ISO/IEC 27001-Based Estimation of Cybersecurity Costs with Caspea

Rafał Leszczyna
Gdańsk University of Technology
Faculty of Management and Economics
Gdańsk, Poland *rafal.leszczyna@pg.edu.pl*

Abstract

In the contemporary, knowledge-based economy, enterprises are forced to bear the costs related to cybersecurity. While breaches negatively affect companies' budgets, accurate decisions on security investments result in visible savings. At the same time, cybersecurity cost assessment methods that support these decisions are lacking. Caspea addresses the gap by enabling the estimation of costs related to personnel activities involved in cybersecurity management. In this paper, new advancements in the research related to the construction of an ISO/IEC 27001-based costing model are described. This includes revising cost centres based on the ISO27k RASCI matrix, minimising input and output data, or implementing a new calculation spreadsheet that contains substantial changes compared to its previous editions. A comparative analysis with the earlier version of Caspea has been performed. The application of the new model to a wood-working company is illustrated. The results show gradual extension and the broader scope of the Caspea framework.

Keywords: computer security, cost estimation, cost evaluation, comparative analysis, ISO/IEC 27001

1. Introduction

Costs of cybersecurity management are the costs related to various types of controls and activities for reducing cybersecurity risks [4]. Among the others, they include the costs induced by security incidents, costs of security management, costs of protection measures, and the costs of capital induced by information security risks [4]. The costs embrace investments, consequences of cybersecurity breaches, responsive actions and indirect costs (e.g. associated with loss of image or loss of customers' trust). In the contemporary, knowledge-based economy and with the omnipresence of information technologies that are largely exposed to cyberattacks, these costs are borne by practically all enterprises. At the same time, the enterprises which decided to invest in appropriate cybersecurity controls noted substantial technology savings [1]. Informed decisions in security expenditures are key for the operation of today's enterprises. Yet, as they compete with other areas of company activities, they require good justifications. However, practical tools for evaluating the cost of cybersecurity needed for effective decision-making regarding cybersecurity investments are lacking.

Caspea – the *C*ost *As*sessment of *Pe*rsonnel *A*ctivities in Information Security Management was introduced in response to this demand [19]. The method enables rough evaluations of the cost of activities of all employees and stakeholders that are related to cybersecurity management in daily work. For security or IT officers, these costs concern, for instance, designing and sharing security policies or organising security workshops. For other personnel, the same activities induce costs related to reading the documents or participating in the events. At the same time, the costs of cyberassets involved in the cybersecurity management, such as physical equipment, hardware or software, are excluded from the estimations. Caspea employs the Activity-Based Costing approach and thus far it has been adopting the NIST SP 800-53 guideline as a source

of cybersecurity activities. While the document is a broadly recognised and acknowledged publication that provides detailed descriptions of cybersecurity controls and for that reason, it was selected as a source for the list of activities, the direct connection of the framework to the primary cybersecurity standard, namely ISO/IEC 27001, has been missing, marked as further research work. As a result, the question of whether Caspea would appropriately estimate the costs of cybersecurity management activities specified in the norm has been remaining open. This paper presents new developments in the method that fill the gap. The primary contributions are:

- The development of a new version of Caspea that directly adopts ISO/IEC 27001.
- The implementation of a worksheet-based tool prototype to facilitate calculations.
- The comparative analysis with the NIST SP 800-53-based version.
- The revision of the method's costing model including the adaptation of cost centres in accordance with the ISO27k RASCI matrix.
- Illustration of the application of the novel version of Caspea through a case study.

The paper has the following organisation. After the introduction of the background knowledge, including the relevant research, ISO/IEC 27001 and NIST SP 800-53 documents, SQUARE and ISO27k RASCI (Section 2), the original Caspea is briefly introduced (Section 3). The new developments related to ISO/IEC 27001 integration are described in Section 4. Section 5 presents a case study of using the new version of Caspea. The comparative analysis of NIST-based and ISO-based methods is described in Section 6. The paper ends with closing remarks.

2. Background

This section commences with a discussion of the relevant research on the cost of cybersecurity. This is followed by a brief presentation of the ISO/IEC 27001 standard and the NIST Special Publication 800-53. Also, an overview of the SQUARE method used in the comparative analysis of Caspea (see Section 6) and the ISO27k RASCI matrix applied to the extended version of Caspea (see Section 4) described in this paper are provided.

2.1. Related work

The research on cybersecurity costs dates from 1979 when the Annual Loss Expectancy (ALE) was pointed out as a measure for incident cost analysis [20]. From that time multiple methods and models have been proposed [20]. Primary *financial indicators* used in the analysis of the costs of cybersecurity are the rate of return (RR), maximum net present value (NPV) or the return of investment (ROI). The studies of the *cost of cybercrime* include the research of Riek et al. [27] on measuring the costs of cyber-crime or Farahmand et al. [9] who proposed the criteria for categorising enterprise information assets and provided a scheme for probabilistic analysis of the impact of security threats.

Among the *economics-based* security studies, Sawik [30] analysed the application of several Stochastic Mixed Integer Programming models to the optimal selection of protection controls in an enterprise supply chain. A similar topic, but with non-linear budget constraints, was studied by Daniele and Scrimali [7] and Nagurney et al. [21]. Ioannidis et al. [13] proposed a dynamic model of security investments that takes into account the confidentiality and availability trade-offs. In 2010 an alternative dynamic model was introduced by Tatsumi and Goto [32]. The same year Böhme et al. [3] designed a model that incorporates penetration testing activities. In the context of cyber-insurance, a policy-purchasing optimisation model based on the impact of secondary losses was introduced by Bandyopadhyay and Mookerjee [2]. Pal et al. [24] developed a model for deriving optimal cyber-insurance contracts for welfare-maximising or profit-maximising strategies. Shetty et al. [31] performed model-based studies on the effects

of cyber insurance on customers' security and welfare. Other economics-related security studies include the research of Havakhor et al. [11] on the capital market's response to enterprises' investments in cybersecurity, Rodrigues et al. [29] who proposed a framework for impact assessment of cybersecurity investments in distributed ecosystems, the Chessa et al.'s [6] cooperative game-theoretic approach to quantify the value of personal data in networks, or the Robinson's et al. [28] application of stated preference discrete choice experiments (SPDCEs) to analysing and quantifying individuals' security and privacy preferences.

Cost calculators are easy-to-use tools for obtaining approximate costing data based on some input information about an organisation. Openly available cybersecurity cost calculators include, for instance, the Kaspersky IT Security Calculator [16] or eSentire Security Operations Center Pricing Calculator [8]. Concerning the *methods for calculating the costs of implementing security controls* only a few solutions have been developed. This includes I-CAMP and I-CAMP II [26], SAEM [5] or SQUARE [35], the latter of which has gained the broadest adoption. A mapping between the NIST Cybersecurity Framework (CSF) and the costs of quality was developed by Radziwill and Benton [25]. The mapping enables linking accounting elements associated with cybersecurity operations and risk management to a quality cost model. An approach for integrating cost–benefit analysis into CSF using the Gordon–Loeb Model was proposed by Gordon et al. [10].

Summarising, the research has been mostly focused on cybersecurity investments or financial consequences from security breaches. Depending on the study, the costs are considered individually or in the cost-benefit analysis. Both, micro- to macro-economic views are provided. In this respect, Caspea provides a complementary view into the costing component associated with personnel activities related to cybersecurity.

2.2. ISO/IEC 27001

ISO/IEC 27001 is the primary, "number-one" international standard focused on the security of information systems. It centres around the concept of the Information Security Management System (ISMS) developed in the framework of cyclic risk management. Security controls are presented in Annex A of the publication. The catalogue is comprehensive, however, in contrast to NIST SP 800-53, the descriptions are very concise and high-level. They are mostly one-sentence-based, while the specifications of analogous controls in NIST SP 800-53 contain several pages. This is justified by the general scope of the standard that can be adopted by organisations of various sizes and specialisations, as well as by leaving the choice to organisations on how to implement the controls. Another substantial difference is the possibility of obtaining an internationally recognised information security certificate.

2.3. NIST SP 800-53

NIST SP 800-53 is a guideline-type, technical document developed in response to the US legislation requirements concerning the protection of federal information systems. It provides a catalogue of cybersecurity and privacy controls organised in three baseline sets that correspond to the criticality of the systems. Revision 4 of the publication contains 115 controls for systems with low impact on organisations and individuals, 159 for systems with moderate impact and 170 for high-impact systems. The document is comprehensive in terms of the portfolio of cybersecurity controls as well as the level of detail in their descriptions. It was developed by the Joint Task Force Interagency Working Group formed by a large group of experts from various national civil, defence and intelligence organisations including the Department of Commerce, the Department of Defense, the Office of the Director of National Intelligence, or the Committee on National Security Systems. Additionally, the work of the working group is supported by contributions from other relevant bodies. The publication is reviewed and updated periodically. Since

its first version in 2005, it has evolved from a single, around a hundred pages, self-contained document into a small library with the main publication and multiple supporting documents. The document is broadly recognised worldwide and earned the status of de facto standard. It is compatible with ISO/IEC 27001 which is documented by a bidirectional mapping of all NIST and ISO controls [22].

2.4. SQUARE

The Cost/Benefit Analysis-based framework was introduced in 2005 by the System Quality Requirements Engineering (SQUARE) Team from Software Engineering Institute (SEI), Carnegie Mellon University [35], meeting a visible interest of researchers. From the time of its proposal, the method has been applied to various contexts and broadly documented while the associated research, associated primarily with the elicitation of cybersecurity requirements (with substantial consideration of costs) has been continued. The method estimates the costs of computer security-related projects conducted in small enterprises based on threat categories that are publicly available from national surveys. For each category of threats, costs, benefits, baseline risks, and residual risks can be estimated assuming average yearly probabilities of categorised threats and averaged extent of financial loss resulting from the exposure to threats in the categories [35]. The steps of calculation include the analysis and description of misuse cases, the categorisation of the cases into categories of threats, the derivation of categories of preventions, the calculation of total implementation costs, the net project value, the total system value or the benefit/cost ratio for several alternatives of cybersecurity improvement projects, and the selection of the optimal project [35].

2.5. ISO27k RASCI matrix

The ISO27k RASCI matrix was published by the ISO27k Forum [33]. The table associates roles (posts) in an organisation with ISO/IEC 27001 cybersecurity activities and participation types. The roles adopted in the model as cost centres comprise the executive management (senior-level executives or managers), ISMS Steering Committee, information security professionals, the heads of various units, or regular workers. Five main participation types are distinguished in the responsibility assignment matrix. *Responsible* participants have first responsibility for performing a cybersecurity management activity. *Accountable* participants are called to account when risks materialise. They are usually budget holders. *Supportive* actors actively assist in the design, implementation or management of a cybersecurity management activity. *Consulted* parties provide information or advice to the actors actively involved in a cybersecurity management activity. *Informed* parties have an interest in the risk status of cybersecurity management activity.

3. NIST-based Caspea

Caspea – *C*ost *As*sessment of *Pe*rsonnel *A*ctivities in Information Security Management is a method dedicated to the estimation of the costs related to human involvement in cybersecurity management. In other words, Caspea facilitates the assessment of costs of cybersecurity management activities performed by employees and other stakeholders. Examples of the activities include developing cybersecurity policies, participating in training courses, and configuring and deploying technical protection measures or cybersecurity testing. The main components of the method are presented in Figure 1. All the elements were revised and modified in the new, ISO-based, version of Caspea. The components that were newly introduced to the Caspea method are indicated by a bold style. They are described in the next section (Section 4).

In accounting, a *costing system* enables the grouping and assignment of costs to cost objects (e.g. units of production, departments, or other activities) to facilitate monitoring of the

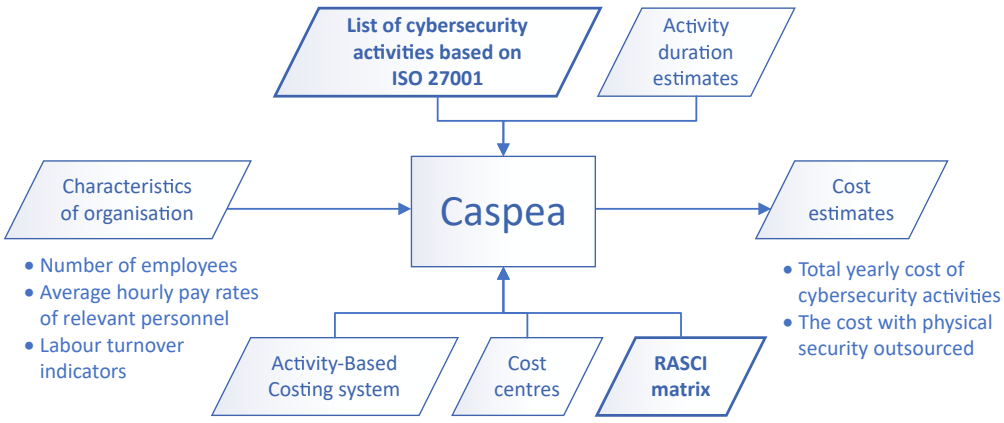


Fig. 1. The main components of the Caspea method. The elements newly introduced to the ISO-based Caspea are depicted by a bold style.

costs incurred by an organisation. There are various costing systems, including direct costing systems, traditional absorption costing systems and hybrid costing systems. Caspea adopts the *Activity-Based Costing (ABC) system* as it is most suitable due to recognising activities (human or machine operations) as fundamental objects that induce costs in enterprises. The total cost in an organisation is calculated as a sum of the costs of all activities performed in an enterprise. Then, to derive the costs of activities, the proper *cost centres* must be assigned to them using relevant cost drivers. Duration driver in the form of working time expressed in hours was chosen as the activity cost driver. In the earlier research, the list of 115 first-baseline cybersecurity controls from NIST SP 800-53 Revision 4 published in 2013 was used as a reference *list of the activities* [18].

For its input, Caspea requires only a small set of data that characterise an organisation (*Characteristics of organisation*). This includes the number of employees, average hourly pay rates of personnel that are responsible for, accountable, supportive, consulted or informed during cybersecurity management, or labour turnover indicators. Based on the data, the minimum, maximum, and usual approximated total cost of personnel activities related to cybersecurity management are calculated. To facilitate the estimations, a calculation spreadsheet was developed [18]. By design, Caspea is primarily dedicated to supporting decision-making in medium or small enterprises, or divisions of larger organisations. However, through adjustments in the activity duration estimates that serve for calculations of the total values (see Section 3), the framework can be adapted to organisations of larger sizes. Similarly, while the direct total cost estimates obtained with Caspea can be interpreted as generally valid for organisations of different types, the tailoring of the activity duration times can lead to more precise results for specific sectors. These adjusting/tailoring activities require additional, sometimes substantial, effort from organisations as all the relevant data need to be gathered.

4. Integration of ISO/IEC 27001 into the costing model

This paper presents new developments in the Caspea framework, where the ISO/IEC 27001 standard [14] forms the direct foundation of the costing model. The primary objectives of the research were as follows:

1. Providing a costing model that directly adopts the ISO/IEC 27001 international standard.
2. Evaluating potential differences in cost estimates obtained with the NIST and ISO-based models.
3. Extending the portfolio of tools to be used for estimations.
4. Supporting the choice of which of the publications, the NIST's or ISO's, to follow when

establishing a cybersecurity management system.

To assure consistency with the earlier research, the ISO/IEC 27001:2013 version convergent with NIST SP 800-53 Rev. 4 used in the NIST-based model was adopted. At the same time, it needs to be noted that the current edition of the standard, namely ISO/IEC 27001:2022 [15] introduced mostly minor or moderate alterations to its previous version. Although the number of controls was reduced from 114 to 93 and the controls were organised into 4 instead of 14 sections, the changes resulted primarily from merging and reorganisation of controls. 11 new controls were introduced that follow the trends in ICT and information security [17]. However, the direct incorporation of the modifications and their study in reference to the newer version of NIST SP 800-53 i.e. its Revision 5 [23] is envisaged as a subsequent incremental step of the research.

With relation to the earlier NIST SP's 800-53-based version, cost centres were revised to more precisely match the information security management according to the ISO/IEC 27001 norm. This was done based on the ISO27k *RASCI matrix* (see Section 2.5). A crucial component of the model is the *estimation of the duration of each activity* performed by a cost centre. Three-point estimations have been provided based on expert judgement and analogous estimating [34]. Similar to NIST-based Caspea, the evaluations were carried out by a single appraiser and are subjective. This forms a limitation of the study that calls for further research. For instance, multiple organisations, ideally from different sectors, that already established cybersecurity management systems can be surveyed for costing figures. At the same time, the current implementation of the model enables obtaining rough estimations that should support decision-making. Moreover, companies can adopt the model by adjusting the estimations to their context.

For multiple activities, their duration depends on the size of an organisation. Thus, variable dependencies were introduced in the calculations. They come from the observation of general practices applied in organisations. Based on the characteristics of each specific activity, the dependencies have linear (1) or logarithmic forms (2):

$$D_A = N_E \times x + y \tag{1}$$

$$D_A = \log_z N_E \times x + y \tag{2}$$

where: D_A – activity duration time [hours], N_E – number of employees, z – logarithm base that reflects the level of effort required for an activity, usual values include 10 or 100, x – variable factor [hours], y – fixed factor [hours].

For instance, the time needed for user registration and granting system access rights (ISO/IEC 27001 security control no. A.9.2.1) depends linearly on the number of users. At the same time, the time for devising information security policies (ISO/IEC 27001 security control no. A.5.1.1) by security professionals exhibits logarithmic dependence on the number of employees.

The assignment of cost centres to activities and the estimation of the duration of each activity can be explained in an example. Referring to the user registration activity, according to the ISO27k RASCI matrix, four main roles are involved in the task, namely the head of HR (responsible), IT officers (supportive), ISMS Steering Committee (supportive) and information security professionals (consulted). The time used by IT officers necessary to register or unsubscribe enterprise employees depends on the number of employees, also the involvement of the head of HR who is responsible for the task changes depending on the size of the organisation. As a result, the formulas, as presented in Table 1 were assigned to the activity.

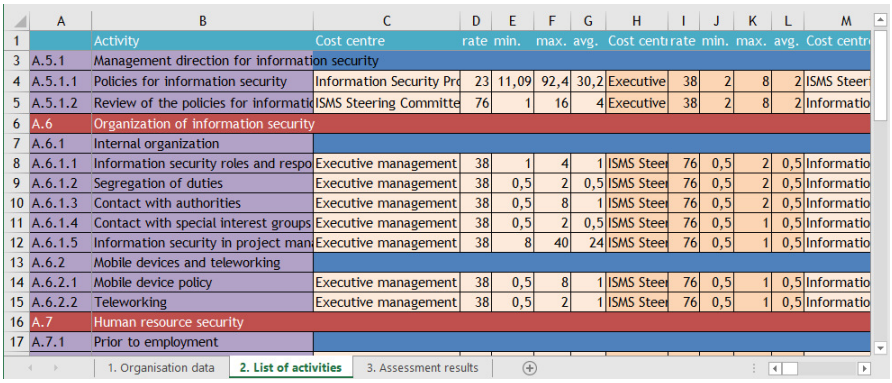
The Caspea spreadsheet developed to facilitate calculations was modified substantially, compared to its NIST SP 800-53-based version. Now, it comprises three (instead of four) worksheets representing subsequent steps of the assessment process. The *Organisation data* worksheet for entering the input data was updated to represent the roles associated with the implementation of the ISO/IEC 27001 Information Security Management System. To increase the intuitiveness of working with the tool and reduce the effort related to its learning, the set of input data

Table 1. The assignment of cost centres to activities and estimated task durations for the activity related to ISO/IEC 27001 security control A.9.2.1 User registration and de-registration. N_E – number of employees

Role	Head of HR			IT officers			ISMS Steering Committee			IT security professionals		
Participation type	Responsible			Supportive			Supportive			Consulted		
Estimation type	Min.	Max.	Usual	Min.	Max.	Usual	Min.	Max.	Usual	Min.	Max.	Usual
Estimation formula	$8 + 4\log_{100} N_E$	$40 + 4\log_{100} N_E$	$16 + 4\log_{100} N_E$	$0,15 \times N_E$	$0,5 \times N_E$	$0,25 \times N_E$	0,5	2	0,5	4	24	8

has been minimised. It contains the number of employees, hire rate, termination rate, promotion/demotion/transfer rate, the planned number of ISMS Steering Committee members and average hourly pay rates of personnel. At the same time, the mobile devices usage index and the average number of outsiders having access to the system input data have been removed from the worksheet. Multiple experiments with the earlier, NIST-based, version of the tool showed that these factors had a negligible impact on the total cost estimations. The number of ISMS Steering Committee members is used to calculate the ISMS Steering Committee pay rate by being multiplied by the pay rate at the executive management position. The worksheet *List of activities* (see Figure 2) comprises the formulas for the calculation of the total cost of activities. The activities reflect the ISO/IEC 27001 control areas. The roles according to the ISO27k RASCI table from ISO27k Forum and new activity duration estimations were introduced.

To improve the clarity of the results and to focus on the most important aspects, the *Assessment results* worksheet was simplified. It currently contains solely the estimations of the minimum, maximum and usual total values of the information security management activities and the analogous estimations assumed that the physical security of facilities was outsourced by the organisation. This means that three tables in the NIST-based version concentrated only on the activities of cybersecurity professionals were removed from the tool. The tables provided information of secondary importance, namely the estimations of total costs of activities performed exclusively by information security professionals, the estimated numbers of required working hours for information security professionals and the forecast required number of information security professionals. At the same time, the table with estimated total yearly costs of activities associated with information security management in the enterprise with physical security outsourced was introduced. This is because analyses performed for various organisations showed that outsourcing physical security has a substantial impact on costing figures and thus visualising that in a dedicated table should form a helpful aid during decision-making.



	A	B	C	D	E	F	G	H	I	J	K	L	M
1		Activity	Cost centre	rate	min.	max.	avg.	Cost centr	rate	min.	max.	avg.	Cost centr
3	A.5.1	Management direction for information security											
4	A.5.1.1	Policies for information security	Information Security Pr	23	11,09	92,4	30,2	Executive	38	2	8	2	ISMS Steer
5	A.5.1.2	Review of the policies for informati	ISMS Steering Committe	76	1	16	4	Executive	38	2	8	2	Informatio
6	A.6	Organization of information security											
7	A.6.1	Internal organization											
8	A.6.1.1	Information security roles and respo	Executive management	38	1	4	1	ISMS Steer	76	0,5	2	0,5	Informatio
9	A.6.1.2	Segregation of duties	Executive management	38	0,5	2	0,5	ISMS Steer	76	0,5	2	0,5	Informatio
10	A.6.1.3	Contact with authorities	Executive management	38	0,5	8	1	ISMS Steer	76	0,5	2	0,5	Informatio
11	A.6.1.4	Contact with special interest groups	Executive management	38	0,5	2	0,5	ISMS Steer	76	0,5	1	0,5	Informatio
12	A.6.1.5	Information security in project man	Executive management	38	8	40	24	ISMS Steer	76	0,5	1	0,5	Informatio
13	A.6.2	Mobile devices and teleworking											
14	A.6.2.1	Mobile device policy	Executive management	38	0,5	8	1	ISMS Steer	76	0,5	1	0,5	Informatio
15	A.6.2.2	Teleworking	Executive management	38	0,5	2	1	ISMS Steer	76	0,5	1	0,5	Informatio
16	A.7	Human resource security											
17	A.7.1	Prior to employment											

1. Organisation data | 2. List of activities | 3. Assessment results

Fig. 2. The ISO/IEC 27001-based Caspea *List of activities* worksheet, the centre of calculations, contains new ISO27k RASCI-related roles and revised task duration formulas.

5. Case study

In the earlier research, the NIST SP 800-53-based Caspea was applied to estimate the costs in public and private sector organisations, including critical infrastructures. The aim of the case study presented in this section is to illustrate the process of using the new ISO/IEC 27001-based version of Caspea. The subsequent steps of the estimation are presented in the context of a shared services centre of a European woodworking company. The shared services centre is a local unit of the entire international woodworking group that constitutes a good, structured and non-complex basis for the illustration. It shows the most common context in which Caspea is applied, namely a division of a medium- or large- size company or a small organisation that reflects the typical level on which cybersecurity decisions and investments are made. Also, the company is a good representative of a large group of medium-size, production-based, highly computerised and international enterprises.

The entire enterprise provides services in thirty countries all over the world. It comprises five main divisions: paper and board production, pulp processing, wood products and timber, tissues and paper towels, and forest services. The shared services centre handles financial transactional and accounting processes for the group companies located in Europe. It has over 150 employees. The structure of the IT system operating in the local centre is presented in Figure 3.

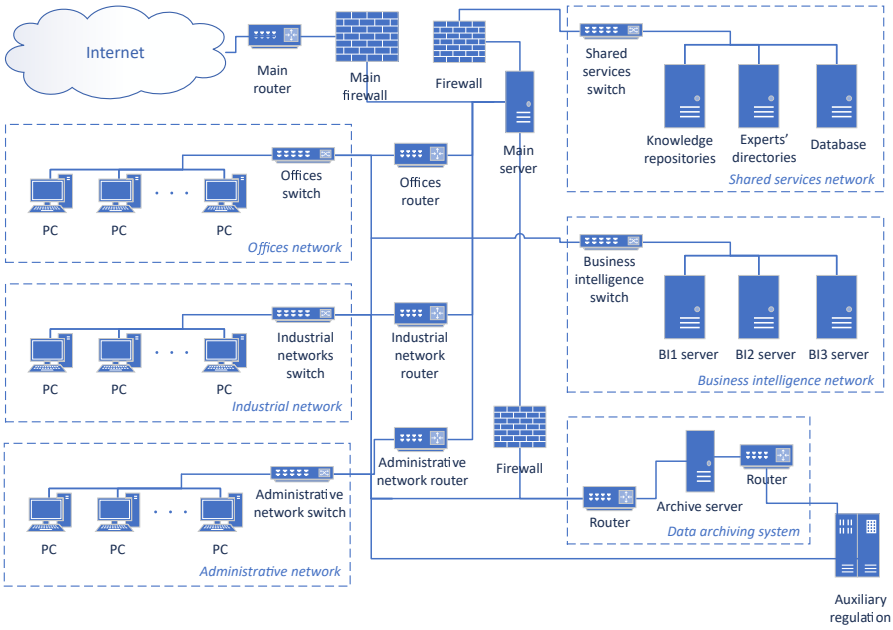


Fig. 3. IT system in the shared services centre of the woodworking company

5.1. Input data

The local centre has five main departments that report to a general director. The divisions have the following employment structure. The *General Ledger Department* employs the head of the unit, 4 team leaders and a team of 25 accountants. The *Accounts Receivable Department* has the head of the unit, 3 team leaders and 20 accountants. The *Accounts Payable Department* embraces the head of the unit, 5 team leaders and a team of 40 accountants. The *Customer Contact Department* encompasses the head of the unit, a team leader and 12 agents. The *Technical Department* employs one expert, a senior specialist and a specialist. Thus, as far as the input data for Caspea are concerned, the *Number of employees* equals to 35, the *Planned number of ISMS Steering Committee members* was assigned 2, and the *Hire rate*, *Termination rate* and *Promotion/demotion/transfer rate* are at the level of 10%.

The average hourly gross pay rates necessary to estimate the total cost of information security activities were based on the data from the Hays Poland Salary Guide [12] and converted to Euro from Polish Złoty with a rounded average exchange rate equal to 4,7[1]. The rate can be also used to approximate the values in US dollars (USD). The *Average hourly gross pay rates* introduced to Caspea ranged from 5,7 Euro for physical security officers, to 76 Euro for the members of ISMS Steering Committee.

5.2. Results

The cost estimates are obtained immediately (real-time) after the introduction of input data into the calculation spreadsheet. The estimated typical total yearly cost of activities associated with information security management in the enterprise is around 242 thousand Euro. This cost can be reduced by 50% if the organisation decides to perform just the baseline cybersecurity management. At the same time, the sum to be spent when extensively implementing all security actions reaches as much as 650 thousand Euro yearly.

These values reflect the entire annual cost of personnel activities involved in implementing the ISO/IEC 27001 Information Sharing Management System (ISMS) [14]. Especially for the non-IT employees, the cost should be interpreted as 'deduced' from regular annual salaries and associated with the workers' time spent on the ISMS implementation. It shows which part of the regular workforce remuneration will go to cybersecurity management. For frontline actors, such as the ISMS Steering Committee, information security professionals or IT officers the cost may exceed the currently paid amounts. This means that additional crew needs to be recruited. For a large, international enterprise such as the woodworking group, the estimated monthly cost of around twenty thousand Euro should justify the decision to introduce the ISO/IEC 27001 controls to protect data in the important unit that performs finance and accounting operations.

6. Comparative analysis with NIST 800-53

In the earlier research [19], as a part of the method's evaluation, Caspea was subjected to a comparative analysis with SQUARE [35] based on two existing small and medium enterprises that operate in the global and national (Polish) market: a boatyard and an IT support company. The SQUARE method was chosen for a reference method in the evaluation due to its broad application and acceptance (see Section 2.4). This section presents an analogous analysis that aims at comparing the earlier, NIST SP 800-53-based version of Caspea with the new one. To maintain the continuity of the approach that enables also comparing to SQUARE, the same organisations were taken for reference in the study.

6.1. Analysed organisations

The shipyard designs and builds custom-made luxury sailing and motor catamarans as well as superyachts. The company operates in the global market. It realises contracts with individual customers and specialises in the production of vessels where designs and their implementation are customised to the requirements of the contractor. The company very intensively applies information technologies, thus assuring the security of information assets is crucial.

The IT support company provides its services to a publishing group which is one of the largest publishers in Poland. It develops and maintains a large portfolio of Internet portals. The most popular of them is an advertisement service recognised in all country regions. Another is the Internet issue of one of the oldest journals. The internet traffic reaches a few million page hits daily for each service. The company databases store hundreds of thousands of personal

[1]Source: https://www.exchangerates.org.uk/EUR-PLN-exchange-rate-history.html. Last access: 11 October 2023.

Table 2. Input data for the comparative analysis of ISO/IEC 27001- and NIST SP 800-53-based Caspea for two organisations

Caspea	NIST-based	ISO-based	NIST-based	ISO-based
Organisation	Boatyard		IT support company	
Indicator	**Input data**			
Number of employees	35		95	
Planned number of information security professionals	0	n.a.	1	n.a.
Planned number of ISMS Steering Committee members	n.a.	2	n.a.	2
Hire rate	34,29%		24,21%	
Termination rate	28,57%		26,32%	
Promotion/demotion/transfer rate	8,57%		32,63%	
Mobile devices usage index	25,71%	n.a.	42,11%	n.a.
Average number of outsiders having access to the system	6	n.a.	30	n.a.

Table 3. Estimates of the total yearly cost [in USD] of activities associated with cybersecurity management obtained with ISO/IEC 27001- and NIST SP 800-53-based Caspea for two organisations. Also, the ratio between the two models' results is indicated.

	Total cost of security management activities [USD]			
Caspea	Min.	Max.	Avg.	Usual
Boatyard				
NIST-based	39 949,48	128 278,19	84 113,83	57 875,19
ISO-based	52 689,28	279 188,22	165 938,75	104 234,79
ISO/NIST	131,89%	217,64%	197,28%	180,10%
IT support company				
NIST-based	50 774,37	190 843,97	120 809,17	70 646,55
ISO-based	76 338,07	441 813,21	259 075,64	159 920,08
ISO/NIST	150,35%	231,50%	214,45%	226,37%

data, which again, require effective protection. A more detailed description of the organisations is presented in [19].

6.2. Input data

During the analysis, the same input data as during the earlier comparative analysis with SQUARE were introduced to the new version of Caspea. The only adjustments resulted from the modifications of the input data set that are described in Section 4. The input data that characterise analysed organisations are summarised in Table 2. The average hourly gross pay rates from the earlier study were adopted for the analysis.

6.3. Estimations

Based on the input data presented in Table 2, the estimates summarised in Table 3 were obtained. The values were converted to US dollars (USD) from Polish Złoty with a rounded average exchange rate equal to 4 congruently with the comparative analysis described in [19]. It needs to be noted that a revised version of NIST-based Caspea was applied to the analysis. Thus, the results for the version differ from the earlier analysis.

6.4. Results analysis

Looking at the results, the estimates of usual total costs obtained with the new ISO/IEC 27001-based model of Caspea are approximately two times higher than NIST-based (see the columns with ratios between the two models' results in Table 3). The reasons for that situation are primarily twofold. First of all, while both models reflect compatible processes that aim at providing comprehensive cybersecurity protection, which is documented in the mappings between NIST 800-53 and ISO/IEC 27001 controls (see Tables H-1 and H-2 in [22]), the structure of the tasks

is different. This results in differences in individuals' efforts assigned to a particular activity. Moreover, the NIST and ISO/IEC controls are highly equivalent but not fully equivalent. NIST notes that there is a degree of subjectivity in the mapping analysis that results in not always one-to-one representation. Also, organisation-specific implementations may play a role in control equivalency. In addition, a few ISO/IEC 27001 security controls could only be directly mapped to a NIST SP 800-53 control enhancement, while Caspea does not incorporate control enhancements at the current moment. The difference between the formulation of security management activities in the two models also results in a different structure of individual task duration estimations. For instance, the variable dependency component (see Section 4) occurs around 50 times in NIST-based Caspea, while more than 800 in the ISO/IEC version.

Secondly, in the NIST-based model, only one role is associated with an activity (for 74 out of 115 activities). Two roles occur sporadically (19 times) and three (the maximum) only once. In the ISO version, due to adopting the ISO27k matrix of roles and responsibilities (see Section 4), typically 4 or 5 roles are assigned to an activity (for 72 out of 114 activities). There are 16 activities with more than 5 roles assumed and the minimal assignment is 2, occurring only for 5 activities. These findings can be summarised into an observation, that the new version of Caspea more comprehensively reflects the involvement of other organisation roles in information security management tasks.

7. Conclusions

The paper presented the new research on the Caspea cybersecurity cost estimation method that centres around the integration of the ISO/IEC 27001 international standard. In the study, ISO/IEC security controls were transposed to the Caspea costing model, including the assignment and evaluation of related activity duration times as well as the adaptation of cost centres in accordance with the ISO27k RASCI matrix. The assignment of duration times to activities represents a subjective component of the study that has an impact on the precision of cost estimations especially in the context of a variety of organisations to which Caspea is dedicated. For that reason, further exploration of activity duration times, for instance through surveying companies of different sizes and sectors constitutes a prospective study area. Moreover, the study, at its current stage, forms an opening voice, a proof of concept, rather than a final proposal.

Multiple areas of the research deserve further exploration. Among the others, they include analysing the applicability of Caspea in various economic sectors, evaluating the method's fitness and accuracy to a particular economic sector, or including the risk as a driving factor of estimations. Also, extending the set of organisations included in the comparative analysis could provide additional insights into the differences between different costing models incorporated in Caspea. At the same time, the rough estimations obtained with Caspea should constitute a valid argument in cybersecurity investments-related decision-making. Supported by the two versions of Caspea, organisations can choose which of the two most common information security standards and guidelines (ISO/IEC 27001 or NIST 800-53) to follow when establishing a cybersecurity management system.

References

1. Accenture and Ponemon Institute. The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. Technical report, Ponemon Institute LLC (2019)
2. Bandyopadhyay, T., Mookerjee, V. A model to analyze the challenge of using cyber insurance. *Information Systems Frontiers*, 21(2):301–325 (2019) ISSN 1572-9419. https://doi.org/10.1007/s10796-017-9737-3.
3. Böhme, R., Félegyházi, M. Optimal information security investment with penetration testing. In *Lecture Notes in Computer Science*, pages 21–37. Springer, Berlin, Heidel-

berg (2010) ISBN 3642171966. https://doi.org/10.1007/978-3-642-17197-0_2.
4. Brecht, M., Nowey, T. A closer look at information security costs. In *The Economics of Information Security and Privacy*, pp. 3–24. Springer, Berlin, Heidelberg, 2013. ISBN 9783642394980. https://doi.org/10.1007/978-3-642-39498-0_1.
5. Butler, S.A. Security Attribute Evaluation Method: A Cost-Benefit Approach. In *Proceedings of the 24th international conference on Software engineering - ICSE '02*, pp. 232, New York, New York, USA, ACM Press (2002) ISBN 158113472X. https://doi.org/10.1145/581339.581370.
6. Chessa, M., Loiseau, P. A cooperative game-theoretic approach to quantify the value of personal data in networks. 2016. https://doi.org/10.1145/3106723.3106732.
7. Daniele, P., Scrimali, L. *Strong Nash Equilibria for Cybersecurity Investments with Nonlinear Budget Constraints*, pp. 199–207. Springer International Publishing, Cham, (2018) ISBN 978-3-030-00473-6. https://doi.org/10.1007/978-3-030-00473-6_22.
8. eSentire. Security Operations Center Pricing Calculator. Website, 2024. Available at https://www.esentire.com/security-operations-center-pricing-calculator. Last accessed: June 2024.
9. Farahmand, F., Navathe, S.B., Sharp, G.P., Enslow, P.H. Evaluating Damages Caused by Information Systems Security Incidents. In *Economics of Information Security*, pp. 85–94. Kluwer Academic Publishers, Boston (2004) https://doi.org/10.1007/1-4020-8090-5_7.
10. Gordon, L.A., Loeb, M.P., Zhou, L. Integrating cost-benefit analysis into the NIST Cybersecurity Framework via the Gordon-Loeb Model. *Journal of Cybersecurity*, 6(1), 03 (2020) ISSN 2057-2085. https://doi.org/10.1093/cybsec/tyaa005.
11. Havakhor, T., Rahman, M., Zhang, T. Cybersecurity Investments and the Cost of Capital. *SSRN Electronic Journal* (2020) https://doi.org/10.2139/ssrn.3553470.
12. Hays PLC. CHays Poland Salary Guide 2023. Technical report, Hays PLC (2023)
13. Ioannidis, C., Pym, D., Williams, J. Investments and Trade-offs in the Economics of Information Security. pp 148–166. Springer Berlin Heidelberg (2009) https://doi.org/10.1007/978-3-642-03549-4_9.
14. ISO/IEC. ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements (2013)
15. ISO/IEC. ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection – Information security management systems – Requirements (2022)
16. Kaspersky. Kaspersky IT Security Calculator. Website, 2024. Available at https://calculator.kaspersky.com/. Last accessed: June 2024.
17. Kosutic, D. ISO 27001 2013 vs. 2022 revision – What has changed? Website, 2024. Available at https://advisera.com/27001academy/blog/2022/10/25/iso-27001-iso-27002/. Last accessed June 2024.
18. Leszczyna, R. *Cost of Cybersecurity Management*, pages 127–147. Springer International Publishing, Cham, 2019. ISBN 978-3-030-19538-0. https://doi.org/10.1007/978-3-030-19538-0_5.
19. Leszczyna, R., Litwin, A. Estimating the cost of cybersecurity activities with caspea: A case study and comparative analysis. In Kanhere, S., Patil, V.T., Sural, S., Gaur, M.S. editors, *Information Systems Security*, pp. 267–287, Cham (2020) Springer International Publishing. ISBN 978-3-030-65610-2.
20. Mercuri, R.T. Analyzing security costs. *Communications of the ACM*, 46(6):15–18 (2003) ISSN 0001-0782. https://doi.org/10.1145/777313.777327.
21. Nagurney, A., Daniele, P., Shukla, S. A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annals of Operations Research*, 248(1):405–427 (2017) ISSN 1572-9338. https://doi.org/10.1007/

s10479-016-2209-1.

22. National Institute of Standards and Technology (NIST). *NIST SP 800-53 Rev. 3 Recommended Security Controls for Federal Information Systems and Organizations*. U.S. Government Printing Office (2009) https://doi.org/10.6028/NIST.SP.800-53r4.
23. National Institute of Standards and Technology (NIST). *NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations*. U.S. Government Printing Office (2020) https://doi.org/10.6028/NIST.SP.800-53r5.
24. Pal, R., Golubchik, L. On the economics of information security. *ACM SIGMETRICS Performance Evaluation Review*, 38(2):51 (2010) ISSN 01635999. https://doi.org/10.1145/1870178.1870196.
25. Radziwil, N.M., Benton, M.C. Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management. *Software Quality Professional*, 19(3) (2017) https://doi.org/10.48550/arXiv.1707.02653.
26. Rezmierski, V., Carroll, A., Hine, J. Incident Cost Analysis and Modeling Project II. Final Report. Technical report, Committee on Institutional Cooperation Chief Information Officers Committee (2000)
27. Riek, M., Böhme, R., Ciere, M., Gañán, C., Van Eeten, M. Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries. Technical report (2016)
28. Robinson, N., Potoglou, D., Kim, C., Burge, P., Warnes, R. Security At What Cost? pp. 3–15. Springer Berlin Heidelberg (2010) https://doi.org/10.1007/978-3-642-16806-2_1.
29. Rodrigues, B., Franco, M., Parangi, G., Stiller, B. SEConomy: A Framework for the Economic Assessment of Cybersecurity. In: Djemame, K., Altmann, J., Bañares, J.A., Agmon Ben-Yehuda, O., Naldi, M. (eds), *Economics of Grids, Clouds, Systems, and Services*, pp. 154–166, Cham, Springer International Publishing (2019) ISBN 978-3-030-36027-6.
30. Sawik, T. Selection of Cybersecurity Safequards Portfolio. In *Supply Chain Disruption Management Using Stochastic Mixed Integer Programming*, pp. 315–335. Springer International Publishing, Cham (2018) ISBN 978-3-319-58823-0. https://doi.org/10.1007/978-3-319-58823-0_11.
31. Shetty, N., Schwartz, G., Felegyhazi, M., Walrand, J. Competitive Cyber-Insurance and Internet Security. In *Economics of Information Security and Privacy*, pp. 229–247. Springer US, Boston, MA (2010) https://doi.org/10.1007/978-1-4419-6967-5_12.
32. Tatsumi, K., Goto, M. Optimal Timing of Information Security Investment: A Real Options Approach. In *Economics of Information Security and Privacy*, pp. 211–228. Springer US, Boston, MA, 2010. https://doi.org/10.1007/978-1-4419-6967-5_11.
33. Wagner, M., Hinson, G., Zamora, M.G., Melville, D., Legastelois, L. ISO27k RASCI table version 5 (2018)
34. Wilson, R. *Mastering Project Time Management, Cost Control, and Quality Management*. Pearson Education, Inc., Old Tappan, New Jersey (2015)
35. Xie, N., Mead, N.R. SQUARE Project: Cost/Benefit Analysis Framework for Information SecurityImprovement Projects in Small Companies. Technical report, Carnegie Mellon University (2004)