SECURITY MANAGEMENT AND RISK MANAGEMENT APPROACH IN CYBERSECURITY AND INFORMATION SECURITY MANAGEMENT

Maciej Szmit[*)]

ABSTRACT

Risk management approach is the most popular one in contemporary security management. However all types of risk are - more or less closely - related to the security, in information security management risks associated with security constitute the greater part of all risks. That situation frequently leads to misunderstandings both terms: security and risk management. The article is an attempt to organize these terms and basic concepts in the field of information security and cybersecurity.

Key words: Risk management, information security management, cybersecurity.

ABSTRAKT

Manažment rizík je jeden z najpreferovanejších prístupov v súčasnom bezpečnostnom manažmente. Všetky typy rizík sú – viac, či menej- spojené s bezpečnosťou. Riziká manažmentu informačnej bezpečnosti v súvislosti s bezpečnosťou predstavujú veľkú časť z celej množiny rizík. Táto situácia často vedie k nedorozumeniam pri chápaní oboch pojmov: bezpečnosť a manažment rizík. Tento článok má ambíciu vysvetliť tieto termíny a základné pojmy v oblasti informačnej a kybernetickej bezpečnosti.

Kľúčové slová: Riadenia rizík, riadenia bezpečnosti informácií, kybernetická bezpečnosť.

1 RISK-BASED SECURITY MANAGEMENT

Information security-related terms are often used in the literature in ambiguous way. Relating to well-know schema (see Figure 1), illustrating the relationships between main information security elements, near all of components (including security itself) seem to be somehow manageable (see [19] – figure 3, [18] p. 39). One

*) Maciej Szmit, Ph.D., Orange Labs Poland, Obrzeżna 7; 01-261 Warszawa; Poland; maciej.szmit@orange.com +48 228470730

can find “vulnerability management” (see: [14]), “safety management” (see e.g. [16]), “security management” (see e.g. [6]),“threat management” (e.g. in Microsoft™ Forefront Threat Management Gateway – see [17]), “risk management” etc.

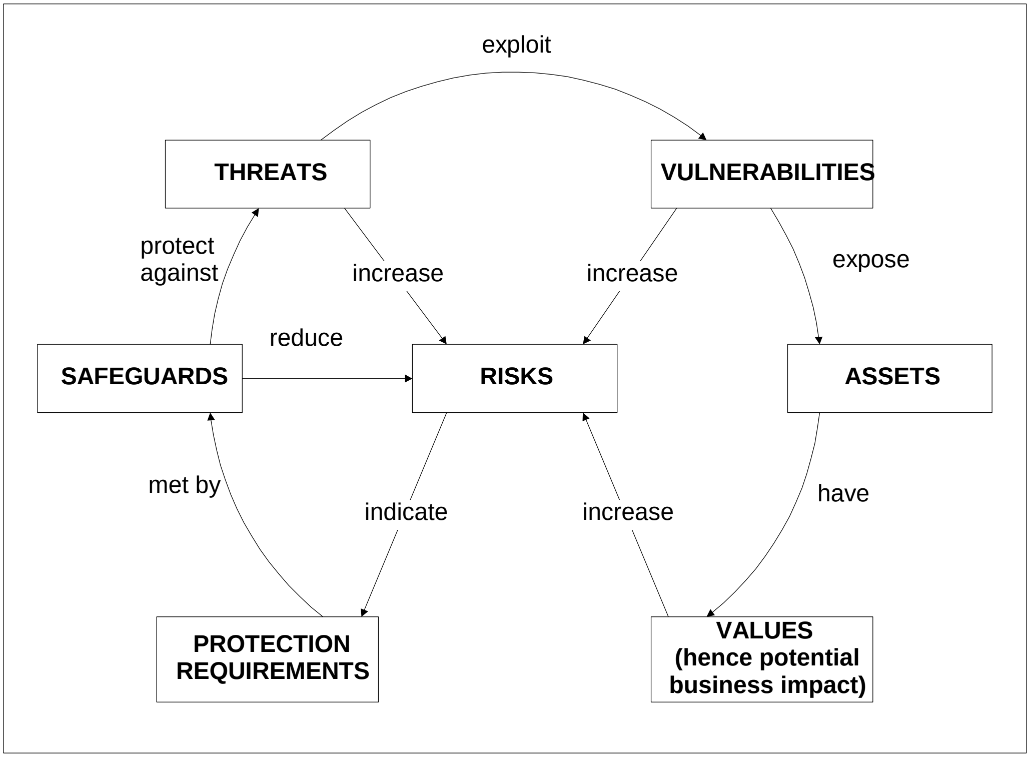

Figure 1 Risk Relationships Model. Source: [19].

The main semantic ambiguity occurs between risk management and security management. The risk is usually defined as effect of uncertainty on objectives (see: [21] – 2.21) and information security is defined as preservation of a set of properties such as confidentiality, integrity, availability of information and also its authenticity, accountability and non-repudiation (see: [8] – 2.33). From risk manager’s point of view, risks strictly related to assets’ security (e.g. information security risk) are only a specific group of risk, and management of this type of risk (sometimes erroneously identified with particular subject security management) may be treated as part of overall risk management (see e.g. [4]). This is tricky situation, which may lead to mistakes in understanding interactions between risk and security.

It is obvious that all types of risks are – more or less – closely related to the security, especially when security is understood in the broader sense, not only as a state of being free from danger or threat, but also as a guarantee of achieving subject (organization, group, man) objectives (see e.g. [5]). Additionally in some areas of risk management, security breaches (frequently intentional) represent the major part of all possible risks so the management of particular security risks becomes the main part of risk management process. This situation also applies to information-related risks. The minority of information-related risks may concern low quality (precisions, adequacy, topicality, timeliness etc.) of information content (see e.g. [7] p. 28) and usually are considered with other aspects of organization activities (like market analysis, management control system, public relations etc.), due to non-material character of information, most of possible problems with information concerns data processing, which is related to information security (strictly defined as preservation of confidentiality, integrity, availability and other properties like authenticity, accountability or non-repudiation of information – see: [8]-2.33), including availability and efficiency of IT assets (information systems). This group of risks may be implicated by security breaches.

In other contexts (management of security of assets other than information) there are a lot of different aspects, which have been included in overall security management processes, for example in ISO 22301 approach one of steps of creating BCMS (Business Continuity Management Systems), preceding risk assessment, is BIA ("Business Impact Analysis – process of analyzing activities and the effect that a business disruption might have upon them", see: [9]-3.8.), which may be understood as a form of asset evaluation (see e.g. [6]) from business continuity point of view (business continuity management is defined as „holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities" – see: [9]-3.4). Also particular risk in business continuity has been considered from the organization's objectives and assets point of view, which offers much more general approach than focusing on security of particular asset (like information). In the ISO/IEC 27001 approach creation of the ISMS (Information Security Management System) has no analogous step: the process focuses on risk management.

2 BEYOND OF RISK-BASED APPROACH

Potential problems with information security include wide spectrum of issues, including i.a. technical accidents, legal issues (e.g. personal data processing) and intentional information systems security breaches, so information security management cannot cover only management of general technical risks of computer systems. The other problem with risk-based approach is bound with narrow sense of „security" understood only form „ex ante" point of view. The security issues may be analyzed from at least three points of view:

- before the problem (fraud, security breach etc.) occurs,
- during the moment or period when the risk is being materialized,
- after risk's materialization.

Respectively one can distinguish: information security preventive actions, intruder detection and reaction and – in ex post perspective – corrective actions and investigations.

Obviously the term "risk" (understood as combination of particular threat's likelihood and impact) cannot be seriously analyzed when the threat already occurred. In that circumstance the likelihood becomes simply certainty: the problem just happened, probability of its occurrence is one. The term "likelihood" may be used in ex-post analysis when frequency of particular problem occurrence may be treated as a measure of likelihood of its future materialization. However the ISO 27k standards tries to cover all aspects of information security management systems (including i.a. digital evidence – see [24]), a few aspects of security are reserved for law enforcement and courts rather then for particular organizations and, of course, law enforcement and applications of the law processes should be deterministic.

The other problem concerns risk-based information security in multi-actor environment: there are strategies (like risk sharing or risk transfer), which decreasing risk from one actor point of view, increase risk for another actor. It is possible to find a compromise and build consistent and compatible ISMSes in situations, when all the actors play fair and have full information, but as one knows there are another situations and strategies too. Specific problems may relate to cybersecurity (security of the cyberspace).

International standard [10] includes two definitions: cybersecurity (adopted definition of information security from [8]: „Cybersecurity, Cyberspace security - preservation of confidentiality, integrity and availability of information in the Cyberspace" with note that „In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved" – see: [10]-3.20) and Cybersafety („Cybersafety - the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable", with two notes: „NOTE 1: This can take the form of being protected from the event or from exposure to something that causes health or economical losses. It can include protection of people or of assets" and „NOTE 2: Safety in general is also defined as the state of being certain that adverse effects will not be caused by some agent under defined conditions" see: [10]-3.19). The cyberspace is defined in the same standard as „The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" (see: [10]-3.21). More detailed (but still ambiguous) definitions of cybersecurity can be found in legal acts. The current Polish Government's Program for the Protection of Cyberspace in Poland (see: [11]) defines Cyberspace as „an area of processing and exchange of information, created by the computer systems and networks, along with links between them and the relationship with users" and Cyberspace of the Polish Republic as „cyberspace within the territory of the Polish State and in locations outside the territory where there are representatives of the Polish Republic (diplomatic institutions, military contingents)". The Act of August 30th 2011, amending the Act on the state of the war and the competence of the Supreme Commander of the armed forces and the basis for its reporting of the constitutional authorities of the Republic of Poland and certain other laws (see: [12]) defines it as follows: "space, processing and exchange of information created by ICT systems referred to in article 4. 3 section 3 of the Act of February 17th 2005 on the computer activities of entities realizing public tasks, together with the links between them and the relationships with the users" (all translations from [12]).

Although these definitions are far from clarity, it may be expected that the „cyberspace" term (in ISO meaning) denotes i.a. synergistic effect of contemporary Internet (especially associated with social networks, massively multiplayer online role-playing games e government, cloud computing etc.) and – due to "metaphysical" character of cyberspace – that cybersecurity should pass over information systems security (because information systems has physical form of course). It is hard to understand how any information security properties may be guaranteed without taking into consideration security of information processing systems. In the above legal definitions' meaning the cyberspace seems to be something what is a field of activity of entities realizing public tasks and may be protected and regulated by law (which, as mentioned above, should be deterministic) and – however the above Program ([11]) refers to definitions and concepts from ISO 27k standards – it is unclear how may be possible to evaluate and manage risks associated with losing the State ability to carry out its particular functions.

3 CONCLUSION

Risk management approach is the most popular approach in contemporary security management (see e.g.: [1], [2]). R.N.R van Os in the essay [3] analyses a lot of definitions concerning security management and risk management and finally concludes that risk management and security management are not the same (however both terms are ambiguous) and propose that risk management should be treated a part of security management. In relation to the information security management, risk management may be treated as the main part of security management process and as the base contemporary approach, however there are a few elements of information security management, when pure risk based approach seems to be inadequate or insufficient to provide satisfactory level of information security. The other strategies (deterministic, compliance-based etc. – see e.g. [22], [23]) may be an option worth considering in such situations.

REFERENCES

[1]. Lusková M., Buganová K.: Risk management and transport companies, Mechanics, Transport, Communications, 2011, art. ID: 491, http://www.mtc-aj.com/library/491_EN.pdf

[2]. Спиридонова Х., Андонов А., Михова М.: Анализ и оценка на риска при защита на информацията в аналитични системи за управление, Mechanics, Transport, Communications, 2013, art. ID:863, http://www.mtc-aj.com/library/863.pdf

[3]. van Os. R.N.R: Risk management and security management are the same thing?, http://members.chello.nl/~y.de.vries/Essays/Fa1r2.pdf

[4]. Staniec I., Zawiła Niedźwiecki J.: Zarządzanie ryzykiem operacyjnym, C.H. Beck, Warszawa 2008

[5]. Minisłownik Biura Bezpieczeństwa Narodowego http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html

[6]. Krause M., Tipton H.F.: Handbook of Information Security Management, CRC Press LLC, https://www.cccure.org/Documents/HISM/244-246.html

[7]. Korzeniowski L.F.: Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych, EAS, Kraków 2008, http://www.sbc.org.pl/Content/13871/Korzeniowski_Securitologia.pdf

[8]. ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO 2014

[9]. ISO 22301:2012 Societal security — Business continuity management systems — Requirements, ISO 2012

[10]. ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity, ISO 2012

[11]. Ministerstwo Spraw Wewnętrznych i Administracji, Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, http://bip.msw.gov.pl/portal/bip/6/19057

[12]. Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. 2011 nr 222 poz. 1323)

[13]. Lisiak-Felicka D., Szmit M.: "Tango Down" – Some Comments to the Security of Cyberspace of Republic of Poland, [in:] Biały W. Kaźmierczak J. (ed. ed.), Systems supporting production engineering, pp. 133-145, PKJS, Gliwice 2012

[14]. Foreman P.: Vulnerability Management. Auerbach Publications, 2010

[15]. Gustin J.F.: Safety Management. A Guide for Facility Managemers, Fairmount Press Inc., Lilburn GA, 2008, 2nd ed.

[16]. Petersen D.: Safety Management: A Human Approach, American Society of Safety Engineers, 2001

[17]. Microsoft Forefront Identity Manager – official webpage http://www.microsoft.com/en-us/server-cloud/products/forefront-identity-manager/

[18]. Śimâk L.: Krizový manaźment vo verejnej správe, Žilinska univerzita, Žilina 2001

[19]. ISO 13335-1994 (withdrawn standard) Information technology – Security techniques – Guidelines for the management of IT security - Part 1: Concepts and models for managing and planning IT security, ISO 1994

[20]. ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management, ISO 2011

[21]. ISO 31000:2009 Risk management — Principles and guidelines, ISO 2009

[22]. Kirschen D.S., Jayaweera D.: Comparison of risk-based and deterministic security assessments., IET Generation, Transmission & Distribution, Volume 1, Issue 4, July 2007, p. 527 – 533, DOI: 10.1049/iet-gtd:20060368

[23]. Klinke A., Ortwin R.: A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies, Risk Analysis Volume 22, Issue 6, December 2002, pp. 1071–1094, DOI: 10.1111/1539-6924.00274

[24]. ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence, ISO 2012

Článok recenzovali dvaja nezávislí recenzenti.