EDUCATION OF ECONOMISTS AND MANAGERS
Volume 55, Issue 1, March 2020

Received 15 October 2019; Revised 10 January 2020; Accepted 31 January 2020

DOI: 10.33119/EEiM.2020.55.6

Antczak, J. (2020). Costs of Cyber-Security in a Business Entity. *Education of Economists and Managers*, 55(1), 81–93.
Retrieved from: https://econjournals.sgh.waw.pl/EEiM/article/view/2353

Costs of Cyber-Security in a Business Entity

Joanna Antczak

Institute of Logistics, Faculty of Management and Command, War Studies University

Abstract

Functioning of any business entity in the cyberspace is unavoidable. Most commercial transactions, marketing activities, e-mail contact with employees or contractors are carried out in virtual space. The aim of this article is to indicate and analyse selected costs for cyber security of a business unit. Costs related to cyber security constitute a new category in the management of an entity. Considering costs at the enterprise level, two areas should be taken into account. On the one hand, costs incurred to prevent cyber threats and, on the other hand, to eliminate the negative effects of cyber-attacks. In order to function in a stable way and at the same time develop in the future, the management of an entity should strengthen information security activities which are associated with costs that will minimise the risk of a cyber-attack.

Keywords: costs, costs of cyber-security, cyber threats, direct costs of cyber-security, indirect costs of cyber-security

JEL Classification Code: G000

Introduction

The economic conditions in which a modern company has to operate are conducive to the liberation of initiatives in many areas of managing its activities. The introduction of new solutions and the use of innovative cost management concepts determine the financial success of an enterprise (Karmańska, 2007, p. 11).

Functioning of any business entity in cyberspace is unavoidable. Most commercial transactions, marketing activities, e-mail contact with employees or contractors take place in virtual space. As early as in 1984, Gibson (2009, p. 53), in his novel *Neuromancer*, described the term *cyberspace* as "a consensual hallucination experienced every day by billions of authorised users in all countries, by children taught mathematical concepts [...] Graphical representation of bank data of all the world's computers. An unimaginable complexity". In turn, Sienkiewicz (2009, p. 195) believes that access to it provides opportunities to meet a range of social needs in the areas of education, culture, economy, communication, etc. At the same time, cyberspace has become a source of threats, which has given rise to the notions of cybercrime, cyberterrorism, cyber-spying or cyber-war.

The purpose of this article is to indicate and analyse selected costs for the cyber-security of a business unit. In order to achieve the aim, the starting point was to define the costs of a company's cyber-security. Then, the inclusion of cyber-security costs in financial and management accounting was analysed.

Taking into account the costs at the company level, two areas should be taken into account, on the one hand, incurred in order to prevent cyber threats and, on the other hand, to eliminate the negative effects of cyber-attacks.

Costs of a business entity's cyber-security

Costs can be analysed both in the microeconomic and macroeconomic area from a retrospective as well as prospective point of view.

In the literature there are many definitions of costs that depend on the context in which they are defined. Cost as an "economic category means the monetary value of the living labour and capital resources used in a given period to produce products and may be represented by multiplying the price by the consumption of the production factor" (Nowak, 2005, p. 23). "In principle, cost should be understood as the monetary resources (goods and services) used (spent) to obtain current or future benefits" (Dobija, Kucharczyk, 2009, p. 55).

According to the Accounting Act, "costs and losses shall mean probable decreases in economic benefits during the reporting period of a reliably determined value in the form of a decrease in the value of assets or an increase in the value of liabilities and provisions, which will lead to a decrease in equity or an increase in its deficiency in a manner other than the withdrawal of funds by shareholders or the owner" (Act..., 1994, Article 3 Act 1 Point 3). According to the tax law, "tax deductible costs are costs incurred in order to earn revenue or to preserve or secure a source of revenue" (Act..., 1992, Article 15 Act 1). The International Accounting Standards define "costs as reductions in economic benefits during a financial year in the form of an outflow or decrease in the value of assets or the creation of liabilities, resulting in a decrease in equity, except for the distribution of equity to owners" (SKwP, 1999, p. 338).

When considering the costs related to cyber security at the company level, two areas should be considered (Table 1), on the one hand, incurred in order to prevent cyber threats (indirect costs) and, on the other hand, to eliminate the negative effects of cyber-attacks (direct costs).

The cyber-threat catalogue was defined by the Government Computer Emergency Response Team (Table 2).

Table 1. Direct and indirect costs of cyber-security

INDIRECT COSTS	DIRECT COSTS
• purchasing a license for antivirus software • remuneration of cyber-security employee(s) • cyber-attack insurance policies • external data clouds • specialist advisory and legal services • costs related to data security – external drives, servers, etc. • training of employees in cyber-security	• court fees and lawyers' fees • contractual penalties • loss of money, e.g., hacking into bank accounts • costs for external parties restoring the system, data recovery • stagnation on the production line • lost value of customer relations • image loss • costs related to customer protection after stealing their data • loss of intellectual property • brand devaluation

Source: own elaboration.

Indirect costs are characterised by the fact that their value can be determined in advance. In the case of direct costs, it is different, e.g., court costs, contractual penalties or loss of funds may be specified in value. This loss of image is difficult to estimate.

Table 2. Catalogue of threats by CERT.GOV.EN

TYPE	TYPE			
Malware	Virus	Ransomware	Botnet client	
Security breach	account intrusion	system intrusion	infrastructure hacking	
Publications on the Internet	harmful content	disinformation	punishable threats	
	identity theft/fraud		publication of sensitive data	
Collection of information	scanning	social engineering	sniffing	SPAM
Computer sabotage	unauthorised change of data	unauthorised access	access denied attack (e.g., DDoS, DOS)	damage to the resource
The human factor and random events	breach of security policy	Negligence	technical work	breakdown
Vulnerability	vulnerability disclosure		misconfiguration	
Cyberterrorism	terrorist incidents			

Source: *Katalog zagrożeń stosowany przez CSIRT GOV*, Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, Retrieved from: https://www.cert.gov.pl/cer/publikacje/katalog-zagrozen-stosow/731, Katalog-zagrozen-stosowany-przez-CERTGOVPL.html (01.07.2018).

Defence against cyber threats "consists of developing, operating, managing, protecting, defending and commanding the elements of cyberspace. Systems (hardware and software solutions) for cryptographic shielding of connections, masking motion generators, detection systems (IDS), detecting soft reconnaissance and probing actions, own services, trusted 'cloud', including services: storage and file sharing, synchronisation and password storage, strong authentication mechanisms" (Najgebauer et al., 2018).

It should be remembered that the costs associated with cyber-security are not the same for every company. According to the taxonomy used by the British in a study that concerned cyber-security breaches, victims should calculate the cost of the attack by adding three categories:

1) Direct effects – related to the loss of revenue due to periodic interruptions of operations, other losses resulting from theft and destruction of data;
2) Repair activities – including additional workloads imposed by hacking into systems and expenditure on repairing damaged equipment or infrastructure;
3) Long-term effects – penalties, incurred legal costs and loss of value of the company's shares or sources of financing (UK Department for Culture, 2017).

According to the Deloitte report, costs incurred by companies and institutions should be considered at two levels: direct costs and hidden costs. From the point of view of the company's CFO, the most important thing should be hidden costs, such as:

- an increase in the insurance premium for buying or renewing a cyber-insurance policy;
- an increase in borrowing costs;
- disruption of operations or loss of data;
- lost value of customer relations;
- value of lost revenues from contracts;
- brand devaluation – a devaluation of a trade name is a category of intangible costs related to the impairment of names, signs or symbols used by an organisation to distinguish its products and services;
- loss of intellectual property – the loss of IP is an intangible cost associated with the loss of sole control of trade secrets, copyrights, investment plans and other proprietary as well as confidential information that may lead to the loss of competitive advantage, the loss of revenue and permanent as well as potentially irreparable economic damage to the company (Deloitte, 2016).

In 2016, Ponemon Institute (Ponemon Institute, 2016) conducted another study on the cost of cybercrime in selected countries (in the United States it was the seventh year, in the United Kingdom, Germany, Australia and Japan it was the fifth year and the second year in Brazil). The aim of the study in 2016 was to estimate the impact of cyber-attacks on the economy, to indicate what the cost directions are over time and how much a successful cyber-attack could cost. The costs identified in the study did not include all the expenses and investments incurred in order to maintain the cyber-security of the entity.

The study defines a successful cyber-attack as one that infiltrates a company's main networks or systems. However, the study did not include attacks detained by the company firewall protection system.

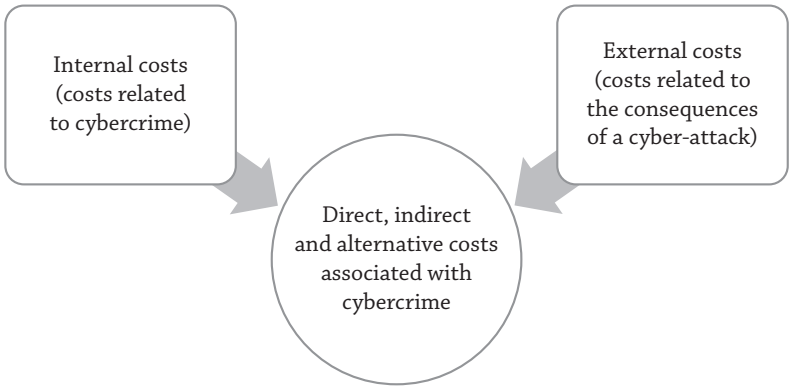
Figures 1 and 2 show the range of costs of cybercrime which were used to calculate the average cost of a cyber-attack. The costs were divided into two streams:

1) Costs related to cybercrime or what might be called the cost of the entity's internal centres of operations.
2) Costs related to the consequences of a cyber-attack or what might be called the external consequences of a cyber-attack.
3) The total external costs have been correlated to nine noticeable cyber-attacks:
   a) viruses, worms, trojans;
   b) malware;
   c) botnets;[1]

[1] Botnet is a network of malware-infected computers that gives the hacker remote control of machines to send spam, spread viruses or carry out DDoS attacks without the knowledge and consent of the actual owners.

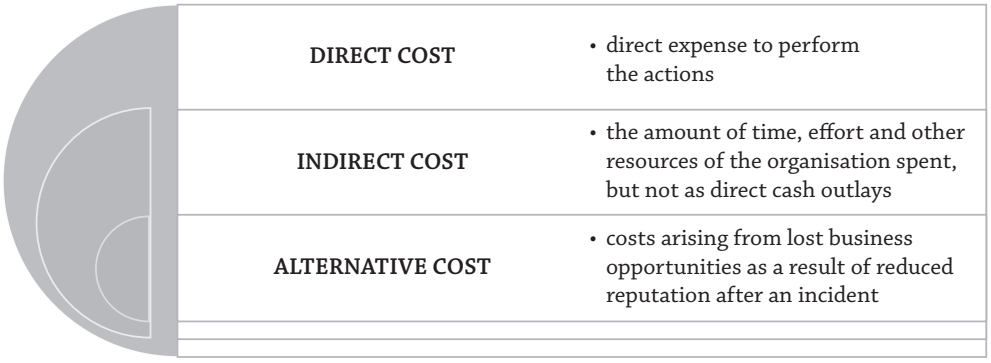
d) network attacks;
e) phishing[2] and social engineering;
f) malicious insiders;[3]
g) stolen or damaged equipment;
h) malicious code (including SQL injection);
i) refusal of services.

Figure 1. Cybercrime cost structure



Source: own elaboration based on Ponemon Institute (2016, p. 29).

Figure 2. Direct, indirect, alternative costs of cybercrime



Source: Ponemon Institute (2016. p. 29).

[2] Phishing – a scamming method in which the offender impersonates another person or institution in order to scam certain information (e.g., login details, credit card details) or to induce the victim to act.

[3] Insider trading (or insider dealing) – transactions in securities listed on the stock market of a given company made by persons having access to non-public information concerning that company and using that information for private profit.

In the area of internal costs of cybercrime, the following can be distinguished: detection of the incident, investigation and escalation, reduction, improvement and ultimately consequences. In terms of external costs, the following activities can be distinguished: the loss or theft of information, disruption of operations, damage to equipment, the loss of income.

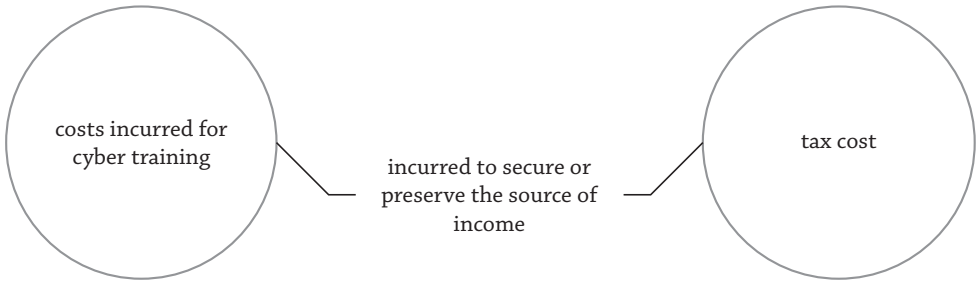
Cyber-security costs in financial accounting

In order to counteract cyber-threats, the approach to security should be changed, which is associated with, on the one hand, an increase in security investment expenditure and, on the other hand, providing employees with training in the field of threats and their effects, in particular, cyber threats.

When considering the inclusion of cyber-security costs in the area of financial accounting, these costs are related to, among others: training of employees, hiring a security specialist, purchasing an insurance policy, and purchasing software.

Expenditure on employees' training (Figure 3) is eligible for recognition as a deductible expense with the training being closely related to the employee's responsibilities.

Figure 3. Costs for cyber training



Source: own elaboration.

The costs related to the improvement of employees' professional qualifications are included in the books of accounts as operating costs of the company.

Purchasing a license of antivirus software or updating software and mechanisms for controlling access to networks, applications, system functions and data are another costs related to cyber-security. The accounting of the purchased license depends on the purchase price and the period of use.

If the value of the purchased license exceeds 10,000 PLN and at the same time it will be used in the company for more than twelve months, then it must be classified as

an intangible asset. However, if the value of the purchased software does not exceed 10,000 PLN and the settlement is made proportionally to the period of use or, in accordance with the company's accounting policy, it is not significant in relation to the balance sheet total, it is recorded in the cost accounts of the core business.

An extremely important aspect is the employment of an IT security officer. The costs of remuneration and surcharges are included in the books of accounts as operating costs of the company.

Another cost associated with cyber insurance is purchasing a cyber-insurance policy. The value of the policy depends on many factors.

In the case of an enterprise with a turnover of up to 10,000,000 PLN, for each one million PLN of the insurance sum the cost of the policy is on average about 5000 PLN. The purchase of an insurance policy is recognised in the cost accounts for basic activities.

Table 3 shows a breakdown of the costs of cyber threats and their inclusion in the accounts and reporting.

Table 3. Breakdown of costs of cyber threats (bookkeeping and reporting)

Costs of cyber threats	Types of risks	Entry in the books
Costs related to the theft or phishing of confidential information for the purpose of using it to the detriment of the business entity.	• theft of identity, employee data • offensive and illegal content incidents involving employees or individuals • breach of security access within the system • computer hacking – bypassing system security and gaining unauthorised access to the information of a business entity • computer eavesdropping – unauthorised interception of all information of a business entity in cyberspace	• included in operating costs • presented in the profit and loss account
Costs related to destruction, damage to the property and information.	• unlawful damage, destruction or deletion of information, e.g., attacks using malicious virus software • hardware and software destruction • disruption of automatic information processing • computer sabotage – disrupting or paralysing the functioning of information system in an economic entity	• included in other operating costs • presented in the profit and loss account

Costs of cyber threats	Types of risks	Entry in the books
Costs of litigation related to cybercrime.	• payment of a fee for hiring a law firm to write a statement of claim	• included in other operating costs or release of the provision (accrued expenses) • presented in the income statement or balance sheet
Costs of measures taken to protect against cybercrime.	• insurance policies • antivirus programs • remuneration of an employee responsible for cyber security	• included in the costs of basic operating activity or prepayments • presented in the income statement or balance sheet

Source: own elaboration based on Dratwińska-Kania (2017, pp. 94–97).

Cyber-security costs in management accounting

When considering the inclusion of costs of cyber-security in the area of management accounting, it is reasonable to:

1) make a cost classification for decision-making purposes;
2) introduce actions from the change management model or management by change;
3) take into account the risks and possible consequences of cyber-attacks on specific areas of business: the size of the company, the sector to which it belongs and the degree of dematerialisation.

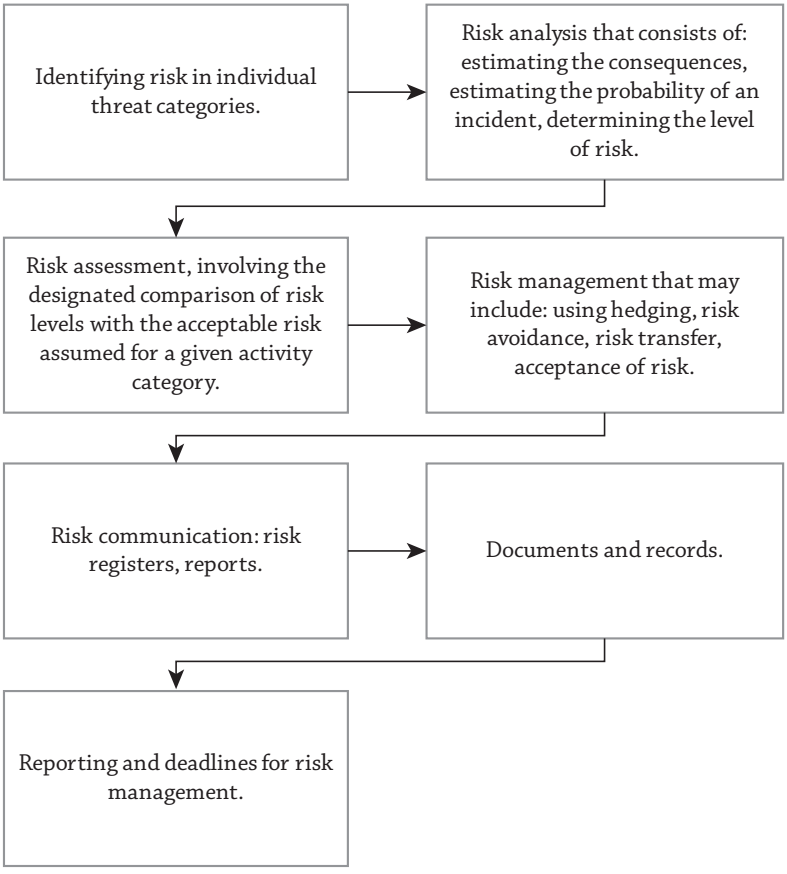
The main costs generated from the point of view of management accounting in the area of cyber-security are related to legislative and regulatory activities in the form of developing instructions, procedures and internal regulations. In creating its own regulations, procedures or orders, an entity may use, among other things, the methodology of cyber risk management in government information security management systems (Figure 4) (Łobko, 2019).

"The most appropriate management process for cybercrime is the process of change management, which, due to its complexity and staggered nature over time, aims to achieve the initial goal. An indication for change is both the environment in relation to which the enterprise should have a specific policy and the enterprise in which everyone is potentially affected by the change. The first step is to prepare people and companies for change, the second step is the change itself, and the third is to consolidate the changes in the system" (Furman, Kuczyńska-Chałada, 2016).

The importance of costs as a decision-making element results from the fact that an entity can optimise them. By setting specific goals, it aims to achieve them at the lowest cost, sacrificing certain funds, wants to achieve the best effect so that the

proper revenue-to-cost ratio is maintained, i.e., that revenues exceed costs (Dobija, Kucharczyk, 2009, p. 107).

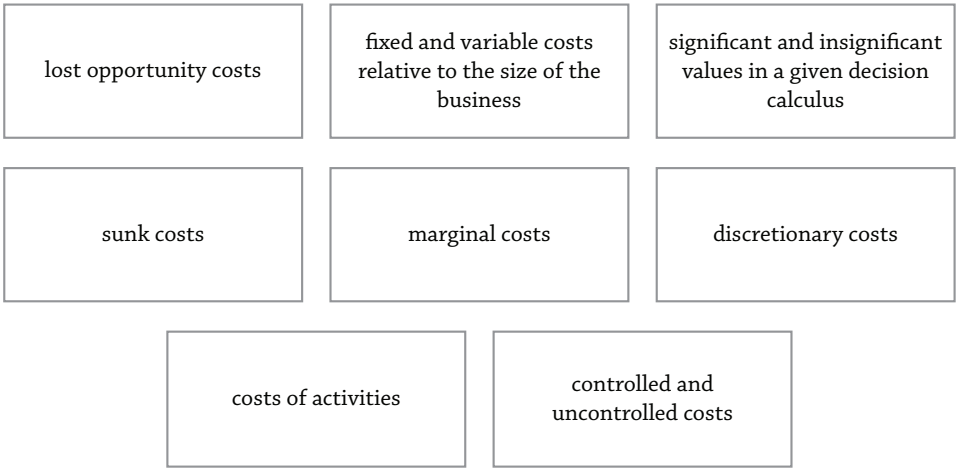
Figure 4. Cyber risk management approach



Source: own elaboration based on Łobko (2019, pp. 7–11).

An extremely important category of costs, from the point of view of managing an enterprise and at the same time making the related decisions, are the so-called costs of lost opportunities, which appear whenever an individual takes any action, even the simplest and most obvious ones. These costs mean income lost as a result of one action being abandoned in favour of another. They show what an individual can lose by rejecting an alternative possibility of action (Dobija, Kucharczyk, 2009, p. 109). The lack of decisions on the prevention of cyber threats due to, e.g., their high costs can cause various types of losses, including losses that are difficult to value, such as those related to the lost image.

Figure 5. Cost allocation for decision-making purposes



Source: own elaboration.

Conclusion

The management and employees of a business unit should be aware of the conditions in which they operate; cyberspace and its associated facilitations and threats are becoming a daily reality. In order to function in a stable way and at the same time develop in the future, the management should strengthen information security activities, which is associated with costs that will minimise the risk of a cyber-attack.

Costs related to cyber-security constitute a new category in the management of an entity at the accounting, both financial and management level, starting with the recognition of their accounts, then presentation in the statements to a significant category in the entity's management process.

References

Deloitte (2016, July). *CFO Insights. Seven hidden costs of a cyberattack*.

Dobija, D., & Kucharczyk, M. (Eds.) (2009). *Rachunkowość zarządcza. Teoria. Perspektywa. Aspekty behawioralne*. Warszawa: Wydawnictwo Akademickie i Profesjonalne.

Dratwińska-Kania, B. (2017). Koszty cyberprzestępczości – perspektywa rachunkowości. *Studia i Prace Kolegium Zarządzania i Finansów. Zeszyty Naukowe*, 157. Warszawa: SGH Warsaw School of Economics.

EFNI (2015, 30 September–2 October). *Relacje. Europa wobec rosnących nierówności społecznych, radykalizmów i zagrożeń geopolitycznych*. Europejskie Forum Nowych Idei. Sopot.

Furman, J., & Kuczyńska-Chałada, M. (2016). Change management in lean enterprise. *Economics and Management*, 2.

Gibson, W. (2009). *Neuromancer*. Katowice: Wydawnictwo Książnica.

Karmańska, A. (Ed.) (2007). *Zarządzanie kosztami jakości, logistyki, innowacji, ochrony środowiska a rachunkowość finansow*a. Warszawa: Difin.

Katalog zagrożeń stosowany przez CSIRT GOV, Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. Retrieved form: https://www.cert.gov.pl/cer/publikacje/katalog-zagrozen-stosow/731, Katalog-zagrozen-stosowany-przez-CERTGOVPL.html (01.07.2018).

Łobko, M. (2019). Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych. In: *Rekomendacje i zalecenia Komitetu Rady Ministrów do spraw Cyfryzacji z 12 listopada 2015 r.* Retrieved from: https://ryzyko.pro/baza-wiedzy/metodyka-zarzadzania-ryzykiem-cyberprzestrzeni-w-systemach-zarzadzania-bezpieczenstwem-informacji-podmiotow-rzadowych/ (02.07.2019).

Najgebauer, A., Antkiewicz, R., Tarapata, Z., Kulas, W., Pierzchała, D., Rulka, J., Chmielewski, M., Kasprzyk, R., & Dyk, M. (2018). *Analiza zdolności cybernetycznych za pomocą symulacji komputerowej*, Wydział Cybernetyki WAT, Warszawa. Retrieved from: https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5890/14/1/1/wat_analiza_zdolnosci_cybernetycznych_za_pomoca_symulacji_komputerowej.pdf (01.07.2018).

Nowak, E. (2005). *Rachunek kosztów przedsiębiorstwa*. Wrocław: Ekspert Wydawnictwo i Doradztwo.

Ponemon Institute (2016, October). *Cost of cybercrime study & the risk of business innovation*.. Retrieved from: https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf (01.07.2018).

Sienkiewicz, P. (2009). Terroryzm w cybernetycznej przestrzeni. In: T. Jemioło, J. Kisielnicki, K. Rajchel (Eds.), *Cyberterroryzm. Nowe wyzwania XXI wieku*. Warszawa: Wyższa Szkoła Informatyki, Zarządzania i Administracji.

SKwP (1999). *Międzynarodowe Standardy Rachunkowości 1999. International Accounting Standards Committee*. Warszawa: Stowarzyszenie Księgowych w Polsce za zgodą IASC.

The Act of 15 February 1992 on corporate income tax (Journal of Laws of 2010, no. 229, item 1496 as amended).

The Act of 29 September 1994 on accounting (Journal of Laws of 2009, no. 152, item 1223 as amended).

UK Department for Culture, Media and Sport (2017). *Cyber-security breaches survey: Main report*. London.

Joanna Antczak

PhD, Assistant Professor at the War Studies University in Warsaw. Her research and publication output concern a wide range of subjects such as accounting, including financial security, controlling, as well as economic and defense state security, along with cyber-security, and the use of tools such as financial analysis, bankruptcy risk assessment models. She has gained her knowledge and professional experience in financial institutions and an accounting office.
e-mail address: j.antczak@akademia.mil.pl