Postprint of: Leszczyna R., Litwin A. (2020) 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. (eds) Information Systems Security. ICISS 2020. Lecture Notes in Computer Science, vol. 12553, Springer, Cham. DOI: 10.1007/978-3-030-65610-2_17

Estimating the Cost of Cybersecurity Activities with CAsPeA: a Case Study and Comparative Analysis

Rafał Leszczyna[1][0000−0001−7293−2956] and Adrian Litwin[2]

[1] Gdańsk University of Technology, Faculty of Management and Economics, Narutowicza 11/12, 80-233 Gdańsk, Poland rle@zie.pg.gda.pl
[2] Homerun, Singel 542, 1017 AZ Amsterdam, the Netherlands

Abstract. Contemporary approaches to the estimation of cybersecurity costs in organisations tend to focus on the cost of incidents or technological investments. However, there are other, less transparent costs related to cybersecurity management that need to be properly recognised in order to get a complete picture. These costs are associated with everyday activities and the time spent by employees on cybersecurity-related actions. Such costs constitute a substantial component of cybersecurity expenditures, but because they become evident only during scrupulous analyses, often they are neglected. This paper presents new developments on CAsPeA – a method which enables estimating the cost of these activities based on a model derived from the Activity-Based Costing (ABC) and the NIST SP 800-53 guidelines. The application of the method is illustrated by a case study of a civil engineering enterprise. The method's evaluation based on comparative analysis in respect to SQUARE is described.

Keywords: Cybersecurity management · Organisational management · Business management · Cost · Estimation · Computer security · Information security

1 Introduction

With the dynamically evolving threat landscape, the number of organisations forced to bear the costs associated with cybersecurity incidents is inevitably raising. According to the study of Accenture Security and Ponemon Institute [1], during the last five years, the average number of security breaches (in the study defined as 'successful cyberattacks that cause business disruptions') increased 67%[1]. The attacks cost enterprises on average 13 million US dollars (USD) each year [1] which corresponds to the costs' increase of 12% in the last five years. The expenses are associated with interruptions in performing business operations, loss of data, loss of revenue and damaged information system assets. The cost of data loss represents the largest cost component (5,9 million USD).

[1] The study covered 355 organisations worldwide from various economic sectors.

On the other hand, enterprises which decided to acquire security intelligence and threat sharing systems noted around 2 million USD on technology savings. Also, investments in cybersecurity automation, AI and machine learning resulted in around 2 million USD of savings. At the same time, expenditures on advanced perimeter controls have not brought in the expected financial returns [1]. Proper decisions in cybersecurity investments are crucial for the operation of contemporary enterprises. The investments compete for funds with other areas of company activities and thus they require rational economic justifications [2]. To plan effective cybersecurity strategies [3], practical tools for measuring the cost of cybersecurity are demanded [4].

In response to this demand, CAsPeA – the *C*ost *As*sessment of *Pe*rsonnel *A*ctivities in Information Security Management (`https://zie.pg.edu.pl/cybsec/caspea`) was introduced [5–8]. The method enables evaluations of the costs of employees' effort and time spent on cybersecurity-related actions during their daily work. These costs regard, for instance, participation in cybersecurity training and awareness sessions, setting up protections for devices and applications, or adopting organisational cybersecurity policies and procedures. Such costs constitute a substantial component of cybersecurity spendings, but because they become evident only during scrupulous analyses, often they are neglected.

This paper presents the recent developments on the method. After a brief discussion of the relevant terminology (Section 2) and the analysis of related studies (Section 3), the key characteristics of CAsPeA are presented (Section 4). The method's application based on a case study of a civil engineering company is described in Section 5. The main goal of the case study is to demonstrate the straightforwardness of CAsPeA-based estimations. As a part of the method's evaluation, CAsPeA was subject to a comparative analysis with respect to SQUARE. The analysis is presented in Section 6. The paper concludes with closing remarks.

2 Costs of cybersecurity

Costs of cybersecurity management can be defined as *the evaluated use of resources in monetary terms* [9, 10]. These costs are associated with various types of measures and activities that are aimed at reducing cybersecurity risks, including technical as well as organisational. They embrace [10]:

- the costs caused by information security incidents,
- costs of information security management,
- costs of security controls,
- and the costs of capital induced by information security risks.

In the Detica's research [11], classification of costs associated with cybercrime is presented, which distinguishes between:

- *costs in anticipation of cybercrime* that include the costs of security controls, insurance costs, and the costs of compliance with security standards,

- *costs as a consequence of cybercrime* comprising direct losses, such as disaster recovery costs and indirect losses related for instance to reduced competitiveness,
- *costs in response to cybercrime*, for instance, compensation payments to victims, fines imposed by regulatory bodies or the costs of legal or forensic conducts,
- *indirect costs associated with cybercrime*, including the costs resulting from damage of reputation, loss of trust of customers or reduced public sector revenues.

Anderson et al. [12] propose an alternative framework for categorising the costs of cybercrime presented in Figure 1.

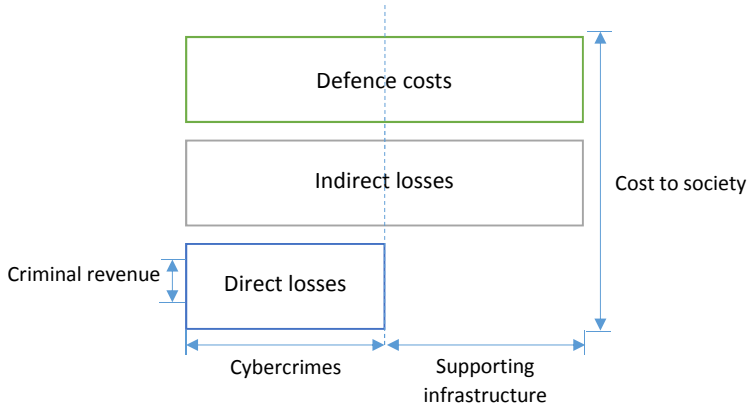


Fig. 1. Framework for categorising the costs of cybercrime. Source [12]

3 Related work

The studies of the cost of cyber-crime focus on the identification of reliable data on cyber incidents and their structured analysis [12, 11, 13, 14]. For instance, Riek et al. [15] developed an instrument to measure the costs of cyber-crime for consumers that incorporates the findings of earlier studies in this domain and applied it to obtain data in six European countries. Farahmand et al. [16] discussed the criteria for categorising enterprise information assets and provided a three-dimensional scheme for probabilistic evaluation of the impact of security threats.

Sawik [17] studied the problem of the optimal selection of cybersecurity measures to reduce the impact of information flow disruptions in enterprises' supply chains given a constrained budget. Various Stochastic Mixed Integer Programming models were applied to the analyses. Cybersecurity investments with

nonlinear budget constraints were researched by Daniele and Scrimali [18] and Nagurney et al. [19]. A dynamic model of security investments that acknowledges the trade-off between confidentiality and availability of information was introduced by Ioannidis et al. [20]. Another dynamic model is described by Tatsumi and Goto [21]. In 2010 Böhme et al. [22] presented a model which extends the iterated weakest link (IWL) model with penetration testing.

Among the studies on cyber-insurance, Bandyopadhyay and Mookerjee [23] constructed a model for deriving the overall optimal decision to purchase cyber-insurance based on the determination of the impact of secondary loss in structuring the use of cyber-insurance and backward analysis of multiple incident scenarios. Bartolini et al. [24] analysed the processes performed by insurance companies that aim at evaluating an enterprise's cybersecurity risk level. Pal et al. [25] developed a model for deriving optimal cyber-insurance contracts which considers two types of cyber-insurance agency strategies: welfare maximising or profit maximising [25]. Shetty et al. [26] devised a model to study the effects of cyber-insurance on user security and their welfare in which a probability of a successful attack depends on the individual security of a user and on the network security (independent of the user).

Other interesting economics-based security studies include the work of Havakhor et al. [27] who investigated the capital market's response to an organisation's cybersecurity investments. The study demonstrated that properly communicating cybersecurity investments to investors would likely reduce information asymmetries surrounding enterprises' risks and result in the cost of capital reduction. Rodrigues et al. [28] proposed a framework for evaluating the economic impact of cybersecurity measures in distributed ecosystems with several participants. The framework provides models for cost estimations and the mapping of relations between interdependent systems and their components. Chessa et al. [29] proposed a cooperative game-theoretic approach to quantify the value of personal data in networks. Robinson et al. [30] presented an application of stated preference discrete choice experiments (SPDCEs) to analyse and quantify the security and privacy preferences and views of individuals.

Cost calculators are straightforward applications for deriving rough cost figures based on the input data characterising a given organisation e.g. the number of users, the number of servers or the cost of electricity, training, bandwidth etc. Publicly available cost calculators include Data Breach Risk Calculator of the Ponemon Institute and IBM [31], CyberTab [32], Websense Hosted Email Security Calculator [33] and Small Business Risk Calculator [34]. In addition, it is popular to apply widely recognised financial metrics including the Rate of Return, maximum Net Present Value or the Return on Investment [4, 35] to analyse the results of the estimations.

As far as the methods for calculating the costs related to implementing security controls are concerned only few proposals have been developed including I-CAMP [36], I-CAMP II [37], SAEM [38] or SQUARE [39]. Cyber Incident Cost Assessment (CICA) is also mentioned in the literature, but its documentation is unavailable. The methods' descriptions can be found, for instance, in [5, 10,

40, 35, 41]. Radziwill and Benton [42] developed a mapping between the NIST Cybersecurity Framework (CSF) and the costs of quality that can be adopted by organisations that apply the framework to plan, manage, and improve their cybersecurity operations. In addition, the mapping enables linking elements in accounting systems that are associated with cybersecurity operations and risk management to a quality cost model.

The Cost/Benefit Analysis-based framework developed by the System Quality Requirements Engineering (SQUARE) Team from Software Engineering Institute (SEI) [39] is a method that earned interest of researchers and practitioners [43–46, 6]. 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 [39]. The results of SQUARE calculations can be used to obtain the *cost of mitigation of a vulnerability* which Zineddine specifies as [47]:

$$c\nu_j = \lambda CL\nu_j - \mu CS\nu_{ij} \tag{1}$$

$$\lambda + \mu = 1 \tag{2}$$

where $CL\nu_j$ is the cost of damage resulting from the exploitation of the vulnerability v_i. CLv_j can be calculated based on the SQUARE findings. $CS\nu_{ij}$ is the cost of alleviating the vulnerability v_i. λ and ν are coefficients that can be arbitrarily set, within the range depicted in (2), by an organisation depending on the targeted level of security. In Section 6 a comparative analysis of CAsPeA in respect to SQUARE is presented.

The analysis of the related work revealed that the studies and methods focus on cybersecurity investments into technical or organisational cybersecurity controls and financial losses resulting from security breaches. The costs are investigated individually or introduced into a cost-benefit analysis. Also, they are studied at different levels, from micro- to macroeconomic. However, the insight into the costing component associated with personnel activities related to cybersecurity management in companies and organisations has been missing.

4 Method description

CAsPeA – *C*ost *As*sessment of *Pe*rsonnel *A*ctivities in Information Security Management (`https://zie.pg.edu.pl/cybsec/caspea`) – is a method that complements the portfolio of the available methods for estimating the cost of cybersecurity management by enabling the estimation of the costs of human effort and time spent on cybersecurity-related actions during their daily work [5–8]. These costs regard, for instance, employees' participation in cybersecurity training, managing secure configurations of utilised hardware and software or reading cybersecurity policy documents. Such costs constitute a substantial component of cybersecurity spendings, but because they become evident only during

scrupulous analyses, often they are neglected. By enabling their estimations, the method should provide a more complete view of the costs of cybersecurity. In the following text, the highlights of the methods are provided. More detailed descriptions can be found in [5–8].

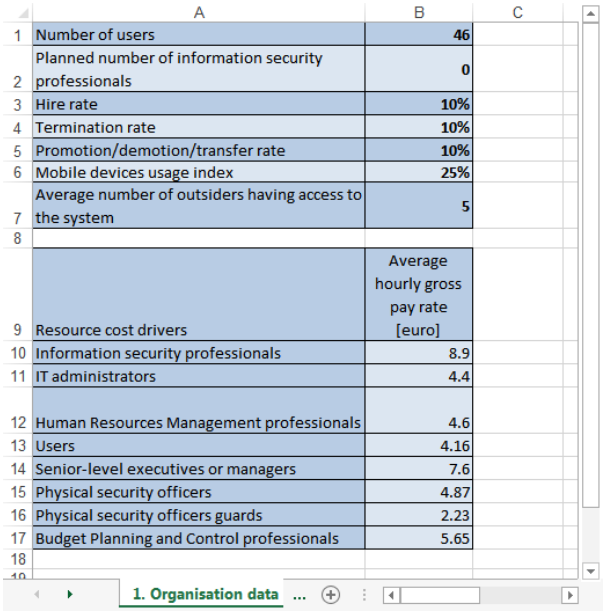
To enable the calculations, the Activity-Based Costing (ABC) system was selected and adapted to the costing model [5–8]. The advantage of the ABC is that it recognises activities (human or machine operations) as fundamental objects that induce costs in enterprises. In CAsPeA, the total cost in organisation is calculated as a sum of costs of all activities performed in an enterprise. Then, to derive the costs of activities, 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.

For the reference list of the activities to be included in the model, NIST SP's 800-53 list of security controls was selected after a thorough literature analysis. The list embraces multiple cybersecurity areas that altogether comprehensively address the organisational cybersecurity context. Examples of the areas include the *AT Awareness and Training*, *CM Configuration Management* or *PS Personnel Security* [48]. Another strength of the document is that it is fully compatible with ISO/IEC 27001 (see the mapping between the documents in Appendix H, Table H-1 of NIST SP 800-53) – the most recognised cybersecurity standard worldwide.

The method enables estimations based on a baseline set of input data that characterise an organisation such as the number of employees that utilise computer devices, average hourly pay rates of personnel that performs or is responsible for security activities or hire/termination rate/promotion/demotion/transfer rates. Minimum, maximum, average and usual duration times are assigned to the cost drivers and the posts of personnel performing or responsible for relevant cybersecurity activities (e.g. IT administrators, users or Human Resources Management professionals) associated with resource cost drivers.

Based on the input data, the total cost of staff activities related to information security management, the cost of exclusive IT security professionals' activities, the minimum amount of work time of information security professionals indispensable for assuring sufficient level of information security in an organisation and the related minimum required quantity of information security professionals are calculated. Each of the parameters is represented by its minimum, maximum, average and the usual value.

To facilitate calculations, a spreadsheet was developed and updated periodically. It comprises four worksheets that correspond to subsequent steps of the assessment process. The *Organisation data* worksheet (see Figure 2) enables entering all required input data, such as the number of employees, human resources metrics or hourly pay rates. The worksheets *List of activities* (see Figure 3) and *Cost of information security professionals* comprise formulae for calculation of the total cost of activities. In the *Assessment results worksheet* (see Figure 4) the outcomes of the assessment are presented.



	A	B	C
1	Number of users	46	
2	Planned number of information security professionals	0	
3	Hire rate	10%	
4	Termination rate	10%	
5	Promotion/demotion/transfer rate	10%	
6	Mobile devices usage index	25%	
7	Average number of outsiders having access to the system	5	
8			
9	Resource cost drivers	Average hourly gross pay rate [euro]	
10	Information security professionals	8.9	
11	IT administrators	4.4	
12	Human Resources Management professionals	4.6	
13	Users	4.16	
14	Senior-level executives or managers	7.6	
15	Physical security officers	4.87	
16	Physical security officers guards	2.23	
17	Budget Planning and Control professionals	5.65	
18			

Fig. 2. The *Organisation data* worksheet provides fields for all the required input data, such as the number of employees, human resources metrics, or hourly pay rates.

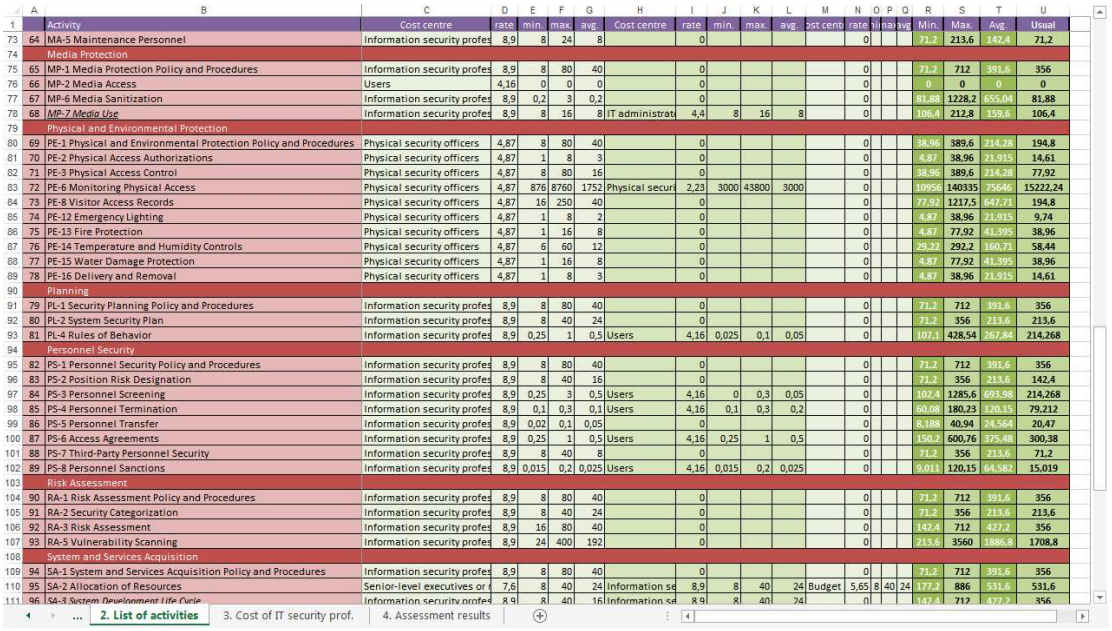
5 Case study

This section illustrates the application of CAsPeA in a case study of a civil engineering company that specialises in designing public and private sector objects including hospitals, industrial and technological facilities or shopping centres. The designs represent various types of structures and buildings in practically all branches of industry, and vary from complex endeavours that cover all functions and components of completely new facilities (starting from their 'founding stone') to the projects that focus on enhancing or reorganising existing constructions. Figure 5 presents the structure of the IT system of the enterprise. The main goal of this case study is to demonstrate how straightforward is the process of estimating the costs with CAsPeA.

5.1 Input data

The company employs 48 workers including:

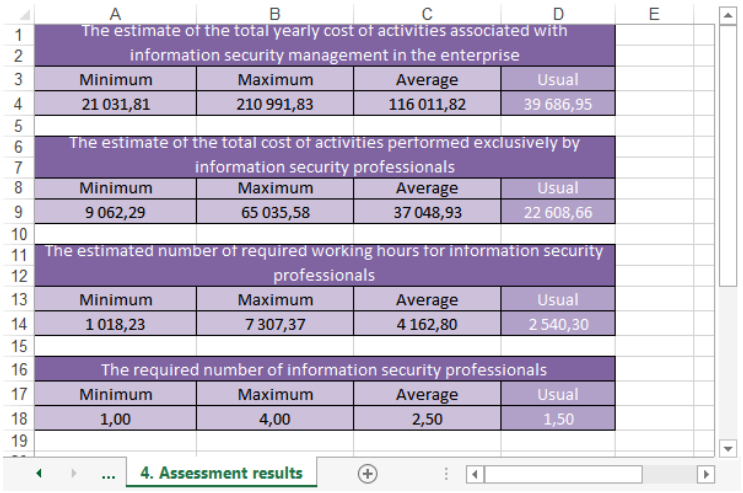
- executives (2),
- secretaries (2),
- accountants (3),
- architects (38),
- auxiliary staff (1),



	Activity	Cost centre	rate	min.	max.	avg.	Cost centre	rate	min.	max.	avg.	Min.	Max.	Avg.	Usual
73	64 MA-5 Maintenance Personnel	Information security profes	8,9	8	24	8		0				71,2	213,6	142,4	71,2
74	Media Protection														
75	65 MP-1 Media Protection Policy and Procedures	Information security profes	8,9	8	80	40		0				71,2	712	391,6	356
76	66 MP-2 Media Access	Users	4,16	0	0	0		0				0	0	0	0
77	67 MP-6 Media Sanitization	Information security profes	8,9	0,2	3	0,2		0				81,88	1228,2	655,04	81,88
78	68 *MP-7 Media Use*	Information security profes	8,9	8	16	8	IT administrati	4,4	8	16	8	106,4	212,8	159,6	106,4
79	Physical and Environmental Protection														
80	69 PE-1 Physical and Environmental Protection Policy and Procedures	Physical security officers	4,87	8	80	40		0				38,96	389,6	214,28	194,8
81	70 PE-2 Physical Access Authorizations	Physical security officers	4,87	1	8	3		0				4,87	38,96	21,915	14,61
82	71 PE-3 Physical Access Control	Physical security officers	4,87	8	80	16		0				38,96	389,6	214,28	77,92
83	72 PE-6 Monitoring Physical Access	Physical security officers	4,87	876	8760	1752	Physical securi	2,23	3000	43800	3000	10956	140335	75646	15222,24
84	73 PE-8 Visitor Access Records	Physical security officers	4,87	16	250	40		0				77,92	1217,5	647,71	194,8
85	74 PE-12 Emergency Lighting	Physical security officers	4,87	1	8	2		0				4,87	38,96	21,915	9,74
86	75 PE-13 Fire Protection	Physical security officers	4,87	1	16	8		0				4,87	77,92	41,395	38,96
87	76 PE-14 Temperature and Humidity Controls	Physical security officers	4,87	6	60	12		0				29,22	292,2	160,71	58,44
88	77 PE-15 Water Damage Protection	Physical security officers	4,87	1	16	8		0				4,87	77,92	41,395	38,96
89	78 PE-16 Delivery and Removal	Physical security officers	4,87	1	8	3		0				4,87	38,96	21,915	14,61
90	Planning														
91	79 PL-1 Security Planning Policy and Procedures	Information security profes	8,9	8	80	40		0				71,2	712	391,6	356
92	80 PL-2 System Security Plan	Information security profes	8,9	8	40	24		0				71,2	356	213,6	213,6
93	81 PL-4 Rules of Behavior	Information security profes	8,9	0,25	1	0,5	Users	4,16	0,025	0,1	0,05	107,1	428,54	267,84	214,268
94	Personnel Security														
95	82 PS-1 Personnel Security Policy and Procedures	Information security profes	8,9	8	80	40		0				71,2	712	391,6	356
96	83 PS-2 Position Risk Designation	Information security profes	8,9	8	40	16		0				71,2	356	213,6	142,4
97	84 PS-3 Personnel Screening	Information security profes	8,9	0,25	3	0,5	Users	4,16	0	0,3	0,05	107,4	1285,6	693,98	214,268
98	85 PS-4 Personnel Termination	Information security profes	8,9	0,1	0,3	0,1	Users	4,16	0,1	0,3	0,2	60,08	180,23	120,15	79,212
99	86 PS-5 Personnel Transfer	Information security profes	8,9	0,02	0,1	0,05		0				8,188	40,94	24,564	20,47
100	87 PS-6 Access Agreements	Information security profes	8,9	0,25	1	0,5	Users	4,16	0,25	1	0,5	150,2	600,76	375,48	300,38
101	88 PS-7 Third-Party Personnel Security	Information security profes	8,9	8	40	8		0				71,2	356	213,6	71,2
102	89 PS-8 Personnel Sanctions	Information security profes	8,9	0,015	0,2	0,025	Users	4,16	0,015	0,2	0,025	9,011	120,15	64,582	15,019
103	Risk Assessment														
104	90 RA-1 Risk Assessment Policy and Procedures	Information security profes	8,9	8	80	40		0				71,2	712	391,6	356
105	91 RA-2 Security Categorization	Information security profes	8,9	8	40	24		0				71,2	356	213,6	213,6
106	92 RA-3 Risk Assessment	Information security profes	8,9	16	80	40		0				142,4	712	427,2	356
107	93 RA-5 Vulnerability Scanning	Information security profes	8,9	24	400	192		0				213,6	3560	1886,8	1708,8
108	System and Services Acquisition														
109	94 SA-1 System and Services Acquisition Policy and Procedures	Information security profes	8,9	8	80	40		0				71,2	712	391,6	356
110	95 SA-2 Allocation of Resources	Senior-level executives or	7,6	8	40	24	Information se	8,9	8	40	24	Budget	5,65	8	40	24	177,2	886	531,6	531,6
111	96 *SA-3 System Development Life Cycle*	Information security profes	8,9	8	40	16	Information se	8,9	8	40	24		0				142,4	712	427,2	356

... 2. List of activities 3. Cost of IT security prof. 4. Assessment results

Fig. 3. The worksheet *List of activities* comprise formulae for calculation of the total cost of information security management activities.



The estimate of the total yearly cost of activities associated with information security management in the enterprise			
Minimum	Maximum	Average	Usual
21 031,81	210 991,83	116 011,82	39 686,95
The estimate of the total cost of activities performed exclusively by information security professionals			
Minimum	Maximum	Average	Usual
9 062,29	65 035,58	37 048,93	22 608,66
The estimated number of required working hours for information security professionals			
Minimum	Maximum	Average	Usual
1 018,23	7 307,37	4 162,80	2 540,30
The required number of information security professionals			
Minimum	Maximum	Average	Usual
1,00	4,00	2,50	1,50

... 4. Assessment results

Fig. 4. The *Assessment results* worksheet shows the outcome of the cost assessment.

– cleaning staff (2).

In the first step of the cost assessment process, the number of employees who can use the information system was determined. In the company the majority

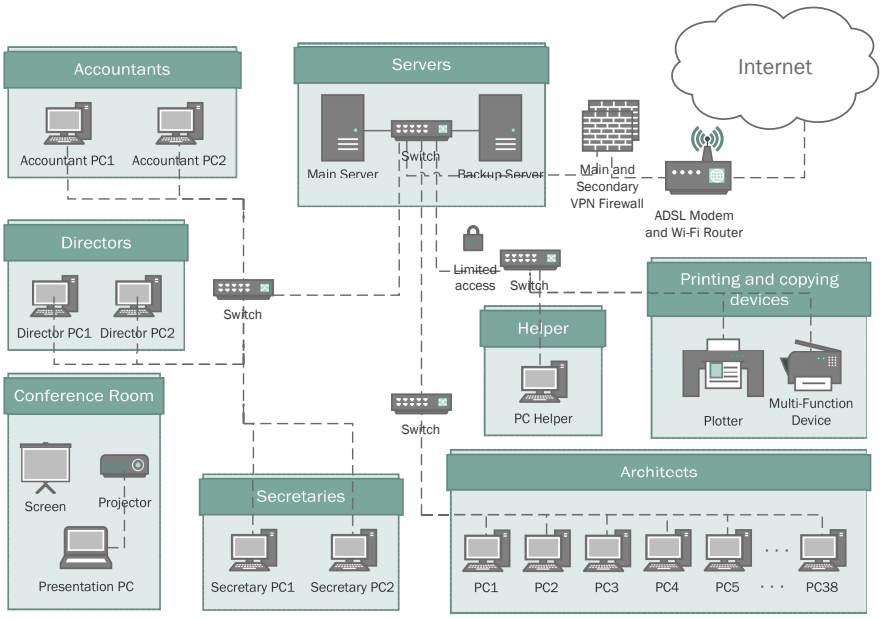


Fig. 5. Information system of the civil engineering design company

of the workers had their personal working stations apart from the cleaning staff. Thus, 46 employees were authorised to use the information system. Further data required for the calculation of cost estimates were as follows:

- percentage of personnel hired in the current year (hire rate) – 10%,
- percentage of workers that terminated their employment in the current year (termination rate) – 10%,
- the rate of employees' promotions, demotions and transfers – 10%,
- mobile devices usage index (i_{mdui}) – 25%,
- the approximate number of external users authorised to access the organisation's information system – 5.

The average hourly gross pay rates necessary to estimate the total cost of information security activities were based on the data from Sedlak&Sedlak consulting[2] and converted to US dollars (USD) from Polish Złoty with a rounded average exchange rate equal to 4[3]. Roughly, the rate can be also used to interpret the values in Euro. The input data are presented in Figure 2.

5.2 Results

The obtained cost estimates are presented in Tables 1 and 2.

[2] Available at `http://www.wynagrodzenia.pl/`. Last access: 10.10.2020.
[3] Source: `www.exchangerates.org.uk/USD-EUR-exchange-rate-history.html`. Last access: 10.10.2020.

Table 1. The estimate of the total yearly cost of activities associated with information security management in the enterprise, depending on whether Physical Access Monitoring and Control (PAMC) activities are included/excluded. The values were converted to US dollars (USD) from Polish Złoty with a rounded average exchange rate equal to 4.

Total cost of activities [USD]			
Excluding PAMC			
Minimum	Maximum	Average	*Usual*
10,075.69	70,656.62	40,366.16	*24,464.70*
Including PAMC			
Minimum	Maximum	Average	*Usual*
21,031.81	210,991.83	116,011.82	*39,686.95*

Table 2. Estimates of parameters associated with information security professionals: cost of their activities, the number of required working hours, and the required number of posts. The values were converted to US dollars (USD) from Polish Złoty with a rounded average exchange rate equal to 4.

Estimated parameters associated with IT security professionals			
Cost of activities [USD]			
Minimum	Maximum	Average	*Usual*
9,062.29	65,035.58	37,048.93	*22,608.66*
Required working hours			
Minimum	Maximum	Average	*Usual*
1,018.23	7,307.37	4,162.80	*2,540.30*
Required positions			
Minimum	Maximum	Average	*Usual*
1.0	4.0	2.5	*1.5*

The results show that there are two factors which highly influence the estimated total cost of cybersecurity management. The first of them is whether the organisation already manages its physical security. Then, if it does, the second question regards the extent to which the cost of the management is attributed to information security.

If an organisation already manages its physical security and monitoring and control of physical access to the information system, then the estimated total cost of activities is around 24,465 US dollars (USD) during a year (see Table 1). This estimate is coherent with an expectation of the cost of security management in the system of this scale. It is worth to note that the major part (around 92%) of the cost is associated with the activities performed by information security professionals (see Table 2), and only around 1,856 USD will be spent on the activities of other employees. The evaluation indicates also that for managing information security in the company, employing one information security professional is sufficient.

A significantly different situation occurs when the organisation starts to consider its physical security only after evaluating the decision of the establishment of information security management and associates the physical security just with the protection of its information assets. Then, the estimated cost boosts significantly, and it reaches the value of approximately 39,687 USD (see Table 1). This is due to the fact, that in this case, the activities linked with physical security become dominant. Precisely, the activities connected to PE-3 Physical Access Control and PE-6 Monitoring Physical Access security components, are expensive. The cost of the activities reached as much as 15,222 USD, which corresponds to around 38% of the total activities cost.

Such a high cost of physical access control and monitoring activities stems from the fact that the activities require the continuous presence of guards and security specialists. To estimate the cost, the following assumptions were made:

- Information system physical access control requires the continuous presence of a security guard for 12 hours (from 8:00 am to 8:00 pm) in weekdays (on average 250 days during a year).
- Information system physical access monitoring is part of the entire monitoring of the organisation headquarters and requires on average one tenth its time. The headquarters are monitored 24 hours a day, each day of a year. The monitoring requires the continuous presence of at least one guard or security professional.

In this perspective, the yearly cost of activities associated with the establishment and maintenance of information security may constitute a significant position in the organisation's budget, depending on the turnover. This fact would need to be taken into careful consideration in the organisation tactical planning. At the same time, it must be borne in mind that at the other end lies much higher cost, which the organisation will have to meet in the event of failure caused by a successful computer attack.

Other estimates that refer to the total cost of work of IT security professionals, namely the minimum amount of work time of information security professionals indispensable for assuring sufficient level of information security in the organisation and the related number of information security professionals – remain the same as they are independent of physical security (Table 2). It is worth to note that in everyday practice the first scenario is much more common than the second, as most organisations protect their physical resources, whether on their own or by delegating this task to security agencies.

For the organisation, the estimated cost is acceptable. The performed estimation provides an incentive for extending the existing cybersecurity level.

6 Comparative analysis with SQUARE

As a part of the method's evaluation, CAsPeA was subject to a comparative analysis with respect to SQUARE (see Section 3) 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 boatyard designs and builds customised luxury sailing and power catamarans and super-yachts from 17 to 60 meters (60 to 200 feet). The company operates on the world market carrying out orders from individual clients. It specialises in the unit production, where the projects and their implementation are always accommodated to the requirements of an orderer. The company very intensively utilises information technologies during yacht design and in production management. Additionally, the entire documentation is stored in the electronic form and printed only on demand. Thus, for the company, it is paramount to assure the security of the data.

The IT support company provides IT support for a publishing group which is one of the largest publishers in Poland. The company creates and maintains a wide portfolio of internet applications. The most popular of them is an advertisement service recognised in all country regions and the internet issue of one of the oldest journals. The internet traffic reaches as much as a few million page hits daily for each service. The company databases store hundreds of thousands of personal data.

6.1 Input data

The boatyard employs in total around 200 workers. The number is approximated because the quantity of production personnel varies depending on the actual production needs. In the boatyard, the production personnel, which constitutes the majority of the workforce has a very limited (practically null) access to the system, while the system users are management, designers and engineers. Further analysis reveals that 35 workers are authorised to use the information system.

Additional data required for the calculation of cost estimates were as follows: HR - hire rate – 34,29%, TR - termination rate – 28,57%, PDTR - promotion/-demotion/transfer rate – 8,57%, i_{mdui} – mobile devices usage index – 25,71%, approximate number of people outside of the organisation who have access to the organisation's IT system – 6. The data are summarised in the table 3.

Table 3. Input data for the boatyard.

Indicator	Value
Number of users	35
Planned number of information security professionals	0
HR - hire rate	34.29%
TR - termination rate	28.57%
PDTR - promotion/demotion/transfer rate	8.57%
i_{mdui}	25.71%
Approximate number of outsiders with access to the organisation's IT system	6

The average hourly gross pay rates necessary to estimate the total cost of information security activities were estimated based on the data from Sedlak&Sedlak consulting[4]. The analogous input data for the IT support company are presented in the table 4.

Table 4. Input data for the IT support company.

Indicator	Value
Number of employees	104
Number of users	95
Planned number of information security professionals	1
HR - hire rate	24.21%
TR - termination rate	26.32%
PDTR - promotion/demotion/transfer rate	32.63%
i_{mdui}	42.11%
Approximate number of outsiders with access to the organisation's IT system	30

6.2 Results obtained with CAsPeA

Boatyard Based on the input data presented in Table 3, the estimates summarised in Table 5 and Table 6 were obtained[5]. The cost estimates are reasonable for a company which in average sells 3-5 yachts a year for the price varying between 700,000 – 6,000,000 Euro (around 800,000 – 7,000,000 US dollars).

Table 5. The estimate of the total yearly cost of activities associated with cybersecurity management for the boatyard. The values were converted to USD from Polish Złoty with a rounded average exchange rate equal to 4.

Total cost of activities [USD]			
Minimum	Maximum	Average	*Usual*
18,861.60	198,967.79	108,914.70	*34,715.46*

IT support company The cost values estimated for the IT support company are presented in Table 7 and Table 8. The cost figures acquired with CAsPeA are adherent to the operational reality of the IT support company. With a yearly revenues at the level of millions of USD, the average values of the cost seem to be affordable.

[4] Available at `http://www.wynagrodzenia.pl/`

[5] The values were converted to US dollars (USD) from Polish Złoty with a rounded average exchange rate equal to 4. Roughly, the rate can be also used to interpret the values in Euro.

Table 6. Estimates of parameters associated with cybersecurity professionals for the boatyard. The values were converted to US dollars from Polish Złoty with a rounded average exchange rate equal to 4.

Estimated parameters associated with IT security professionals			
Cost of activities [USD]			
Minimum	Maximum	Average	*Usual*
6,622.23	50,719.39	28,670.81	*17,214.45*
Required working hours			
Minimum	Maximum	Average	*Usual*
741.69	5,680.57	3,211.13	*1928.02*
Required positions			
Minimum	Maximum	Average	*Usual*
0.5	3.0	2.0	*1.0*

Table 7. The estimate of the total yearly cost of activities associated with cybersecurity management in the IT support company. The values were converted to US dollars from Polish Złoty with a rounded average exchange rate equal to 4.

Total cost of activities [USD]			
Minimum	Maximum	Average	*Usual*
21,221.10	244,726.62	132,973.86	*39,026.87*

6.3 Results obtained with SQUARE

The same data as for CAsPeA, supplemented with the costs of implementation and a prognosis of a number of incidents of each threat category were used for the input for the SQUARE estimation.

Boatyard The security cost estimation resulted in selecting four most attractive, by means of cost-benefit ratio, scenarios for the implementation of security measures in the company. The highest priority was assigned to the scenarios aiming at protecting from malware, social engineering and cyber-extortion, because these attacks are among the biggest threats to the computer systems of companies (see Table 9).

It is worth to note the relatively high cost-benefit indicators (higher than for the IT support company). This is primarily due to the assumed lower implementation costs, lesser geographical distribution and the number of security staff. Also, there is no need for additional security officer positions or the extension of duties since the implementation of the projects is relatively straightforward.

The IT support company Similarly as in the previous case, four security implementations projects were determined based on SQUARE analysis of a total cost around 12,000 US dollars (USD) yearly. The company can save on them up to 900,000 USD a year, which results from potential avoiding security incidents

Table 8. Estimates of parameters associated with cybersecurity professionals for the IT support company. The values were converted to US dollars from Polish Złoty with a rounded average exchange rate equal to 4.

Estimated parameters associated with IT security professionals			
Cost of activities [USD]			
Minimum	Maximum	Average	*Usual*
8,104.62	90,897.56	49,501.09	*20,141.04*
Required working hours			
Minimum	Maximum	Average	*Usual*
907.723	10,180.53	5,544.12	*2,255.80*
Required positions			
Minimum	Maximum	Average	*Usual*
0.5	5.5	3.0	*1.5*

and the associated costs of the damages and their restoration. Also in this case, the highest priority was assigned to the projects aiming at protecting from malware, social engineering and cyber-extortion. The results are presented in Table 10.

6.4 Results analysis

The analysis reveals significant differences between the maximum and usual estimated cost values. This result can be connected to the observation of Xie [39] that for the enterprises which normally do not perform cybersecurity activities, even very small investments and thoughtful organisational changes bring influential benefits. The upper limit for the security investments does not exist [35]. According to the law of diminishing returns, with the increase of IT security spendings, the marginal benefit achieved from them will be decreasing. There is an opinion among the experts [49], that as it is impossible to reach perfect security no matter how big are the efforts, the security expenses should be kept rational. A good boundary can be defined by potential financial losses due to a security breach.

SQUARE is scenario-oriented. It supports identifying the most profitable ways of protecting an organisation from cybersecurity threats. Thus, the main output of the method are the cost values and financial determinants of different defence scenarios connected to threat categories. CAsPeA, on the other hand, focuses on obtaining the total cost of all human activities related to achieving 'general' cybersecurity level (i.e. protection from various threat types) in an organisation. In this context, the CAsPeA calculation spreadsheet (presented in Section 4) turns out to be inflexible to accommodate different scenarios of cybersecurity provision. Currently, modifications are possible only by explicitly altering the spreadsheet formulas. Enriching the method with a module that enables such estimations would provide an added value and would enable better alignment with SQUARE (e.g. allowing for comparison of results).

Table 9. Yearly cybersecurity costs' estimates obtained with SQUARE for four protection scenarios (associated with threat categories) of the boatyard. The values were converted to US dollars from Polish Złoty with a rounded average exchange rate equal to 4.

Category of Threats	Category of Preventions	Benefit [USD]	Total Implementation Costs [USD]	Benefit to Cost Value (B/C)	Net Project Value [USD]	Total Value of Unprotected System [USD]	Total Value of Protected System [USD]
Social engineering and cyber-extortion	Training and procedures	107,616.65	4,000.00	26.90	103,616.65	-75,744.44	31,872.22
Viruses, worms, spyware, spam	Anti-malware	519,034.68	2,000.00	259,52	517,034.68	-59,670.52	459,364.16
Phishing, identity theft	Use of Data Certification Schemas	32,010.11	2,250.00	14,23	29,760.11	-7,898.84	24,111.26
Botnets, unauthorised use	Network traffic monitoring tools	23,335.00	1000.00	23,33	22,335.00	-2,228.16	21,106.84

The estimations obtained with SQUARE are highly influenced by the input data – the bypass rate and the probability of incident occurrence when there are no security measures in place (basis risk) as well as the expected annual loss for each threat category. For both, CAsPeA and SQUARE estimations, the amount of the costs matches the companies' financial capacities. The results are realistic and based on the broad knowledge security incidents and the protection methods. The overall feedback received during the analysis was that both methods could support the organisations' investment decision processes. At the same time, it becomes evident that the methods diverge in scope. CAsPeA concentrates on the cost of the NIST SP 800-53-indicated activities involved in providing IT security (human factor), while SQUARE is threat category-driven. Also, at the moment, CAsPeA does not contain the entire cost-benefit analysis apparatus is it lacks the 'benefit' part of the cost-benefit equation. Thus, the best option is to use the methods in a complementary manner.

7 Conclusions

The paper presented the recent developments on CAsPeA – a method for the assessment of the cost of employees' activities connected with the establishment

Table 10. Yearly cybersecurity costs' estimates obtained with SQUARE for four protection scenarios (associated with threat categories) of the IT support company. The values were converted to US dollars from Polish Złoty with a rounded average exchange rate equal to 4.

Category of Threats	Category of Preventions	Benefit [USD]	Total Implementation Costs [USD]	Benefit to Cost Value (B/C)	Net Project Value [USD]	Total Value of Unprotected System [USD]	Total Value of Protected System [USD]
Social engineering and cyber-extortion	Training and procedures	107,616.65	6,500.00	16.56	101, 416.65	-78,244.44	29,372.22
Viruses, worms, spyware, spam	Anti-malware	519,034.68	3,000.00	173.01	516,034.68	-60,670.52	458,364.16
Unauthorised access	Firewalls, software updates, IDS	33,350.06	2,000.00	16.68	31,350.06	-4,128.73	29,221.33
Theft of mobile devices	Hard disks encryption	32,380.01	1,000.00	32.38	31,380.01	-2,001.44	30,378.56

and the operation of cybersecurity management system. The use of the method was illustrated in a case study of a civil engineering company. The study demonstrated that CAsPeA can effectively support the decision process of an enterprise with regard to the investments into information security. Applying CAsPeA requires only a few straightforward steps and parameters to obtain rough estimations. Additionally, the study evidenced that physical security can become a dominant component in the cost cybersecurity management and thus it should be appropriately considered. In the particular application, the cost estimated with CAsPeA turned out to be acceptable for the organisation and provided an incentive for extending their existing cybersecurity level. This can be a certain prognostic for other companies considering investments in their cybersecurity management systems.

As a part of the method's evaluation, a comparative analysis of CAsPeA and SQUARE was performed. The study was separate from the case study and regarded applying both solutions to evaluate the costs in two enterprises: a boatyard and an IT support company. The analysis showed that the methods should not be taken as alternatives but as complementary solutions. SQUARE guides through the entire cost-benefit analysis process but focuses on particular protection scenarios without detailed consideration of the human factor. CAsPeA, on the other hand, provides estimations for all activities involved in the cybersecurity management and is human actions-centric but misses the 'benefit' part of the cost-benefit analysis. These observations gave additional insight into

where CAsPeA can be improved. For instance, extending the method with a module that enables flexible definitions of investment scenarios or covering the entire cost-benefit analysis are prospective development directions. Other further studies include:

- enhancing CAsPeA with activities linked to the security controls of the secondary and tertiary NIST SP 800-53 baselines,
- developing a dedicated version based on ISO/IEC 27001,
- performing a comparative analysis with the ISO/IEC 27001-based version,
- including technical cybersecurity controls into the CAsPeA estimations,
- researching the applicability of CAsPeA in various contexts (e.g. entrepreneurial sectors) and analysing its fitness and accuracy (e.g. for instance depending on the sector).

References

1. Accenture and Ponemon Institute. The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. Technical report, 2019.
2. L A Gordon and M Loeb. Return on information security investments: Myths vs. realities. *Journal of Strategic Finance*, 84:26–32, 2002.
3. Thomas A Chapman and Brian J Reithel. Perceptions of Cybersecurity Readiness among Workgroup IT Managers. *Journal of Computer Information Systems*, pages 1–12, feb 2020.
4. Wes Sonnenreich, Jason Albanese, and Bruce Stout. Return On Security Investment (ROSI): A Practical Quantitative Model. *Journal of Research and Practice in Information Technology*, 38:55–66, 2006.
5. Rafał Leszczyna. Cost of Cybersecurity Management, pages 127–147. In *Cybersecurity in the Electricity Sector*, chapter 5. Springer International Publishing, Cham, 2019.
6. R. Leszczyna. Approaching secure industrial control systems. *IET Information Security*, 9(1), 2015.
7. R. Leszczyna. Cost assessment of computer security activities. *Computer Fraud and Security*, 2013(7), 2013.
8. Rafał Leszczyna. Metoda szacowania kosztu zarządzania bezpieczeństwem informacji i przykład jej zastosowania w zakładzie opieki zdrowotnej. *Zeszyty Kolegium Analiz Ekonomicznych*, 2017.
9. Martin Kütz. Controlling der Information Security. In Dieter Burgartz Rohrig and Ralf, editors, *Praxiswissen IT-Sicherheit: Praxishandbuch fur Aufbau, Zertifizierung und Betrieb*, chapter 03710. TÜV Media, 19 edition, 2011.
10. Matthias Brecht and Thomas Nowey. A closer look at information security costs. In *The Economics of Information Security and Privacy*, pages 3–24. 2013.
11. Detica and Office of Cyber Security and Information Assurance. The Cost of Cyber Crime. Technical report, 2011.
12. Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J G van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy*, pages 265–300. 2013.
13. Tyler Moore, Richard Clayton, and Ross Anderson. The Economics of Online Crime. *Journal of Economic Perspectives*, 23(3):3–20, 2009.

14. Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, 11(May 2001):431–448, 2003.
15. Markus Riek, Rainer Böhme, Michael Ciere, Carlos Gañán, and Michel Van Eeten. Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries. 2016.
16. Fariborz Farahmand, Shamkant B. Navathe, Gunter P. Sharp, and Philip H. Enslow. Evaluating Damages Caused by Information Systems Security Incidents. In *Economics of Information Security*, pages 85–94. Kluwer Academic Publishers, Boston, 2004.
17. Tadeusz Sawik. Selection of Cybersecurity Safequards Portfolio. In *Supply Chain Disruption Management Using Stochastic Mixed Integer Programming*, pages 315–335. Springer International Publishing, Cham, 2018.
18. Patrizia Daniele and Laura Scrimali. *Strong Nash Equilibria for Cybersecurity Investments with Nonlinear Budget Constraints*, pages 199–207. Springer International Publishing, Cham, 2018.
19. Anna Nagurney, Patrizia Daniele, and Shivani Shukla. A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annals of Operations Research*, 248(1):405–427, 2017.
20. Christos Ioannidis, David Pym, and Julian Williams. Investments and Trade-offs in the Economics of Information Security, pages 148–166. Springer Berlin Heidelberg, 2009.
21. Ken-ichi Tatsumi and Makoto Goto. Optimal Timing of Information Security Investment: A Real Options Approach. In *Economics of Information Security and Privacy*, pages 211–228. Springer US, Boston, MA, 2010.
22. Rainer Böhme and Márk Félegyházi. Optimal information security investment with penetration testing. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 6442 LNCS, pages 21–37, 2010.
23. Tridib Bandyopadhyay and Vijay Mookerjee. A model to analyze the challenge of using cyber insurance. *Information Systems Frontiers*, 21(2):301–325, 2019.
24. David Nicolas Bartolini, Cesar Benavente-Peces, and Andreas Ahrens. Using Risk Assessments to Assess Insurability in the Context of Cyber Insurance. In Mohammad S Obaidat and Enrique Cabello, editors, *E-Business and Telecommunications*, pages 337–345, Cham, 2019. Springer International Publishing.
25. Ranjan Pal and Leana Golubchik. On the economics of information security. *ACM SIGMETRICS Performance Evaluation Review*, 38(2):51, oct 2010.
26. Nikhil Shetty, Galina Schwartz, Mark Felegyhazi, and Jean Walrand. Competitive Cyber-Insurance and Internet Security. In *Economics of Information Security and Privacy*, pages 229–247. Springer US, Boston, MA, 2010.
27. Taha Havakhor, Mohammad Rahman, and Tianjian Zhang. Cybersecurity Investments and the Cost of Capital. *SSRN Electronic Journal*, 2020.
28. Bruno Rodrigues, Muriel Franco, Geetha Parangi, and Burkhard Stiller. SEConomy: A Framework for the Economic Assessment of Cybersecurity. In Karim Djemame, Jörn Altmann, José Ángel Bañares, Orna Agmon Ben-Yehuda, and Maurizio Naldi, editors, *Economics of Grids, Clouds, Systems, and Services*, pages 154–166, Cham, 2019. Springer International Publishing.
29. Michela Chessa and Patrick Loiseau. A cooperative game-theoretic approach to quantify the value of personal data in networks. 2016.

30. Neil Robinson, Dimitris Potoglou, Chong Kim, Peter Burge, and Richard Warnes. Security At What Cost? pages 3–15. Springer Berlin Heidelberg, 2010.
31. Ponemon Institue & IBM. Data Breach Risk Calculator. Website, 2016.
32. The Economist Intelligence Unit. CyberTab: Free Tool Estimates Damages from Attacks, 2014.
33. Websense. TCO Calculator: Websense Hosted Email Security Calculator. Website, 2016.
34. Symantec. Small Business Risk Calculator. Website, 2016.
35. Xiaomeng Su. An Overview of Economic Approaches to Information Security Management. Technical report, University of Twente, 2006.
36. Virginia Rezmierski, Stephen Deering, Amy Fazio, and Scott Ziobro. Incident Cost Analysis And Modeling Project. Final Report. Technical report, Committee on Institutional Cooperation Chief Information Officers Committee, 1998.
37. Virginia Rezmierski, Adriana Carroll, and Jamie Hine. Incident Cost Analysis and Modeling Project II. Final Report. Technical report, Committee on Institutional Cooperation Chief Information Officers Committee, 2000.
38. Shawn A. Butler. Security Attribute Evaluation Method: A Cost-Benefit Approach. In *Proceedings of the 24th international conference on Software engineering - ICSE '02*, page 232, New York, New York, USA, 2002. ACM Press.
39. Ning Xie and Nancy R Mead. SQUARE Project: Cost/Benefit Analysis Framework for Information SecurityImprovement Projects in Small Companies. Technical report, Carnegie Mellon University, 2004.
40. Ross Anderson and Tyler Moore. Information Security Economics – and Beyond. In *Advances in Cryptology – CRYPTO 2007*, pages 68–91. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.
41. Rebecca T Mercuri. Analyzing security costs. *Communications of the ACM*, 46(6):15–18, 2003.
42. Nicole M. Radziwill and Morgan C. Benton. Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management. *Software Quality Professional*, 19(3), 2017.
43. Chad Heitzenrater and Andrew Simpson. Policy, statistics and questions: Reflections on UK cyber security disclosures. *Journal of Cybersecurity*, 2, 2016.
44. Mehrnaz Akbari Roumani, Chun Fung, Shri Rai, and Hong Xie. Value Analysis of Cyber Security Based on Attack Types. 2016.
45. Yannis Mallios, Lujo Bauer, Dilsun Kaynar, Fabio Martinelli, and Charles Morisset. Probabilistic cost enforcement of security policies. 23:759–787, 2015.
46. Ye Yang, Jing Du, and Qing Wang. Shaping the Effort of Developing Secure Software. *Procedia Computer Science*, 44:609–618, 2015.
47. Mhamed Zineddine. Vulnerabilities and mitigation techniques toning in the cloud: A cost and vulnerabilities coverage optimization approach using Cuckoo search algorithm with Lévy flights. *Computers & Security*, 48:1–18, 2015.
48. National Institute of Standards and Technology (NIST). *NIST SP 800-53 Rev. 4 Recommended Security Controls for Federal Information Systems and Organizations*. U.S. Government Printing Office, 2013.
49. David A Dittrich. Developing an Effective Incident Cost Analysis Mechanism. Internet, 2002.