Risk and legal aspects of company's cyber security
Vladimír Smejkal, František Hortai, Anikó Molnárová

Abstract

The development of the entire IT sector is very dynamic and its consequences penetrate into all spheres of life of society. With the increase in the use of information technology, the risk of its abuse is rising. Targeted attacks against information technologies are a global phenomenon and their impact is causing massive economic damage in both the public and private sectors. The fight against cybercrime is never ending; that is why the issue of preventive measures reducing the risk of cyber-attacks is so significant and permanently present. Risk management, or rather building secure information systems, is an iterative, never-ending process that lasts as long as there are assets that need to be protected. It follows from the above that a company secured against cyber-attacks has a higher market value, even though its book value may be the same as the value of a less stable firm. The paper deals with the mutual influence of risk management and the sustainability of the company's operations, including the projection of risk management indicators into the value of an enterprise.

Keywords: Risk management; company value; cyber security, cyber-attacks, IS security

JEL Classification: G32, K24

Introduction

Currently, the issue of data security in information systems and other devices that collect, process, distribute, transmit, store, and archive data is totally extreme. There is virtually no area without data processing or data transferring devices. The dependence of the society and its functioning on information technologies is growing rapidly in all areas, not only in information society services, such as internet commerce, websites, social networks, etc., but it especially involves the functioning of information systems whose proper function is dependent on a number of basic services such as transport management, energy transmission, execution of public authority, operation of medical facilities, etc.). All advanced countries are already fully dependent on the proper functioning of information and communication systems. All advanced countries are already fully dependent on the proper functioning of information and communication systems.

However, with the increasing dependence of the society on information technology, there is also an increased potential of abuse of the technology, which has an extensive impact on the activities of the entities working with them, and can potentially lead to considerable damage.

Targeted attacks against information technology systems are a global phenomenon, and their impact is causing massive economic damages in both the public and private sectors, and, at the same time, they are capable of provoking negative political consequences, both on a national scale and on an international front. In cases where the attack is directed against elements of critical infrastructure, the safety, or the very existence of the state may ultimately be jeopardized. Attackers are increasingly focusing on elements of critical infrastructure such as power systems, pipelines, health information systems, and public administration information systems.

Attacks on information technology systems are becoming increasingly sophisticated and complex. From the sphere of direct economic benefit of individual assailants, attacks move into the area of organized cyber industrial espionage and cyber-terrorism. A major problem includes the so-called asymmetric threats: attacks on critical information and communication infrastructure by a small group of people.

The dynamics of the IT sector development and the growth of cyber-risks corresponds to the costs of ensuring cyber security that are increasing at the same pace, if not faster. For example, the European

Commission plans to invest more than twelve billion crowns in the fight against cyber-attacks aimed at public institutions and private companies in the EU member states in the period 2017-2020. Most funds spent on safety solutions are paid by banking institutions, the manufacturing industry and the public sector. According to IDC's forecast, the turnover in the segment will grow by 8.3 percent per year on average between 2010 and 2013, reaching $ 101.6 billion. It is therefore understandable that every government, organization or institution is interested in how much to invest in cyber security and how much is enough to secure it. At the same time it is clear that cyber security can never be absolute, but is always relative, directly proportional to the threat or risk.

The fight against cybercrime is a never-ending spiral between the possibilities of new technologies and hence the possibilities of their abuse, as well as the opportunities that these technologies provide in preventing, detecting and investigating this kind of crime. The idea that a more complex system that is part of cyberspace can be secured once and for all is illusory and impossible. That is why the issue of preventive measures reducing the risk of cyberattack is so significant and persistent. Risk management, or rather building secure information systems, is an iterative, never-ending process that lasts as long as there are assets to be protected.

1 Cyber Security in Companies

Information systems (hereinafter also referred to as IS) have become a critical part of modern society (see Czech legislation, Act No. 181/2014 Coll., *on cyber security and the amendment of related laws*). IS play a key role in the functioning of companies (Koch, Chvátalová, 2017). In addition to proper IS functionality, appropriate safeguards must also be in place to prevent misappropriation of the information contained therein and in general reduce the risk of their abuse (for example, to prevent possible unauthorized harmful actions). A failure or disruption of IS could cause huge damages, in some cases even a disaster. Despite the fact that authors do not succumb to the general hysteria due to the GDPR’s entry into force, it is important to keep in mind that in accordance with Article 83 of the Regulation it is possible to impose administrative fines of up to EUR 20 000 000 or, in the case of an enterprise, up to 4% of the total annual worldwide turnover for the preceding financial year, whichever is the higher. Liquidation is the most likely outcome for most businesses, and the reasons may lie "only" in the unsecured and incorrect content of the information system of the company. Cybercrime and cyber terrorism are all the more imminent given the increasing dependence of civilization on information and communication technologies (Smejkal, 2015).

Stability of IS becomes of extreme importance with trends of the gradual digitization of services (e.g. e-government) and internal company structures, such as IoT, BYOD and Industry 4.0, which bring their benefits but also possible threats. IoT ("Internet of Things") is the name of a system entailing linking of embedded devices to the Internet. Device interconnections should bring new possibilities of mutual interaction not only between individual systems, but also new possibilities of their controlling, and monitoring and securing of advanced services. BYOD (Bring Your Own Device) is a lucrative trend meaning that employees bring their own electronic or "smart" devices (such as laptops, tablets, smartphones, etc.) into the corporate environment. Integration of BYOD into company policies is an effective reflection of current IT development in the company, and may mean an increase of the company’s attractiveness, productivity and mobility of its employees with the possibility of virtualization of applications or entire user environments, i.e. desktops (enabling home office, teleworking etc.).

Industry 4.0 transforms production from stand-alone automated units into fully integrated automated and continuously optimized manufacturing environment. New global networks will be created, linking production facilities to Cyber-Physical Systems (CPS). CPSs will be the basic building block of "intelligent factories", will be able to autonomously exchange information, evoke the necessary actions

in response to current conditions and provide mutually independent control. Machines, sensors and IT systems will be interconnected within the value chain beyond the boundaries of an individual company. Such CPSs connected to each other will interact and analyze data using standard Internet-based communication protocols to predict eventual errors or failures, configure themselves and adapt in real time to changed conditions.

The key aspect of the conceptual solution of the Industry 4.0 projects is that the autonomous unit within the complex production system consists not only of production sections, production machines and their tools, but also of transport trucks and conveyor belts, robots, but also products, partially processed products, and input material. People are also considered to be part of the production system, some of whom do not even have to be preset in the production plant. It is expected that all these autonomous units can communicate, transact and cooperate together on a continuous and flexible basis. In order to allow such strong communicative and interactive cooperation to take place despite the fact that some elements cannot even communicate by themselves, all participants can be represented by software modules / agents who act on their behalf and in their place. This creates an idea of the interconnection of two worlds: the world of real physical objects (machines, devices, robots, products, and people) and the virtual world in which each physical entity can be sufficiently virtually represented or embodied in one form or another, and its behavior simulated by a software module. Nowadays, the two worlds are literally interlocking. It is assumed that the elements of the physical world will be linked to each other via connection to the Internet, where each such physical element has its own IP address: then we speak about the Internet of Things (IoT). The software modules, representing physical elements in the virtual space, jointly deal with tasks, coordinate their activities, and make decisions, using the services they provide to each other or which they access through the Internet of Services (IoS). So even though from the methodological point of view we speak about two Internets, IoT and IoS, only one Internet is in fact often physically used, with a single backbone infrastructure across the entire production area that is implemented as an Enterprise Service Bus (ESB). Special interfaces for robots and people that allow mobile communication, also based on natural speech, visual or tactile information, are to be considered as well: then a connection arises to the third type of Internet, Internet of People (IoP). (Mařík, V. 2016)

As stated in the National Initiative INDUSTRY 4.0 document, "Security and Reliability must be understood on a comprehensive and systematic basis: from data and communications security at the lowest level, through infrastructure reliability and security, to global system security at the level of companies or their chains, while maintaining the privacy of data and intellectual property rights." For more details see the documents of the Government of the Czech Republic which, at its meeting on August 24, 2016, approved the Industry 4.0 Initiative prepared by the Ministry of Industry and Trade, whose long-term goal is to maintain and strengthen the competitiveness of the Czech Republic at the time of the onset of the so-called Fourth Industrial Revolution.

Breaking down the boundaries between the company's internal and external environments results in an increased pressure on information security, which modern trends make more difficult, and, without introducing safeguards, even threaten. Therefore a question arises where the limit of the profitability of modern ICT trends is, and how to integrate them into the value of a business and analyze the threats they pose.

2 Value of a Business

When determining the value of a business, it is very important to distinguish between the terms “book value” and “market value” of a business.

The book value can be easily found in the company's balance sheet. This method is based on the calculation of the book value of the company’s assets that is reported in the assets side of the balance sheet (company’s assets), and from which liabilities shown in the balance sheet are then deducted, i.e.

the sum of provisions, long-term and current liabilities, bank loans and other liabilities. The result is the difference representing the equity of the company, which is essentially the net book value of the business. However, the book value is by itself a mere guideline to determine the market value. The market value depends mainly on the results of the company's economy and the development of these results. (Kislingerová, 2005)

Mařík (2007) understands the market value of a business as the value that is determined by expected future earnings either at the level of the owners or at the level of all investors in the company that are translated to their present value, that is, they are discounted. It must be emphasized again that objective value does not exist. The value of a business depends on both the purpose of the valuation and the entity that determines it.

Value, as defined by international valuation standards, is an estimate of the likely price to be paid for goods and services, and, most likely, the price agreed between the buyer and the seller. The market value is used when listing a business on the stock market, or selling a business if its owner does not yet know the buyer and attempts to estimate for how much the business could possibly be sold (Mařík, 2007). In order to determine the market value of a business, the appraiser must have all the relevant data available and the assumption of a functional and active market must be true (Krabec, 2009).

Therefore, the market value usually differs from the book value. The market value thus may be higher than the book value, in particular in cases where a profitable business is sold, or if the business contains big written off assets, but in perfect condition. In cases where a loss-making business is being sold, or in cases where a larger amount of assets is being sold but with limited use, the market price then may be lower than the book value.

Levels of the business value are understood from the point of the amount and ownership of the invested capital being valued. A business can then be valued at different levels. Levels of the business value are defined as (Sabolovič, 2008):

• Gross value (commercial property) means the value of the business unit as a whole, both for the owners and the creditors. When income approach valuation methods are applied, we speak about the Entity method.

• Net value (net asset value) This is the appraisal value at the level of the business owners. This thus means the valuation of the business' equity which may be viewed from multiple angles. When income approach valuation methods are applied, we speak about the Equity method.

Three basic groups of methods are basically used to measure the value of a business: asset-based approach, income approach and market approach methods (Kislengerová, 2001):

Market approach methods are easily comprehensible by ordinary people, and, at the same time, are the most objective, because they determine for how much it is realistic (possible) to sell the asset (business) on the market. As regards businesses, two basic situations can be encountered: direct valuation based on capital market data and market comparison valuation approach.

Asset-based methods are based on the valuation of individual components of assets and resources as they can be found in the accounting books (in the balance sheet). The essence of asset-based methods is the static valuation as of a particular day, not taking into account the time factor (with the exception to the liquidation value method).

Income approach methods primarily use information on what benefit an investor will get when investing in the purchase of assets. The basis, therefore, is the future benefit that can be measured in different ways and which we convert to the current value. Income approach methods currently include, in particular, the discounted cash flow method.

The issue of cyber security is becoming an important factor in every business. Cyber security clearly increases the value of the company, both in terms of book and market values. If we look at it from the accounting perspective, securing cyber security means a certain investment for the company that is reported in the books as long-term assets, namely, long-term intangible assets, i.e. software. In this case, it is valued at acquisition cost, and the investment becomes part of the company's book value. This value, of course, has a very low explanatory power because the established cyber-security system represents a huge competitive advantage over companies that do not address this issue. The market value of these companies, of course, increases.

Taking into account the fact that cyber security increases the efficiency and competitiveness of a business, it is clear that the book value and market value of a business will vary greatly. When determining the market value of a company, we first need to quantify the value of the cyber security system based on the benefits the system will bring us. In these cases, income approach methods are used for the valuation of intangible assets.

If we wish to determine the value a company (whether for internal purposes, due diligence or business negotiation), then we should also be interested in the development of value over time, or the prediction of the development of the value in the future. The value change in relation to assets transactions (sale of company assets, investments), or on the basis of successful or unsuccessful business operations (profit, loss), can be determined relatively well even for a certain future period of time. If we do not take into account the so-called black swans (Taleb, 2008), we can identify the risk factors about the existence of which we can or should know. This includes market changes (in buyers and suppliers, exchange rate changes, etc.), but, undoubtedly, also poorly-estimable risks including their possible impact on the company in the form of criminal activity (by employees and third parties), nowadays going completely outside the scope of ordinary behaviour, as demonstrated by the attitude of public authorities towards entrepreneurs (e.g. freezing orders), and in particular the ever-increasing scope and level of sanctions in the Czech and EU law for various alleged offenses.

3 Stabile vs. Unstable Company

Securing cyber security has an impact on business stability (reduction of costs in case of cyber-attacks, increased benefits as a result of reducing the risk of penalties imposed, for example, in accordance with GDPR, ensuring business continuity, etc.). Securing cyber security means reduction of risks.

For illustration, here is an example in which an attacker uses a stolen or counterfeit identity and disinformation. A primitive technique of sending instructions from an e-mail address similar to the original is assumed. Imagine communication between two foreign companies where one company funds the other one. The finance department of the first company receives an e-mail pretending to be from the other company in which instead of the original email address *Competent@2ndCompany.com* a similar address is used, *Competent@2ndCompany.org*, in which only the domain is changed. The attacker appears to be a competent person from original e-mails. The report contains an invoice and asks for an amount to be paid to the attacker's account abroad. The message looks authentic, it uses the same format as the other company does, as well as logos, etc. Therefore, unskilled personnel of the first company then pay the amount to the account of the attacker. Until theft is detected, the attacker has time to effectively cover the tracks. Such a type of attack results in the loss of the amount stolen, and possible damage to the reputation of the company. Such threats can be eliminated, for example, by training the personnel, without which this risk is addressed only by risk retention.

The example is illustrated graphically using a matrix of risks (see Figure 1); simple staff retraining will get us from Point A to the target point B.

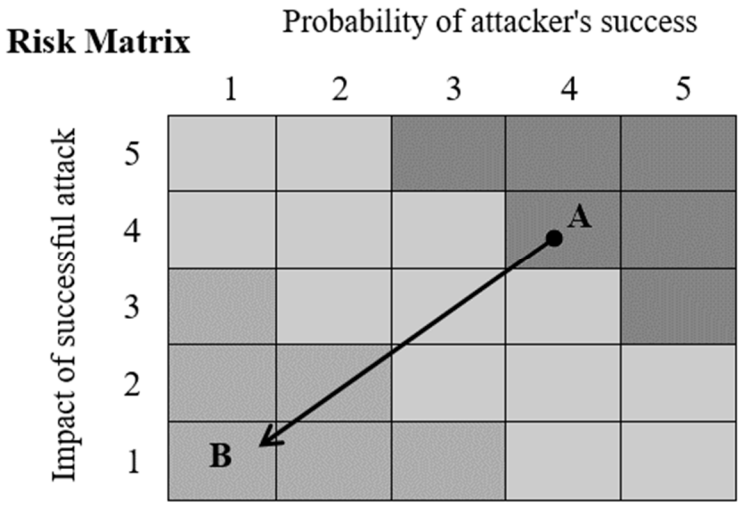

Figure 1: Risk management illustrated by movements in the risk matrix. Source: by own

B

In this case, it is a simple attack, but there are many variations and ways; see (Smejkal, 2015). We can say that securing cyber security will reduce the risk, and it could be quantified. A possible example follows:

For non-compliance with the GDPR requirements, the company may pay a fine of up to € 20 million, or 4% of the total turnover for the previous financial year. The example company is an average medium-sized company with a turnover of CZK 100 mil. Let us assume that at the beginning the risk of a fine is 80% and the risk remaining after taking measures (compliance with the GDPR requirements) will be 10%. In this way, the threatening higher risks will be reduced from 4% * 100 million * 80% to 4% * 100 million * 10%, i.e. by 4% * 100 million * 70% = 2.8 million.

Then we could compare the indicators: the cost of risk reduction and the benefits of risk reduction: for example, the cost of creating a system to handle GDPR requirements is CZK 1.9 million (a realistic offer for a medium-sized company of 600 employees) and benefits are CZK 2.8 million. This will, however, result in a one-off increase in costs by CZK 1.9 million, plus we can assume costs of about CZK 500 thousand per year for a person authorized to process personal data, but the benefits prevail. In addition, the person authorized to process personal data can be outsourced at a lower cost.

The estimated costs of risk mitigation measures are lower than the expected benefits of the risk reduction. We arrive at the following relationship:

(Greater Security) => (Higher costs) and (Lower risk)

Let us therefore define the upper cost limit up to which it is still worth reducing the risk related to IS security:

(Isolated costs related to risk reduction) ≤ (are less than or equal to:) (The costs of potential damage and restoring the continuity of operations if the event with which the risk is associated will occur).

The risk is expressed as the extent of threat to the assets and the degree of danger that a threat might materialize and an undesirable result will lead to damage occurring (undesirable consequences) (Smejkal, Rais, 2013, p. 99). The terms "more risk" and "less risk" refer to the measure of the possible size of the loss. The estimated (expected) loss value in the given situation is the probability of the loss multiplied by the amount of potential loss. If ten crowns are at risk and the probability of loss is 0.2

(20%), the expected loss value will be two crowns. If the amount at risk is one hundred crowns and the probability of loss is 0.02, the estimated loss value will be equal to two crowns (Smejkal, Rais, 2013, p. 107):

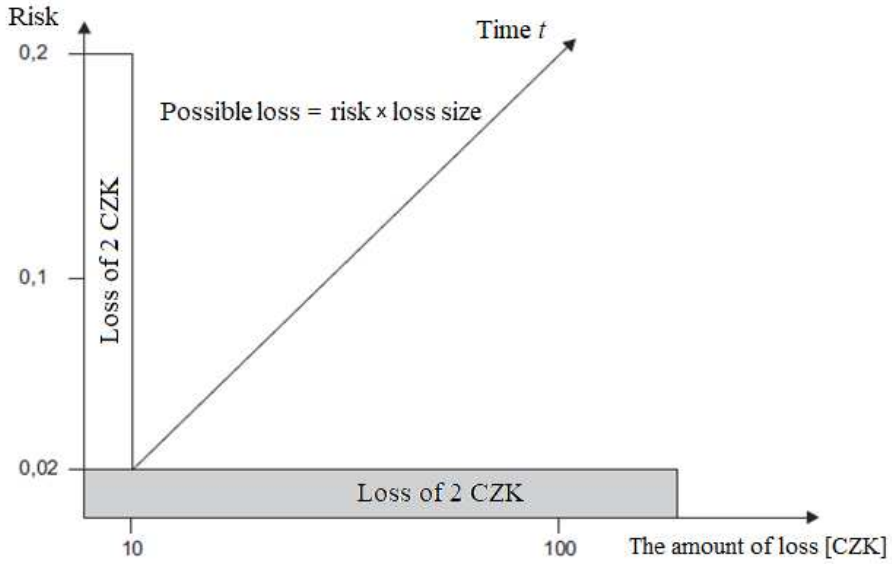

Figure 2: Estimated (expected) loss. Source: by own

If we assume a linear dependence, the risk is a constant value in the range of <0; 100>% and "Possible Loss" depends on the asset that is at risk (see Figure 3):

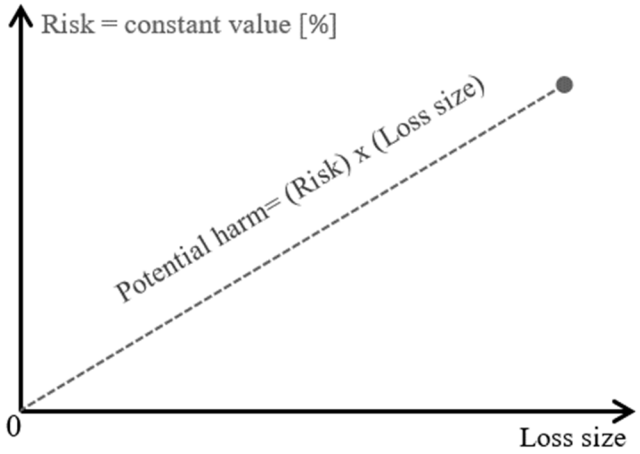

Figure 3: Relationship between potential harm and risk. Source: by own

But we can assume that this dependency is non-linear. A higher value asset has a more lucrative character for possible attacks. Therefore, by increasing the value of assets the threat / attack risk also increases. For example, a hacker is more motivated to a cyber-attack where a greater subjective gain may be achieved. The cyber-terrorist is trying to cause the greatest damage possible. Consequently, the risk is a function of the value of the assets at risk / amount of loss. The risk thus gets dynamic (see Figure 4):

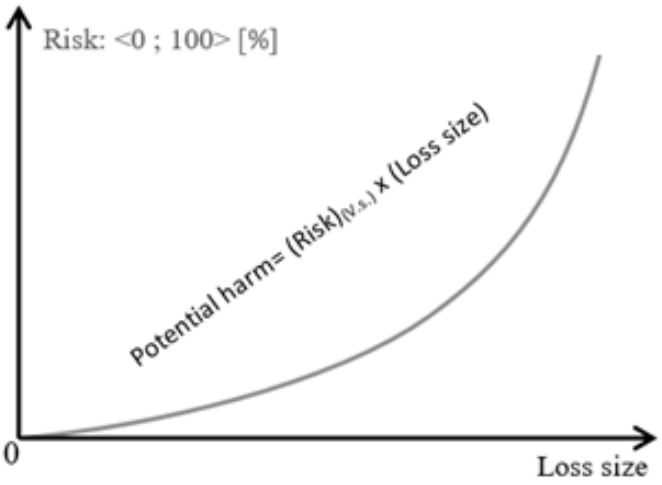

Figure 4 Dynamic relationship of potential harm and risk. Source: by own

Ensuring system security is a continuous process. The reason is new technologies and the development of human knowledge. They both enable new types of attacks and result in the need for continuous innovation of safeguards. That is why time can be considered as the third factor in the calculation. The amount of loss (assets) changes over time as well as the likelihood of the occurrence of events caused by threats. If we plot time on the third axis, we can model the estimated loss size which can be calculated as Z (t) in the time interval <0; T1>, see the equation below:

$$Z_{(t)} = \int_0^{T1} r(t) \cdot v(t) \cdot d(t)$$

Where:

- r(t) is the risk function over time, expressed as probability in the interval <0; 1 >,
- v(t) is the loss function over time.

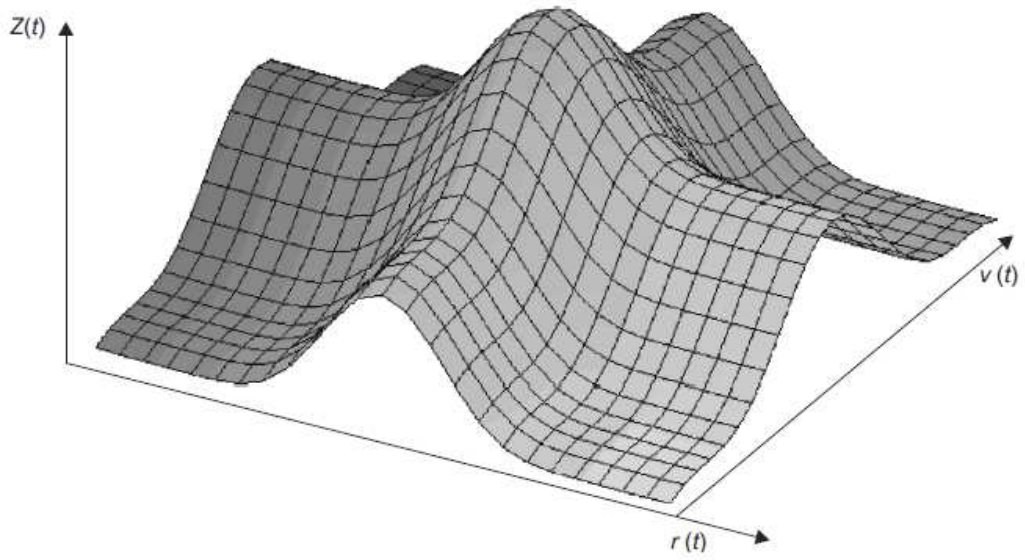

Figure 5: Estimated loss size Z(t) in the time interval < 0 ; T0 >. Source: by own

Z(t) is the estimated loss in the time interval <0; T1>, which we try to optimize so that the final value is minimal. (Smejkal, Rais, 2013, str. 108)

An important part of the decision-making process for reducing identified risks is the cost of risk reduction. A dependency applies according to which there exists an optimal state, a balance between the cost of risk reduction and the magnitude of the risk, or rather of the damage that the threat can cause. Figure 5 shows an ideal or theoretical course, which may vary a bit in a particular case. It is appropriate to invest only so much in the measures aimed at risk reduction or elimination so that the costs are proportional to the potential amount of the imminent damage. (Smejkal, Rais, 2013, str. 170)

From the graph (Figure 6) we can also deduce:

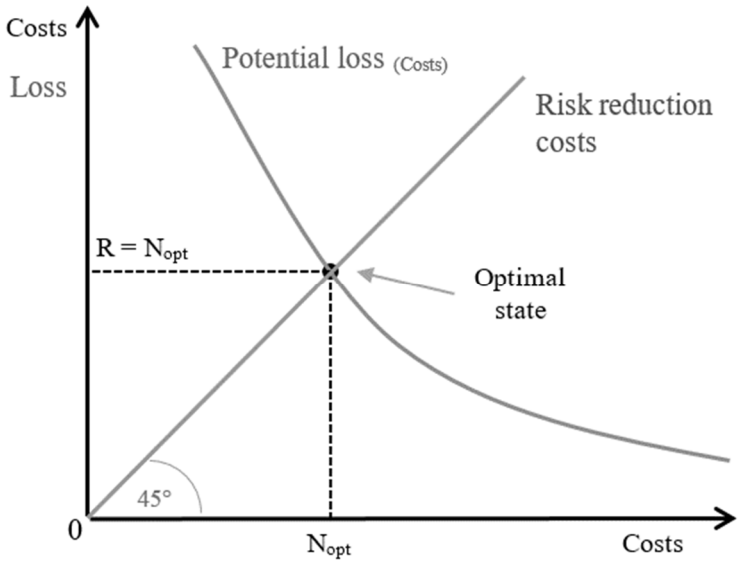

Figure 6: Relationship between risk reduction costs and potential loss: Source: by own

- It is not possible to assume zero risk reduction costs
- 100 percent risk elimination may require up to "infinitely" high costs.

Therefore, the cost reduction project must also include cost management.

Another example may be the threat (and therefore the risk) resulting from Act *No 418/2011 Coll., on criminal liability of legal entities and proceedings against them (CLLE)*. The Act understands criminal liability of a legal entity as independent of criminal liability of a natural person, and comes into question when the vast majority of facts described in Section 7 of CLLE (including property, economic or tax crimes, and others) occur.

Pursuant to Section 15 of the Act, criminal offenses committed by a legal person may be penalized as follows:

a) Dissolution of a legal person;

b) Asset forfeiture;

c) Financial penalty;

d) In rem forfeiture;

e) Prohibition of activity;

f) Prohibition of performance of public contracts or participation in a public tenders;

g) Prohibition of receiving subsidies and grants;

h) Publication of the judgment.

Under Sec. 8 (5), the legal person may be released from criminal liability pursuant to paragraphs 1 to 4 if it has made every effort that could be fairly demanded from it to prevent the commitment of the unlawful act by the persons referred to in paragraph 1. For this purpose, especially the so-called Compliance Programs are used, which mean compliance with legal standards by legal entities as well as creation of and compliance with relevant internal standards, both legal and ethical. Part of the Compliance Program is the implementation and establishment of a management and control system of the legal entity that focuses on compliance with legal and internal standards under which the legal person is required to act. Therefore, if the company wants to eliminate or at least minimize the risk of prosecution, then it will need to develop and operate a Compliance Program, which will require, as in the above case, both one-off and operational costs. The punishments listed in Sec. 15 of CLLE may be so drastic that these costs will pay off. The existence of the Compliance Program should be reflected in the company's intangible assets as it undoubtedly increases its value.

The Compliance Program will be most likely stated at acquisition cost (pursuant to the accounting rules), but in the case of business sale negotiations, the demonstration of a fully functioning Compliance Program may increase the market value by more than its cost was.

Conclusion

The nature of cyber security and its economic securing requires a systemic solution involving the public sector and the economy as a whole, i.e. active state (government) policy, a responsible and purposeful approach of all entities in the industry, banking and financial services, and an active attitude of individual companies and private sector corporations. We believe that it is just the unified system approach for solving these very serious practical tasks, respecting both horizontal and vertical relationships, that is currently not available in practice. It is important that the information and IS security is effective while it is necessary to balance the level of security, funds and applicability.

Ensuring cyber security is a multi-level problem with economic, legislative, technological and organizational aspects and with a significant overlap into the global environment, which requires the application of a system approach.

The main objective was to demonstrate the problem that cyber security is not only a part of IS management that is perceived in companies:

1. From the accounting point of view as intangible assets: software, exceptionally data and hardware costs stated at acquisition cost;
2. In the better case also as a tool evaluated by the rate of increased efficiency (competitiveness) of the company.

It has been demonstrated in several examples that managing cyber security has an impact on the company’s stability (reduction of cost of cyber-attacks, increased benefits by reducing the risk of fines e.g. imposed pursuant to GDPR, ensuring business continuity, etc.). Mastering cyber-security results in risk reduction.

The costs associated with the introduction of IS security (purchase costs, implementation costs, costs of operation, etc.) depend on the type of technology used, the size of the company, number of employees, etc. A crucial role is played by the importance of secured assets, whether it is sensitive data or not. There is no point in introducing a highly secure technology for data the loss or misuse of which would result in less damage than the cost of deploying a security system.

We have identified the upper cost limit up to which it is still worth reducing the risk in companies:

Isolated costs related to risk reduction are less than or equal to:

The costs if potential damage occurs and the renewal of the continuity of activities, if the event with which the risk is associated, occurs.

Acknowledgment

This paper was supported from the Internal Grant Agency at Brno University of Technology by grant: FP-J-17-4137 Expert methods and ICT support for risk management in enterprises.

References

BOHUSLAV, L. (2014). *Jak nastavit compliance programy*. Právní rádce č. 6/2014, str. 20-23.

KISLINGEROVÁ, E. (2001). Oceňování podniku. 2. přeprac. a dopl. vyd. Praha: C. H. Beck.

KISLINGEROVÁ, E. (2005). *Finanční analýza: krok za krokem*. Praha: C.H. Beck.

KOCH, M., & CHVÁTALOVÁ, Z. (2017). Information Systems Efficiency Model. *Journal of Systems Integration*, *8*(3), 3-9.

KRABEC, T., a kol. (2009). *Oceňování podniku a standardy hodnoty*. 1. vyd. Praha: Grada.
MAŘÍK, M. (2007). *Metody oceňování podniku: proces ocenění - základní metody a postupy*. Praha: Ekopress.

MAŘÍK, V. a kol. (2016). *Průmysl 4.0 – výzva pro Českou republiku*. 1. vydání. Praha: Management Press.

Nařízení Evropského parlamentu a Rady č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, které je označováno jako General Data Protection Regulation (GDPR).

SABOLOVIČ, M. (2008). *Oceňování podniku: Jak vytvořit a udržet si nadprůměrný výkon*. 1. vyd. Brno: Rašínova vysoká škola.

SMEJKAL, V. (2016). *Kybernetická kriminalita*. 1. vydání. Plzeň: Aleš Čeněk.

SMEJKAL, V. a RAIS, K. (2013). *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada.

TALEB, N. N.: (2008). *The Black Swan*. The Impact of the Highly Improbable. Penguin Books Ltd.

Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů*.

Zákon *č.* 418/2011 Sb., *o trestní odpovědnosti právnických osob a řízení proti nim.*

Autors contacts

prof. Ing. Vladimír Smejkal, CSc. LL.M.
VUT v Brně
Faculty of business and management
Department of informatics
Kolejní 2906/4, 61200 Brno
Czech republic
Tel.: +420 54114 2603
E-mail: smejkal@znalci.cz

Ing. et Ing. František Hortai
VUT v Brně
Faculty of business and management
Department of informatics
Kolejní 2906/4, 61200 Brno
Czech republic
Tel.: +420 54114 3719
E-mail: hortai@fbm.vutbr.cz

Ing. Anikó Molnárová
VUT v Brně
Faculty of business and management
Department of informatics
Kolejní 2906/4, 61200 Brno
Czech republic
Tel.: +420 54114 3719
E-mail: molnarova@fbm.vutbr.cz