COST-BENEFITS ASPECTS IN RISK MANAGEMENT

Białas A.[*]

Abstract: The paper concerns advanced risk management in the security domain. This approach is based not only on the traditional risk assessment, but also on the financial cost-benefits analysis and on the identification of hidden, non-financial factors, which may harm the operations of security measures in the operational environment. The paper is related to the FP7 ValueSec project and presents its background, methodology and results. Special focus is placed on the cost-benefits assessment (CBA) of the proposed security measures. Cost and benefits categories are discussed along with the operation of the CBA component. The elaborated toolset is used to support decision makers in different security domains.

Key words: risk management, cost-benefits approach, software tools for risk management

DOI: 10.17512/pjms.2016.14.1.03

Article's history:
Received October 15, 2015; *Revised* July 3, 2016; *Accepted* September 9, 2016

Introduction

The paper concerns the risk management issue, which is crucial for business and public organizations, critical infrastructures as well as for different projects, processes, undertakings and actions.

Risk management is understood as a continuous management process which is focused on the identification and analysis of potential hazards, on the assessment of their impacts on systems or activities, and on the proposed risk control measures to eliminate or mitigate potential harms to processes, people, environments or other assets. Risk assessment, a key element of risk management, is an overall process of risk identification, risk analysis and risk evaluation. It helps to understand risks, their causes, consequences and probabilities.

The paper is focused on the following issue: how to select, during the risk management process, the right countermeasures for the given application. Right countermeasures should properly affect the risk volume, bring assumed benefits at an acceptable cost and be free of political, social, cultural, psychological, and other similar soft factors, which may lower the effectiveness of countermeasures in their operational environment. This issue was solved in the FP7 ValueSec project (ValueSec, 2014) in which the author was involved. The objective of the paper is to present research and development results related to the CBA implementation in this project.

There are different risk assessment methods, usually grouped into three big categories: qualitative, semi-qualitative and quantitative methods (ENISA, 2015).

[*] **Andrzej Białas,** Prof., Institute of Innovative Technologies EMAG
✉ Corresponding author: andrzej.bialas@ibemag.pl

Quantitative methods operate on numbers, including monetary values. That is why they are more convenient than cost-benefits assessments/analyses. The basic risk management framework was defined in the standard (ISO 31000, 2009). The related standard (ISO/IEC 31010, 2009) characterizes about 30 risk assessment methods for different applications, which can be implemented within this framework. A very exhaustive discussion of the risk management terms and methodology is placed in the monograph (Rausand, 2011). Cost-benefits assessment (CBA) has been used in business and economy for years. This systematic approach allows to estimate the strengths and weaknesses of alternative solutions, actions, requirements, etc. It is a technique that enables to determine options for a certain application domain. This way it is possible to provide the best approach to be selected for the given domain, i.e. the one with biggest benefits in terms of labour, time, cost savings etc. (Cellini Riegg and Kee, 2010). CBA calculates the costs and benefits of different options and compares the results to make the right decision. The decision may concern, particularly, the countermeasures selection during the risk management process.

During the ValueSec project an exhaustive review of theories, methods and tools (TMT) was performed, with the author's participation, to select best solutions to be implemented in the project domain (i.e. public mass event, mass transportation, air transport/airport, communal security planning, cyber smart grid attack). In the first step the screening of 30 preselected TMTs was done (Kaufmann, 2011) and finally 10 methods/tools were selected for further assessment. The usability criteria were elaborated (Białas et al., 2012) which allowed to achieve the more precise and consistent picture and to elaborate the recommendation for implementation of the given methods in the ValueSec Toolset. Both above mentioned documents present the state of the art in the risk management domain. The risk management issues related to this project are presented in the papers (Bjorheim Abrahamsen et al., 2015; Białas, 2013; Białas, 2014) as well. The cost-benefits and qualitative criteria issues, with respect to the security measures selection, were initially discussed in the paper (Adar et al., 2012).

The paper is based mostly on the review of the state of the art performed during the ValueSec project. The review shows that only few methods consider cost-benefits aspects in the risk management in the project domain, but none of them takes into account the quantitative assessment of soft factors that may lower the effectiveness of security measures. The paper (Gordon and Loeb, 2002) concerns economic aspects of information security and focus on how to determine the optimal amount of money that has to be invested to protect a given set of information. The paper (Acquisti and Grossklags, 2005) concerns the trade-off between information security and privacy and tries to answer "why users' stated privacy preferences differ from their behaviors". The issues discussed in these papers represent a similar approach but do not cover the ValueSec domain. The paper presents the ValueSec R&D background, risk management issues, cost-benefits model, its implementation in the security related projects, and conclusions.

The ValueSec Approach

The ValueSec project was focused on the support of the decision making process related to the selection of such security measures which should be the most convenient for the given application and circumstances.
The related decision making process is important to many organizations, projects, social groups, and individuals. The decision influences the security, business efficiency and social acceptance for the proposed security measures. This decision making process is very complex because it has to take into account a number of factors of different, complicated and still unexplored nature.
The ValueSec approach assumes that the proposed security measure, being the result of the decision making process, should be:

- able to mitigate the risk volume sufficiently in order to provide security on an accepted level and to provide benefits for stakeholders,
- cost-effective in order not to reduce the efficiency of operations and not to incur unnecessary costs,
- free of: social, psychological, political, legal, ethical, economic, technical, environmental, etc. restrictions (qualitative criteria).

The ValueSec methodology was implemented as the Valuesec Toolset, which is equipped with components corresponding to the below listed pillars:

- Risk Reduction Assessment (RRA),
- Cost-Benefit-Assessment (CBA),
- Qualitative Criteria Assessment (QCA).

These three main components are supplemented by others, like: knowledge base, reporting, visualization and authentication components. Figure 1 presents the ValueSec decision making process based on the Valuesec Toolset.
First, the decision maker selects the application context and scenario. During the ValueSec project five context-scenario pairs were elaborated, listed on the left side of Figure 1. Next, the decision maker analyzes the decision context and scenario, i.e. the protected assets or processes, available resources, budget and social values. He/she prepares a set of security measures candidates to assess them with respect to this scenario. The security measures are assessed with respect to the risk affected (RRA), cost-benefits brought (CBA) and non-financial restrictions (QCA) which influence the measure during the operation. For each security measure a vector of values is formed, being a function of the diversified, multidirectional parameters which influence the vector positively or negatively. Using the ValueSec Toolset the decision maker tries to optimize this function from different points of view and decision contexts. Aggregated results in the shape of vectors of values provided by three pillars are worked out for all security measures candidates. On this basis the decision maker elaborates the final recommendation for the security measures to be applied in the given context and scenario.
The ValueSec project (ValueSec, 2014) was performed by 11 partners including the author's organization – Institute of Innovative Technologies EMAG.

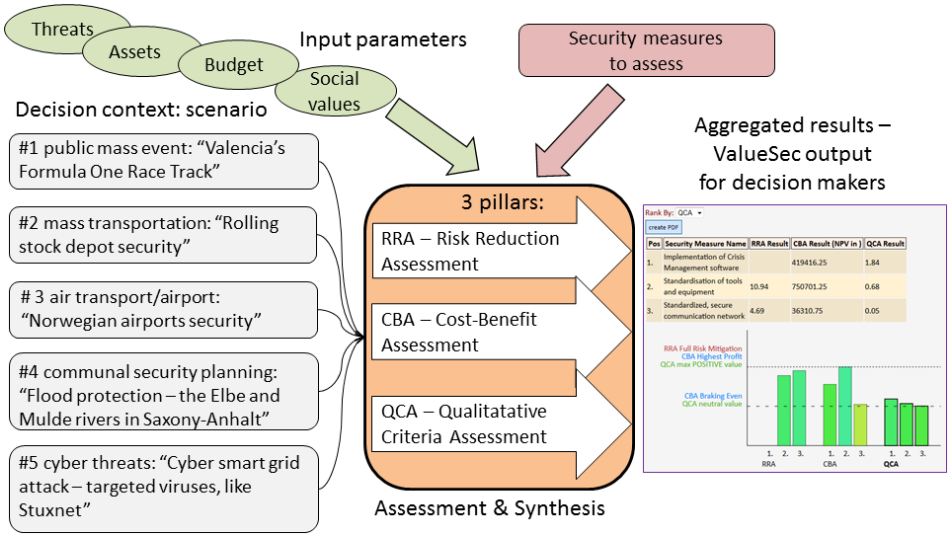


Figure 1. ValueSec decision making process *(Prepared by the author, based on the ValueSec documentation, 2015)*

The author's organization was especially engaged in researches on the risk management methodology, cost benefits model, project ontology elaboration, risk assessment tool and component integration, as well as in the validation in the "Communal security planning" context. The R&D project started from the problem analysis and elaboration of requirements for the decision framework, encompassing the following issues: the identification of decision makers' needs, defining the decision process, cost-benefits analysis for security measures, identification of qualitative criteria and the concept of their assessment (Rosqvist et al., 2011; Poussa et al., 2011). The asset/process-oriented risk analyzer from OSCAD (OSCAD, 2015) was selected as one of four risk management tools for the ValueSec Toolset. The OSCAD software is owned by the EMAG Institute. In the ValueSec project OSCAD was adapted for the communal security planning context. During the review of state-of-the-art, no cost-benefits tools satisfying the project requirements were identified. Therefore the project partners decided to elaborate the CBA component based on state-of-the-art methods and the partners' own experience. The same was with QCA, which supplements the RRA and CBA pillars. These three pillars together form an innovative concept which is the scientific added value of the project.

The ValueSec Framework Operations

There is a recommended main sequence to conduct assessments for the ValueSec Toolset:

1) Use the RRA component; assess the inherent risk (i.e. "risk before" the security measure application). There is a reference point.

2) Select a security measure (or a set of security measures) and reassess the risk (i.e. determine the "risk after" the measure implementation). Compare it with the risk acceptance level. It is possible to identify the subset of security measures, properly reducing the risk (i.e. below the risk acceptance level).
3) Use the CBA component; determine the cost-benefits characteristics of each subset of security measures.
4) Use the QCA component; determine the non-financial characteristics of each subset of security measures.
5) Make decision based on the aggregated results of assessments.

Before the CBA assessment, the risk before/after is assessed, which is shown in Figure 2 on the flood protection scenario. Please note the protected asset "Communication infrastructure", the threat "Rising water level due the heavy rainfall" and the corresponding vulnerability "Inappropriate monitoring of the water level".

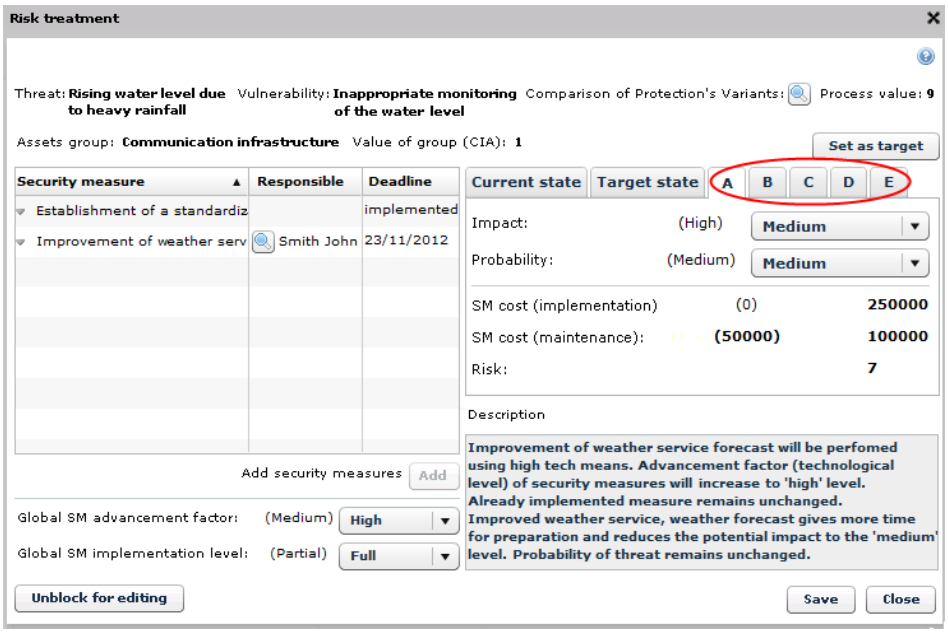


Figure 2. OSCAD risk manager elaborated in the EMAG Institute

(Screen shot prepared by the author, 2015)

To mitigate the risk, a set of 2 security measures (variant A) is proposed: "Establishing a standardized secure communication network" and "Improvement of weather service forecast". OSCAD allows to consider 5 variants of measures (A-E). One of them is selected as the target variant for implementation. The risk calculation is based on four parameters: impact, probability, advancement

(assurance class) of the security measure and its implementation level (planned, under implementation, tested and proven).
The results of the assessment (up to 5 variants) are transferred to the ValueSec Toolset, allowing to start the CBA assessment, and later the QCA assessment.

Implementation and Use of the Cost-Benefits Assessment Methodology in the ValueSec Framework

The elaboration of a new CBA component from scratch was initiated during the project workshop held in Berlin. These common efforts allowed to determine the CBA sequence of operations, data categories, cost-benefits characteristics useful for decision makers, etc. On this basis the CBA excel demo tool was developed (Räikkönen et al., 2013) and transferred to validation at the next project meeting. This allowed to start the software implementation of the CBA component and its integration within the toolset.
It is assumed that the CBA assessment is based on two categories of cost: investment costs and future costs, and one category representing future benefits. The mentioned categories are hierarchical and can be more refined if needed. The categories should be able to express the needs of the decision maker in the security domain.
The category of investment costs, incurred during the security measures implementation, has the following subcategories:

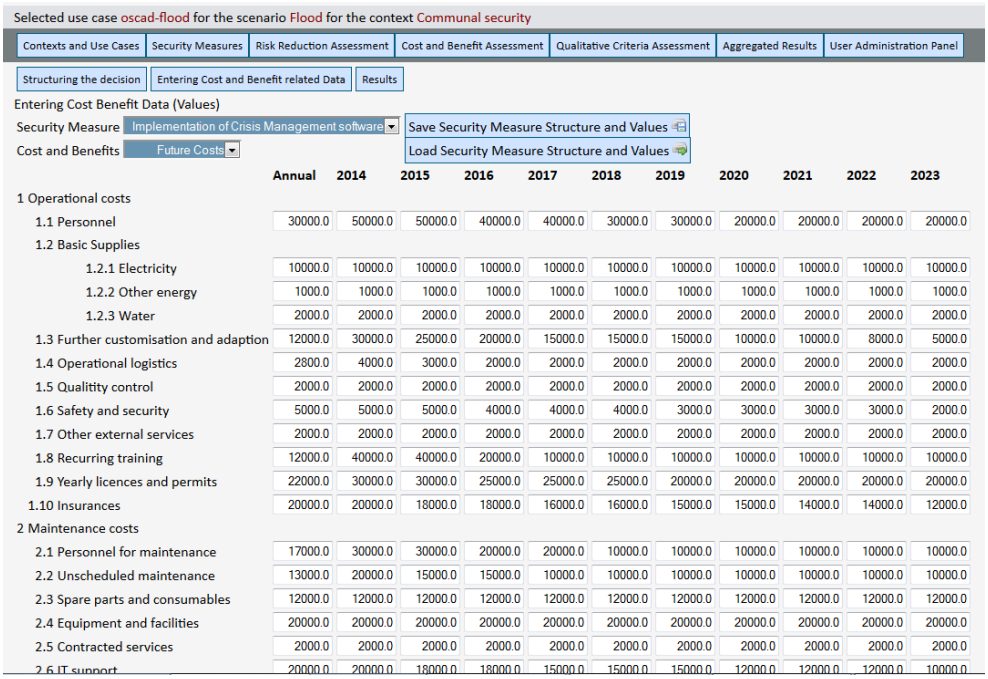
- initial planning cost, encompassing e.g.: project management, market research, concept design, travels, personnel,
- initial procurement process cost, including sub-subcategories: bidding process, licenses and permits, personnel,
- procurement, including: equipment, hardware, software, services, technical data and documentation, spatial facilities, construction,
- setup and integration, encompassing such sub-subcategories as: personnel, equipment, testing, experimenting, infrastructure, subcontracting, integration services, initial training, logistics for implementation, etc.,
- initial set of spare parts.

Future costs are incurred during security measures operation and maintenance. This category can encompass the following subcategories:

- operational costs, like: personnel, basic supplies (water, electricity), further customization and adaption, quality control, operational logistics, security and safety, other external services, recurring services, yearly licenses and fees, insurance fees, etc.,
- maintenance costs, including: personnel, spare parts and consumables, unscheduled repairs, IT support, equipment and facilities, contracted services,
- end-of-lifetime costs, including: personnel, shutdown cost, disassembly and removal, recycling, safe disposal, residual value,

– economic losses, like: business losses, reduced overall consumption, decrease in economic activity, decrease in touristic activity, decrease in quality of life, image losses,
– financing,
– public services disturbances.

Figure 3 presents the structure and values of "Future costs" related to the measure "Implementation of crisis management software".



	Annual	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
1 Operational costs											
1.1 Personnel	30000.0	50000.0	50000.0	40000.0	40000.0	30000.0	30000.0	20000.0	20000.0	20000.0	20000.0
1.2 Basic Supplies											
1.2.1 Electricity	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0
1.2.2 Other energy	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0	1000.0
1.2.3 Water	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0
1.3 Further customisation and adaption	12000.0	30000.0	25000.0	20000.0	15000.0	15000.0	15000.0	10000.0	10000.0	8000.0	5000.0
1.4 Operational logistics	2800.0	4000.0	3000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0
1.5 Qualitity control	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0
1.6 Safety and security	5000.0	5000.0	5000.0	4000.0	4000.0	4000.0	3000.0	3000.0	3000.0	3000.0	2000.0
1.7 Other external services	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0
1.8 Recurring training	12000.0	40000.0	40000.0	20000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0
1.9 Yearly licences and permits	22000.0	30000.0	30000.0	25000.0	25000.0	25000.0	20000.0	20000.0	20000.0	20000.0	20000.0
1.10 Insurances	20000.0	20000.0	18000.0	18000.0	16000.0	16000.0	15000.0	15000.0	14000.0	14000.0	12000.0
2 Maintenance costs											
2.1 Personnel for maintenance	17000.0	30000.0	30000.0	20000.0	20000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0
2.2 Unscheduled maintenance	13000.0	20000.0	15000.0	15000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0	10000.0
2.3 Spare parts and consumables	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0	12000.0
2.4 Equipment and facilities	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0	20000.0
2.5 Contracted services	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0	2000.0
2.6 IT support	20000.0	20000.0	18000.0	18000.0	15000.0	15000.0	15000.0	12000.0	12000.0	12000.0	10000.0

Figure 3. Future costs structure – an example *(Screen shot prepared by the author during the ValueSec validation, 2014)*

The costs are distributed along the applied time horizon.

The future benefits can encompass different subcategories, e.g.:

– reduction of casualties – saved lives, fewer injured people,
– reduction of damages – property-, infrastructure-, critical infrastructure-, environmental damages,
– reduced probability and/or frequency of threat,
– image benefits, etc.,
– reduction of operational cost and resources related to: assets, personnel, consumables,
– reduction of insurance fees,
– increasing business profits,

– residual value.

Figure 4 summarizes costs and benefits for 2 of 3 measures: "Implementation of crisis management software" and "Establishing a standardized secure communication network".

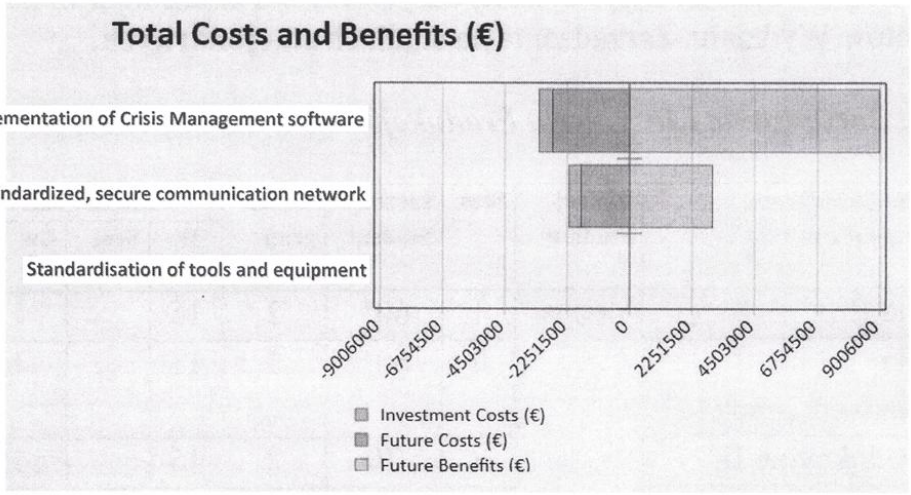


Figure 4. Cost-benefits summary *(Screen shot prepared by the author during the ValueSec validation, 2014)*

The bars on the left represent investment costs (violet) and future costs (dark blue). The right part of the bar (blue) stands for future benefits.

The CBA component is able to define the framing conditions and boundaries, i.e. the external factors and limitations affecting the decision process, e.g. budget. The budget volume is taken into account during the CBA calculation. Other examples of framing conditions can be the following:

– previous decisions implied by a certain security strategy,
– implementation time,
– different agreements, e.g. between industries and the government on certain security issues,
– threat perception and urgency, e.g. security incidents may trigger urgent needs to initiate some security measures,
– security governance, e.g. the rules of interacting with the government and other stakeholders,
– uncertainty and risk attitude of the decision maker.

The CBA setup needs to configure some variables, relevant for calculations:

– the time span and starting year – the time horizon for calculations, e.g. 10 years,
– the security measure functional lifetime used in the time span, e.g.: physical lifetime, technological lifetime, economic lifetime, or social lifetime,
– currency value,

- discount rate,
- budget limit.

Thanks to the CBA component it is possible to calculate the following key indicators (Räikkönen et al., 2012):

- Net Present Value NPV. NPV is the difference between the present value of cash inflows and the present value of cash outflows; the security measure is profitable if NPV > 0; according to CBA, the higher the NPV, the better the security measure;
- Present Value of Benefits PVB, Present Value of Costs PVC. The present value of benefits /costs is the estimated current value of a future amount which will be received or paid out, discounted at the specified discount rate;
- Benefit Cost Ratio. The benefit-cost ratio (BCR) is a ratio which attempts to identify the relationship between the costs and benefits of the proposed security measure /measures; the benefit-cost ratio (BCR) is calculated as the NPV of benefits divided by the NPV of costs where BCR >1 is good;
- Internal Rate of Return IRR (%). The internal rate of return is the discount rate when NPV=0; according to CBA, the higher the IRR, the better the security measure;
- Pay Back Period (years). The pay-back period is the time duration required to recover the cost of a security measure; the shorter the pay-back time, the better the security measure; the costs and benefits are not discounted;
- Discounted Pay Back Period (years). The discounted payback period is the time duration needed to cover the cost of a security measure, by adding positive discounted cash flow coming from the benefits of the implementation of a security measure; the shorter the pay-back time, the better the security measure;
- Total costs and benefits. Total costs and benefits are the total of discounted costs and benefits for the calculation period.

Figure 5 presents an example of the break-even diagram for “Implementation of crisis management software”. Please note that benefits will be higher than costs near the year 2020.

It is possible to present other diagrams as the analysis results, for example: costs and benefits, cash flows, break-even point (BEP). BEP shows the point in which the costs line crosses the benefits line (here costs and benefits are equal). The assessed countermeasures related to the risk and cost-benefits parameters pass to QCA to assess soft factors (Białas, 2013), not discussed there. The RRA, CBA and QCA aggregated results support the decision makers in their decision processes.

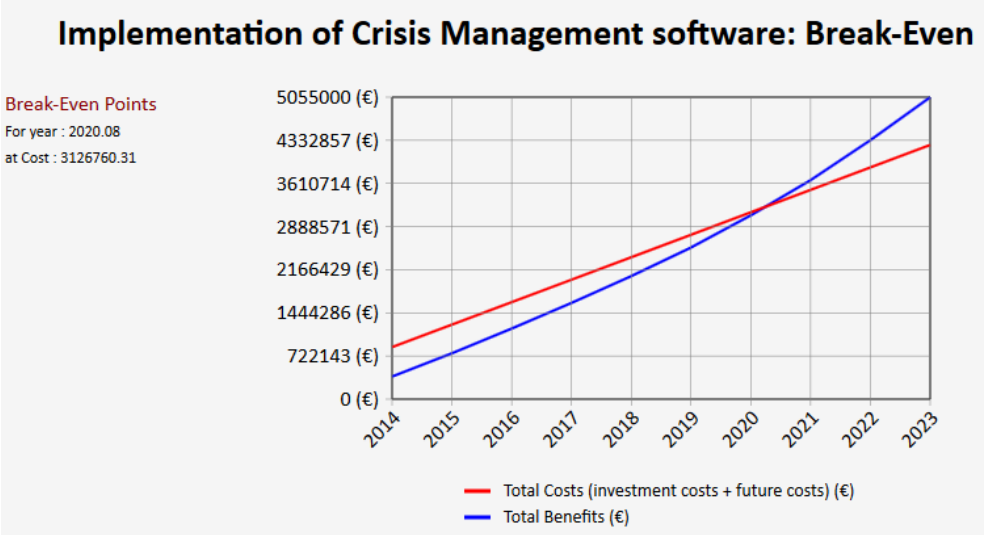


Figure 5. Break-even chart for the selected measure implementation *(Screen shot prepared by the author during the ValueSec validation, 2014)*

Conclusions

The decision making process in the security domain is very complex because each decision requires the trade-off between many factors of diversified nature. Besides, there are some fuzziness and uncertainties in the process. Each decision may have big financial consequences:

- insufficient countermeasures may cause incidents with tangible losses,
- overinvestment in security may decrease operation efficiency of an organization.

Security investment should be based on precise risk and financial assessments. Even if such assessment is carried out, still the right selected security measures may be ineffective in a crisis situation due to the existing constraints of non-financial and unclear nature (political, social, psychological, cultural, etc. factors). The ValueSec project solves all these issues, proposing the three pillars approach in the security measures selection for the given applications. One of them is the CBA pillar which effectively contributes to the ValueSec Toolset.

The ValueSec Toolset supports the optimization of the vector of values related to the given security measure and allows:

- to reduce the uncertainty related to the decision context,
- to reduce the fuzziness of the decision process,
- to provide better decisions argumentation for stakeholders and citizens.

After the project had been completed, three of ValueSec partners (Atos-Madrid, CESS-Munich, EMAG-Katowice) started to adapt and implement this methodology in a quite new application domain – critical infrastructure protection

in the EPCIP (European Programme for Critical Infrastructure Protection) Ciras project (EPCIP Ciras project, 2015). New problems are encountered in this domain. They are caused by critical infrastructures interdependencies and specific phenomena (cascading, escalation, common cause effects). All components (RRA, CBA, QCA) can be prepared to work in new and more complex application domains.

Ciras project has been funded with support from the European Commission. This publication reflects the views only of the author, and the European Commission cannot be held responsible for any use which may be made of the information contained therein (Grant Agreement clause).

Acknowledgement

I wish to thank my colleagues from the ValueSec project team for their co-operation in the course of the project.

References

Acquisti A., Grossklags J., 2005, *Privacy and Rationality in Individual Decision Making*, "IEEE Security & Privacy", 3(1), January/February.

Adar E., Blobner C., Hutter R., Pettersen K., 2012, *An extended Cost-Benefit Analysis for evaluating Decisions on Security Measures of Public Decision Makers*, CRITIS 2012, 7th Int. Conf. on Critical Inf. Infrastruct, Security, September 17-19, Lillehammer.

Białas A., Bagiński J. et al., 2012, *D4.1 Usability assessment criteria and usability analysis, Part 1, Part 2 (RE)*, http://www.valuesec.eu/content/d41-part-1-usability-assessment-criteria-and-usability-analysis.

Białas A., 2013, *Risk assessment aspects in mastering the value function of security measures*, [In:] Zamojski W. et al. (Eds.): New results in dependability and computer systems. Advances in Intelligent and Soft Computing, Vol. 224, 2013, Springer-Verlag: http://link.springer.com/chapter/10.1007%2F978-3-319-00945-2_3#page-1.

Białas A., 2014, *Enhancement of the ValueSec Risk Management Model*, Annals of Computer Science and Information Systems, Vol. 3, Federated Conf. on Computer Science and Information Systems.

Bjorheim A.E., Pettersen K., Terje A., Kaufmann M., Rosqvist T., 2015, *A framework for selection of strategy for management of security measures*, "Journal of Risk Research".

Cellini Riegg S., Kee J.E., 2010, *Cost-Effectiveness and Cost-Benefit Analysis*, [In:] Wholey J.S. et al., Handbook of practical program evaluation (Eds.), Wiley; Available at: http://home.gwu.edu/~scellini/CelliniKee21.pdf, Access on: 27.10. 2015.

ENISA, *Risk assessment*, 2015, https://www.enisa.europa.eu/activities/risk-management/current-risk /risk-management-inventory/rm-process/risk-assessment; Access on: May 2015.

Gordon L.A., Loeb M.P., 2002, *The Economics of Information Security Investment*, "ACM Transactions on Information and System Security", 5(4).

ISO 31000: 2009, *Risk management – Principles and guidelines*.

ISO/IEC 31010: 2009, *Risk Management – Risk Assessment Techniques*.

Kaufmann M., 2011, *D3.2 ValueSec Catalogue of evaluated methodologies and tools available,* http://www.valuesec.eu/content/d32-catalogue-evaluated-methodologies-and-tools-available.

OSCAD project: http://www.oscad.eu/index.php/en/; Access on: June 2015.

Poussa L., Räikkönen M., Jähi M. et al., 2011, *D2.5 Report on workshop on user needs and requirements*, http://www.valuesec.eu/content/d25-report-workshop-user-needs-and-requirements.

Rausand M., 2011, *Risk Assessment: Theory, Methods, and Applications*, Series: Statistics in Practice (Book 86), Wiley.

Räikkönen M., Rosqvist T., Poussa L., Jähi M., 2012, *A Framework for Integrating Economic Evaluation and Risk Assessment to Support Policymakers' Security-related Decisions*, PSAM11 & Esrel 2012 Int'l conference proc., Finland, June 25-29.

Räikkönen M., Kunttu S., Poussa L., 2013, *User guide – the CBA excel demo. CIRAS project*: http://ciras project.eu/content/project-topic, Access on: June 2015).

Rosqvist T., Räikkönen M., Jähi M., Poussa L., 2011, *2.2 Data model and decision model*, http://www.valuesec.eu/content/d22-data-model-and-decision-model.

ValueSec FP7, 2011 – 2014: *ValueSec – Mastering the Value Function of Security Measures*, Grant agreement No: 261742, www.valuesec.eu; Access date: June 2015.

ASPEKTY KOSZTÓW I KORZYŚCI W ZARZĄDZANIU RYZYKIEM

Streszczenie: Artykuł dotyczy ilościowych metod zarządzania ryzykiem, pozwalających na uwzględnienie w formie pieniężnej kosztów zabezpieczeń oraz korzyści związanych z redukcją ryzyka, uzyskiwanych w wyniku wdrożenia zabezpieczeń. Pokazano przykład zastosowania analizy kosztów-korzyści w projekcie FP 7 ValueSec zrealizowanym z udziałem Instytutu EMAG oraz zamierzenia wykorzystania tego podejścia w aktualnie realizowanym projekcie CIRAS (EPCIP) poświęconym zarządzaniu ryzykiem w infrastrukturach krytycznych. Przedstawiona została przykładowa struktura kosztów i korzyści oraz mierniki efektywności analizowanych rozwiązań. Artykuł przedstawia moduł analizy kosztów-korzyści na tle całego systemu ValueSec, obejmującego także szacowanie ryzyka oraz ocenę czynników pozaekonomicznych, ograniczających efektywność zabezpieczeń.

Słowa kluczowe: zarządzanie ryzykiem, podejście koszty-korzyści, oprogramowanie do zarządzania ryzykiem

風險管理中的成本效益問題

摘要：本文涉及安全領域的高級風險管理。這種方法不僅基於傳統風險評估，而且還基於財務成本效益分析和確定隱藏的非財務因素，這些因素可能危害業務環境中的安全措施的運行。本文與FP7ValueSec項目相關，並介紹其背景，方法和結果。特別關注擬議的安全措施的成本效益評估（CBA）。
成本和效益類別與CBA組件的操作一起討論。精心設計的工具集用於支持不同安全領域的決策者。

關鍵詞：風險管理，成本效益的方法，軟件風險管理