7th International Conference on New Ideas in MANAGEMENT, ECONOMICS & ACCOUNTING
ROME, ITALY 21-23 FEBRUARY, 2020

Business Model Disclosures - support framework for Cyber Security Management

Aleksandra Ferens

University of Economics

Abstract

Background: The selection of the right business model has recently become a key issue for many business entities which aim at maintaining their market position as well as creating their added value. A business model defines a group of financial, strategic and organisational elements that impact one another and explain how the enterprise creates value for the organisation and clients. An important element of individual components of a business model is to ensure security for activities that may infringe the confidentiality and veracity of processed data. The author therefore proposes to introduce a description of the 'cyber security information' model into the overall firm's business model and present it in the integrated report of an enterprise.
Methods: The author used literature analysis in the field of business model and cyber security, and on this basis, applied the methods of analysis and synthesis to the proposed business model. In addition to theoretical studies, empirical studies will be carried out on the integrated reports of selected companies listed on the Warsaw Stock Exchange.
Results: The author of the paper proposes to build a 'business model' of the enterprise which takes into account interactions with the cyber security system in the firm.
Conclusions:
The proposal of a 'business model' which involves aspects of cyber security will increase the firm's value and its competitiveness.

Key words: business model, cyber security, integrated report

1. Introduction

Every year, many new technologies changing entrepreneurs' perception of the world are launched. The dynamic pace of technological innovation triggers substantial changes in the social and economic environment. The way of conducting business moves with the changing business environment and the development of modern technologies. Managers are required to

make right decisions which give them an advantage in a competitive market. That, in turn, is closely linked with the confidence in the way information security is managed. Therefore, there is a need to create appropriate security systems related to cyberspace. The cyber attack

threat can affect information systems of an entire enterprise, among which the accounting information system is extremely important. The threat may appear at any stage of handling information, when it is entered, processed, transferred and archived. For example, PwC warns in its report that in 2015, compared to 2014, the number of IT security incidents in the world increased by 38%, and by over 46% in Poland [PwC report, 2016, www 1]. Consequently, there is a need for research on business models which would address cyber security aspects. The business model makes it possible to understand the business logic and infrastructure necessary to operationalise this concept [Lambert 2008, p. 282]. Companies that undergo the digital transformation build their business models on modern technologies and innovative solutions, gaining new contractors, and thus new sources of revenue. This requires a comprehensive approach to cyber security, which not only will include the company' strategy, but also its effective implementation and risk monitoring. Therefore, there is a need to identify areas most vulnerable to risk factors. The initial stage of this process is to conduct a systematic assessment of the risk of an incident, followed by the development of a management model, including risk, incident and change.

Purpose:

The paper aims at assessing the current scope of information on cyber security presented in business models of enterprises. To achieve this goal, the analysis focused on integrated and consolidated reports of the energy (WIG Energia) and fuel (WIG Paliwa) companies listed on the Warsaw Stock Exchange (WSE).

As a summary, recommendations were issued for companies to build a cyber threat prevention model, and then embed cyber security aspects into their overall business model.

As a result, business entities will gain a competitive advantage by expanding their individual value creation model for various stakeholder groups.

Cyber security – the concept and its meaning for stakeholders

The subject of cyberspace and the threats associated with it has been known since the emergence of the Internet, as evidenced by numerous studies of Polish and foreign authors, e.g. KKR Choo (2011), T. Bass (2000), J.M. Deirmenjian, J. M. (1999), Rabai et al (2013), K.J. Knapp et al. (2009), K.T. Smith et al. (2011). In Poland, studies on this subject have also been published for over 20 years, e.g. J. Kowalewski, M. Kowalewski (2014), Suchorzewska A. (2010), J.W. Wójcik (1999), E.I. Szczepankiewicz, E. Dudek (2009), Grzelak M, Lieder K. (2012), E. I. Szczepankiewicz (2018).

The literature defines the concept of cyberspace in different ways. According to the European Commission, 'cyberspace is a virtual space in which electronic data processed by PCs from around the world circulates.' On the other hand, virtual space is a logically separated space

created by the sum of data, files, websites, applications and processes contained in systems, which are accessed only through ICT systems [Wasilewski 2013]. A broader definition of cyberspace is contained in a government document entitled 'The UK Cyber Security Strategy – Protection and Promotion of the United Kingdom in the Digital World,' in which the authors expanded the scope of cyberspace by stating that it is an interactive domain made of digital networks that is used to store, modify and transfer information. The cited definition of cyberspace also included networks used in large enterprises. This definition emphasises the concept of 'interactivity' which means that not only is cyberspace a source of information for its users, but also an area that is shaped by its recipients [Wasilewski, 2013].
In Poland, the definition of cyberspace was introduced by the Government Programme for Cyberspace Protection for 2011-2016 [www 2], according to which cyberspace is a space for processing and exchange of information created by ICT systems with connections between them and relationships with users. This definition pays particular attention to relationships with users concerning various areas of the enterprise's operations and their exposure to misuse. The adoption of a specific method of defining cyberspace has a significant impact on the method of determining the material scope of cyberspace security. In the context of the definition of cyberspace covering the digital domain and relationships between users, cyberspace security should include not only a separate space, but also the security of what is happening in cyberspace. These requirements are met by the definition of cyber security in the Act on the National Cyber Security System [2018], according to which cyber security is the resilience of information systems to activities violating the confidentiality, integrity, accessibility and authenticity of processed data or related services offered by these systems.

This definition adopts a functional approach to cyber security. There is a reference to a wide catalogue of actions that must be taken to protect information systems. Particularly noteworthy is the fact that in addition to strictly technical activities related to ICT devices, the importance of legal, ethical, social and educational activities was emphasised. First, technical and organisational measures aimed at strengthening information systems were highlighted , and second, the security of processed data was mentioned. This definition has a direct impact on the 'importance of security' of information processed by the accounting information system as well. The definition leads to a definite conclusion – there has been an increase in awareness among entrepreneurs and their environment as to the value of information.

The digital reality that surrounds us means that access to information is possible from virtually any place on the earth. Services are increasingly provided in the so-called cloud computing technology, presenting new challenges in the field of information security. Providers of this type of services are among the most vulnerable entities when it comes to information security. The use of cloud computing brings a lot of benefits, but also the risk of control and security loss, see: P. Fulmański, S. Wojczyk (2014), J. Shayan et al. (2013), A.S. Elmaghraby, & M.M. Losavio, (2014).

In fact, trusting own data provider and key users (individuals, organisations) one must consider dependence on the accessibility, confidentiality and integrity of the data. Accessibility may change if the subscriber's data are unavailable due to a denial of service attack; confidentiality

may be breached if the data are accidentally or maliciously made available by an unauthorised user; integrity may be compromised if the data are accidentally or maliciously damaged or destroyed. As noted by S.A. Hussain et al. it is necessary to consider the problem of cloud security attacks for each cloud layer separately. They propose a multi-level classification of security attacks and submit a proposal of security contract for each cloud player. It is worth considering this classification in the security system development of the accounting system, which is the most important information system for each manager, supported by modern ICT systems. Financial and accounting systems functioning both in domains and in the 'cloud' store sensitive business data, which must be properly secured. The methods of securing them are subject to various legal regulations. In Poland, the issues of securing financial and accounting systems are primarily regulated by the Accounting Act and in relation to essential service entities, essential service operators, the Cyber Security Act[1] and the Personal Data Protection Act. Enterprise's systems related to finance and accounting services processing sensitive data for managers should be protected not only from outside but also from inside. That is why, the multilevel data security system, which should be an inherent part of the firm's business model at all levels, is extremely important.

1. The identification of cyber security in the business model of the surveyed entities

The business model is defined differently in the literature. Review of research in this area was carried out by: G. George & A.J. Bock (2011). G. M. Karwowski (2015), J. Brzóska (2014), Lai, Melloni, Stachenzini (2013), Boulton, Libert and Samek [2000, pp. 2-18].

In broad terms, it can be assumed that the business model expresses logic and provides data and other evidence to demonstrate how a firm creates and delivers value [Teece, 2010]. A detailed definition describing elements of the business model is the definition presented by the IIRC (International Integrated Reporting Council) [IIRC, 2013], according to which the business model is defined as 'the organization's chosen system of inputs, business activities, outputs and outcomes that aims to create value over the short, medium and long term.'

Despite significant definition differences, it is stated that there are some recurrent elements in them. According to Osterwalder, Pigneur (2012) these are: key partners, key activities, key resources, value proposition, customer relationships, channels, customer segments, cost structure and revenue stream [B. Rymkiewicz, B. Bek-Gaik, 2017). Customers are also believed to be the axis of every business model, while the value proposition is an element for which customers put a firm's offer above other competitive offers [Lambert 2008].

[1] The Cyber Security Act is an act implementing Directive 2016/1148. It is the first legal act that the Cyber Security Act is an Act implementing Directive 2016/1148. It is the first legal act which, in a cross-cutting manner, sets out the tasks and responsibilities that should be undertaken in order to ensure the efficient organisation of the national cyber security system. This Act is addressed to entities recognised as key service operators and digital service providers and sets out the tasks and responsibilities that should be taken to ensure the efficient organisation of the national cyber security system.

According to the framework structure of the business model created by IIRC, the business model should comprise the following areas:

- disclosures concerning input elements – financial capital, human capital, intellectual capital, natural capital, social capital, relational capital,
- disclosures concerning business activities – planning, design, production of products, activities contributing to the long-term success of the organisation,
- disclosures concerning output items – products, services, by-products, waste,
- disclosure of results – internal and external consequences that are the result of the organisation's business activities.

Consequently, the business model exists at the very core of every organisation and uses a variety of capitals as input elements and, through business activities, transforms them into output elements (products, services, by-products and waste).

Therefore, the author believes that elements of the cyber security model, which will generate value for a specific customer segment, should be embedded in the business model of the enterprise.

Methodology:

In order to identify disclosures on cyber security in the described business models, the author analysed the content of integrated reports (IR), consolidated reports (CR), management reports (MR), published by energy and fuel industry companies listed on the WSE as part of the WIG Energia and WIG Paliwa index for 2017, 2018.

Selected examples of cyber security disclosures identified by the Author are presented in Tables 1 and 2.

Table 1

Enterprise	Report type	Does the Company present information on BM?	Does the Company present information on cyber security?
1 Enea	CR, MR	yes	yes
2 Tauron	CR, MR, IR	yes	yes
3 Kogeneracja	CR, MR	yes	no
4 Zepak	CR, MR	yes	no
5 Polenergia	CR, MR	no	no
6 PGE	CR, MR, IR	yes	no
7 Energa	CR, MR	Yes	yes
8 ML System	CR, MR	No	no
9 Będzin	CR, MR	No	no
10 Lotos	CR, MR, RI	yes	yes
11 Orlen	IR, CR, MR	yes	no
12 PGNIG	CR, MR	yes	no
13 SKOTAN	CR, MR	No	no

14 Unimot	CR, MR	No	no

Source: Own elaboration

Table 2

Enterprise	***Category of disclosures on cyber risk***	***Content of disclosures on cyber security***
1 Enea	Specification of the cyber risk category: the risk of losing the accessibility of billing systems, the risk of an attack on the IT infrastructure, the risk of losing business continuity of ICT environments and infrastructure, the risk of lack of the Internet connectivity.	In 2019, further improvement of the ICT security system and its adaptation to new legal provisions is envisaged, in particular to the requirements of the Act on the National Cyber Security System. One of the important areas of this improvement is the development of processes to respond to incidents in the field of ICT security, as an extremely important element in ensuring the continuity of services provided to clients.
2 Tauron	Impact: The growing number of cyber threats and infrastructure vulnerable to such attacks	-
3 Energa	Risk of the Group's non-compliance with new legal provisions,	Setting up a Working Group on adapting the Group's activities to legal provisions (including energy prices, cyber security)
4 Lotos	IT systems risk: External or internal interference (cyber attack) in information (IT) and control (CT) systems, and failures as a result of non-sufficient resources and inefficient processes in IT area	Being aware of a new type of threat – related to cyber space – we have launched a programme increasing the level of cyber security in the entire Capital Group. It aims at raising employees' awareness of cyber threats as well as implementing new technological solutions and infrastructure minimising such risks.

Source: own elaboration

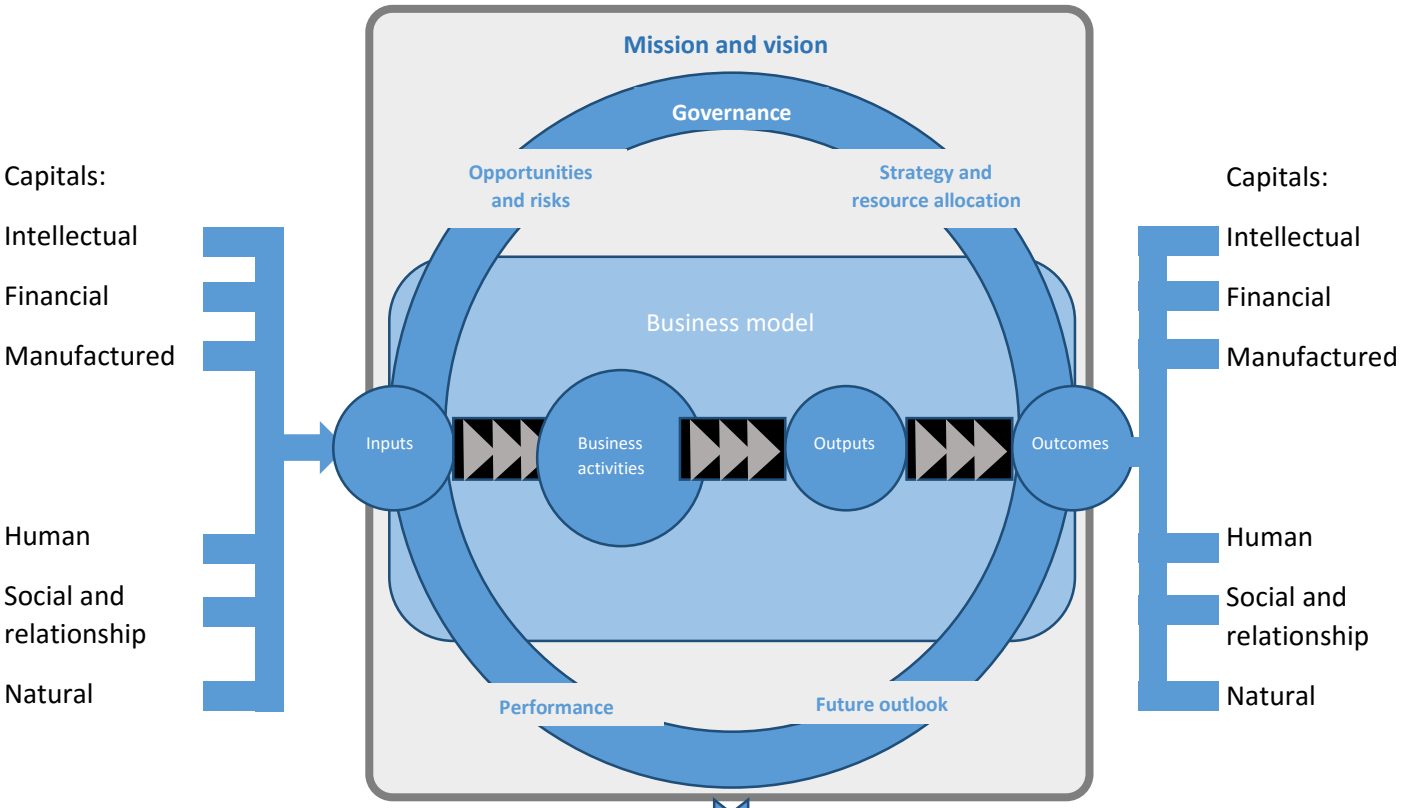
Results and discussion:

The presented studies show that disclosures on the business model are dispersed in various corporate documents, i.e. the consolidated report, management report, integrated reports. The issues related to the business model are most widely recognised in integrated reports. Out of the 13 companies surveyed, 9 publish information on the business model, but only 4 present any information on cyber risk and cyber threats. The Enea, Tauron, Energa companies are aware of the areas that are exposed to cyber risk, which may be related to the attack and loss of business continuity of ICT environments and infrastructure, lack of the Internet connectivity, failure to comply with legal regulations. Lotos recognises the most widespread range of cyber risk, which, apart from an attack on information and control systems, considers the lack of sufficient resources and inefficient processes in the IT area to be significant risk. The information presented on cyber security is of a qualitative nature and includes:

1. Plans to adapt the security system to new legal requirements
2. Development of processes for responding to incidents in the field of IT security
3. Raising employees' awareness of cyber threats
4. Implementation of new technological and infrastructure solutions that minimise risks.

Due to the minimum degree of information presented on cyber security, the author proposes that companies expand the scope of the business model, which will contribute to strengthening existing and building new lasting relationships with stakeholders.

Taking into account the framework of the business model proposed in the *Business Model Background Paper for IR* [IIRC 2013] and the Act on the National Cyber Security System (the Act), the author proposes to build a cyber security management model, whose the basic assumptions and stages are presented in Figure 1.



Mission and vision – entering cyber security into company's mission statement

Security audit – estimating and managing the risk of an incident

Implementation – adoption of appropriate and proportionate technical and organisational measures to the estimated risks

Monitoring – collecting information on cyber security threats and vulnerabilities to information system incidents

Incident Management

Vulnerability management – the use of measures to prevent and limit the impact of incidents on security

Change management – the use of communication means enabling proper and secure communication within the National Cyber Security System

The proposed model of information security management in an enterprise is based on several assumptions:

1. The proposed information security management model applies primarily to entities which, according to the Act, have been classified as essential services operators;[2]
2. The proposed model is also a good solution for all other entities which want to build their individual business model;
3. There is a need to adopt a specific sequence of actions as part of creating an individual cyber security model

According to the presented scheme, *the first stage* proposes to include the cyber security problem in the company's strategy. This is the main goal which enables the implementation of the proposed model. A well-chosen company strategy should define strategic goals aimed at achieving and maintaining a high level of cyber security, in particular: goals and priorities in the field of cyber security, measures to achieve the goals of the strategy, approach to risk assessment.
The second stage involves estimating and managing the risk of an incident,[3] which involves the coordination of cyber security management in relation to the estimated risk. Estimating this risk may be based on a security audit which consists in determining the level of maturity in cyber security reached by the organisation. It involves conducting interviews and analyses in the field of security and business continuity of significant areas of the organisation's audit activity.
The third stage is the implementation of appropriate and proportionate to the estimated risk technical and organisational measures, taking into account the latest state of knowledge, including:

a) maintenance and safe operation of the information system,
b) safety and environmental security, taking into account access control,
c) security and continuity of service delivery, which determines the provision of an essential service,
d) implementation, documentation and maintenance of action plans enabling continuous and uninterrupted provision of an essential service and ensuring confidentiality, integrity, accessibility and authenticity of information,
e) taking the information system used to provide the essential service under a continuous monitoring system;

The next stage is the collection of information on cyber security threats and vulnerability to incidents of the information system used to provide the essential service. At this stage, the question should be answered, where is the weakness that can be exploited by the attacker? To this end, it is necessary to systematically verify the security of the systems, assess the detected weakness and decide on appropriate countermeasures.
The fifth stage is the most important in the author's opinion – incident management, i.e. events that have or may have an adverse effect on cyber security. Incident handling should consist of

[2] Essential service – a service that is crucial for maintaining critical social or economic activities [the Act]
[3] Incident handling – activities enabling detection, recording, analysing, classifying, prioritising, taking corrective actions and limiting the effects of an incident [the Act]

searching for links between incidents, removing the causes of their occurrence and deriving conclusions resulting from incident handling.
The penultimate stage is the application of measures to prevent and limit the impact of incidents on the security of the information system used to provide the essential service, including:
a) applying mechanisms ensuring confidentiality, integrity, accessibility and authenticity of data processed in the information system
b) attention to software update,
c) protection against unauthorised modification in the information system,
d) immediately taking action after noticing vulnerabilities or threats to cyber security;
The last stage is the use of communication means enabling correct and secure communication within the National Cyber Security System.
The specified stages of the cyber security management model should be included in the business activities of the enterprise model. According to the IIRC guidelines, business activities include planning, design, research and development, relationship management that contribute to the long-term success of the enterprise. Supplementing existing business activities with those that relate to cyber security will cover both input elements – financial capital, production capital, natural capital, intellectual capital, human capital as well as social capital and elements of the output – products, services, by-products, waste. This process will surely contribute to improving the quality of report inputs and outputs as well as ensure an appropriate level of security.
Conducting various activities within the management will primarily affect outcomes, among which IIRC includes customer satisfaction, profit/loss, shareholder return, asset consumption, job creation, employee development and engagement, improved standard of living, environment impact, license to operate, contribution to local economy through taxes. A properly developed business model of the company will describe the way in which an enterprise creates, maintains and delivers value to customers, thus encouraging customers to pay for this value, transforming the payments obtained into profit (B.Rymkiewicz, B.Bek-Gaik, 2015).

Conclusions

The fast pace of development and the complexity of IT technologies make weaknesses in the security of IT systems a widespread phenomenon. If we add employees' susceptibility to manipulation, effective information protection becomes an extremely difficult issue. It is no wonder then that cybercrime is now the largest and fastest-growing area of activities of international criminal groups. In order to secure the company against the possibility of threatening the security of its information, the Act of 28 September 2018 on the National Cyber Security System was introduced. As research has shown, companies present limited information on cyber security, which is due to the lack of mandatory reporting of this information.
The author of the paper believes that it is important for all entities subject to the Act to introduce the cyber security management model into the operating business model of the enterprise, because:

1. The business model is treated as a carrier of various types of process innovations (new energy generation technologies, protection against cyber attacks) and as a business architecture it strengthens cyber security.
2. The business model is a response to the requirements of energy policy and legal regulations in the field of the National Cyber Security System.
3. The business model is a business path which is a proposal for potential investors and lenders willing to cooperate with enterprises for whom cyber security has a primary role.

The system of ensuring the protection of accounting IT resources is the responsibility of all enterprises, therefore, in the author's opinion, the model of protecting IT accounting resources against cyber attacks should be included in all business models of business entities.

To this end, the author proposes to build a cyber security model based on the assumptions of the Act on the National Cyber Security System, and then to include its elements in the enterprise's business model, which will surely increase the protection of systems related to accounting and finance services. The cyber security model is a proposal that offers benefits to stakeholders in the form of:

- its practical implementation guidelines that promote security-related decisions based on qualitative and quantitative analysis,
- increasing the transparency of the concept of value creation, both for the customer and for the business owners,
- achieving competitive advantages, among which quality features (e.g. reliability of ICT networks and security of relationships between various information users) play an increasingly important role.

References:

Bass, T. (2000). Intrusion detection systems and multisensor data fusion: Creating cyberspace situational awareness. *Communications of the ACM*, *43*(4), 99-105.

Bek-Gaik, B., & Rymkiewicz, B. (2015). Model biznesu w sprawozdawczości polskich spółek publicznych na przykładzie branży energetycznej. *Research Papers of the Wroclaw University of Economics/Prace Naukowe Uniwersytetu Ekonomicznego we Wroclawiu*, (398).

Bek-Gaik, B., & Rymkiewicz, B. (2016). Model biznesu w raportowaniu zintegrowanym. *Research Papers of the Wroclaw University of Economics/Prace Naukowe Uniwersytetu Ekonomicznego we Wroclawiu*, (442), p.34.

Bek-Gaik, B., & Rymkiewicz, B. (2017). Model biznesu w raportowaniu organizacji-wybrane problemy. *Research Papers of the Wroclaw University of Economics/Prace Naukowe Uniwersytetu Ekonomicznego we Wroclawiu*, (471).

Boulton R., Libert B., Samek S., (2000). Cracking the Value Code. How Successful Business Are Creating Wealth in the New Economy, Harper Collins, USA, http://credu.bookzip.co.kr/Resource/EnglishBook/PDF/AH30013.pdf (11.12.2019).

Brzóska J., (2014). *Innowacje jako czynnik dynamizujący modele biznesowe*, Wydawnictwo Politechniki Śląskiej,

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719-731.

Deirmenjian, J. M. (1999). Stalking in cyberspace. *Journal of the American Academy of Psychiatry and the Law Online*, *27*(3), 407-413.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, *5*(4), 491-497.

Fulmański, P., & Wojczyk, S. (2014). Potencjalne korzyści i zagrożenia związane z chmurą obliczeniową. *Zeszyty Naukowe. Studia Informatica/Uniwersytet Szczeciński*. Gliwice 2014, s. 136-165.

George, G., & Bock, A. J. (2011). The business model in practice and its implications for entrepreneurship research. *Entrepreneurship theory and practice*, *35*(1), 83-111.

Grzelak, M., & Liedel, K. (2012). Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski–zarys problemu. *Bezpieczeństwo Narodowe*, *22*, 125-139.

Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing. *Applied Computing and Informatics*, *13*(1), 57-65.

IIRC, 2013, *The International <IR> Framework*, 2013/12/13-12-08-THE-INTERNATIONAL-IR-FRAMEWORK-2-1.pdf.

Karwowski, M. (2015). Model biznesu jako nowe wyzwanie sprawozdawczości zewnętrznej. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, (388), 256-257.

Knapp K.J., Morris R.F, Marshall T.E., Byrd T.A. (2009), *Information security policy: An organizational-level process model*, "Computer & Security", 28 (7), p. 493.

Kowalewski, J., & Kowalewski, M. (2014). Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa. *Telekomunikacja i Techniki Informacyjne*, (1-2), 24-32.

Lai A., Melloni G., Stacchezzini R., (2013), Disclosing Business Model in the „Integrated Report": Evidence Froim European Early Adopters; AIDEA Biscentenary Conference, Leece, September 19-21, 2013, http://www.aidea2013.it/docs/400_aidea2013_accounting.pdf

Lambert S., 2008, A conceptual framework for business model Research, 21 st Bled eConference eCollaboration: Overcoming Boundaries through Multi – Channel Interaction, June 15-18, Bled, Slovenia.

Osterwalder A., Pigneur Y., 2012, *Tworzenie modeli biznesowych. Podręcznik wizjonera*, Wydawnictwo Helion, Gliwice.

Rabai, L. B. A., Jouini, M., Aissa, A. B., & Mili, A. (2013). A cybersecurity model in cloud computing environments. *Journal of King Saud University-Computer and Information Sciences*, *25*(1), 63-75.

Shayan J., Azarnik A., Chuprat S., Karamizadeh S., Alizadeh M. (2013), Identifying Benefits and Risks Associated with Utilizing Cloud Computing, „The International Journal of Soft Computing and Software Engineering" 2013, nr 1, s. 416–421.

Smith K.T, Smith L.M., Smith J.L. (2011), *Case Studies of Cybercrime and The Impact on Marketing Activity and Shareholder Value*, „Academy of Marketing studies Journal", 15 (2), p. 76.

Suchorzewska, A. (2010). *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*. Wolters Kluwer.

Szczepankiewicz E., Dudek M. (2009), Rozwój technologii informatycznych a zagrożenia i zarządzanie bezpieczeństwem informacji w przedsiębiorstwach, [w:] M. Grzybowski, J. Tomaszewski (red.), Logi-styka. Komunikacja, Bezpieczeństwo. Wybrane problemy, Wydawnictwo Wyższej Szkoły Administracji i Biznesu im. E. Kwiatkowskiego w Gdyni, Gdynia, s. 263–274.

Szczepankiewicz, E. I. (2018). Zarządzanie bezpieczeństwem zasobów informatycznych rachunkowości w polskich jednostkach–wyniki badań. *Zeszyty Teoretyczne Rachunkowości*, (97), 115-138.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509–533.

Wasilewski, J. (2013). Zarys definicyjny cyberprzestrzeni. *Przegląd Bezpieczeństwa Wewnętrznego*, *5*(9), 225-234.

Wójcik J.W. (1999), *Przestępstwa komputerowe, Część 1 – Fenomen cywilizacji*, CIM, Warszawa.