Safety Science 135 (2021) 105143

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

Defining cyber risk

Grzegorz Strupczewski

Department of Risk Management and Insurance, The Cracow University of Economics, Poland

ARTICLE INFO

JEL:
D81
G00
K24

Keywords:
Cyber risk
Definition
Meta model of cyber risk
Cybersecurity
Cyber threats

ABSTRACT

Rapid digitization of the economy and social relations is the main reason why the issues of cyber risk, cyber threats and cybersecurity are continually gaining importance. Despite the increase in the number of research papers in these areas, scholarly articles defining cyber risk are relatively scarce. Moreover, the uniform broadly accepted definition of cyber risk has not been adopted yet, probably due to the interdisciplinary nature of this concept and the dynamics of its change. The paper contributes to the literature on the cyber risk, cybersecurity and cyber risk management. The author presents a comparative content analysis of existing definitions of cyber risk. Based on identification of three key characteristics of the cyber risk concept (source of cyber risk, cyber risk object, impact of cyber risk) in each definition, the analysed definitions are categorised as one-dimensional, two-dimensional or comprehensive definition. Among the collected 20 definitions of cyber risk, there is only one that can be called comprehensive. The remaining definitions address only selected aspects of this notion. The author proposes a new, comprehensive and universal definition of cyber risk. As an extension to the proposed approach, the ontological meta model of the cyber risk concept is developed. It supports deeper description of the cyber risk concept by depicting functional interdependencies with other terms and factors that constitute the cyber risk framework.

1. Introduction

In the last decade the global economy has been transforming from an economy based on traditional capital goods (land, capital, labour) into a digital economy in which information and a business model based on electronic data processing are the most important. Development of advanced technologies, cloud solutions, 5G communication, the Internet of Things, autonomous means of transport and artificial intelligence as well as the use of robotics in automated production processes, the acquisition of huge amounts of data (big data) thanks to ubiquitous Internet communication and inherent mobile devices - contribute to expansion of the digital economy. Digitisation of the economy and social relations do not account for the single source of huge development opportunities and innovations but also a source of serious and completely new threats. Digital information is exposed to a loss of availability, integrity and confidentiality as a result of cyber incidents, both accidental and deliberate. The continuous increase in the IT security expenditure does not translate into more effective reduction of cyber threats. A human being is still the weakest link. Carelessness, haste, misinformation, susceptibility to social engineering trickery are human attitudes that ensure a high rate of success of phishing campaigns. The above mentioned circumstances create a new research area in which cyber risk is the focal point.

The issue of cyber risk is continually gaining importance. It is evidenced by the increase in the number of scientific papers devoted to this topic. The concept of cyber risk is used in computer science, engineering, business management, economics and social sciences. According to Scopus, the number of scientific papers containing the keyword 'cyber risk' was: 4 in 2013, 5 in 2015, 21 in 2017, 41 in 2018 and 31 in 2019. However, scholarly articles defining cyber risk has not been easy to find. Most of them refer to a couple of established definitions instead of developing their own original approach. Despite the scarcity of theory-based definitions, the uniform broadly accepted definition of cyber risk has not been adopted yet. It might be caused by numerous reasons and one of them is complexity. Cyber risk is an interdisciplinary issue that has appeared in scientific discourse fairly recently as far as diversity of cyber risk and extremely fast rate of change in cyber threats and cybersecurity are concerned. The notion of cyber risk combines two aspects: technical and economical. Technically, it is characterised by high design complexity, (re)programmable behaviour of networked components, and a global dynamic threat surface. In terms of the economical aspect, incomplete information, externalities, and correlation caused by common risk factors are the main features of cyber risk (Böhme et al., 2018, p. 181). Some attempts to develop a coherent

E-mail address: Grzegorz.Strupczewski@uek.krakow.pl.

https://doi.org/10.1016/j.ssci.2020.105143
Received 6 February 2020; Received in revised form 27 October 2020; Accepted 20 December 2020

definition of cyber risk have been made by both authors of scientific papers and representatives of practice.

Underdevelopment of the methodologically sound, comprehensive definition of cyber risk has encouraged the author of this paper to redefine the concept of cyber risk in order to increase the understanding of this fundamental term.

This paper analyses how cyber risk is defined within the existing body of literature. To such purpose, the study is centered on a systematic and comprehensive review of literature on cybersecurity in order to select peer-reviewed articles (supplemented by some relevant industry reports) related to the research question of determining how cyber risk is defined. A keyword search on the term 'cyber risk' was performed in EBSCOhost and Science Direct, and finalized on December 2018. Twenty definitions of cyber risk have been identified but there is only one that may be called comprehensive. Then the author proposes his own comprehensive definition of cyber risk. The proposed definition has been cross-checked by means of the thorough content analysis of alternative definitions of cyber risk that had been found in both academic literature and official publications of governmental and non-governmental organisations. The methodology used in this paper enables the concept of cyber risk to be operationalised by breaking it down into basic elements that constitute a particular definition (called 'key components'). This approach has a great cognitive value and contributes to the current scientific achievements in the field of cyber risk description. To address the research questions, beyond understanding how the articles define the cyber risk construct, there is an emphasis on understanding complex relations between cyber risk and other terms within the cybersecurity terminology. They have been depicted by the proposed ontological meta model of the cyber risk concept.

Regarding the main research goal of this paper, namely defining cyber risk, it is preliminary to study the relation of cyber risk to other closely-related terms – security and safety. The distinction between them is based on different intentions of an acting agent or the location of a source of threat. As Aven (2014, p. 17) explains, safety covers accidental events (e.g. server breakdown) whereas security relates to intentional situations (e.g. cyber attack attempted by a hacker). According to Pettersen and Bjørnskau (2015), safety deals with internal threats and security's primary target is external (p. 169). Undoubtedly, safety is linked to risk. Safety can be considered the antonym of risk, which means that situation of low and acceptable risk is recognized as safe (Aven, 2014, p. 16). Better understanding of risk, the cornerstone of the risk management process, is one of the goals of safety science (Hopkins, 2014, p. 7).

Cyber risk is particularly important issue in the context of work safety. There is a lot of research on cybersecurity and information security behaviour of employees' in the workplace. Among others, they have focused on motivations to comply with cybersecurity policies (Alalwan et al., 2017; Herath and Rao, 2009; Khansa and Liginlal, 2012; Soomro et al., 2016), or on how employees view cybersecurity threats and develop coping responses (Vance et al., 2012). Ability of fighting cybercrime in the workplace is another field of research where cyber risk and work safety meet together (Ahmad et al., 2015; Moon et al., 2018; Ng et al., 2009). In these and many other studies, cyber risk has not been defined although it's the central point of interest of the papers. In this context it is worth noting that employees' capabilities to carry out cybersecurity coping actions require not only experience and training, but also strong understanding of fundamental cybersecurity concepts, such as cyber risk (Ng and Xu, 2007).

The literature points out numerous cyber risks to the workplace safety. Remote working and access to confidential company's data from personal laptops and even smartphones, can mean that one careless employee is able to compromise cybersecurity of the entire organization (Allen et al., 2019). As technology is a significant enabler for workplace fraud (Pandit, 2018, p. 40), it is predicted that the frequency of technology-related fraud will probably rise if younger, tech-savvy employees rise through the ranks (KPMG, 2016, p. 21). Cyber-bullying[1] impacts negatively employee's efficiency, well-being and mental health (Beirne and Hunter, 2013). Thus, organizations need to establish codes of cyber conduct, build employees' resilience and raise their awareness about the caution in online interactions (Beirne and Hunter, 2013). Workplace safety may be also undermined by cyberslacking which means "overuse of the Internet in the workplace for purposes other than work" (Whitty and Carr, 2006, p. 238). Cyberslacking includes accessing social network sites, news sites, pornographic websites, shopping online, managing personal emails, etc. (Hernández et al., 2016).

The above arguments highlight the need for development of academic, comprehensive and broadly-accepted definition of cyber risk. The importance of this task is significant in many disciplines, in particular for workplace safety science (Komljenovic et al., 2016; Torabi et al., 2016). Human is the weakest link in the information security chain (Dodel and Mesch, 2019, p. 75). Even the best-developed security measures might be bypassed by poor user behaviour. Individual users, including company staff, have limited cyber-safety skills and knowledge about protection against cyber threats (Arachchilage and Love, 2014).

The remainder is divided into five sections. First, the methodology applied by the author to complete the research goal is briefly explained. Section 3 discusses the categorisation of existing definitions of cyber risk. The analysis of previously published cyber risk definitions provides the basis for the development of a new definition of this term. The new definition suggested by the author is presented in Section 4. The ontological meta model of the cyber risk concept has been developed in the next section. Finally, Section 6 concludes.

2. Methodology

Based on the author's own methodology, the collected definitions have been analysed and categorised. The approach used in this paper is based on the sequence of steps enabling to achieve the research goal.

The initiating step of the study was the collection of existing cyber risk definitions based on systematic literature review. The review of literature on defining cyber risk has been conducted using a standardized search and identification process. First, the term "cyber risk" was searched in the journal databases EBSCOhost (Business Source Ultimate, Academic Search Ultimate, EconLit) and Science Direct. The former returned 119 hits, and the latter 176. In addition, the same term was searched in the Social Science Research Network (SSRN) and via Google Scholar. Moreover, a review of citations in the retrieved papers was carried out in order to capture additional relevant materials (not necessarily scientific). Based upon this selection process, a database of more than 200 papers was created. The database contains papers published in English between January 2000 and December 2018. In order to ensure the consistency of the approach, papers from disciplines such as economics, risk management, insurance, IT, law, finance were only taken into account. Secondly, all papers from the database were scanned for definitions of cyber risk. As most of the authors do not propose their own definitions of cyber risk but refer to existing ones, a short list of 20 publications has been created where the original definitions of the term 'cyber risk' can be found (see Table 1). The list contains not only academic papers, but also relevant industry reports and white papers of professional organizations. As Bromiley et al. (2015, p. 273) pointed out, 'practitioners need to understand how different individuals and groups within organization define risk (…)'. However, working out definitions

[1] Cyber-bullying means inappropriate, repeated and thus hurtful social exchange behaviors such as unwanted messages, spreading rumors, harassment (Gardner et al., 2016).

Table 1
Definitions of cyber risk.

Source of definition	Definition
Biener et al. (2015), p. 134.	Cyber risk may be defined as a function of 3 parameters: (i) Impact expresses the level of damage that a given risk may cause; (ii) Threat expresses whether or not a given risk is probable; (iii) Vulnerability expresses whether or not existing information security measures are effective.
BIS (2016), p. 24.	The combination of the probability of an event occurring within the realm of an organisation's information assets, computer and communication resources and the consequences of that event for an organisation.
Böhme et al. (2018), p. 164	Cyber risk is characterised by: digital cause of damage to digital assets, digital cause of damage to physical assets, or physical cause of damage to digital assets.
Böhme and Kataria (2006)	Cyber risk is defined as a breach of integrity and failure of information & communication technology systems (ICT).
Brewer (2000)	Cyber risk is a vulnerability (i.e. weakness) that may be exploited by threats to gain access to certain assets. It is measured by multiplying threat, vulnerability and asset value.
Cebula and Young (2010), p. 13.	Cyber risk is defined as operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems.
CRO Forum (2014), p. 5.	Cyber risk covers any risks emanating from the use of electronic data and its transmission, including: (i) technology tools such as the Internet and telecommunication networks; (ii) physical damage that may be caused by cyber attacks; (iii) fraud committed by misuse of data; (iv) any liability arising from data use, storage and transfer, and (v) the availability, integrity and confidentiality of electronic information – be it related to individuals, companies or governments.
Eling and Schnell (2016), p. 12.	Cyber risk encompasses any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (OT) eventually leads to business disruption, (critical) infrastructure breakdown, and physical damage to humans and properties.Cyber risk is either caused by natural disasters or is man-made where the latter may emerge from human failure, cyber criminality (e.g. extortion, fraud), cyberwar or cyber terrorism. It is characterised by interdependencies, potential extreme events, high uncertainty with respect to data and modelling approach, and the risk of change.
Gordon et al. (2003), p. 81	Cyber risk is an Internet-related risk.
IRM (2014), p. 10.	Cyber risk means any risk of financial loss, disruption or damage to the reputation of an organisation as arising from some sort of failure of its information technology systems. Such a risk could materialise in the following ways: (i) Deliberate and unauthorised breach of security to gain access to information systems for the purposes of espionage, extortion or embarrassment; (ii) Unintentional or accidental breach of security, which nevertheless may still constitute an exposure that needs to be addressed; (iii) Operational IT risks due to poor system integrity or other factors.
ISACA (2009), p. 7.	IT risk is business risk - specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It consists of IT-related events that could potentially impact the business.
ISO/IEC (2014), p. 8	Information security risk is associated with the potential threats that will cause vulnerabilities of an information asset or group of information assets to be exploited and thereby cause harm to an organisation.
Mukhopadhyay et al. (2013), p. 11.	Cyber risk is defined as the risk involved with a malicious electronic event that causes disruption of business and monetary loss.
NAIC (2018)	Cyber risk covers all risks related to online activity, such as storing personal data in the Internet or conducting online transactions that may result in damage to reputation, financial loss, disruption of life or business.
Nieuwesteeg et al. (2015), p. 3.	Cyber risk is the potential physical harm (to persons or property) and loss of profitsdue to malfunction of digital systems or corrupted data.
NIST (2002), p. 61.	IT-related risks arise from legal liability or mission loss due to: (i) Unauthorised (malicious or accidental) disclosure, modification, or destruction of information; (ii) Unintentional errors and omissions; (iii) IT disruptions due to natural or man-made disasters; (iv) Failure to exercise due care and diligence in the implementation and operation of the IT system.
NIST (2006), p. 8.	The level of impact on organisational operations (including mission, functions, image or reputation), organisational assets or individuals resulting from the operation of an information system, given the potential impact of a threat and its likelihood.
Öğüt et al. (2011), p. 497.	The authors use information security as a synonym for cyber risk. It is defined as the risk of incurring in financial, reputational and market share losses in relation to the use of information and communication technology (ICT).
Refsdal et al. (2015), p. 33.	Cyber risk is a risk that is caused by a cyber-threat occurring in cyberspace.
World Economic Forum (2012), p. 24.	Cyber risk is a combination of the probability of an event in the field of network information systems and the effects of this event on assets and reputation of an organisation.

of RM-related concepts is not purely an academic task. Practitioners and academics must collaborate on the development of the RM body of knowledge, in order to extend the depth and breadth of the theoretical matter, while remaining relevant to organizations and their managers (Bromiley et al., 2015).

Next, the identified definitions of cyber risk were reviewed for content and categorized. The approach derived from content analysis was applied.[2] It involved systematic reading of texts which are assigned labels (codes) to indicate the presence of interesting, meaningful pieces of content. By systematically labeling the content of a set of texts, it becomes possible to analyze meanings of content within texts (Krippendorff, 2004). Based on preliminary review of the identified cyber risk definitions in search for their key components, the following labels (codes) have been indicated: "sources of cyber risk", "cyber risk objects", and "impact of cyber risk". Label "Sources of cyber risk" refers to description of cyber threats that may result in loss. The next label "cyber risk objects" groups cyber risk definitions that include references to objects on which the cyber risk may materialise. The third label focuses on specification of possible negative consequences of cyber risk. Contrary to general rules of content analysis (GAO, 1996, p. 20), the categories represented by codes aren't mutually exclusive.[3] Indeed, they represent the most relevant features of the cyber risk concept. This means that a definition may contain one, two or three units of coding (labels) combined. Then the wording of each definition was broken down into parts that could be assigned to one of the three labels. The

[2] Content analysis is a research technique for making inferences by systematically and objectively identifying specified characteristics within text (Krippendorff, 2004, p. 25).

[3] Mutually exclusive categories exist when no unit falls between two data points, and each unit is represented by only one data point (Stemler, 2000, p. 2).

results of the content analysis are shown in Table 2.

After the existence of key components of the cyber risk concept in each definition was identified (source of cyber risk, cyber risk object, impact of cyber risk), the definitions were divided into three homogeneous groups representing their information content. A definition that contains one key component in its wording is called a one-dimensional definition and assigned to the first group. Similarly, if a definition contains two of the three named key components, it is called two-dimensional definition and allocated in the second group. Finally, the definition referring to all three key components of the cyber risk concept will fall into the third group dedicated to so called comprehensive definitions.

Table 2 shows that among the collected 20 definitions of cyber risk, there is only one that may be called comprehensive. The count of one-dimensional definitions is nine and the count of two-dimensional expressions equals 10. Most definitions (14) address a possible impact of cyber risk, and twelve of them (12) focus on sources of cyber threats. Addressing objects of risk in the cyber risk definitions appears to be a relatively rare case (7). The proposed typology of cyber risk definitions according to the criterion of information content (i.e. the number of dimensions) is shown in Fig. 1. It will be discussed further in the following section.

The presented approach proved to be useful when studying the informational content of definitions and searching for ways to divide them into homogeneous groups.

In the next part of the study the ontological meta model of the cyber risk concept is developed. It supplements the proposed cyber risk definition which refers to generals. The objective of the meta model is to supply deeper description of the concept in question, to picture functional interdependencies with other terms and factors that constitute the cyber risk framework and determine its nature.

Table 2
Key components in the cyber risk definitions.

Source of Definition	Name of Key Component			Number of Key Components per Definition
	Sources of Cyber Risk	Risk Objects	Impact of Cyber Risk	
Biener et al. (2015), p. 134		■		1
BIS (2016), p. 24		■		1
Böhme and Kataria (2006), p. 3			■	1
Böhme et al. (2018), p. 164	■		■	2
Brewer (2000)	■			1
Cebula and Young (2010), p. 13		■	■	2
CRO Forum (2014), p. 5	■		■	2
Eling and Schnell (2016), p. 12	■	■	■	3
Gordon et al. (2003), p. 81	■			1
IRM (2014), p. 10	■		■	2
ISACA (2009), p. 7	■		■	2
ISO/IEC (2014), p. 8		■		1
Mukhopadhyay et al. (2013), p. 11	■		■	2
NAIC (2018)		■	■	2
Nieuwesteeg et al. (2015), p. 3			■	1
NIST (2002), p. 61	■		■	2
NIST (2006), p. 8			■	1
Öğüt et al. (2011), p. 497	■		■	2
Refsdal et al. (2015), p. 33	■			1
World Economic Forum (2012), p. 24		■	■	2

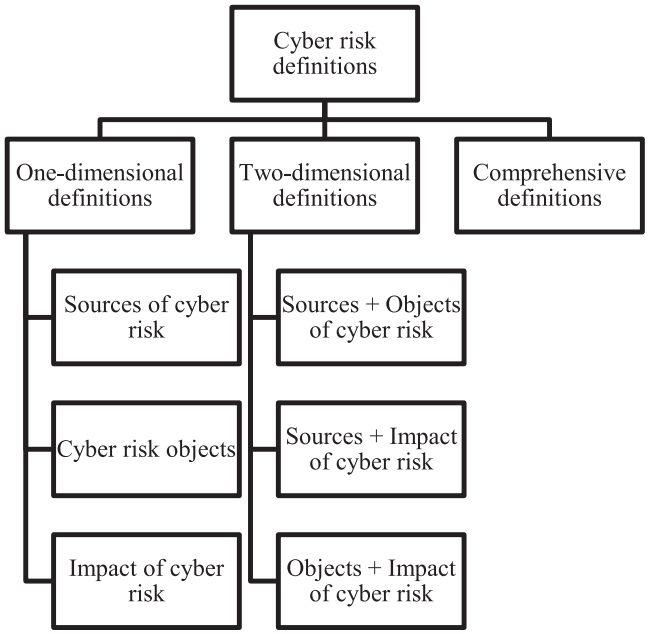

Fig. 1. Typology of cyber risk definitions according to the information content criterion.

3. Discussion

3.1. One-dimensional definitions of cyber risk

3.1.1. Sources of cyber risk

Initially, cyber risk was associated with threats arising from the use of the Internet (Gordon et al., 2003, p. 81). Later, along with the spread of the idea of cyberspace, cyber risk was referred to types of risks that originated from threats occurring in cyberspace (Refsdal et al., 2015, p. 33). Brewer represents a different way of thinking about this concept. He matches the term 'cyber risk' with some weaknesses of digital assets that could be exploited by threats originated in the cyberspace (Brewer, 2000). Moreover, he points out that there are three types of safeguards against cyber threats: threat-reducing safeguards (e.g. firewalls, locked doors, safe boxes and personnel vetting), vulnerability-reducing safeguards (e.g. procedures, hot-fixes and service packs) and asset value-reducing safeguards (e.g. back-ups and encryption).

3.1.2. Cyber risk objects

Definitions in this section differ in terms of the catalogue of 'places' where cyber risk occurs. The Bank for International Settlements (BIS) mentions three groups of resources (information assets, computer and telecommunication resources) as the potential targets of cyber attacks (BIS, 2016, p. 24). Biener et al. (2015) speak in a similar vein. In their opinion the term 'cyber risk' refers to a variety of sources of risk affecting the company's information and technology assets. In contrast, the international standard for information security management ISO/IEC 27000 defines cyber risk very generally (risk in the broad sense) as the impact of uncertainty on the organisation's goals, which may cause negative or positive deviations of actual effects from intended results (ISO/IEC, 2014, p. 8). Uncertainty is a condition resulting from unconsciousness, misunderstanding or scarcity of information related to an event, its consequences or the probability of occurrence. Risk is the product of the probability of a random event and its possible effects (not necessarily in a purely financial dimension). In addition to this definition, the Standard presents the concept of information security risk as a risk in the strict sense. Information security risk means that the threat

may materialise in the forms of an attacker making use of a vulnerability of an information resource, which will lead to the organisation's damage (ISO/IEC, 2014, p. 8). It bears noting that in the terminology of the ISO/IEC 27000, a risk in the broad sense is a speculative risk, while the risk of information security (i.e. risk in the narrow sense) is classified as pure risk.

3.1.3. Impact of cyber risk

Researchers see more or less extensive effects of cyber risk. Böhme and Kataria (2006, p. 4) in their definition only mention a breach of integrity or damage to ICT systems as potential effects of this risk. In a broader sense, Nieuwesteeg et al. (2015, p. 3) understand cyber risk as potential physical harm or loss of profit due to malfunction of digital systems or unlawfully disclosed data. However, the most comprehensive way of presenting possible extent of losses may be found in the definition of cyber risk developed by the National Institute of Standards and Technology (NIST), affiliated to the US Department of Commerce. In their Cybersecurity Framework NIST, cyber risk is defined as a potential negative impact on organisation's operation (including its mission, functions, image and reputation), its resources and employees, resulting from the use of information system, taking into account the potential effects of cyber threats and their probability of occurrence (NIST, 2006, p. 8).

3.2. Two-dimensional definitions of cyber risk

3.2.1. Sources of cyber risk + cyber risk objects

No definition found matching this combination of dimensions.

3.2.2. Sources of cyber risk + impact of cyber risk

Many of the analysed definitions have been classified in this category. To start with, it is worth quoting the wording of cyber risk developed by the Institute of Risk Management (IRM) where the essence of cyber risk is captured in a concise and legible way. Namely, it means any risk of financial loss, disruption of activity or damage to the reputation of the organisation caused by the failure of its IT systems (IRM, 2014).

Böhme et al., starting from the classic approach to risk as a product of probability and potential effects, define cyber risk by providing its attributes, i.e. those characteristics that allow distinguishing cyber risk from other types of risk. The first attribute is the source of the threat, which may be physical or digital. Natural phenomena may serve as an example of a physical source, while a hacker attack or a virus may be considered a digital source. The second risk attribute is the object of risk materialisation which may also be material or digital (e.g. computer data, software, computer network). They define risk as 'cyber' when:

> a digital cause has caused damage to digital goods,
> a digital cause has caused damage to physical goods,
> a physical cause has caused damage to digital goods (Böhme et al., 2018, p. 164).

Mukhopadhyay et al. (2013, p. 11) argue that this is a risk associated with a malicious digital event that causes disruptions in business processes and monetary losses. Cyber risk may also have an impact on opportunity costs, negatively affecting the brand value and market capitalisation of an organisation. Similar definition may be found in Öğüt et al. (2011, p. 497). Additionally, they underline the correlated nature of cyber risk.

According to the guidelines of the NIST 800-30 framework, cyber risk may result in legal liability or failure to achieve the organisation's goals as a consequence of:

> unauthorised (malicious or accidental) disclosure, modification or destruction of information,
> unintentional error or omission,
> IT system disruption caused by a natural or man-made disaster,
> lack of due diligence in the implementation and operation of an IT system (NIST, 2002, p. 61).

In 2014 CRO Forum released its own cyber risk definition. Cyber risk covers all risks arising from the use of electronic data and their electronic transmission on the network. It also includes physical damage that may be caused by cyber attacks, fraud committed by misuse of data, all liability arising from data processing (including ensuring their availability, integrity and confidentiality) - regarding individuals, organisations and public entities (CRO Forum, 2014, p. 5).

3.2.3. Cyber risk objects + impact of cyber risk

This category includes three definitions of great importance for the theory and practice of cyber risk management. Their weight is mainly due to the impact on academic studies and the significance of the persons or organisations that have authored the formulae in question. The paper by Cebula and Young (2010) has become the canon of defining cyber risk. According to these authors, cyber risk is defined as operational risk in relation to information and technology assets that affects confidentiality, availability or integrity of information or information systems (Cebula and Young, 2010, p. 13).

Another definition was presented in the report commissioned by the World Economic Forum in 2012. That annual, prestigious study contains the analysis of the most important threats to the global economy. Cyber risk has been characterised as 'a combination of the probability of an event in the field of network information systems and the effects of this event on assets and reputation of an organisation' (World Economic Forum, 2012, p. 24). It seems that this definition should be supplemented with the issue of threats to information security, in particular to personal data.

The definition formulated by the NAIC is free from the above mentioned defect. It explains that: 'Cyber risk covers all risks related to online activity, such as storing personal data on the Internet or conducting online transactions that may result in damage to reputation, financial loss, disruption of life or business' (NAIC, 2018).

3.3. Comprehensive definition of cyber risk

One of the comprehensive definitions has been proposed by Eling and Schnell (2016). Cyber risk results from the use of information and communication technology (ICT), which threatens confidentiality, availability or integrity of digital data and services, and leads to business interruption, infrastructure failure or other material damage. Those authors also claim that the sources of cyber risk may be natural disasters or human actions, such as accidental errors, cybercrime, cyber war or cyber terrorism. They also mention that cyber risk is characterised by interdependence of incidents, possible catastrophic impact, and high uncertainty in relation to data and methods of cyber risk modeling (Eling and Schnell, 2016, p. 12). That definition most accurately reflects the current state of knowledge on cyber risk. It underlines its most significant characteristics. Nevertheless, it is a pity that its authors have not decided to use more general expressions with regard to types of cyber events. In the face of dynamic changes in the nature, forms and types of cyber risk that we undoubtedly deal with, the content of the definition might become outdated in the near future. Moreover, possible indirect loss, such as loss of reputation, loss of customer trust or goodwill, have been omitted.

Finally it is worth quoting the view of Böhme and Schwartz (2010). They indicate two aspects that distinguish cyber risk from conventional risk. First of all, it is the interdependence of elements of ICT systems that generates increased risk of accumulation. The second aspect relates to cyber risk exposure of many automated devices that are used in business. An added value for an organisation is created, provided that the automated devices work properly. However, in the case of a breakdown, they may become a source of serious losses. Moreover, such a breakdown may

be caused by accidental failure and deliberate action of an enemy entity. The aforementioned cyber risk features must be admitted to be extremely important from the perspective of insurance industry but have not been explicitly articulated in the definitions presented above.

The concept of 'IT risk', which is more common in technical sciences, may be found to be closely related to the term 'cyber risk'. According to the 'Risk IT', the fundamental framework of digital risk management developed by the ISACA (Information Systems Audit and Control Association), the 'IT risk' (i.e. information technology risk) is a business risk associated particularly with the use, ownership, operation, involvement, impact and adoption of information technology (IT) in an enterprise. It includes events that are uncertain as to the probability of occurrence and their size, that may adversely affect a company's operations and its ability to achieve strategic goals (ISACA, 2009, p. 7). The ISACA's approach to defining the 'IT risk' is special. This risk is not treated as a separate type of risk or as a subtype of operational risk. The 'IT risk' may always be pointed out if any activities, tasks or functions are implemented in the cyberspace, regardless of their assignment to the classical risk categories such as strategic, market, credit, operational or legal risk (Fig. 2). Consequently, a constitutive feature of the 'IT risk' is the way a firm's operations are performed, and not their formal description defining a place in a given risk category. In fact, it is an extremely broad understanding of cyber risk ('IT risk'), flexible and ready for new challenges of the digital economy.

Taking into consideration a possible impact on strategic goals and objectives of an enterprise, the ISACA categorises 'IT risk' in three groups (ISACA, 2009, p. 7):

IT benefit/value enablement (e.g. technology enabler for new business initiatives or efficient operations),
IT programme and project delivery (e.g. project quality, project relevance, project overrun),
IT operations and service delivery (e.g. IT service interruptions, security problems, compliance issues).

The concept of 'IT risk' developed by the ISACA focuses on possible sources of risk as well as on its impact, so it may be labelled as a two-dimensional definition (sources & impact of cyber risk). The expected impact is not only negative, which is the typical feature of operational risk, but also positive.

4. Comprehensive cyber risk definition proposal

In the face of the huge variety of definitions of cyber risk, there is a clear need to adopt a uniform, broadly accepted wording that would simplify future research in the field of cybersecurity. Another advantage of the universal definition of cyber risk is the unification of 'cyber'-terminology that is really needed in many practical applications such as the cyber insurance market or the cybersecurity policymaking. Based on the comparative analysis and the typology of cyber risk definitions presented so far, the following comprehensive definition of cyber risk is proposed:

Cyber risk is an operational risk associated with performance of activities in the cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption or reputational harm. The term 'cyber risk' also includes physical threats to the ICT resources within organisation.

The proposed definition highlights the most important features of cyber risk. They are as follows:

cyber risk is located in the domain of operational risks,
the cyberspace is the most relevant source of cyber risk, although sometimes the reason for cyber risk materialisation may be physical (e.g. fire of server room, accidental damage to a network cable),
objects that are exposed to losses caused by cyber risk include: information assets (e.g. data, software, computer operating systems), ICT resources (e.g. hardware, telecommunications systems, video monitoring), technological assets (e.g. electronically controlled devices, assembling lines, industrial computer systems, transportation systems, energy supply),
cyber risk may occur both in a single, separate computer device or local computer networks (e.g. corporate LAN) and in interconnected, interdependent wide IT systems, including the Internet,
the potential impact of cyber risk may be threefold:
(i) property damage, meaning not only material loss but also the obligation to compensate damage caused to third parties in the case of data breach (civil liability), and profit lost due to malfunction of a computer system;
(ii) disruption of an organisation's operations (without direct financial loss);
(iii) damage to reputation, that may additionally be associated with a loss of customer confidence and further negative business consequences.
property damage may concern tangible assets (e.g. cash, real property, material assets) and intangible assets (goodwill, intellectual property, patents).

Placing cyber risk among operational risks, initiated by Cebula and Young (2010), has gained widespread acceptance in research and practice (Pengelly, 2016). There are numerous arguments accounting for this approach (Eling and Wirfs, 2015):

facilitating the placement of cyber risk in the existing business risk typology,[4]
possibility to use existing operational risk classifications for the purpose of studies on cyber risk,[5]
relatively good availability of operational risk databases[6] as compared to scarcity of cyber risk databases,
potential application of proven operational risk modeling methods for the purpose of cyber risk[7].

To summarise, cyber risk is located in the cyberspace but impacts not only the virtual world but also the physical one. This term refers to a range of events that may cause damage or otherwise undesirably affect digital data and ITC resources of enterprises, individuals or public institutions.

The new definition suggested in this paper represents a needed improvement over existing definitions of cyber risk. Only one previously published definition addressed all the three key characteristics of cyber risk (Eling and Schnell, 2016). But unfortunately it is a broader description of the term rather than a compact definition. Except for this one, none of the studied definitions addressed more than two of the identified key characteristics of cyber risk. The diversity of cyber risk sources was earlier highlighted by 11 (55%) definitions (Brewer, 2000; NIST, 2002; Gordon et al., 2003; ISACA, 2009; Öğüt et al., 2011; Mukhopadhyay et al., 2013; CRO Forum, 2014; IRM, 2014; Refsdal

[4] The main risk categories indicated by banking supervision are: market, credit, liquidity, legal and operational risk (BIS, 2006). Insurance supervision uses four risk categories: market risk, insurance risk, credit risk, operational risk (CEIOPS, 2009).

[5] Typology of operational risks adopted in Basel II/III for banking industry and Solvency 2 for the insurance sector.

[6] The leading providers of operational risk databases are: SAS Global OpRisk Database, ORX, ORIC.

[7] For instance, Extreme Value Theory (Thlon, 2012).

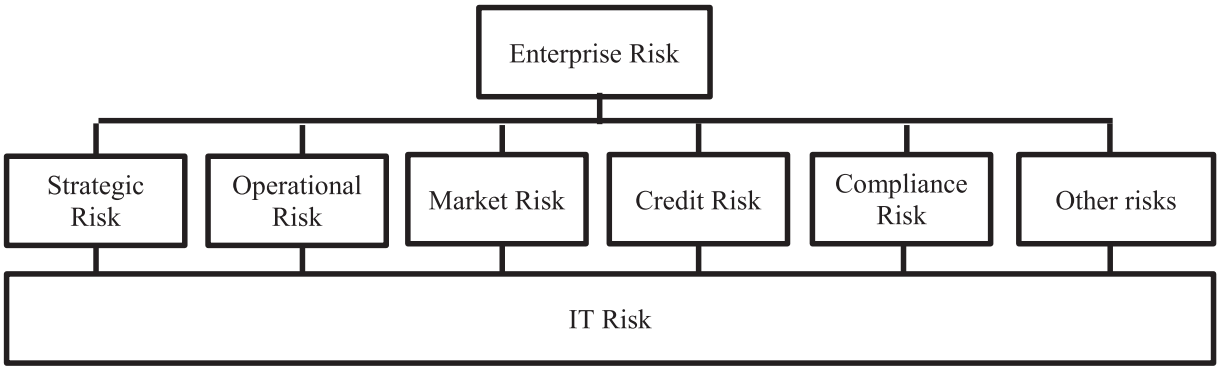

Fig. 2. 'IT risk' in the risk hierarchy.
Source: ISACA (2009, p. 11).

et al., 2015; Eling and Schnell, 2016; Böhme et al., 2018). Identification of objects vulnerable to cyber threats was most explicitly addressed by Cebula and Young (2010), World Economic Forum (2012), ISO/IEC (2014), Biener et al. (2015), BIS (2016), Eling and Schnell (2016), NAIC (2018). Both of these cyber risk features are clearly emphasized in the new suggested definition. As an earlier analysis demonstrated, various kinds of cyber risk impact are addressed in the majority (70%) of the existing definitions. It is also explicitly highlighted in the proposed definition. This focus was captured by Böhme and Kataria (2006), Cebula and Young (2010), Öğüt et al. (2011), Mukhopadhyay et al. (2013), Nieuwesteeg et al. (2015), Eling and Schnell (2016), Böhme et al. (2018). Organizations such as NIST (2002, 2006), ISACA (2009), World Economic Forum (2012), CRO Forum (2014), IRM (2014), NAIC (2018) also addressed the need to name types of potential cyber losses. Consequently, it is argued that they not fully capture the meaning of cyber risk. The proposed definition can therefore provide a reference point for future research in cyber risk theory and for policymakers.

5. Ontological meta model of cyber risk concept

The review of the definition of cyber risk presented above leads to the following conclusion: due to the multi-faceted nature of the term 'cyber risk', it cannot be limited to a narrow definition. Although such attempts are made (also by the author himself), one may get the impression that the concise approach to the problem will diminish the depth and adequacy of a given definition. An in-depth description of the cyber risk concept might be a solution to the problem. The idea presented here is to supplement the definition of cyber risk - which refers primarily to generalisation - with an ontological meta model of the cyber risk concept. Its task is to develop a specific description of the term in question, to show functional interdependencies with other terms, conditions and factors that create the cyber risk framework and determine its nature.

Ontology is an important tool for building models and meta models reflecting the current state of knowledge (Ayadi et al., 2006, p. 415). The history of the first ontology dates back to the ancient times. Aristotle created ontology in the form of a system for categorising contemporary knowledge about the world. Christian Wolff, who published the philosophical treatise '*Philosophia prima, sive Ontologia*' in the 13th century, contributed to the dissemination of that concept (Kusztina et al., 2007). Nowadays, Neches explains that ontology defines the basic terms and relationships that create a terminology of a given thematic area, and rules for combining terms, as well as expanding the terminology (Neches et al., 1991). According to B. Smith, ontology is the science of 'types and structures of objects, properties, events, processes, relationships in each area of reality' (Smith, 2004). In turn, Fensel (2004) perceives the role of ontology in enabling the construction of a model of a given field of knowledge. Therefore, ontology is a tool for describing the field of knowledge, which provides the basis for modeling the content of concepts and relationships among them, resulting in ontological models (Kusztina et al., 2007).

Although the concept of ontology originates from philosophy, today it remains in the area of interest of computer science, natural language engineering, theory of knowledge management. Referring to the last of those research areas, knowledge should be presented in a manner appropriate to the particular field and problems being solved (Oliveira, 1992, p. 9). Ontology is defined as a rigorous and exhaustive organisation of some knowledge domain that is usually hierarchical and contains all the relevant entities and their relations (Vocabulary.com, 2019). Technologies of knowledge representation are designed to model and present knowledge structures in a human-readable way. This is done, among others, by categorising concepts that form meta language. Categorisation means the ability to organise symbols appearing in a message that belongs to a strictly defined group of objects with specific features (Bassara, 2004). Ontology is a description of a part of reality that serves the task of creating and processing knowledge (Grzelak, 2013). According to Gruber (1993), ontology should effectively convey the intended meaning of defined terms.

The state of knowledge about cyber risk needs to be structured due to its complexity and the multitude of factors that need to be taken into account. Creating meta models is one way of doing this (Gutenbaum, 2003). Meta models serve as tool supporting the creation of hypotheses by researchers. A meta model is a diagram that shows relationships among various factors and a defined concept. It enables to understand the location of the analysed construct in a context broader than in individual models. The model of the cyber risk concept illustrates causal relationships between cyber risk and other concepts and factors. It is assumed that there are influential factors that determine the behaviour of impact factors. They may also interact with one another.

The categories of modeling, concepts and their mutual relations presented in Fig. 3 represent the most general, conceptual structure of the term 'cyber risk'. Table 3 summarizes the key elements of the definition of cyber risk that has underlain the proposed meta model.

In the proposed ontological meta model of cyber risk, there are two spheres that interpenetrate one another. One of them is the real sphere which includes an organisation and its assets. The other one is the abstract sphere (conceptual) that covers such concepts as risk, vulnerability, probability or threat.

Let's start the analysis of the proposed meta model with cyber risk. Classically understood risk is presented as the product of probability of occurrence of an event and the size of potential impact. These abstract measures are estimated based on real incidents that occurred in the past. The number of cyber incidents allows for estimating the probability of their occurrence in a given period of time, while values of losses from the past are the basic data when modeling impact of cyber risk in the future. Cyber incident is the result of a specific threat that may be described by four parameters: a source of threat, actor, motives for action and location of the source of danger. Each of these parameters may transform

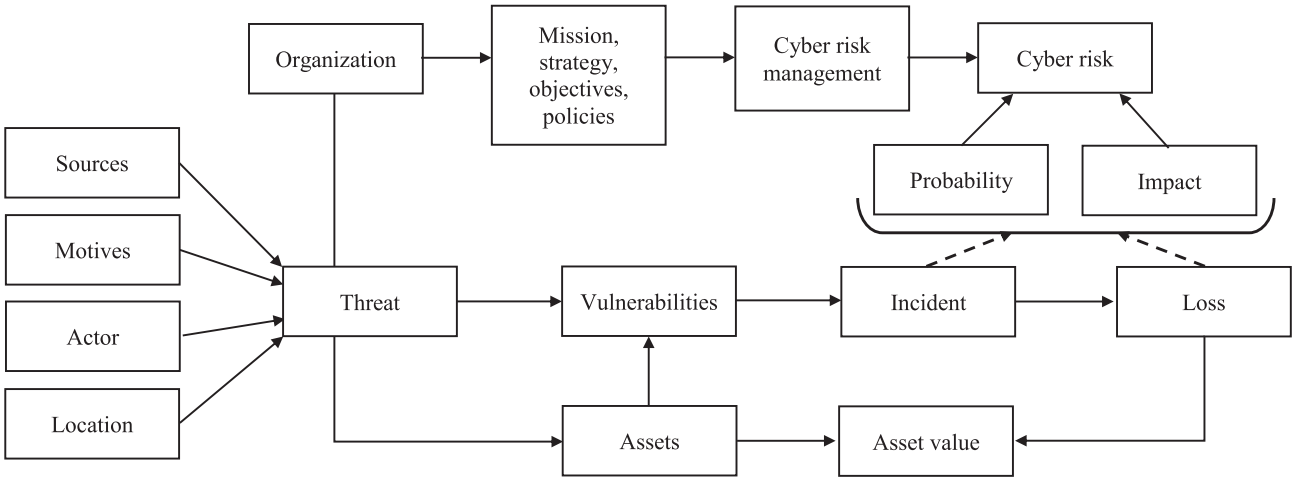

Fig. 3. Ontological meta model of cyber risk concept.

Table 3
Terms used in meta model of cyber risk concept.

Term	Explanation
Assets	Tangible and intangible assets that are valuable for an organisation, in particular: information, software, tangible assets, services, human resources, intangible assets.
Cyber incident	A cyber event that results from vulnerabilities of assets exploited by threats that may have an adverse impact on an organisation's assets.
Vulnerability	Weakness of assets or their safeguards that may be exploited by one or many threats.
Risk	Combination of probability of an adverse event and its consequences.
Cyber risk	Risk related to the threats that may exploit vulnerabilities of an organisation's assets, leading to a cyber incident that could result in losses for an organisation.
Impact	Negative consequences of a cyber incident for an organisation.
Threat	A potential cause of a cyber incident that may result in a loss for an organisation, characterised by specific parameters such as a source of threat, actor, motives of the actor, location.

Source: Amutio and Candau (2014), Caralli et al. (2007), Edgar and Manz (2017), ISO/IEC 27000:2014 (2014), MEHARI (2010).

into diverse states (values) that are constantly evolving, following the changes in the landscape of cyber threats. For example, the 'actor' category is divided into human actions and random events (e.g. natural perils, technical failures). A potential 'human' perpetrator of a cyber attack may be: an employee of an organisation, a subcontractor, a contractor, a client, a former employee, a competitor, a hacker, an organised crime, a government of a hostile country, a cyber terrorist. In turn, a list of sources of threats may be very extensive as are the circumstances in which security breach may occur in the cyberspace. Following the ISO/IEC 27,005 standard, numerous sources of cyber threats may be referred to, such as: technical failures, lack of access to media, breach of security of IT operations, information security breach, unauthorised access, radiation interference, natural disaster, physical damage [ISO/IEC, 27000:2014, 2014]. Another feature that characterises a cyber threat is the motive of a perpetrator. It may be an act (or omission) of an intentional or unintentional nature, or a result of incompetence. The source of a cyber threat may be located inside or outside the affected organisation. A cyber threat does not have to lead to a cyber incident. In most cases, cyber threats will not have an adverse impact upon an organisation. Probability of cyber risk materialisation is determined by a kind of weakness or rather an imperfection of a company's assets, that is called vulnerability. Vulnerability may be seen in two aspects: generic and quantitative. The generic aspect determines where vulnerability occurs and what the weaknesses of an asset are. The quantitative aspect indicates to what extent functionality (efficiency) of an asset will be reduced in the event of cyber risk materialisation. The result of a cyber incident is a loss - both direct and indirect. It reduces the value of assets (tangible or intangible) at the disposal of an organisation. This fact gives an impulse to take remedial actions in the form of the cyber risk management policy. In particular, the policy may be limited to the information security management system, consistent with the ISO/IEC 27001 framework. The specification of the adopted solution will depend on the mission, strategy, policies and objectives of an organisation.

The proposed meta model of cyber risk has several advantages. It identifies four groups of factors that characterise the diverse nature of cyber threats (sources of cyber threats, actors, their motives, location). Another benefit of the meta model is placing cyber risk in the context of mission, strategy, risk management policy and objectives of an organisation. And last but not least, the model indicates that, although cyber risk measures (probability of occurrence and potential impact) are abstract (i.e. determined using mathematical and statistical tools), they are estimated on the basis of historical data about the actual, not simulated, cyber incidents. It creates a special link between the past and the present. Currently applied cyber risk predictive models are fed with data from the past but it is highly doubtful if it is a reasonable solution for the fast evolving cyber risk.

6. Conclusions

The public debate is frequently burdened with confusion about the notion of cyber risk. Ale et al. (2015, p. 232) point out that, in the public discourse on cybersecurity, risk has been defined and redefined countless times in order to reflect those aspects that an author deemed important. The need for a comprehensive cyber risk definition stems from the desire to unify different views on cyber risk (e.g. regulatory, technical, safety science, computer programming), and thus make them more understandable and easier to implement in safety science (Aven, 2014, p. 19).

A focal point of the literature review, which is incorporated in the methodological design of this study, was to determine whether in the broad body of academic and industry literature there are definitions of cyber risk and if so, what they include. The paper provided an indication of the three key components of cyber risk concept, i.e. sources of cyber risk, cyber risk objects, and impact of cyber risk.

The proposed definition of cyber risk is not claimed to be a silver bullet solution to kick-start an academic discussion on cybersecurity and cyber insurance. However, one should remain an optimist. It is hopeful that such a unifying definition will provide more formal basis for future research and policy recommendations involving cybersecurity. It may

also help standardise cyber insurance terminology and thus foster the development of the cyber insurance market.

It is plausible to state that no abstract concept – such as cyber risk – has an isolated and independent meaning. There being the need for an abstraction mechanism that provides broader description of knowledge hidden in conceptual models. An insight into semantics of cyber risk has been delivered to show how the meta model and ontological approach may enrich established definitions of this term. The proposed meta model provides for ontological distinctions in order to correctly interpret existing and emergent conceptual models of cyber risk.

Despite the growing number of literature devoted to cybersecurity, cyber risk theory is still a relatively new topic and will continue to gain from contributions – especially around terminology. Thus further research should be focused on deeper integration of diverse attitudes to defining cyber risk. More efforts might be invested in the development of cyber risk assessment techniques that could help manage the risk.

Acknowledgements

The Project has been financed by the Polish Ministry of Science and Higher Education within the framework of the 'Regional Initiative of Excellence' Programme for 2019-2022. Project no: 021/RID/2018/19. Total contribution amounts to PLN 11 897 131,40.

References

Ahmad, A., Maynard, S.B., Shanks, G., 2015. A case analysis of information systems and security incident responses. Int. J. Inf. Manage. 35 (6), 717–723.

Alalwan, A.A., Rana, N.P., Dwivedi, Y.K., Algharabat, R., 2017. Social media in marketing: a review and analysis of the existing literature. Telematics Inform. 34 (7), 1177–1190.

Ale, B., Burnap, P., Slater, D., 2015. On the origin of PCDS – (Probability consequence diagrams). Saf. Sci. 72, 229–239.

Allen R., Bloom R., Janes S., 2019.The challenges of mobile workforce security – and how to solve them, Kingstone Technology [online] https://media.kingston.com/europe/landing/pdf/2019/12/Workforce-Security-eBook_WF498812_EN_1219.pdf (accessed 3 February 2020).

Amutio, M.A., Candau, J., 2014. MAGERIT- version 3.0. Methodology for Information Systems Risk Analysis and Management. Book I - The Method, Ministry of Finance and Public Administration (Spain).

Arachchilage, Nalin Asanka Gamagedara, Love, Steve, 2014. Security awareness of computer users: a phishing threat avoidance perspective. Comput. Hum. Behav. 38, 304–312.

Aven, Terje, 2014. What is safety science? Saf. Sci. 67, 15–20.

Ayadi, N., Ben Ahmed, M., Pollet, Y., 2006. Ontology-based meta-model for semantically interoperable systems. In: Proceedings of the Eighth International Conference on Information Integration and Web-based Applications Services, 4-6 December 2006, Yogyakarta, Indonesia, pp. 413–422.

Bassara, A., 2004. I weź tu dogadaj się – Ontologie (ang. Try to get along - Ontologies), Gazeta IT", 2004, nr 1(20).

Beirne, Martin, Hunter, Paul, 2013. Workplace bullying and the challenge of pre-emptive management. Personnel Rev. 42 (5), 595–612.

Biener, C., Eling, M., Wirfs, J.H., 2015. Insurability of Cyber Risk: An Empirical Analysis, "Geneva Papers on Risk and Insurance", No. 40, pp. 131–158.

BIS, 2016. Guidance on Cyber Resilience for Financial Market Infrastructures, Bank of International Settlements (BIS), June 2016, https://www.bis.org/cpmi/publ/d146.htm (accessed 18 October 2019).

BIS, 2019. International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version, Bank of International Settlements (BIS), www.bis.org/publ/bcbs128.pdf (accessed 30 October 2019).

Böhme, R., Kataria, G.,2006. Models and measures for correlation in cyber-insurance. In: Workshop on the Economics of Information Security (WEIS), 26–28 June 2006, University of Cambridge, UK.

Böhme, R., Laube, S., Riek, M., 2018. A fundamental approach to cyber risk analysis. Variance 12 (2), 161–185.

Böhme, R., Schwartz, G., 2010. Modeling cyber-insurance: Towards a unifying framework. In: Workshop on the Economics of Information Security (WEIS), Harvard, June 2010, https://informationsecurity.uibk.ac.at/pdfs/BS2010_Modeling_Cyber-Insurance_WEIS.pdf (accessed 22 February 2019).

Brewer, D., 2000. Risk assessment models and evolving approaches, IAAC Work. http://www.gammassl.co.uk/research/archives/events/IAAC.php (accessed 7 November 2019).

Bromiley, Philip, McShane, Michael, Nair, Anil, Rustambekov, Elzotbek, 2015. Enterprise risk management: review, critique, and research directions. Long Range Plan. 48 (4), 265–276.

Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R., 2007. Introducing octave Allegro: Improving the information security risks assessment process, Tech. Rep. CMU/SEI-2007-TR-012, Software Engineering Institute.

Cebula, J.J., Young, L.R., 2010. A Taxonomy of Operational Cybersecurity Risks. Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

CEIOPS, 2009. CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR Standard Formula—Article 111 (f): Operational Risk, CEIOPS-DOC-45/09, Committee of European Insurance and Occupational Pensions Authority (CEIOPS) 2009, https://eiopa.europa.eu/CEIOPS-Archive/Documents/Advices/CEIOPS-L2-Final-Advice-on-Standard-Formula-operational-risk.pdf (accessed 21 November 2019).

CRO Forum, 2014. Cyber resilience - the cyber risk challenge and the role of insurance, Chief Risk Officers (CRO) Forum, December 2014, http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance (accessed 7 November 2019).

Dodel, Matias, Mesch, Gustavo, 2019. An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. Comput. Security 86, 75–91.

Edgar, T.W., Manz, D.O., 2017. Research Methods for Cybersecurity. Elsevier, Cambridge, MA.

Eling, M., Schnell, W., 2016. Ten key questions on cyber risk and cyber risk insurance. Technical Report 2016. The Geneva Association, Zurich.

Eling, M., Wirfs, J.H., 2015. Modelling and Management of Cyber Risk, Lecture given at the IAA Colloquium 2015, 7-10.06.2015, Oslo, http://www.actuaries.org/oslo2015/presentations/IAALS-Wirfs&Eling-P.pdf (accessed 30 October 2019).

Fensel, D., 2004. Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce. Springer.

GAO, 1996. Content Analysis: A Methodology for Structuring and Analyzing Written Material, U.S. General Accounting Office. GAO/PEMD-10.3.1, Washington.

Gardner, D., O'Driscoll, M., Cooper-Thomas, H.D., Roche, M., Bentley, T., Catley, B., Teo, S.T., Trenberth, L., 2016. Predictors of workplace bullying and cyber-bullying in New Zealand, 448 Int. J. Environ. Res. Public Health 13 (5), 1–14. https://doi.org/10.3390/ijerph13050448.

Gordon, Lawrence A., Loeb, Martin P., Sohail, Tashfeen, 2003. A framework for using insurance for cyber-risk management. Commun. ACM 46 (3), 81–85.

Gruber, T.R., 1993. Toward Principles for the Design of Ontologies Used for Knowledge Sharing, Stanford Knowledge Systems Laboratory. http://tomgruber.org/writing/onto-design.pdf (accessed 23 November 2019).

Grzelak, W., 2013. Ontology – an attempt to systematize concepts. Bus. Inform. 4 (30), 159–168.

Gutenbaum, J., 2003. Modelowanie matematyczne systemów (ang. Mathematical modeling of systems), Exit Publishing, Warsaw.

Herath, Tejaswini, Rao, H. Raghav, 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inform. Syst. 18 (2), 106–125.

Hernandez, W., Levy, Y., Ramim, M.M., 2016. An empirical assessment of employee cyberslacking in the public sector: the social engineering threat. Online J. Appl. Knowledge Manage. 4 (2), 93–109.

Hopkins, Andrew, 2014. Issues in safety science. Saf. Sci. 67, 6–14.

IRM, 2014. Cyber Risk. Resources for Practitioners, The Institute of Risk Management (IRM), https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf (accessed 9 November 2019).

ISACA, 2009. The Risk IT framework, Information Systems Audit and Control Association (ISACA) 2009, https://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf (accessed 21 November 2019).

ISO/IEC, 2014. ISO/IEC 27000:2014: Information technology - Security techniques – Information security management systems - Overview and vocabulary, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC).

Khansa, Lara, Liginlal, Divakaran, 2012. Whither information security? Examining the complementarities and substitutive effects among IT and information security firms. Int. J. Inf. Manage. 32 (3), 271–281.

Komljenovic, Dragan, Gaha, Mohamed, Abdul-Nour, Georges, Langheit, Christian, Bourgeois, Michel, 2016. Risks of extreme and rare events in Asset Management. Saf. Sci. 88, 129–145.

KPMG, 2016. Global profiles of the fraudster: Technology enables and weak controls fuel the fraud, KPMG International Report. https://assets.kpmg/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf (accessed 1 February 2020).

Krippendorff, K., 2004. Content Analysis. An Introduction to its Methodology, 2nd ed. Sage Publications, Thousand Oaks (CA).

Kusztina, E., Różewski, P., Ciszczyk, M., Sikora, K., 2007. Struktura ontologii jako narzędzie opisu wiedzy dziedzinowej (ang. Ontology structure as a tool for describing domain knowledge), ,Metody informatyki stosowanej", Nr 2/2007, Szczecin, pp. 73–88.

MEHARI, 2010. Overview, Club de La Securite de L'Information Francais (CLUSIF), Paris 2010. http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-Overview-PL.pdf.

Moon, Yun Ji, Choi, Myeonggil, Armstrong, Deborah J., 2018. The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. Int. J. Inf. Manage. 40, 54–66.

Mukhopadhyay, Arunabha, Chatterjee, Samir, Saha, Debashis, Mahanti, Ambuj, Sadhukhan, Samir K., 2013. Cyber-risk decision models: to insure IT or not? Decis. Support Syst. 56, 11–26.

NAIC, 2018. Cybersecurity Risk Management, National Association of Insurance Commissioners (NAIC), National Association of Insurance Commissioners (NAIC). https://www.naic.org/documents/consumer_alert_cybersecurity_risk_management.htm (accessed 21 October 2019).

Neches, R., Fikes, R.E., Finin, T., Gruber, T.R., Senator, T., Swartout, W.R., 1991. Enabling technology for knowledge sharing. AI Magazine 12 (3), 36–56.

Ng, Boon-Yuen, Kankanhalli, Atreyi, Xu, Yunjie (Calvin), 2009. Studying users' computer security behavior: a health belief perspective. Decis. Support Syst. 46 (4), 815–825.
Ng, B.Y., Xu, Y., 2007. Studying users' computer security behavior using the health belief model. In: PACIS 2007 Proceedings, No. 45, pp. 423-437.
Nieuwesteeg, B., Visscher, L., de Waard, B., 2015. The law & economics of cyber insurance contracts: a case study, Centre for Safety and Security. http://www.safety-and-security.nl/uploads/cfsas/attachments/The%20Law%20%26%20Economics%20of%20Cyber%20Insurance%20Contracts%20-%20A%20Case%20Study.pdf (accessed 24 October 2019).
NIST, 2006. Minimum security requirements for federal information and information systems, Federal Information Processing Standards Publication FIPS PUB 200, National Institute of Standards and Technology (NIST), Gaithersburg, MD.
NIST, 2002. Risk management guide for information technology systems. Technical report, National Institute of Standards and Technology (NIST), Gaithersburg, MD.
Öğüt, H., Raghunathan, S., Menon, N., 2011. Cybersecurity risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. Risk Anal. 31 (3), 497–512. https://doi.org/10.1111/j.1539-6924.2010.01478.x.
Oliveira, Armando, 1992. In: Hypermedia Courseware: Structures of Communication and Intelligent Help. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 3–10. https://doi.org/10.1007/978-3-642-77702-8_1.
Pandit, M., 2018. Workplace Fraud Insurance: It's time businesses paid heed. J. Insurance Institute India, 40–43.
Pengelly, M., 2016. Cyber is the biggest operational risk fear, say practitioners, Risk.Net, Technical Report, 19 January 2016, http://www.risk.net/operational-risk-and-regulation/news/2441963/cyber-is-biggest-operational-risk-fear-say-practitioners (accessed 14 October 2019).
Pettersen, Kenneth A., Bjørnskau, Torkel, 2015. Organizational contradictions between safety and security – perceived challenges and ways of integrating critical infrastructure protection in civil aviation. Saf. Sci. 71, 167–177.
Refsdal, A., Solhaug, B., Stolen, K., 2015. Cyber-risk Management. Springer. https://doi.org/10.1007/978-3-319-23570-7_5.
Smith, B., 2004. Ontology and Information Systems. http://ontology.buffalo.edu/ontology(PIC).pdf (accessed 24 October 2019).
Soomro, Zahoor Ahmed, Shah, Mahmood Hussain, Ahmed, Javed, 2016. Information security management needs more holistic approach: a literature review. Int. J. Inf. Manage. 36 (2), 215–225.
Stemler, S., 2000. An overview of content analysis, "Practical Assessment, Research, and Evaluation", vol. 7, Article 17, https://doi.org/10.7275/z6fm-2e34.
Thlon, M., 2012. Operational risk management in enterprises- using Delta EVT method to estimate risk. Publishing house of the Cracow University of Economics, Cracow.
Torabi, S. Ali, Giahi, Ramin, Sahebjamnia, Navid, 2016. An enhanced risk assessment framework for business continuity management systems. Saf. Sci. 89, 201–218.
Vance, Anthony, Siponen, Mikko, Pahnila, Seppo, 2012. Motivating IS security compliance: insights from habit and protection motivation theory. Inform. Manage. 49 (3-4), 190–198.
Vocabulary.com, 2019, https://www.vocabulary.com/dictionary/ontology (accessed 11 November 2019).
Whitty, M.T., Carr, A.N., 2006. New rules in the workplace: applying object-relations theory to explain problem Internet and email behavior in the workplace. Comput. Human Behav. 22, 235–250.
World Economic Forum, 2012. Global risks 2012. Seventh edition, Insight Report, Geneva.