Post-print of: Leszczyna R. (2020) Evaluating the Cost of Personnel Activities in Cybersecurity Management: A Case Study. In: Park N., Sun K., Foresti S., Butler K., Saxena N. (eds) Security and Privacy in Communication Networks. SecureComm 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 336. Springer, Cham. https://doi.org/10.1007/978-3-030-63095-9_17

Evaluating the Cost of Personnel Activities in Cybersecurity Management: a Case Study

Rafał Leszczyna[1][0000−0001−7293−2956]

Gdańsk University of Technology, Faculty of Management and Economics, Narutowicza 11/12, 80-233 Gdańsk, Poland rle@zie.pg.gda.pl

Abstract. The methods of cybersecurity costs' evaluation are inclined towards the cost of incidents or technological acquirements. At the same time, there are other, less visible costs related to cybersecurity that require proper recognition. These costs are associated with the actions and the time spent by employees on activities connected to cybersecurity management. The costs form a considerable component of cybersecurity expenditures, but because they become evident only during scrupulous analyses, often they are disregarded. CAsPeA is a method that enables estimating the costs based on a model derived from the Activity-Based Costing (ABC) and the NIST SP 800-53 guidelines. This paper presents the application of CAsPeA in a steel structures manufacturing company.

Keywords: Cybersecurity management · Cost · Estimation · Information security.

1 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 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 [4, 2, 1, 3]. 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.

To enable the calculations, the Activity-Based Costing (ABC) system was selected and adopted to the costing model [4, 2, 1, 3]. 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 an 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 chosen 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* [5]. 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 rough estimations based on a small set of input data that characterise an organisation, namely:

- the number of employees with access to the IT system,
- the number of cybersecurity professionals,
- the hire rate (the percentage of personnel hired in the current year),
- the termination rate (the percentage of workers that terminated their employment in the current year),
- the fluctuation rate (associated with employees' promotions, demotions and transfers)
- the mobile devices usage index (the number of employees that use mobile devices divided by the total number of employees),
- and hourly pay rate values for eight categories of employees.

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 (typical, based on other organisations) value. The application of the method is presented in the next section.

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 enables entering all required input data, such as the number of employees, human resources metrics or hourly pay rates. The worksheets *List of activities* and *Cost of information security professionals* comprise formulae for calculation of the total cost of activities. In the *Assessment results worksheet* the outcomes of the assessment are presented. More details on CAsPeA can be found in [4, 2, 1, 3].

2 Case study

This section illustrates the application of CAsPeA for a manufacturer of steel structures and filtering devices for water purification in crisis situations. The filters are designed for quick relocation, manoeuvring and deployment. They remove various types of contaminants, including natural, chemical, biological and radioactive. In addition, the company produces devices for storing drinkable water in a field. Figure 1 presents the structure of the IT system of the enterprise. It is worth to note that the main site and the sales office are located in two different cities.

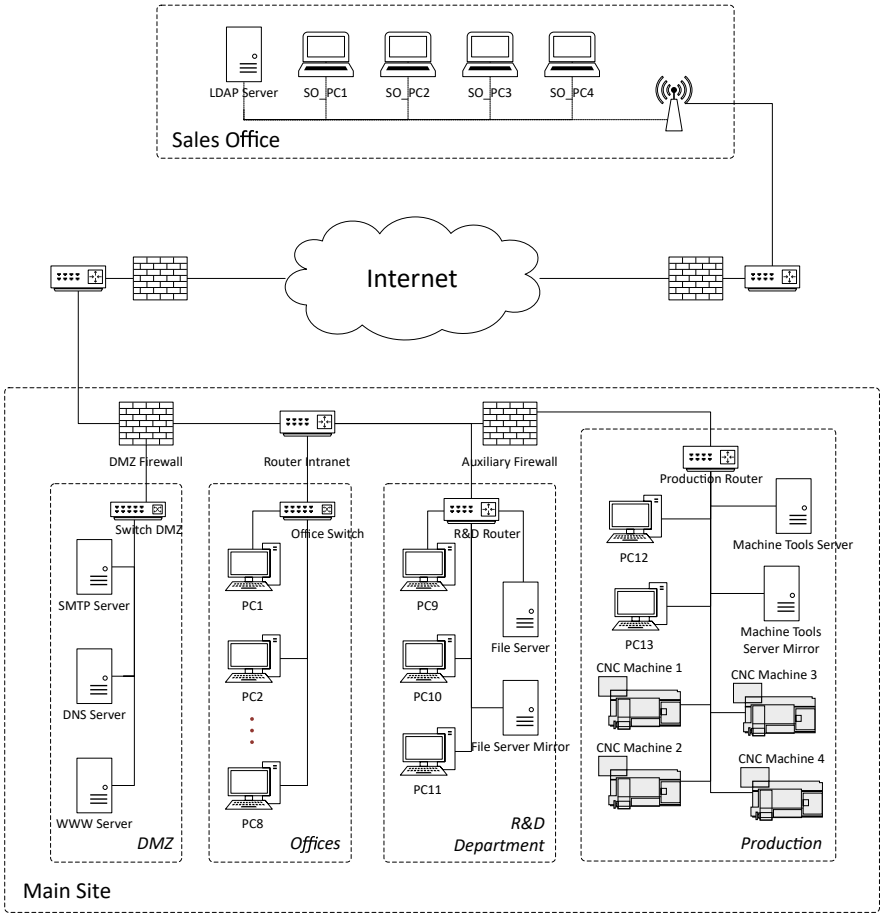

Fig. 1. The IT system of the manufacturer of steel structures and filtering devices for water purification in crisis situations.

2.1 Input data

The enterprise employs more than 50 workers. In the first step of the cost evaluation process, the number of posts with access to the IT system needed to be determined. Table 1 presents the extract of the company's employment structure showing the relevant positions. The wanted value is 40. The hire rate, termination rate, fluctuation rate and the mobile devices usage index are subsequently 13%, 8%, 3% and 10%. Finally, the average hourly gross pay rates for eight categories of employees are presented in Table 2.

Table 1. The employment structure of the manufacturer of steel structures and filtering devices (employees that have access to the IT system).

	Position/Department	Number of employees
1.	Chief Executive Officer	1
2.	Director	3
3.	Management Assistant	1
4.	Plenipotentiary	2
5.	Secretariat	2
6.	Quality Control	2
7.	Managers	7
8.	Specialists	11
9.	IT officers	2
10.	Other employees	9
	Total	40

Table 2. The average hourly gross pay rates in the analysed enterprise.

Resource cost drivers	Average hourly gross pay rate [PLN]
Information security professionals	48
IT administrators	51
Human Resources Management professionals	42
Users	32
Senior-level executives or managers	53.5
Physical security officers	20
Physical security officers guards	20
Budget Planning and Control professionals	49

2.2 Results

Based on the input data, cost estimates presented in Tables 3 and 4 were obtained. The total cost of personnel activities associated with cybersecurity is

202,287.20 PLN (Polish Złoty) which is equivalent to around 55,000 USD or 46,000 EUR. This cost is calculated based on typical (usual) values from other companies assigned to the activities in the CAsPeA model. Alternatively, the minimum (when baseline cybersecurity level is maintained), maximum (when extensive cybersecurity measures are introduced) and average values are consequently 122,934.66 PLN (around 33,000 USD or 28,000 EUR), 1,358,004.10 PLN (around 370,000 USD or 310,000 EUR) and 740,469.38 PLN (around 200,000 USD or 170,000 EUR). It becomes evident that these values are not negligible. Contrarily, they can become a visible component in a yearly budget. Thus, they need to be appropriately considered when planning company activities, cybersecurity strategies etc.

Table 3. The estimate of the total yearly cost of activities associated with cybersecurity management for the manufacturer of steel structures and filtering devices.

Total yearly cost of activities [PLN]			
Minimum	Maximum	Average	*Usual*
122,934.66	1,358,004.10	740,469.38	*202,287.20*

Table 4. Estimates of parameters associated with cybersecurity professionals: cost of their activities, the number of required working hours, and the required number of posts.

Estimated parameters associated with cybersecurity professionals			
Yearly cost of activities [PLN]			
Minimum	Maximum	Average	*Usual*
35,553.12	250,516.80	143,034.96	*91,779.60*
Required working hours (yearly)			
Minimum	Maximum	Average	*Usual*
740.69	5,219.10	2,979.90	*1,912.08*
Required positions			
Minimum	Maximum	Average	*Usual*
0.5	3.0	1.5	*1.0*

Further analysis of the results reveals that a substantial part of the costs is associated with the activities connected to Physical Access Monitoring and Control (PAMC). These activities include surveillance of both company sites located in two different cities and require continuous presence of security guards and specialists. However, the IT system is one of many assets monitored within the activities. Thus, the associated cost can be entirely or partially deduced from the cost of cybersecurity. Table 5 presents the estimate of the total yearly cost of activities associated with cybersecurity management with PAMC excluded.

Table 5. The estimate of the total yearly cost of activities associated with cybersecurity management for the manufacturer of steel structures and filtering devices **excluding Physical Access Monitoring and Control (PAMC) activities**.

Total yearly cost of activities excluding PAMC [PLN]			
Minimum	Maximum	Average	*Usual*
44,554.66	296,284.10	170,419.38	*104,607.20*

3 Conclusions

The paper illustrated the application of CAsPeA to an enterprise that specialises in manufacturing steel structures and filtering devices. CAsPeA revealed the hidden costs that normally are not considered, but apparently, constitute a considerable costing component. These costs are associated with employees' daily activities connected to cybersecurity (e.g. getting familiar with cybersecurity policies or 'processing' cybersecurity incidents) and should be taken into account when planning company activities or cybersecurity strategies. Based on a small set of input parameters, a rough estimation of minimum, maximum, average and typical cost values was obtained. Also, indications on the required working hours and posts for cybersecurity officers were provided. Further works on the method include:

- development of ISO/IEC 27001-based version and comparing it to the current, NIST SP 800-53-based edition,
- enhancing CAsPeA with activities linked to the security controls of the secondary and tertiary NIST SP 800-53 baselines,
- and acquiring empirical data on the cost of personnel activities and comparing them to the results from CAsPeA.

References

1. Leszczyna, R.: Cost assessment of computer security activities. Computer Fraud and Security **2013**(7) (2013). https://doi.org/10.1016/S1361-3723(13)70063-0
2. Leszczyna, R.: Approaching secure industrial control systems. IET Information Security **9**(1) (2015). https://doi.org/10.1049/iet-ifs.2013.0159
3. Leszczyna, R.: Metoda szacowania kosztu zarządzania bezpieczeństwem informacji i przykład jej zastosowania w zakładzie opieki zdrowotnej. Zeszyty Kolegium Analiz Ekonomicznych (2017)
4. Leszczyna, R.: Cost of Cybersecurity Management, pp. 127–147. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-19538-0_5, https://doi.org/10.1007/978-3-030-19538-0_5
5. 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)