Feng, "Learning to predict severity of software vulnerability using only vulnerability description," in *Proc. IEEE International Conference on Software Maintenance and Evolution (ICSME)*, 2017, pp. 125-136.
19. Verizon, "2021 Data Breach Investigations Report," Verizon Business, 2021.
20. Hossain, I., Lindon, A. R., Rahman, M., Khan, H. A., Tohfa, N. A., Shagar, M. T. M., ... & Nasif, M. R. I. (2026). Hybrid ensemble learning for robust DDoS detection and attack classification with a web-based analytical tool for cybersecurity analysts. *Journal of Electrical Engineering*, 11(5).



21. Chy, M. S. K., Abdullah, S. M., Nabil, M. A., Alam, A., Himeluzzaman, M., Onik, T. A., ... & Khan, H. A. (2022). QShield-NS: A variational quantum machine learning model for zero-day cyber threat detection in national security systems. *International Journal of Future Innovative Science and Technology (IJFIST)*, 5(5), 9283.
22. Hossain, M. S., Biswas, B., & Rahaman, M. M. (2023). THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENHANCING CYBERSECURITY DEFENSE MECHANISMS. *International Journal Of Engineering Technology Research & Management (IJETRM)*, 7(07), 157-166.