A Capability-based Approach to Evaluate and Mitigate Identified Cybersecurity Gaps in Critical Infrastructures

Eetu Laakso[1], Vesa Kuikka[2] and Kimmo K. Kaski[2]
[1]Cyberwatch Finland Oy, Helsinki, Finland
[2]Department of Computer Science, Aalto University School of Science, Finland

eetu@cyberwatchfinland.fi
vesa.kuikka@aalto.fi
kimmo.kaski@aalto.fi

Abstract: Recently, the number of cyber threats has shown a rapid increase all over the world. Different public and private infrastructure organisations of a society have varying capabilities and resources to address these threats and protect themselves from their harmful impact. Among these sectors, critical infrastructures are most vulnerable as they hold valuable data, the protection of which is both crucial and expected from a societal perspective. As data protection relies on different capabilities, it is vital to understand what a specific capability a particular infrastructure sector and an individual company will need and can achieve. There is a wealth of high-quality information available on the best practices of cybersecurity, for example in frameworks like the ISO series and the National Institute of Standards and Technology Cybersecurity Framework (CSF) 2.0. These frameworks contain actions that are generally considered beneficial for any company but provide limited guidance on how individual controls translate into actionable capabilities in a specific organisational context. However, very few companies have the resources to implement all the controls presented in these frameworks to reach the highest maturity levels possible in cybersecurity. In these situations, it is crucial to maximise the benefits gained from any chosen action. In this paper, we investigate how a capability-based assessment model, developed originally for the defence domain, can be adapted to evaluate cybersecurity capabilities in the context of critical infrastructure and explore its performance when applied to a healthcare sector company. This model assesses capability gaps by comparing the current state with a target level capability and applies this approach to the cybersecurity context of a healthcare organisation. The general aim of our study is to support simpler and more effective decision-making when selecting the next cybersecurity upgrade or systemic improvement. In future research, we plan to extend this model to other critical infrastructure sectors and compare its performance and generalisability to these sectors.

Keywords: Cyber risk analysis, Cybersecurity capability gap, Decision support, Healthcare cybersecurity, Control action prioritisation

1. Introduction

In recent years cyber threats have increased both in volume and complexity. Rapid digitalisation across organisations has expanded the use of interconnected information systems, including cloud-based services, which in turn have broadened the landscape of cyber threats. While digitalisation enables greater efficiency, flexibility, and scalability, it also introduces new dependencies and potential vulnerabilities that organisations must manage. Yet these organisations across infrastructure sectors differ significantly in terms of their risk exposure and their capabilities to implement effective cybersecurity controls. Critical infrastructure organisations are no exception, for example, a healthcare organisation and a municipal water utility may both be classified as critical infrastructure, but they face distinct cybersecurity challenges and operational requirements. What such organisations have in common is that cybersecurity is not limited to technical functions alone but affects the entire organisation and requires informed decision-making beyond the IT domain.

To address these challenges, decision-makers have access to a wide range of high-quality guidance on potential actions that an organisation can take to improve its cybersecurity preparedness. This guidance is typically provided in the form of cybersecurity frameworks. Widely adopted frameworks include, for example, the ISO/IEC 27000 series and the National Institute of Standards and Technology CSF (National Institute of Standards and Technology, 2024). While these frameworks contain highly valuable guidance, their scope and level of detail make practical applications challenging. This is particularly the case for organisations that lack dedicated IT expertise or specialised IT teams, such as small and medium-sized enterprises (SMEs), where prioritising appropriate actions often becomes difficult to realise (El-Hajj and Mirza, 2024).

Within critical infrastructure sectors, healthcare is frequently targeted by cyber actors (ENISA, 2023). This is partly due to factors such as dynamic operational environment and frequent staff turnover. One major reason is also the fact that the primary function of the healthcare sector is to deliver services that support individual well-being and safety rather than cybersecurity. From a cybersecurity point of view, the healthcare industry faces multiple challenges such as the data availability requirements, as critical systems must operate

continuously. At the same time, sensitive patient data must be strongly protected against unauthorised access. Different laws and regulations affect the healthcare industry as well; one example is the General Data Protection Regulation (GDPR) and the national law about cybersecurity derived from the NIS2 directive. Social and healthcare organisations represent a critical infrastructure context in which capability gaps in cybersecurity can have significant operational consequences, while available resources for systematic improvements are often limited (Kruse et al., 2017).

Despite the demands outlined above, many organisations struggle to meet regulatory and recommended baselines of cybersecurity. This combination of limited resources, regulatory requirements, and insufficient current capabilities highlights the need for structured approach to cybersecurity capability assessment and prioritisation. Capability-oriented approaches have previously been applied to cybersecurity assessment using probabilistic and structural models, particularly to support reasoning about system-level security properties rather than individual controls (Sommestad et al., 2013). In this paper, we address these challenges by adopting a capability-based approach to support cybersecurity decision-making in resource-constrained organisational contexts.

2. Method

In this study, we apply a capability-based evaluation approach (Kuikka and Peltotalo, 2022) to assess cybersecurity within an organisation's IT department to analyse its ability to deliver cybersecurity outcomes that support organisational operations, data protection, and service continuity. Cybersecurity is treated as a socio-technical capability that emerges from the combined effect of technical, organisational, and operational measures. Our approach is based on a capability-gap formulation that structures expert judgement and supports prioritisation of cybersecurity improvements in resource-constrained environments.

Cybersecurity capability is decomposed into a finite set of sub-capabilities indexed by j, each of which is evaluated relative to a defined target level. The capability gap of sub-capability j is denoted as $g_j \in [-1, 1]$, where the sign and magnitude of g_j expresses the relationship between the current state and the target level. Positive values ($g_j > 0$) indicate that the current capability is below the target level, while negative value ($g_j < 0$) indicates that the current capability exceeds the target and the value of $g_j = 0$ corresponds to the target level being met. Then the vector of sub-capability gaps is defined as $G = (g_1, g_2, \ldots g_s)$.

In this study, a capability gap is defined as a signed normalised deviation from a predefined target level of a given cybersecurity sub-capability, where positive values indicate insufficient capability and negative values indicate capability exceeding the target. In earlier capability models applied to military contexts (Kuikka and Peltotalo, 2022), importance is implicitly embedded in the definition of capability as the likelihood of mission success. In the cybersecurity context considered in this study, capability is decomposed into multiple sub-capabilities supporting different organisational objectives, requiring the relative importance of achieving target levels to be represented explicitly. To support scenario comparisons, our method distinguishes between the initial capability gap and the capability gap after improvement actions. The initial capability gap of sub-capability j is denoted as g_j^0 and represents the state before any improvement actions are applied. The difference ($g_j^0 - g_j$) represents the reduction in the capability gap achieved through improvement actions.

Improvements in cybersecurity capabilities are characterised as functional enhancement actions rather than as separate technical systems. These actions can include changes to processes, improvements in configurations, updates to policies or procedures, training activities, or enhancements to existing tools and systems. Each improvement action i is assigned a positive weight $b_i > 0$ that reflects its relative importance, and its contribution to sub-capabilities is represented by the coefficient $c_{i,j}$, typically greater than or equal to zero.

Then the contribution of improvement action i to sub-capability j is first combined into a weight $w_{ij} = c_{ij} \cdot b_i$, which is then normalised as $p_{ij} = \frac{w_{ij}}{\Sigma_i w_{ij}}$, representing the relative influence of action i on sub-capability j. The capability gap is then allocated across actions as

$$d_{ij} = g_j \cdot p_{ij}. \quad (1)$$

This proportional decomposition allocates the post-action capability gap across improvement actions according to their relative contribution and ensures conservation of gaps, such that $\sum_i d_{i,j} = g_j$. For strategic decision-making, the overall cybersecurity capability gap after improvement actions is aggregated additively as $\sum_j g_j$. The aggregated gap is used as a comparative indicator for evaluating alternative improvement scenarios rather than as an absolute measure of cybersecurity performance.

Our approach includes also an economic interpretation based on the reduction of the capability gap. Expert-defined reference importance values $I_j \geq 0$ represent the potential consequences of insufficient capability. The expected consequence reduction achieved by improvement actions at the sub-capability level is defined as

$$L_j = \left(g_j^0 - g_j\right) I_j . \quad (2)$$

Reference importance values are defined through an initial expert evaluation and represent the relative consequences of achieving target capability levels within the organisational context. They remain constant across scenarios and are not re-evaluated for each set of improvement actions. Now, the aggregated consequence reduction across all the sub-capabilities is defined as the following sum

$$L = \sum_j \left(g_j^0 - g_j\right) I_j . \quad (3)$$

The initial gap g_j^0 represents the baseline scenario, while alternative scenarios are evaluated based on their ability to reduce positive capability gaps relative to this baseline. Conceptually, consequence-related measures combine normalised signed deviations from the target level with the relative importance of achieving that target, supporting comparison of improvement effectiveness without implying realised or future financial losses.

In addition to the expected consequence reduction, each improvement action is associated with an implementation cost (denoted by E_i) that is the relative effort required to perform functional improvement actions by the organisation and is evaluated independently of the importance and the capability gaps. Here, the notation E_i refers to the implementation effort associated with improvement actions and should not be confused with the importance values I_j, that are defined separately at the sub-capability level. The effort of implementation is evaluated using an ordinal scale with five qualitative categories (Low, Low/Medium, Medium, High, Very High). These categories capture aspects such as personnel workload, organisational effort, process changes, and operational complexity. To enable aggregation and comparative scenario analysis, the ordinal categories are mapped to numerical values on a linear scale. This mapping preserves the relative ordering of cost levels while avoiding assumptions about exact cardinal or monetary differences between categories. The resulting numerical cost values are therefore used as comparative indicators to support scenario evaluation and prioritisation, and they do not imply economic optimisation, precise cost estimation, or financial valuation of cybersecurity improvements.

Throughout the method cybersecurity capability is interpreted as an organisation's assessed ability to reach a defined target level, and all capability gaps represent deviations from this target, while cost and consequence considerations are introduced to support comparative interpretation of improvement scenarios. The method assumes that cybersecurity capability can be represented through a finite set of sub-capabilities and that capability gaps can be expressed as signed normalised deviations from a defined target level. The method is intended for comparative scenario analysis and decision support within IT departments and does not aim to predict cyber incidents, realised losses, or optimal investment portfolios.

3. Critical Infrastructure use Case

This use case study is based on a private healthcare organisation operating across multiple service locations. The organisation provides continuous nursing and care services and processes sensitive health-related data as well as other personally identifiable information. The company does not have a dedicated IT department or a separate cybersecurity unit. Due to the critical nature of its services, the organisation is classified as part of the national critical infrastructure under cybersecurity legislation derived from the EU NIS2 Directive. A significant number of individuals depend on the continuity of the services provided, placing high requirements on both operational resilience and data protection within a resource-constrained organisational setting.

3.1 Risk Register

Prior to this study, the organisation had established an IT risk register to document cybersecurity-related risks in its operating environment. Business risks and IT risks are assessed separately, and the IT risk register serves as the primary input for this use case study. It provides a structured and organisation-specific view of the current cybersecurity situation by identifying areas where existing capabilities are insufficient to manage recognised risks. The risk register categorises risks into strategic, operational, and tactical risks. Strategic risks include threats that could significantly disrupt operations or lead to regulatory intervention, such as reputational damage, compliance failures, or insufficient preparedness for critical system outages. Operational risks relate to disruptions in daily healthcare activities, including system unavailability and limited access to patient information. Tactical risks focus on people, processes, and technologies, such as inadequate access control,

weaknesses in offboarding procedures, delayed security updates, and ageing IT infrastructure. While these categories support structured risk management, individual risks may span multiple levels if left unaddressed over time.

3.2 Controls and Constraints

In this study, controls refer to improvement actions identified in the risk register that aim to mitigate recognised cybersecurity risks. These actions include organisational, procedural, and technical measures. A single control may address multiple risks across different risk categories, and its impact is not binary: implementing a control typically reduces the likelihood and/or impact of a risk rather than eliminating it entirely. Therefore, controls are treated as optional improvement actions of which the organisation must prioritise those that provide the greatest benefit relative to available resources. Controls are linked to cybersecurity capabilities through the risk register, in which identified risks are interpreted as indicators of existing capability gaps. Improvement actions are selected as means to strengthen the organisation's ability to manage these gaps.

Here, the case organisation faces significant constraints related to both financial resources and available expertise, as the IT and cybersecurity activities are largely outsourced and the organisation operates without a dedicated IT or cybersecurity leader. Responsibilities are distributed according to a "multiple hats" principle, limiting systematic evaluation of improvement options and increasing reliance on external service providers. Budgetary constraints further restrict the organisation's ability to implement multiple improvements simultaneously. These constraints directly shape cybersecurity decision-making by limiting which improvement actions are feasible. In practice, prioritisation is unavoidable, and suboptimal investment choices may result in limited improvement despite significant effort. This increases the need for structured decision-support methods that help organisations compare alternative improvement options and assess their potential impact before committing scarce resources.

4. Model and Application

In this use case, the organisation's IT risk register served as the primary input for the capability-based analysis. Identified cybersecurity-related risks were interpreted as indicators of insufficient cybersecurity capability rather than as isolated issues. Each risk was mapped to one or more cybersecurity sub-capabilities reflecting different aspects of cybersecurity, including governance, technical, organisational, and operational dimensions. This mapping was based on expert judgement and considered how each identified risk reflects underlying weaknesses in the organisation's ability to prevent, detect, or respond to cybersecurity-related events. The relationship between risks and cybersecurity capabilities is not one-to-one but many-to-many, meaning that a single risk may be associated with multiple capability gaps, while a single capability gap may contribute to several identified risks. For example, risks related to reputational damage and regulatory consequences were mapped to governance and response-related capabilities, whereas risks associated with data misuse and system disruptions were linked to access control, monitoring, and technical preparedness.

Figure 1 provides an overview of the capability-based evaluation workflow applied in this study. The process starts from the identification of cybersecurity-related risks and the assessment of current organisational capabilities, followed by the definition of improvement actions and the construction of alternative improvement scenarios. The scenarios are then evaluated by comparing their effects on capability gaps, expected consequence reduction, and implementation effort. The workflow is iterative in nature: after scenario comparison, decision-makers may return to earlier phases to refine assumptions, adjust improvement actions, or construct new scenarios before committing to control propositions. This iterative structure supports learning and refinement prior to resource allocation in resource-constrained organisational contexts.

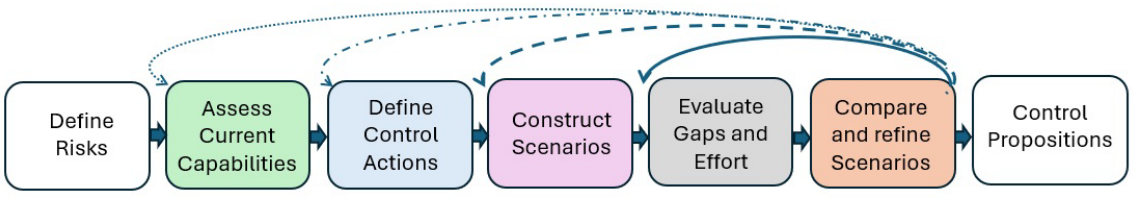

Figure 1: Capability-based workflow for cybersecurity improvement, from defining risks to scenario comparison and iterative refinement prior to control proposition

4.1 Defining Baseline and Capability Gaps

The current state of cybersecurity capability in the case organisation was defined based on the IT risk register at the time of assessment. The risk register was developed through expert judgement in collaboration with key organisational personnel and provides a documented, organisation-specific overview of identified cybersecurity-related risks. As such, it serves as a suitable and transparent starting point for the capability-based evaluation. Defining a target level is necessary to identifying capability gaps. In this case, the target level was defined as a contextually appropriate baseline level of cybersecurity capability, reflecting what can reasonably be expected from an organisation of similar size and resource constraints operating in the healthcare sector. As a fail-safe condition, the baseline level was anchored to regulatory and legal requirements, representing the minimum acceptable level of cybersecurity capability. In addition, best practices were considered only insofar as they were deemed realistic and achievable within the constraints of a small or medium-sized enterprise.

A capability gap is defined as an estimated deviation between the current state and the defined baseline level. Identified risks were interpreted as manifestations of insufficient cybersecurity capability, and the current state was compared against the baseline to determine the magnitude of each capability gap. Therefore, the capability gaps represent relative assessments of organisational capability shortfalls rather than risk probabilities or realised impacts.

The capability gaps are assessed using an asymmetric five-level expert-based scale reflecting deviations from the baseline level. The baseline level is defined as zero, with positive values indicating slight overperformance and negative values indicating increasing degrees of underperformance relative to the baseline. In practice, the scale takes the discrete values {−30, −20, −10, 0, +10}, where 0 represents the baseline level, −10 to −30 represent increasing shortfalls from the baseline, and +10 indicates marginal overperformance. This expert scale uses the opposite sign convention to the analytical formulation in Section 2, where positive values represent capability shortfalls. The discrete scale serves as a practical rating tool for expert assessment and scenario comparison. The resulting gap values are combined with the corresponding importance weights in the aggregation, as illustrated in Figure 2.

Control Actions for Scenario Evaluation	Weak cybersecurity governance	Reputational damage	Supply chain disruptions	Regulatory non-compliance	Poor data oversight	Lack of technical readiness	Data breach or manipulation	Post-attack reputational and regulatory impact	= Risks	Weak cybersecurity governance	Reputational damage	Supply chain disruptions	Regulatory non-compliance	Poor data oversight	Data breach or manipulation	Data breach or manipulation	Post-attack reputational and regulatory impact
				Importance × gap					$I_j g_j$ =	0.080	0.180	0.086	0.087	0.092	0.083	0.088	0.188
Action–capability contribution				Importance					I_j =	0.95	1	0.9	0.95	1	0.9	1	1
	$c_{i,j}$ =			Capability gap					g_i =	8.4 %	18.0 %	9.6 %	9.2 %	9.2 %	9.2 %	8.8 %	18.8 %
Staffing adequacy	25	5	10	0	10	15	10	0	1	3.0 %	2.3 %	3.2 %	0.0 %	1.9 %	2.5 %	1.1 %	0.0 %
Backups	0	0	0	5	5	15	20	0	1	0.0 %	0.0 %	0.0 %	0.9 %	1.0 %	2.5 %	2.2 %	0.0 %
IAM usage	0	0	0	10	5	0	10	0	1	0.0 %	0.0 %	0.0 %	1.8 %	1.0 %	0.0 %	1.1 %	0.0 %
Supply chain	0	5	10	10	0	5	5	0	1	0.0 %	2.3 %	3.2 %	1.8 %	0.0 %	0.8 %	0.6 %	0.0 %
Data encryption	0	0	5	10	10	0	5	0	1	0.0 %	0.0 %	1.6 %	1.8 %	1.9 %	0.0 %	0.6 %	0.0 %
Information security guidance	5	5	0	5	5	5	5	0	1	0.2 %	1.9 %	0.0 %	0.5 %	0.6 %	0.4 %	0.2 %	0.0 %
Cybersecurity training	10	5	0	5	5	5	5	0	1	0.4 %	1.9 %	0.0 %	0.5 %	0.6 %	0.4 %	0.2 %	0.0 %
Crisis communication instructions & exercises	5	15	5	0	0	0	5	15	1	0.2 %	5.6 %	1.2 %	0.0 %	0.0 %	0.0 %	0.2 %	6.9 %
Cybersecurity management model	20	5	0	0	3	5	5	10	1	2.4 %	2.3 %	0.0 %	0.0 %	0.6 %	0.8 %	0.6 %	5.4 %
Monitoring and reporting	5	0	0	5	5	5	10	10	1	0.6 %	0.0 %	0.0 %	0.9 %	1.0 %	0.8 %	1.1 %	5.4 %
Staffing adequacy				Effort/Cost					E_i =	0.6							
Backups										0.6							
IAM usage										0.8	Scenario selection						
Supply chain										1							
Data encryption										0.6							
Information security guidance										0.2	-0.4 %	-0.4 %		-0.4 %	-0.4 %	-0.4 %	-0.4 %	
Cybersecurity training										0.2	-0.8 %	-0.4 %		-0.4 %	-0.4 %	-0.4 %	-0.4 %	
Crisis communication instructions & exercises										0.2	-0.4 %	-1.2 %	-0.4 %				-0.4 %	-1.2 %
Cybersecurity management model										0.4								
Monitoring and reporting										0.6								

Controls

Control actions

Figure 2: Excel-based application implementing the capability-based scenario evaluation method, illustrating the main model variables and their aggregation for comparative scenario analysis

4.2 Linking Improvement Actions to Capability Gaps

Improvement or control actions identified in the risk register are interpreted as measures aimed at addressing identified cybersecurity risks. As defined earlier, risks are understood as insufficient cybersecurity capability. Consequently, reducing a risk implies that one or more underlying capabilities related to that risk have been strengthened. Based on this interpretation, improvement actions are treated as capability-enhancing measures, as their implementation contributes to improving the organisation's ability to prevent, detect, or respond to cybersecurity-related events. Not all improvement actions contribute equally to reducing capability gaps in cybersecurity. Identified risks often consist of multiple dimensions, each of which may require specific actions

to be addressed. As a result, a single risk may be associated with several improvement actions, and the same improvement action may contribute to different risks and capabilities to varying degrees. By the same logic, implementing an improvement action does not necessarily result in uniform capability improvement across all related capability gaps. Even when the same action is applied, its effect on reducing different capability gaps may vary depending on how strongly the action addresses the underlying weaknesses reflected by each risk.

The model we apply here supports decision-making by making differences in the impact of improvement actions explicit. In practice, improvement options are often implicitly treated as equally important, particularly when using traditional risk registers where identified risks are addressed by corresponding control actions without explicitly considering their broader effect on organisational cybersecurity capability. By explicitly linking improvement actions to capability gaps, the model reveals interdependencies between actions and capabilities that may otherwise remain unrecognised. This is particularly relevant in small and medium-sized enterprises, where resource constraints are a well-documented challenge. Under such conditions, the model supports prioritisation by highlighting improvement actions that offer greater capability enhancement relative to the resources invested.

Unlike earlier military capability models, where importance is implicitly embedded in the probability of mission success, cybersecurity capabilities support multiple organisational objectives and therefore require explicit representation of relative importance. The scenario analysis demonstrates that capability-based evaluation can reveal differentiated and sometimes non-uniform risk reduction patterns across alternative improvement strategies, while still highlighting risks that are structurally sensitive to both high-impact and low-effort functional improvements. This supports the use of the proposed method as a comparative decision-support tool rather than as a predictor of individual incidents or losses.

4.3 Scenario Construction

In this study we constructed two comparative improvement scenarios to reflect decision-making under SME resource constraints, where only a limited set of actions can be implemented within a given planning cycle. In both scenarios, the number of selected improvement actions was limited to three. Scenario 1 (high-impact) prioritised actions expected to yield the largest reduction in importance-weighted capability gaps, using the product of the baseline capability gap and the corresponding importance value as the primary selection criterion. Scenario 2 (low effort) prioritised actions with lower implementation effort. In this study, the cost is interpreted as relative implementation effort rather than as a monetary value. The effort estimates are used solely for comparative scenario construction and do not represent actual financial costs or investment calculations. Implementation effort was assessed using an ordinal five-level scale (Low–Very High) and used only as a comparative indicator for scenario construction. The effort estimates do not represent monetary costs and are not used for economic optimisation; instead, they provide a pragmatic way to contrast “high-impact” versus “low-effort” improvement strategies within the same modelling structure.

4.4 Numerical use Case Results

An Excel-based application shown in Figure 2 implements a capability-based scenario evaluation method, highlighting the key model variables for comparative analysis. The risk categories and control actions used as inputs to the model are summarised in Tables 1 and 2, respectively.

Table 1: Risk categories

ID	Risk category
1	Weak cybersecurity governance
2	Reputational damage
3	Supply chain disruptions
4	Regulatory non-compliance
5	Poor data oversight
6	Lack of technical readiness
7	Data breach or manipulation
8	Post-attack reputational & regulatory impact

Table 2: Controls actions

ID	Control actions
1	Staffing adequacy
2	Backups
3	IAM usage
4	Supply chain
5	Data encryption
6	Information security guidance
7	Cybersecurity training
8	Crisis communication instructions & exercises
9	Cybersecurity management model
10	Monitoring and reporting

Figure 3 illustrates the effects of two alternative improvement scenarios on cybersecurity capability gaps across the risks shown on the horizontal axis. Scenario 1 (Figure 3a) represents a high-impact strategy, in which functional improvement actions are selected based on their overall effectiveness in reducing importance-weighted capability gaps. When multiple actions demonstrate comparable effectiveness, preference is given to those that contribute most strongly to the product of the capability gap and importance (see Table 3). The selected actions address personnel adequacy, crisis communication guidance and exercises, and the establishment of a cybersecurity management model. In Scenario 1, the gap reductions are unevenly distributed across risks, with particularly pronounced reductions for risks associated with weak cybersecurity governance and organisational preparedness (Risk 1). This reflects the strong alignment between the selected actions and the underlying capability gaps contributing to that risk rather than a uniform reduction across all risk areas.

Scenario 2 (Figure 3b) represents a low-effort improvement strategy, where actions are selected primarily based on lower implementation effort while applying the same capability-based aggregation logic. Overall reductions are more moderate and more evenly distributed; however, a notable reduction is again observed for Risk 1. This indicates that certain risks are structurally sensitive to relatively feasible functional improvements, even when actions are not chosen to maximise overall impact.

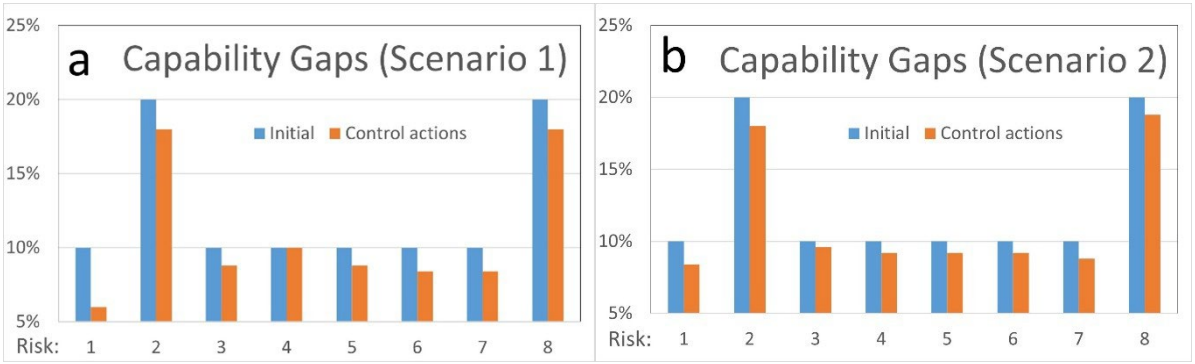

Figure 3: a) Scenario prioritising maximum reduction of importance-weighted cybersecurity capability gaps through selected functional improvement actions. b) Scenario prioritising low implementation effort while applying the same capability-based aggregation logic for cybersecurity improvement

The results show that importance-weighted capability gaps are reduced to different extents depending on the prioritisation strategy, with high-impact actions yielding the largest overall reduction and low-effort actions still providing meaningful improvement relative to the baseline. In Table 3, the quantity $\sum_j I_j g_j$ represents the residual importance-weighted capability gap, where lower values correspond to greater improvement from the baseline.

Table 3: Importance values I_j and products of importance and residual gap values $I_j g_j$ for the two Scenarios 1 and 2. For comparison in Scenario 0, no improving actions are implemented

Risk		1	2	3	4	5	6	7	8	
I_j	All scenarios	0.95	1	0.9	0.95	1	0.9	1	1	$\sum_j I_j g_j$
$I_j g_0$	Scenario 0	0.095	0.200	0.090	0.095	0.100	0.090	0.100	0.200	97.0 %
$I_j g_j$	Scenario 1	0.057	0.180	0.079	0.095	0.088	0.076	0.084	0.180	83.9 %
$I_j g_j$	Scenario 2	0.080	0.180	0.086	0.087	0.092	0.083	0.088	0.188	88.4 %

4.5 Interpreting Scenario Results

The scenario results are intended for comparison rather than as exact measures of cybersecurity performance. Because the effects of improvement actions are allocated proportionally based on their links to different capabilities, the same action may reduce some capability gaps more than others. As a result, some capability gaps are expected to remain after the improvements. Therefore, the results show how different prioritisation choices affect which capability gaps are reduced and to what extent.

From the decision-support perspective, our method helps to make trade-offs visible between (i) improvement actions that provide broader capability gains and (ii) the effort required to implement those actions. As shown in Table 3, the baseline scenario (Scenario 0) yields an importance-weighted capability gap of 97.0%. Scenario 1 reduces this value to 83.9%, representing the largest overall improvement when selecting three actions based on high impact, whereas Scenario 2 achieves a more moderate reduction to 88.4% when selecting three actions with the lowest implementation effort. This confirms that prioritising actions based on high-impact strategy of Scenario 1 leads to greater overall capability gap reduction of 13.5% than the low-effort strategy still leading to a meaningful reduction of 8.9% relative to the baseline.

5. Conclusion

In this study we investigated how a capability-based evaluation model, originally developed in a military context, can be adapted to support cybersecurity decision-making in a resource-constrained critical infrastructure organisation. The model was applied to a healthcare company using an existing IT risk register as the primary input to assess capability gaps and evaluate alternative improvement scenarios.

The results indicate that the model provides a structured and transparent way to reason about how different improvement actions contribute to cybersecurity capabilities and how limited resources can be prioritised more systematically. In particular, the scenario analysis helped to distinguish between high-impact and low-effort improvement strategies and demonstrate that capability gaps are reduced in non-uniform ways depending on the prioritisation logic applied. This supports the use of the model as a comparative decision-support tool rather than as an absolute measure of cybersecurity performance.

Several limitations should be considered when interpreting the findings. First, the evaluation was conducted as a single use case study within the healthcare sector, which could limit the method's generalisability to other organisations or critical infrastructure domains. Second, representatives of the use case organisation did not directly participate in the modelling or scenario construction. The analysis relied on previously produced organisational material and expert judgement, which ensured contextual realism but limited direct validation from decision-makers. Third, the assessment of capability gaps, control impacts, and scenarios was inherently subjective and based on a single evaluator. Finally, the implementation effort estimates used in the scenarios were intentionally coarse and context-specific, supporting relative comparison rather than precise economic evaluation.

In the future we will apply the proposed approach to multiple organisations and across different critical infrastructure sectors to evaluate its generalisability and sector-specific applicability. Involving multiple evaluators and organisational stakeholders would further support validation and reduce subjectivity. In addition, future development could explore the use of artificial intelligence–based methods to support estimation of control impacts, sensitivity analysis, and scenario generation. Such extensions could lower the threshold for applying the model in practice while preserving its role as a comparative decision-support tool.

Ethics declaration: This study did not involve the collection or processing of personal data. The case material was fully anonymised and contained no identifiable information about individuals or the organisation. Ethical approval was therefore not required for this study.

AI declaration: AI tools were used to support language refinement and clarity of expression. All analytical content, modelling decisions, interpretations, and conclusions were produced by the authors.

References

El-Hajj, M. and Mirza, Z.A. (2024) "Protecting Small and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool", *Electronics, 13(19), Article 3910*. doi:10.3390/electronics13193910

ENISA (2023) *Health Threat Landscape Report*, European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/health-threat-landscape (Accessed: 18 January 2026).

Kruse, C.S., Frederick, B., Jacobson, T. and Monticone, D.K. (2017) "Cybersecurity in healthcare: A systematic review of modern threats and trends", *Technology and Health Care*, Vol. 25, No. 1, pp. 1–10. doi:10.3233/THC-161263

Kuikka, V. and Peltotalo, S. (2022) "A Method for Assessing Effects of Technological Development on Military Capabilities", Proceedings of the International Conference on Decision Aid Sciences and Applications (DASA), IEEE, pp. 1634–1639. doi:10.1109/DASA54658.2022.9765009

National Institute of Standards and Technology (2024) Cybersecurity Framework 2.0, NIST, Gaithersburg. Available at: https://www.nist.gov/cyberframework (Accessed: 27 December 2025)

Sommestad, T., Ekstedt, M. and Holm, H. (2013) "The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures", *IEEE Systems Journal*, Vol. 7, No. 3, pp. 363–373. doi:10.1109/JSYST.2012.2221853