Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P5785-cd

Using Simplified Metrics for Cost-Benefit Analysis (CBA) and Pareto Optimality in Physical Security Concepts

Thomas Termin

Institute for Security Systems, University of Wuppertal, Germany. E-mail: thomas.termin@gmx.de.

Dustin Witte

Institute for Security Systems, University of Wuppertal, Germany. E-mail: witte@uni-wuppertal.de.

Daniel Lichte

Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center, Germany. E-mail: daniel.lichte@dlr.de.

Kai-Dietrich Wolf

Institute for Security Systems, University of Wuppertal, Germany. E-mail: wolf@iss.uni-wuppertal.de.

Critical infrastructures (CRITIS), as the backbone of our society, must be safeguarded against attacks through effective security measures. Since implementing such measures often entails significant costs, it is essential to provide tools that enable operators to make well-informed decisions based on objective analyses. A sound decision, from the operator's perspective, balances the costs of investing in security measures with benefits such as risk reduction. Quantitative metrics are a widely used tool in CRITIS risk assessment, valued for their ability to deliver objective, comparable, and reproducible results. However, these metrics can be challenging for users and decision-makers to manage, especially when quantitative data is unavailable or in instances where only a rudimentary assessment is requested. A simpler alternative is scoring, which categorizes security contributions using expert knowledge. Yet, due to the inherent uncertainty of scoring, it becomes crucial to determine the conditions under which cost-benefit analyses (CBA) can yield results comparable to those of quantitative assessments. This paper builds on prior work by Termin et al. (2024, a) and Witte et al. (2024), demonstrating how scoring-based assessments of physical vulnerability can be adapted to assess potential attack paths within an exemplary series-connected barrier topology. This approach aims to identify Pareto-optimal configurations of security measures. Ultimately, it is expected that this straightforward scoring-based methodology will assist users in optimizing physical security concepts more effectively.

Keywords: Metrical Analysis, Physical Security, Vulnerability Analysis, Decision-Making, Generic Approach.

1. Introduction

The increasing threat landscape (Mathas et al., 2020) and the enactment of regulatory requirements for conducting physical security assessments (Izuakor & White, 2016) present critical infrastructure operators with the challenge of finding suitable tools to produce results that are as objectively reproducible as possible and scalable to different topologies, which can be used as a basis for deciding whether to invest in security measures (Yusta et al., 2011).

There are already validated approaches for performing quantitative assessments, such as those developed by Lichte et al. (2019). In practice, however, scoring-based approaches that use expert knowledge to categorize security contributions and aggregate them into an overall score are increasingly used, see e.g. Chauke & Mphadzha (2022) and Harnser (2010). Compared to quantitative methods, scorings have the advantage that they are often more intuitive and easier to understand, especially for people without deep mathematical knowledge.

They allow for a quick assessment based on predefined criteria presented in the form of scores (Krisper, 2021). Scoring systems also make it

easier to prioritize risks and actions, as decision makers can easily identify which areas require the most attention based on simple calculations using the score assigned. By their very nature, scoring systems are inherently uncertain. This uncertainty results from several factors.

First, scores involve a range of subjective judgments that can be influenced by individual interpretations and experiences. This is because scoring systems generally lack an underlying (objective) metric that measures the differences between scores using data and numbers. This means that it is not possible to make a general statement that a score of "2" is twice as high as a score of "1" (Braband, 2008).

Quantitative assessments, in contrast, are predicated on scientific models that can be analyzed with the aid of stochastic tools. By contrast, scorings can amalgamate disparate types of data and expert knowledge and can be structured in a multitude of complicated ways. The metric algorithm, i.e., the injection of expert knowledge into the metric to obtain a result score, can theoretically be n-step and not based on real (attack) processes. Consequently, there is a possibility for discrepancies between the outcomes of quantitative metrics and scoring-based metrics. This has led to the hypothesis that poor security decisions could be made with scoring-based assessment approaches, as evidenced by Termin et al. (2023), Braband (2008), and Krisper (2021).

From the user's perspective, there is therefore a need for a user-friendly assessment methodology that can be applied to different use cases (topologies of infrastructure elements) and can reflect the results of quantitative metrics under defined boundary conditions. This is a prerequisite for being able to make good decisions regarding investment in security measures.

The quality of a decision is contingent upon the acceptance by the decision-maker of the ratio of costs (damage or expenditure for the implementation of security measures) and benefits (in the form of risk reduction caused by security measures). The applicability of simple scorings when conducting cost-benefit analyses (CBA) in physical security assessments must therefore be carefully considered. This paper is dedicated to this question, and the results are summarized and discussed at the end of this contribution.

2. Background

The application of cost-benefit analysis (CBA) and the principle of Pareto optimality are crucial for designing effective security measures – that is, measures that reduce risk – and efficient security measures – that is, measures that optimize cost (Boardman, 2008; Sun et al., 2018).

In the context of physical security assessments, a CBA endeavors to quantify the trade-offs between the costs of implementing security measures and the benefits derived in the form of reduced risks and potential loss reduction. The fundamental objective of CBA is to ensure that the limited resources allocated to security barriers are commensurate with the anticipated risk reduction (Hicks et al., 1997).

The CBA process involves the collection of detailed data on the frequency of potential threats, the impact of security measures on potential attacks (e.g. resistance against overcoming attempts), and the expected consequences in case of a successful attack. This comprehensive data set is then used to assess risk. Traditionally, risk is determined by integrating threat, vulnerability, and consequences. If the three elements are strictly independent of each other, then risk can be expressed as a product of threat, vulnerability, and consequences.

The elicitation of CBA-related information can be particularly challenging due to the variability of threats and the unpredictability of attacks (Wyss et al., 2010). To address the challenge of threat-inherent epistemic uncertainty, the risk formula can be simplified by assuming that the threat scenario under consideration is certain to occur, i.e., the probability of the threat is $p = 1$ (100%).

This approach enables the operator to concentrate their risk assessment on the elements that can be influenced by security measures. This is predicated on the assumption that the efficacy of security measures and the ramifications of a successful attack can be evaluated through the application of expert knowledge. From a worst-case perspective, it can also be assumed that there is a maximum monetary value for the consequences of a specific successful attack.

It is imperative to regard the consequences as a scalar variable, which can be incorporated as a constant into the costs of the security measures. That is to say, the severity of the consequences directly correlates to the total costs, which follows

a linear relationship. These boundary conditions enable the execution of a CBA to assess the risk contribution of vulnerability (at the physical security concept level). Within the CBA framework at the security concept level, the vulnerability of each security measure configuration is evaluated in relation to the costs of the security measures, expressed in the form of a matrix.

The objective is to identify configurations that exhibit minimal costs while maintaining an acceptable vulnerability level, such as 10% from the operator's perspective. An optimal configuration of measures in the CBA is therefore described as Pareto-efficient if no reduction in physical vulnerability is possible without increasing the cost of security measures to an extent that is not accepted by the decision-maker (Ojamaa et al., 2008).

Quantitative approaches are traditionally used to justify investment in security measures. However, these methods are often characterized by complexity and intricacy, potentially hindering their accessibility and actionability for CRITIS security decision makers in comparison to scoring-based approaches. The risk-appropriate design of scoring metrics is a challenge that has already received initial attention in functional safety, e.g., from Braband (2008) or Krisper (2021).

In the context of CRITIS's physical security assessment, this subject matter is novel. Earlier contributions, including those by Termin et al. (2023) and Termin et al. (2024), examined the adaptability of a scoring metric's rating scale for assessing physical vulnerability to specific barrier types or measure configurations, using a quantitative assessment metric to inform the calculation results. Termin et al. (2024) demonstrate how properties of security measures available to a CRITIS operator can be transferred as input to a scoring-based metric for assessing physical vulnerability of specific barrier types.

Accordingly, a locally adjusted vulnerability scale can be developed for each barrier of a CRITIS, which can be used to replicate the calculation results of a quantitative metric. This approach entails the isolation of the vulnerability adjustment process for each barrier of a designated attack path, thereby excluding the consideration of residual protection time along the attack path.

This paper builds on these considerations and investigates how scorings can also be used to make global adjustments to the vulnerability scales in which the path-specific residual overcoming time is included. The assessment methodology developed will serve as the foundation for conducting a CBA using scorings.

4. Approach

The following steps are conducted in this paper to investigate the research question of how large the differences are between a quantitative CBA and an adjusted, scoring-based CBA:

(1) The exemplary system architecture is defined, as are the constraints for scoring.
(2) Implementation of a CBA assuming the locally adjusted vulnerability approach according to Termin et al. (2024).
(3) Implementation of a CBA assuming the globally adjusted vulnerability approach, which is introduced in this paper.
(4) Summarizing and discussing the results.

4.1. System Assumptions

The infrastructure under consideration, illustrated in Figure 1, consists of the barriers B0, B1, B2, B3, and the asset A. The attack path under consideration is assumed to be B0-B1-B2-B3-A, i.e., the attacker must overcome all four barriers to reach his target. It is further assumed that the physical vulnerability is assessed along this attack path.

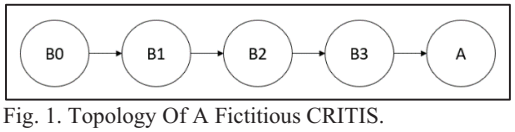

Fig. 1. Topology Of A Fictitious CRITIS.

The scoring-based Harnser metric (Harnser, 2010) and the quantitative Intervention Capability Metric (ICM) according to Lichte et al. (2016) are used to assess physical vulnerability. In the Harnser metric, the three vulnerability contributions of protection, observation, and intervention are traditionally scored on a scale of "1" to "5", and then aggregated to derive an overall vulnerability score. The underlying assumptions are as follows: (a) The higher the

score, the better the security measure. To illustrate, a protection score of "1" signifies minimal protection, while a score of "5" denotes optimal protection. (b) A high vulnerability score indicates low vulnerability or high measure effectiveness, while a low vulnerability score indicates high vulnerability. (c) An existing security measure is assigned to a single score.

The ICM conceptualizes an attack scenario as a temporal process, commencing with the first barrier being overcome and culminating in the asset being reached. During this attack, the defender must first recognize the attacker as such before intervening. The ICM assesses an attack path as vulnerable if the attacker reaches the asset faster than the defender reaches the attacker for successful intervention.

The following assumptions are made:

(a) The attack is regarded as unidirectional, meaning that an attacker selects an initial attack path and advances along it until reaching the asset, without returning via the same path.
(b) In the ICM, a security measure is assigned to a probabilistic density function to account for uncertainties in the performance of the security measure under consideration.
(c) The assumption is made that normally distributed variables are employed for protection, observation, and intervention, which can be characterized by a variance and a standard deviation.
(d) Each Harnser score is assigned to a "time" (a probabilistic density function) in the ICM.
(e) The vulnerability contributions are abbreviated as follows: Protection is represented by P, Observation by O, and Intervention by I. The time t is specified in seconds.

The implementation of a CBA entails the introduction of monetary costs for the security measures employed. The following assumptions are made:

(a) Only vulnerability contributions with multiple options incur a cost amounting to monetary units.
(b) The costs of vulnerability contributions with only one option are negligible. This assumption may not be realistic, yet it is ultimately inconsequential to the resultant findings.
(c) Intervention costs along the entire attack path under consideration, B0-B1-B2-B3-A, are only considered once.

The assumptions employed for the assessment of the fictitious system under consideration are summarized in Table 1.

Table 1. Assumptions For The CRITIS Topology Assessment Under Consideration.

Barrier 0: Mapping of Harnser Scores to Probability Density Functions (PDF) of normal distributions with given mean and variance, and to Costs in Money Units.			
Score	t_P	t_O	t_I
1	N(250, 60^2)	N(100, 60^2)	N(300, 60^2)
2			N(240, 60^2)
3			N(100, 60^2)
1	0	0	100000
2			125000
3			200000
Barrier 1: Mapping of Harnser Scores to PDF and to Costs in Money Units.			
Score	t_P	t_O	t_I
1	N(200, 60^2)	N(100, 60^2)	N(300, 60^2)
2			N(240, 60^2)
3			N(100, 60^2)
1	0	0	0
2			0
3			0
Barrier 2: Mapping of Harnser Scores to PDF and to Costs in Money Units.			
Score	t_P	t_O	t_I
1	N(250, 60^2)	N(100, 60^2)	N(300, 60^2)
2	N(300, 60^2)		
3	N(350, 60^2)		
1	10000	0	0
2	40000		
3	60000		
Barrier 3: Mapping of Harnser Scores to PDF and to Costs in Money Units.			
Score	t_P	t_O	t_I
1	N(100, 60^2)	N(100, 60^2)	N(300, 60^2)
2	N(130, 60^2)		
3	N(200, 60^2)		
1	5000	0	0
2	20000		
3	30000		

The potential configurations of security measures per barrier are illustrated in Table 2 for illustrative purposes.

Table 2. Possible Configurations (Permutations) per Barrier on the Example of Barrier 0.

P	O	I
1	1	1
1	1	2
1	1	3

To generate all permissible combinations, the distinct scores for the barriers B0, B1, B2, and B3 are amalgamated in accordance with the stipulated criteria:

(a) For B0 and B1: P = 1, O = 1, I can be 1, 2, or 3.
(b) For B2 and B3: P can be 1, 2, or 3, O = 1, and I = 1.

For B0 and B1, three possible combinations exist since I can take three different values: 3 (for B0) × 3 (for B1). The number of possible combinations for B2 is three, and the number of possible combinations for B3 is three, as P can take three different values: 3 (for B2) × 3 (for B3).

The total number of variants is calculated by multiplying the possibilities for each barrier: 3 (for B0) × 3 (for B1) x 3 (for B2) × 3 (for B3) = 81. The complete list of combinations is therefore 81 (= 34).

3.2. CBA With The Approach Of Local Vulnerability Adjustment

First, the approach of local adjustment of scoring-based vulnerability scales according to Termin et al. (2024) is applied to the application example. In this approach, barriers are regarded as "isolated" units, without considering the attack path-dependent residual protection time.

Given that the score sum of the vulnerability contributions at B0 ranges from "3" to "5" and the reliability of the scoring results according to Harnser in replicating the quantitative outcomes of the ICM is not yet established, a uniform distribution of 100% probability is assigned to the scores. The vulnerability scoring table can be found in Table 3.

Table 3. Reference Vulnerability Scoring Table For Barrier 0.

V Score (P, O, I Score Sum)	3	4	5
Lower Interval Limit (LIL) in %	61	31	0
Upper Interval Limit (UIL) in %	100	60	30

The subsequent mapping of scores to probabilistic density functions in the ICM is selected for the calculation (see Table 4 for comparison):

Table 4. Mapping of Scores of P, O, and I of B0 to PDF for the ICM.

B0		
P	O	I
1	1	1
1	1	2
1	1	3
ICM Configuration 0		
t_P	t_O	t_I
N(250, 60^2)	N(100, 60^2)	N(300, 60^2)
N(250, 60^2)	N(100, 60^2)	N(240, 60^2)
N(250, 60^2)	N(100, 60^2)	N(100, 60^2)

The scoring adjustment approach, as outlined by Termin et al. (2023), involves the calculation and comparison of vulnerability metrics across all possible combinations. The ICM provides the results in Table 5:

Table 5. ICM Config 0: Vulnerability Calculation.

Score	V_B0, ICM Config 0	Costs_B0
3	0.9284129889613206	100000
4	0.814211201570481	125000
5	0.3416122167617115	200000

A comparison of the ICM results with the scoring-based results reveals significant disparities, as illustrated in Figure 2.

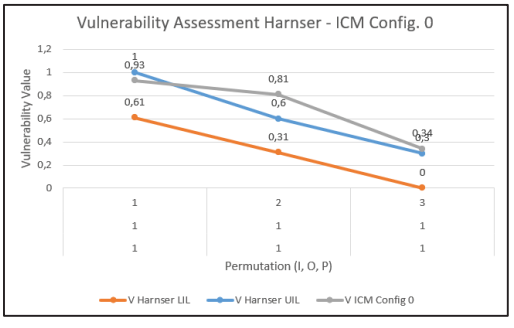

Fig. 2. Vulnerability Results For All B0 Combinations (UIL: Upper Interval Limit, LIL: Lower Interval Limit).

The adjustment of the scoring system is illustrated in Table 6.

Table 6. Vulnerability-Adjusted Harnser Scale (V: Vulnerability).

V Harnser LIL	V Harnser UIL	V ICM Config 0	V Harnser Adjusted
0.61	1	**0.93**	**0.93**
0.31	0.6	**0.81**	**0.81**
0	0.3	**0.34**	**0.34**

The adjustment can be conducted as in Table 6, as each permutation generates a clearly distinguishable vulnerability score that occurs only once and leads to a vulnerability interval that is also clearly distinguishable from the other vulnerability intervals. Consequently, a vulnerability value of the ICM can be distinctly assigned to a score. Consequently, the results of the scoring process and those of the ICM are identical in this instance, as illustrated in Figure 3.

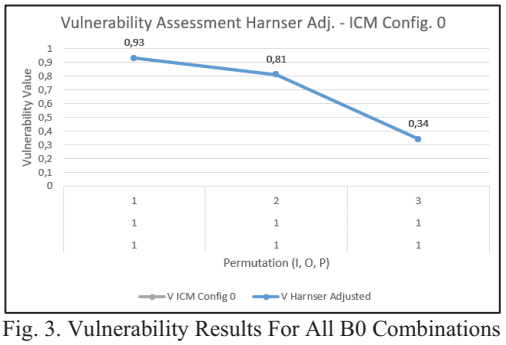

Fig. 3. Vulnerability Results For All B0 Combinations (ICM And Adjusted Harnser Metric).

As barrier B0 to barrier B3 each have three permissible permutations that generate a scoring result that does not occur twice, an adjusted Harnser metric or vulnerability scale can be generated for all four barriers that delivers identical results to the ICM. Consequently, the scoring results in further analysis (assessment of the attack path B0 to B3, including the CBA) are identical to a genuine quantitative assessment. That is to say, no difference can be determined between the ICM and the scoring for the exemplary system setup defined in this work.

3.3. CBA With The Approach Of Global Vulnerability Adjustment

In global adjustment, the barriers of the attack path under consideration are not regarded as isolated units, but rather as a composite (see Figure 4). Of particular relevance to the CBA is the aggregate vulnerability of the path, taking into account the path-dependent residual protection time.

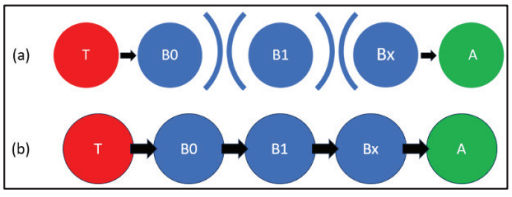

Fig. 4. Comparison Of The Attack Models In The Variants (a) Local Adjustment And (b) Global Adjustment.

In the context of the global adjustment of the Harnser scoring, it is imperative to recognize that the summation of the barrier-specific scores pertaining to protection, observation, and intervention must be recalibrated. Instead, the aggregate sum of the scores associated with all security measures implemented in each configuration must be calculated (refer to Table 7 for a detailed comparison). In this particular use case, a scoring range of "12" to "20" is attainable.

If the global Harnser scale consists of a total of nine categories ("12" to "20"), then according to the approach of Termin et al. (2023), 100% probability is distributed equally among the nine categories (100%/9 ≈ 11.11%) in an initial step. This approach culminates in the correlations depicted in Table 8.

Table 7. Example of Global Harnser Scoring.

B3.P	B0-B3 else	Global Sum Score	Total Costs in Money Units
1	1	12	115000
2	1	13	130000
3	1	14	140000

Table 8. Global Harnser Vulnerability Scale (Equal distribution of 100 % to the sum scores).

Global Sum	12	13	14	…	20
UIL	1	0.8888	0.7777	…	0.1111
LIL	0.8889	0.7778	0.6667	…	0

To execute the global adjustment to the Harnser scoring, the overall vulnerability of the pathway is calculated for all possible configurations using both metrics. This calculation is performed along the path in contrast to the calculation of vulnerability at a single barrier. Please refer to Table 9 for a comparison of the two metrics.

Table 9: Overall Vulnerability of the Attack Path Exemplarily Calculated With The Scoring Metric And The ICM. *Else* does mean "all other configuartions".

B3.P	B0-B3 (else)	Global Sum Score	Total V ICM
1	1	12	0.000358223
2	1	13	0.001108684
3	1	14	0.000358223
B3.P	**B0-B3 (else)**	**Harnser LIL**	**Harnser UIL**
1	1	0.8889	1
2	1	0.7778	0.8888
3	1	0.6667	0.7777

Subsequently, a comparison of the results with each other is conducted, and the assumed probability intervals behind the score categories "12" to "20" of the Global Harnser Vulnerability Scale in Table 9 are adjusted to the quantitative results (see also Termin et al., 2023). This adjustment results in the new correlations presented in Table 10.

Table 10. Adjusted Global Harnser Vulnerability Scale.

Globa	12	13	14	…	20
UIL	0.00035	0.001108	0.003376	…	0.000358
LIL	0.00035	0.000696	0.000358	…	0.000358

As demonstrated in Figure 5, the adjustment was executed successfully. Concretely, this indicates that the adjusted scoring for this particular use case exhibits a maximum deviation of 1.2% compared to the quantitative calculation. While this may appear negligible, it is important to note that this 1.2% discrepancy encompasses the entire range of possible ICM values, indicating that the lowest and highest values differ by a similar margin.

In summary, the scoring system's performance is contingent on the specific context; in some instances, it provides a reliable approximation of quantitative results, while in others, it does not.

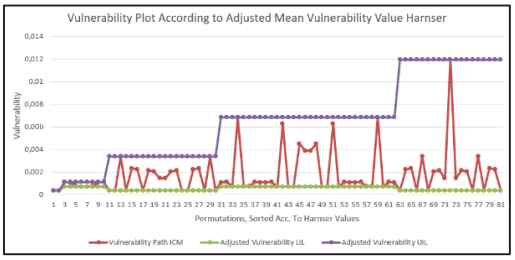

Fig. 5. Plot of Vulnerability Values, ICM and Globally Adjusted Harnser Scores.

Subsequent to the preceding steps, the actual CBA can be conducted. To achieve this objective, the vulnerability values are initially grouped according to cost (see Table 11).

Table 11. Grouped Vulnerability Values According To Costs (Excerpt).

Total Costs In Money Units	**Vulnerability Path ICM**		
115000	0.00035822	0.00075961	0.00035822
130000	0.00110868	0.00235114	0.00110868
140000	0.00035822	0.00075961	0.00035822
Total Costs In Money Unity	**Mean Vulnerability Harnser Adjusted**		
115000	0.00035822	0.00090255	0.00186715
130000	0.00090255	0.00186715	0.00376834
140000	0.00186715	0.00376834	0.00615817

To illustrate the disparities between the quantitative CBA based on the ICM and the scoring-based CBA based on the globally adjusted Harnser metric, two matrices are constructed. In the initial matrix, the vulnerability values, determined through quantitative means, are plotted against the costs associated with the respective configurations (refer to Figure 6). The second matrix plots the vulnerability values determined by means of scoring against the costs for the corresponding configurations (see Figure 7).

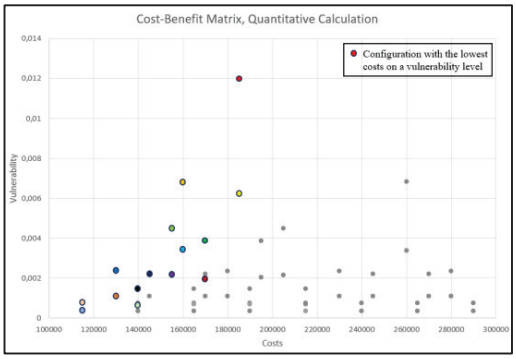

Fig. 6. Quantitative Cost-Benefit Matrix For The Exemplary Use Case.

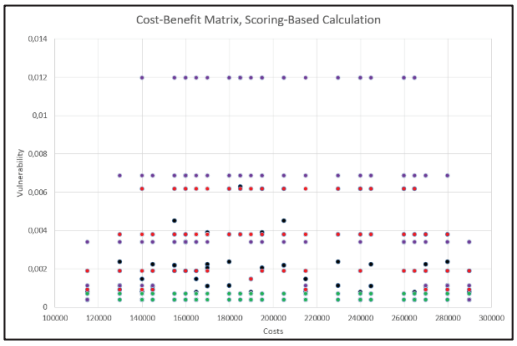

Fig. 7. Scoring-based Cost-Benefit Matrix (Black: Quantitative Value, Red: Mean Harnser, Violet: Upper Limit Harnser, Green: Lower Limit Harnser).

4. Summary

This research introduces a simplified scoring-based approach to CBA, with the objective of facilitating more practical and accessible decision-making for security investments. It addresses the complexity of traditional quantitative methods, offering a user-friendly framework suited for security professionals in CRITIS use cases. While the approach simplifies calculations, its practical implementation poses challenges. The adaptation of the scoring system to quantitative methods or different infrastructure configurations necessitates adjustments.

The vulnerability scores derived from this study, while beneficial in certain scenarios, may not consistently provide optimal decision-making support, particularly when strict vulnerability acceptance thresholds are employed. Future research endeavors will further explore the adaptability of this scoring-based approach to other use cases and refine its application for broader contexts.

References

Boardman, A. E. (2008). Cost benefit analysis. Pearson Education India.

Braband, J. (2008). Beschänktes Risiko. QZ. Qualität und Zuverlässigkeit 53.2 (2008): 28-33.

Chauke, M. D., & Mphadzha, F. R. (2022). Framework for critical infrastructure security rating.

Harnser Group (2010). A Reference Security Management Plan for Energy Infrastructure. European Commission.

Hicks, M. J., Yates, D., & Jago, W. H. (1997). Cost and performance analysis of physical security systems (No. SAND-97-1353C; CONF-9706109-4). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

Izuakor, C., & White, R. (2016). Critical infrastructure asset identification: policy, methodology and gap analysis. In Critical Infrastructure Protection X: 10th IFIP WG 11.10 International Conference, ICCIP 2016, Arlington, VA, USA, March 14-16, 2016, Revised Selected Papers 10 (pp. 27-41). Springer International Publishing.

Krisper, M. (2021). Problems with Risk Matrices Using Ordinal Scales. arXiv preprint arXiv:2103.05440.

Lichte, D., S. Marchlewitz and K.-D. Wolf (2016). A Quantitative Approach to Vulnerability Assessment of Critical Infrastructures With Respect to Multiple Physical Attack Scenarios. In: Future Security 2016, Proc. intern. conf., Berlin, Germany.

Lichte, D., Witte, D., & Wolf, K. D. (2019, September). An approach to software assisted physical security risk analysis and optimization. In 29th European Safety and Reliability Conference (ESREL 2019), Beer, M. & Zio, E.(Eds.) Hannover, Germany (pp. 3943-3949).

Mathas, C. M., Grammatikakis, K. P., Vassilakis, C., Kolokotronis, N., Bilali, V. G., & Kavallieros, D. (2020, August). Threat landscape for smart grid systems. In Proceedings of the 15th international conference on availability, reliability and security (pp. 1-7).

Ojamaa, A., Tyugu, E., & Kivimaa, J. (2008, November). Pareto-optimal situaton analysis for selection of security measures. In MILCOM 2008-2008 IEEE Military Communications Conference (pp. 1-7). IEEE.

Sun, Y., Xiong, W., Yao, Z., Moniz, K., & Zahir, A. (2018). Analysis of network attack and defense strategies based on Pareto optimum. Electronics, 7(3), 36.

Termin, T., D. Lichte and K.-D. Wolf (2023). Risk Adjusting of Scoring-based Metrics in Physical Security Assessment. In: Proceedings of the 32th European Safety and Reliability Conference and 18th Probabilistic Safety Assessment and Management Conference.

Wyss, G. D., Clem, J. F., Darby, J. L., Dunphy-Guzman, K., Hinton, J. P., & Mitchiner, K. W. (2010, October). Risk-based cost-benefit analysis for security assessment problems. In 44th Annual 2010 IEEE International Carnahan Conference on Security Technology (pp. 286-295). IEEE.

Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. Energy policy, 39(10), 6100-6119.