KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.128-134
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

COST-BENEFIT ANALYSIS AS A TOOL TO STRENGTHEN ORGANISATIONAL CYBER RESILIENCE

KATARÍNA KAMPOVÁ, MATÚŠ MADLEŇÁK, TIMOTEJ MAČUHA, SAMUEL HUBOČAN, MARTIN HROMADA

ABSTRACT: Organisations face a wide range of cyber threats with significant operational, financial and reputational impacts. Strengthening resilience therefore requires not only technical and organisational measures, but also clear economic justification. Cost–Benefit Analysis (CBA) is a well-established method that compares the costs of security measures with their benefits, such as reducing the likelihood of incidents, limiting their impact or shortening recovery times. In line with NIS2 and ISO/IEC 27001:2022 and ISO/IEC 27005:2023, CBA supports proportionate, risk-based and cost-effective security. This paper outlines the methodology, its role in decision-making, and a practical example of its application in enhancing cyber resilience and trust.

KEYWORDS: *Risks. Resilience. Cybersecurity. Cost–Benefit Analysis. Measures.*

INTRODUCTION

Strengthening the cyber resilience of organisations has become a key challenge as they face many different types of threats. These threats can be intentional, such as cyberattacks or misuse of access rights, unintentional, such as human errors or misconfigurations, or caused by technical and natural factors, including infrastructure failures, power outages, or natural disasters. Such events may result in incidents with serious operational, financial, and reputational impacts. For this reason, effective risk management requires not only technical and organisational measures but also clear economic justification. One of the proven approaches is Cost–Benefit Analysis (CBA), which helps organisations evaluate whether investments in cybersecurity and resilience are adequate compared to the expected benefits. CBA compares the overall costs of introducing, operating, and maintaining security measures with the benefits they bring. These benefits include reducing the likelihood of a cyber incident, limiting its impact on the confidentiality, integrity, and availability of information, or shortening recovery time objectives (RTO, RPO). In practice, CBA can help organisations decide whether it is more efficient to implement multi-factor authentication, network segmentation, endpoint detection and response (EDR/XDR), or extended user training programs.

According to the NIS2 Directive and international standards ISO/IEC 27001:2022 and ISO/IEC 27005:2023, organisations are required to implement security measures that are proportionate to risks and cost-effective. CBA is one of the recommended methods that can support this requirement. It helps management make informed decisions, improves transparency in budget allocation, and provides evidence to regulators that measures follow the principle of proportionality. This paper explains the methodology of CBA and shows its use in evaluating organisational cyber resilience. It outlines how CBA can compare alternative security measures, identify those with the best balance of benefits and costs, and strengthen protection against cyber threats. A practical example demonstrates how CBA can support strategic decision-making and improve trust in the organisation among partners, customers, and regulators.

The main aim of this paper is to present a clear and structured application of CBA as a decision-support tool in cybersecurity, and to demonstrate its practical value in strengthening organisational cyber resilience. The contribution of the paper lies in linking risk management obligations under the NIS2 Directive and ISO/IEC standards with an economically justified methodology for selecting proportionate and cost-effective security measures. A practical model example illustrates how CBA can support transparent, evidence-based decision-making.

1. RISK ASSESSMENT AND ITS LINK TO THE RISK MANAGEMENT PLAN

Cyber risk management is a logical and systematic process of identifying, analysing, evaluating, and treating risks with the aim of minimising negative impacts or exploiting emerging opportunities. It is not just about methods and tools; according to Šimák, it also includes the culture, processes, and organisational structures that support the management of uncertainty and the continuous improvement of the quality of decision-making (Šimák, 2006). In a well-managed organisation, the process is embedded in strategic, operational, and project management and is supported by policies, procedures, and practices for communication and consultation, context determination, risk assessment, risk treatment, monitoring, documentation, and reporting (ISO/IEC 27001:2022).

The ISO/IEC 27005:2023 standard provides a specific framework for assessing information security risks and complements the requirements of ISO/IEC 27001:2022 for an ISMS management system. In accordance with the NIS2 Directive, essential and important entities have an obligation to implement appropriate and cost-effective technical, organisational and procedural measures, including proper incident management and top management accountability (European Union, 2022). Determining the context is a preliminary step in risk assessment, the organisation systematically evaluates external factors (legislation, technology, market, threats) and internal factors (structure, culture, resources, IS/IT architecture, existing controls), defines asset protection requirements and sets risk criteria (appetite, tolerance, consequence and probability metrics, time aspects, risk combinations). It includes the choice of analysis method (qualitative, quantitative or combined). Risk assessment consists of three steps (ISO 31000:2018), (ISO/IEC 27001:2022):

1. Risk identification: systematic search and description of risks (threats, vulnerabilities, causes, scenarios, affected assets).
2. Risk analysis: estimation of probability and severity of impacts on confidentiality, integrity and availability (CIA), taking into account the effectiveness of existing controls, working with uncertainty and input sensitivity.
3. Risk evaluation: comparison with acceptance criteria and setting priorities for treatment.

The output is a risk list, which is a direct input to the Risk Treatment Plan. This plan documents:

- risks to be treated;
- the chosen strategy (avoidance, reduction of probability/impact, sharing/transfer, acceptance);
- specific technical, organisational and procedural measures;
- responsibilities, deadlines, resources;
- and effectiveness metrics (e.g. incident rate, MTTD/MTTR, RTO/RPO compliance).

As the NIS2 Directive emphasises the principle of proportionality and cost-effectiveness, when selecting security measures, organisations are expected to be able to demonstrate their proportionality – that is, that the costs of the measures are in reasonable proportion to the risk reduction they bring. It is therefore not enough to have a technically effective solution, but also to have an economic justification for it. CBA thus forms a decision gateway between the risk assessment and the final design of the risk treatment plan. Since decision-making on measures often takes place in conditions of limited resources and multiple alternatives, it is necessary to ensure not only the technical effectiveness, but also the economic adequacy of the solutions. This is where CBA plays a key role, allowing to quantify and compare different risk treatment scenarios, for example whether it is more profitable to invest in technical measures (e.g. multi-factor authentication, EDR), organisational measures (user training, policy updates) or a combination of them. The results of CBA provide the basis for management to be able to transparently justify that the chosen measures are not only effective, but also cost-effective and in accordance with the principle of proportionality according to the NIS2 Directive (Figure 1).

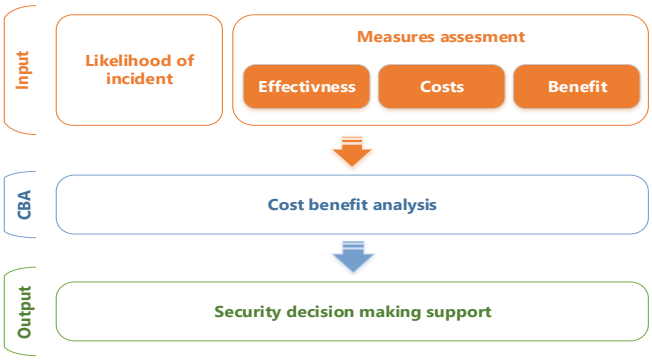

Figure 1 Cost–Benefit Analysis process within the security framework (Kampová, 2020)

As illustrated in Figure 1, CBA follows the risk assessment and is an input to the risk treatment plan. The process builds on the results of the threat identification, vulnerability assessment and impact assessment that are part of the risk analysis according to ISO/IEC 27005. CBA works with two main inputs:

- Incident probability – based on the combination of threats and vulnerabilities identified in the risk analysis and determines how often an incident is likely to occur.
- Evaluation of measures – involves assessing the proposed security measures in terms of their effectiveness in mitigating vulnerabilities and impacts, as well as the costs of their implementation and operation.

The output of CBA is an economically justified selection of measures that reduce risks to an acceptable level. At the same time, it meets the proportionality principle required by the NIS2 Directive – measures must not only be effective, but also appropriate and cost-effective.

2. COST-BENEFIT ANALYSIS

Strengthening the cyber resilience of organisations requires not only the implementation of technical and organisational security measures but also their clear economic justification. One of the proven methods is CBA, which makes it possible to compare the costs of implementing, operating, and maintaining security measures with the benefits they bring - from reducing the likelihood of cyber incidents, through limiting their impact on the confidentiality, integrity, and availability of information, to shortening recovery times (RTO, RPO). The CBA process typically includes the following steps:

- Definition of the problem and identification of alternatives.
- Identification and categorization of costs and benefits.
- Quantification and monetization of all impacts.
- Discounting future costs and benefits.
- Calculation of indicators such as NPV, BCR, ROI, and payback period.
- Conducting a sensitivity analysis.
- Selection of the most cost-effective and proportionate measure.

In accordance with the NIS2 Directive and the ISO/IEC 27001:2022 and ISO/IEC 27005:2023 standards, organisations are required to implement measures that are proportionate to risks while also being cost-effective. CBA provides a methodological framework that supports this principle of proportionality, increases transparency in budget allocation, and offers evidence for regulatory authorities. The article describes the CBA methodology and demonstrates its use in assessing the cyber resilience of organisations. It focuses on comparing alternative security measures, identifying those with the best cost-benefit ratio, and showing how CBA supports strategic decision-making and strengthens the trust of partners, customers, and regulatory authorities in the organisation (Sieber, 2004).

The fundamental principles of CBA rest on several conditions that determine its application in the evaluation of investment projects, policies, or security measures. One of the key principles is economic efficiency (Messonnier & Meltzer, 2002), (Boardman, 2018). CBA examines whether the proposed

project or measure represents an effective use of available resources, based on an estimate of social costs and benefits. Another principle is the quantification of costs and benefits. CBA makes it possible to translate even social effects - both positive and negative - into monetary units, thereby creating an objective basis for comparing alternative options. However, this approach also brings philosophical and ethical dilemmas, especially when it comes to valuing incomparable goods such as human life or the environment. Therefore, it is advisable to complement CBA with broader deliberative approaches when making decisions about public policies or security strategies. When applying CBA, it is necessary to distinguish between financial and economic analysis (Gunes, 2020).

- Financial analysis focuses on the actual financial costs and revenues of a project or measure. It assesses efficiency exclusively from the perspective of the organisation—that is, whether the investment is worthwhile in terms of cash flows, return on investment, or profitability. This approach does not take into account broader social consequences such as external costs or benefits. Its goal is to evaluate the financial sustainability of the project.
- Economic analysis, on the other hand, considers the overall societal effects. It includes in its calculations not only direct costs and benefits but also indirect and external impacts—for example, effects on employment, quality of life, reputation, or environmental factors. The focus is not on profit, but on the socio-economic benefits for the wider environment.

In the context of cybersecurity, an example can be given:

- Financial analysis will evaluate the costs of implementing multi-factor authentication (MFA) against the expected savings from preventing incidents.
- Economic analysis, however, will add a broader dimension: increased customer trust, improved organisational reputation in the market, greater stability of critical infrastructure, or savings in the form of reduced state expenditures for addressing the consequences of cyberattacks.

The combination of both approaches enables decision-makers to choose measures that are not only financially effective for the organisation but also bring broader societal benefits. CBA must take into account that individual costs and benefits occur at different stages of the project life cycle (Table 1). Their precise identification makes it possible to determine when the budget is most heavily burdened and when the benefits begin to materialize.

Table 1 Project life cycle phases and their characteristics (European Commission, 2014)

Project Phase	**Characteristics**
Pre-investment phase	Planning, preparatory analyses, decision-making; includes so-called “sunk costs.”
Investment phase	Implementation of the measure or project; high capital expenditures.
Operational phase	Regular operation of the project; generation of benefits and partial operating costs.
Post-operational phase	Project closure, sale or disposal of assets, evaluation of results.

The allocation of individual items to a specific phase enables a realistic assessment of the return and effectiveness of investments. For systematic and comparable processing of CBA, the categorization of costs and benefits is essential. This categorization increases transparency and allows for effective comparison of project or measure alternatives.

Table 2 Criteria for categorizing costs and benefits (Sieber, 2004)

Criterion	**Classification**
By affected entity	State, enterprises, households, non-profit organisations.
By project phase	Pre-investment, investment, operational, post-operational.
By nature of impact	Tangible (e.g., hardware), intangible (reputation), financial.
By measurability	Quantifiable, non-quantifiable.
By causality	Direct (e.g., technology purchase), indirect (secondary effects, reputational impacts).

3. EXAMPLE OF CBA APPLICATION IN CYBERSECURITY

In the practical application of CBA in the field of information and cybersecurity, standard financial analysis indicators are used to quantify the effectiveness of investments (European Commission, 2014):

- **NPV (Net Present Value):** the net present value, which expresses the difference between discounted benefits and costs. A positive NPV indicates that the project is economically beneficial.
- **BCR (Benefit–Cost Ratio):** the ratio of benefits to costs; a value greater than 1 confirms the efficiency of the project.
- **ROI (Return on Investment):** the return on investment, expressed as a percentage of the ratio of net benefit to total costs.
- **Payback period:** the time period within which the investment is recovered through the savings achieved.

These indicators provide a basis for the comparability of alternative measures and support transparent decision-making. The following model example illustrates how these CBA steps can be applied in practice. It shows the transition from risk-based justification to financial evaluation and demonstrates how CBA supports transparent and proportionate decision-making in line with the NIS2 Directive.

A model example can be given in the public administration environment, where accounting information systems represent critical infrastructure. The organisation is considering an investment in a security module that includes EDR (Endpoint Detection and Response) and automated data backup.

Table 3 Decision Parameters for the Implementation of a Security Module

Parameter	Value	Description/Calculation
Estimated annual loss before the measure	€250,000	System outages, manual processing, reputational losses
Estimated annual loss after the measure	€50,000	Impact reduction thanks to rapid detection and data recovery
Investment costs	€90,000	Licenses, implementation, training
Annual savings (Benefit)	€200,000	250,000 − 50,000
NPV (Year 1)	€110,000	200,000 − 90,000
BCR (Year 1)	2.22	200,000 / 90,000
ROI (Year 1)	122%	110,000 / 90,000 × 100
Payback period	0.45 year	90,000 / 200,000

The results show that the investment is economically effective (Table 3), with a short payback period and a significant reduction in operational risks. From the perspective of the NIS2 Directive, the organisation thus demonstrates the proportionality and cost-effectiveness of the implemented measures. To increase the robustness of the results, it is advisable to carry out a sensitivity analysis. Even with a +20% change in investment costs or a −20% decrease in expected savings, the BCR values remain greater than 1 in both cases, confirming that the measures continue to be economically justifiable.

CONCLUSION

The results of applying the CBA method in the field of information and cybersecurity highlight its significance in several dimensions:

- Financial transparency – Quantified indicators (NPV, BCR, ROI) enable management to effectively justify security investments to founders, shareholders, or regulatory authorities. CBA thus contributes to the rational allocation of limited financial resources.
- Compliance and regulatory requirements – In light of the NIS2 Directive, it is necessary to demonstrate that the implemented measures are proportionate to risks and economically justified. CBA provides an objective framework that supports the fulfillment of legislative obligations while minimising the risk of sanctions.

- Strategic management and priorities – With a limited budget, it is important to prioritize measures with higher BCR values and shorter payback periods. CBA enables the prioritization of investments and their alignment with the strategic goals of the organisation.
- Strengthening resilience and trust – Investments supported by CBA not only reduce the likelihood of incidents but also strengthen the trust of partners, customers, and regulatory authorities. Transparent economic justification contributes to building reputation and long-term organisational stability.
- Support for continuous improvement – The implementation of security measures is not a one-off process. CBA can be repeatedly used to monitor the effectiveness of measures and to guide decisions on their adjustment or modernization.

A significant implication for practice is that CBA links the technical and economic aspects of security. While technical measures are essential for risk reduction, economic rationality ensures that the organisation can maintain its security framework in the long term. This synergy is key to effective risk management in an environment of increasing digitalization and interconnected systems.

CBA is a useful and transparent method, but its results are influenced by several limitations. Estimates of incident probabilities may be inaccurate due to limited or low-quality data. It is also difficult to precisely quantify some intangible impacts, such as reputational damage or loss of trust. In addition, part of the benefits of security measures may appear only over a longer period, which complicates their exact evaluation.

Future research should focus on more accurate methods for estimating probabilities (e.g., using Bayesian approaches), on developing economic benchmarks for different NIS2 sectors, and on combining CBA with other decision-making methods. Another promising area is the application of CBA across various sectors of critical infrastructure to better assess the proportionality and long-term benefits of security measures.

ACKNOWLEDGEMENTS

This paper was supported by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic and the Slovak Academy of Sciences (VEGA) under project No. 1/0257/23 Cyber Risk Assessment as an Essential Tool for Enhancing Cybersecurity in Public Administration.

This publication has been produced thanks to support under the Operational Program Research and Innovation for the project: ICT for smart society, code ITMS2014 +: 313011T462, co-financed by the European Regional Development Fund.

REFERENCES

Boardman, A. E., Greenberg, D. H., Vining, A. R., & Weimer, D. L. (2018). Cost–Benefit Analysis: Concepts and Practice (5th ed.). Harlow: Pearson.

European Commission. (2014). Guide to Cost–Benefit Analysis of Investment Projects. Luxembourg: Publications Office of the European Union.

European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2), repealing Directive (EU) 2016/1148. Official Journal of the European Union, L 333, 80–152.

Gunes, N. (2020). Cost–benefit analysis. SAGE Publications. https://doi.org/10.4135/9781452229669.n858

International Organization for Standardization. (2018). ISO 31000:2018 – Risk management – Guidelines. Geneva: ISO.

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO/IEC.

International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 27005:2023 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Geneva: ISO/IEC.

Kampová, K., Mäkká, K., & Zvaríková, K. (2020). Cost–benefit analysis within organization security management. SHS Web of Conferences, 74, 01010. https://doi.org/10.1051/shsconf/20207401010

Messonnier, M. L., & Meltzer, M. I. (2002). Cost–benefit analysis. In Disease Control Priorities in Developing Countries (pp. 127–155). https://doi.org/10.1093/oso/9780195148978.003.0008

NIS2 Directive. (2022). NIS2 Directive – EU-wide cybersecurity rules. [Online] Available at: https://www.nis-2-directive.com [Accessed 11 Jun 2025].

Sieber, P. (2004). Methodological Guide: Cost–Benefit Analysis. Prague: Ministry for Regional Development.

Šimák, L. (2006). Manažment rizík. Žilina: Žilinská univerzita v Žiline, Fakulta špeciálneho inžinierstva. [Online] Available at: http://fsi.uniza.sk/kkm/old/publikacie/mn_rizik.pdf

Katarína Kampová, doc. Ing. PhD.

Faculty of security engineering, University of Zilina, Univerzitná 8215/1, 010 26 Žilina

e-mail: katarina.kampova@uniza.sk

Matúš Madleňák, Ing.

Faculty of security engineering, University of Zilina, Univerzitná 8215/1, 010 26 Žilina

e-mail: matus.madlenak@uniza.sk

Timotej Mačuha, Ing.

Faculty of security engineering, University of Zilina, Univerzitná 8215/1, 010 26 Žilina

e-mail: timotej.macuha@uniza.sk

Samuel Hubočan, Ing.

Faculty of security engineering, University of Zilina, Univerzitná 8215/1, 010 26 Žilina

e-mail: samuel.hubocan@uniza.sk

Martin Hromada, prof. Ing. PhD.

Faculty of Applied Informatics, Tomas Bata University in Zlín, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic

e-mail: hromada@utb.cz