CONTEMPORARY ISSUES IN BUSINESS, MANAGEMENT AND EDUCATION‘2012
ISSN 2029-7963/ISBN 978-609-457-323-1
doi:10.3846/cibme.2012.48

INFORMATION TECHNOLOGY RISKS IDENTIFICATION: PECULIARITIES OF SMALL AND MEDIUM SIZED ENTERPRISES

Rasma Janeliūnienė[1], Vida Davidavičienė[2]

*[1,2]Vilnius Gediminas Technical University, Faculty of Business Management,
Saulėtekio ave. 11, LT-10223 Vilnius, Lithuania
Emails: [1]rasma.janeliuniene@vu.lt; [2]vida.davidaviciene@vgtu.lt*

Abstract. Information technologies (IT) play a vital role in management and life of organization today. IT are one of most important tools of business process in competitive environment. Effective management of information technologies enables to reach organizational goals, optimize resource planning systems, investments etc. A lot of resources and business process tools are moved to virtual environment what leads to increasing dependence of organization to IT and risks related to IT solutions. The risk identification peculiarities of small and medium sized business are analyzed in the article. Methods of systematic literature analysis and comparison were employed.

Keywords: IT risk, risk identification, small and medium size business.

Jel classification: D81, G32, O31, O32, O33.

1. Introduction

Nowadays organizations are getting more reliant on information technologies. While the rapid growth of Information technologies (IT) and Internet has changed the way we communicate, conduct business and achieve our goals, crime and security threats such as bad ware, spam, phishing and viruses have also increased, undermining users’ trust and confidence in the Internet (Tawileh *et al.* 2007). Development and growing importance of IT in the business activities inevitably are increased amount of the risks associated with IT systems. IT risk and its’ management plays a critical role for today's business. Almost every business decision requires executives and managers to balance risk and reward. IT has a dual role in companies: firstly, IT is becoming increasingly important for an efficient production of goods and services as well as for the efficient coordination of business activities in a mounting interlinked economy; secondly, the importance of IT as tool for managing companies is also increasing (Sackmann 2008). So, effectively managing the business and IT risks is essential to an enterprise’s success (ISACA 2009). Daily work of the company being associated with IT will be effective only when the IT system works properly, correctly, and without interference. For example, large financial and moral losses of e-commerce associated company can by caused by internet connection failure or attacks. The statistics of PandaLabs (2012) show, that type of malware are similar: four out of every five new malware specimens created were Trojans (78.92 percent). Such constant attacks and damage highlights importance of IT risk management for the company. Analyzing IT risk management it is important to emphasize companies specifics. The gap between large and small-to-medium sized enterprises in the information security area has been increasing substantially as a direct result of the scarcity of resources available to SMEs (Tawileh *et al.* 2007). The lack of methodologies for SMEs for IT risk management outdraw the importance of the research as well as Lithuanian situation because in year 2011 about 80 percent of Lithuanian businesses were formed of small and medium sized enterprises (SME). The aim of this article is to analyze IT risk identification specifics of the SME and determine IT risk identification process for SMEs. Research methodology employed: systematic analysis and synthesis, methods of comparison.

2. IT risk peculiarities

The developers of the most frequently used COBIT methodology for IT audits, and risk assessment framework RiskIT, stated that IT risk is business risk associated with the use of IT. Experts points out that in the past IT risk has been relegated to technical specialists outside the boardroom, despite falling under the same ‘umbrella’ risk category as other business risks: failure to achieve strategic objectives (ISACA 2009). In general the risk is described as an action or events that took place in a negative impact on the organization and its information system (ISACA 2002). However, according to the way of action, risk can be described as a potential negative impact on the organization, based on the vulnerability of IT or information systems (e.g. defective or weak point) and benefits from a risk assessment of the likelihood and impact (Stoneburner *et al.* 2004; Bowen *et al.* 2006; VITA 2006). Smith *et al.* (2009) notice that IT risk definition has been changed because incidents harm constituencies within and outside companies they damage corporate reputation and expose weaknesses. Westerman and Hunter (2007) detailed that it’s the potential for an unplanned event involving a failure or misuse of IT to threaten an enterprise objective - and it is no longer confined to a company’s IT department or data center. The business processes, which were outlined by ESRMO (2011) should be added to previous concept. Stoneburner *et al.* (2004) identifies reasons of IT related risks, which can arise from legal liability or mission loss. It is: Unauthorized (malicious or accidental) disclosure, modification, or destruction of information; Unintentional errors and omissions; IT disruptions due to natural or man-made disasters; Failure to exercise due care and diligence in the implementation and operation of the IT system.

Despite named risks organizations are constantly improving performance management in order to optimize resources and increase productivity by implementing new information technologies, information systems and innovative solutions (for example: software for decision-making, customer relationship management, information management and business systems, etc.). So, the a disturbance of IT, e.g. unavailability or no integrity, can cause persistent business failure within a short time, deterioration in the company's reputation and resources loss (Sackmann 2008).

In order to determine specific aspects of IT risk the factors that causing risk should be analyzed as well as main risk management concepts. In the literature risks are classified in different ways, some of them derive and classify by their impact on the organization and others based on appearance of the sources and origins. Most authors divide risks of organization in to two groups: the financial risks and operational risks (Symantec 2007; Fratila, Tantau 2008). In many companies, risk related to information technologies is considered to be a component of operational risk (Teilans *et al.* 2011). Information technologies are going into risky situations, because most of them are moved into the electronic space like outsourcing or cloud computing solutions, SAS (software as a service), etc. IT risks become more and more complex. Analyzing this from the IT security perspective – the risk management is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system (Elky 2006). So, confidentiality, integrity and availability - is triad that important throughout the company's life. Information security refers to the components, procedures and data of information systems are not destroyed altered or leaked, due to accidental or malicious reasons, moreover the system run continuously and reliably, the service was not interrupted (Gao *et al.* 2011). Organizations, which are using IT solutions based software, regardless of whether they are large corporations or small and medium sized businesses, are seeking to protect their assets and to comply with certain standards and requirements such as BS, ISO, DOD, HIPAA, etc.

Symantec Corporation (2008), one of the leading companies in the field of Internet security technology, state that IT risk encompasses the full spectrum of risks that may affect or result from IT operations: external natural disasters or changes in government regulation, internal processes that affect product or service quality, IT organizational and datacenter performance, loss of intellectual property, supervisory or legal controls, and much more (Symantec 2008). According to source and potential impact on organization the risks can be classified into four groups (Symantec 2007; Fratila, Tantau 2008; Savić 2008).

- Security risks – risks sources may be external attacks, malicious code, physical destruction, inappropriate access, disgruntled employees, proliferation of platform and messaging types. Potential impact of these risks is corruption of information, external fraud, identity theft, theft of financial assets, damage to reputation and brand, damage to assets. Main concept of such risk management - ensure that information would be available, modified or used only by authorized persons.
- Availability risk – the failure or delay in delivering IT processes or information needed for business transactions and operations. Availability risks

sources are hardware failures, network outages, poor change management, processes, data center failures, force majeure.

- Performance risk – risks sources are poor system architectures, network congestion, inefficient code, inadequate capacity.
- Compliance risk – Penalties, fines and loss of reputation from failure to comply with laws and regulations, or consequences of non-compliance with IT policies.

Another classification based on risk sources was presented by Tchankova (2002) therefore the sources of risk are represented depending on the environment in which they arise: physical environment, social environment, political environment, operational environment, economic environment, legal environment, cognitive environment. One more point, which were outlined by Westerman and Hunter (2007), in most cases IT risks arise not from technical or low-level employees but from the enterprise's oversight or IT governance failure. Such failures produce a series of poor decisions and badly structured IT assets that are manifested as ineffective IT governance, uncontrolled complexity, and inattention to risk (Westerman, Hunter 2007).

Taking in to account all types of classification and considering peculiarities of SME (small and medium sized enterprises) as a main IT risk groups should be named potentials IT threats and vulnerability of organization concerning IT failures. In order to identify the most relevant IT risk management model the IT risk identification process should be analyzed concerning SME peculiarities.

3. SME IT risk identification process

Tawileh *et al.* (2007) provides a number of characteristics, witch separate SME from large enterprises such as: SMEs do not possess the required resources (human, monetary or technical) that should be invested to solve the problem; SMEs typically operate in very tight budgets; have seriously limited manpower and many needs competing for a very limited supply of resources, leading to information security being pushed down the priorities list. Therefore, SME are very sensitive to any fraud or loss. If large companies have an IT department or a department, which takes care of and security and performance, the SME have no such structure and resources for that.

Significance of IT for SMEs is huge, because enterprises become more flexible, competitive, more consumers oriented then before, when production means were most important (Taylor, Glezen 1988; Ginevičius *et al.* 2005; Ginevičius *et al.* 2006; Elskytė, Raudeliūnienė 2006; Davidavičienė 2008; Davidavičienė *et al.* 2011). According to The Department of Statistics (Statistics Lithuania) the amount of companies using computers growth was 5.2% and internet usage growth was 11% during last five years (Statistics Lithuania 2011). For example, in year 2005 91.7% companies used computers and in year 2010 it was 96.9%. 65.2% enterprises had company's website in year 2010 while in year 2009 it was 61.7%. It was indicated that: 39.4% companies presented product catalogues and price lists, 17% of companies offered an opportunity to choose preferable shape or design of product, 17.1% possibility to order and purchase the products.

In most cases enterprises use Internet for financial operations (92.9%). In year 2009 95% of enterprises used the Internet for communication with public authorities and agencies, in year 2008, 90.4%. 94.6% – downloaded various forms, 91.4% – returned filled-in forms via the Internet. In year 2009, 31.4% of enterprises provided offers in an electronic tendering system (public procurement monitoring information system). At the beginning of 2010, digital authentication tools were used by 68.9% of enterprises having 10 and more employees (in year 2009, 23.9%). Analysis of statistical data leads to conclusions that: growing needs of business entities, competition in markets, quantity of information causes increased use of ICT in SMEs of Lithuania; an increasing number of SMEs using broadband Internet, which ensures reliable and secure data transmission link; during year 2010 the use of information systems in SME was growing, which reflects the growing demand for IT.

According to CERT-LT (Computer Emergency Response Team) in 2009 the mostly problems were: computer viruses (95.2%), unsolicited bulk e-mail (SPAM) (1.0%), e-service disturbance (0.3%), illegal content (0.6%), occupancy (1.4%), fraud (0.3%), manipulation (0.1%) and other incidents (1.0%). 77% research participants said that on network and information security breaches have not experienced any damage, 15.6% of respondents claim to have been tampered with computer software, 3.3% said that it was stolen or destroyed confidential company data. 98.5% of all respondents said that the company against computer viruses using anti-virus software, 49.9% of the data to protect against possible damage or loss of data backups made, and only 1.3% do not use anything to protect personal information (CERT 2012). In order to reduce the security risks and eliminate them the IT risk identification process is vital as it leads to qualified IT audit.

There are many techniques and methodologies for risk identification. Their diversity and a wide selection make it possible for any organization to carry out its risk identification and convenient manner acceptable method. Most of the current approaches require considerable investments of time and resources, and demand high levels of technical expertise (Tawileh *et al.* 2007). In order to maintain good quality of IT risk management and ensure the company's information security, the best way is to do – address this task for experts, because it requires a lot of knowledge and expertise. However, small and medium-sized businesses can't devote sufficient resources to carry out specific risk management and control, where IT infrastructure that is more simple and straightforward in comparison to the large companies. So, it is recommended for SME to do own IT risk identification, with the assistance of all employees directly and indirectly related to information technology and the operations. Continuously monitor the emergence of new risks, promotes continuous development in technology, innovation occurrence rate, just as viruses are spread more subtle and faster. It is important to highlight, that risk-assessment process is iterative and should be repeated every three years at least. Changes in the identification of threats, in the rollout of new technologies, and the identification of new threats may have dramatically shifted the organizational security focus (Whitman 2003). Before assessment, the analyst must understand the business process and its functions (Munteanu 2006), the devices and tools used in order to achieve organization mission and goals. For this purpose detailed all systems involved in the company's activity and then they are divided into components. Main components of IT identification process for SME presented at Fig. 1. IT risk identification process steps were determined after analysis (Bowen *et al.* 2006; Elky 2006; Gregg 2007; Munteanu 2006; Sacmann 2008; Stoneburner *et al.* 2004; VITA 2006):

1. Asset identification / IT system characteristic;
2. Potential threats identification:
3. Vulnerabilities identification;
4. Relating threats to vulnerabilities – IT risk identification.

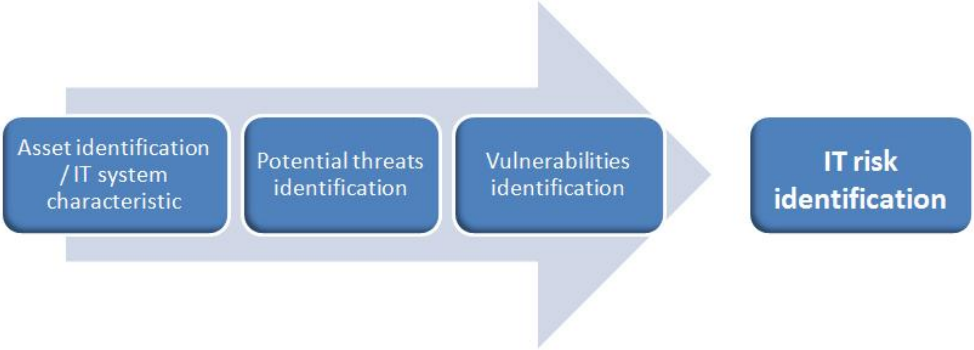
Asset identification / IT system characteristic
Potential threats identification
Vulnerabilities identification
IT risk identification

Fig. 1. Model of IT risk identification process (Source: created by authors)

Separately analysis of each component, help to understand their purpose, characteristics, requirements for proper use, while at the same time and in deviations from the efficient use of energy and resources loss. The next step is identification of threats for each IT element. The analysis of threats provides what may happen, while vulnerability refers to how this can happen, this is what the weak point would be used for threat realization. A threat coupled with vulnerability can lead to a loss. Each step is critical to the next, because the one-step error is passed on to another step, then the next coming next, and the result will be inaccurate.

4. Conclusions

IT risks become more and more complex nowadays and much more attention for IT risk identification and management should be paid in science and practice.

Effective risk identification leads to successful risk management, which is an integral part of an effective IT systems and organizations security. Enterprises use information technologies to support business processes, reputation, and increase the competitive advantage of financial value. For business and financial stability, it is necessary to protect the property, it is critically important to ensure the enterprise data, information security. Therefore, based on the three main aspects of security, seek to prevent emerging risks.

IT risk identification process, which were determined enables further research which will be oriented to IT risk management model for SME formation.

References

Bowen, P.; Hash, J.; Wilson, M. 2006. Information Security Handbook: A Guide for Managers, *NIST Special Publication 800-100.*

CERT 2011 m. CERT-LT incidentų statistika [online] [accessed 22 August 2012]. Available from Internet: <https://www.cert.lt/statistika.html>.

Davidavičienė, V. 2008. Change management decisions in the information age, *Journal of Business Economics and Management* 9(4): 299–307. http://dx.doi.org/10.3846/1611-1699.2008.9.299-307

Davidavičienė, V.; Janeliūnienė, R.; Liberytė, G. 2011. IT audit possibilities in Lithuanian SME companies, in *Management and Engineering'11: IX International Scientific Conference*, June 19-22, 2011 Sozopol, Bulgaria: conference proceedings of the Scientific-Technical Union of Mechanical Engineering. Vol. 1 Sofia: Technical University, 2(122): 129–138. ISSN 1310-3946.

Elky, S, 2006. An Introduction to Information System Risk Management, *SANS Institute InfoSec Reading Room* [online] [accessed 10 August 2012]. Available from Internet :< http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204 >.

Elskytė, V.; Raudeliūnienė, J. 2006. ITT plėtros sąlygotų verslo pokyčių vadyba. *Organizacijų vadyba: sisteminiai tyrimai* 38, 53-66 p. ISSN: 1392–1142.

ESRMO 2011. Risk Management Guide [online] [accessed 20 August 2012]. Available from Internet: <http://www.esrmo.scio.nc.gov/riskManagement/default.aspx>.

Fratila, L.; Tantau, A., 2008. Aspects of IT Rsk Management for a company, in *International Scientific Conference "European Integration – New Challenges for the Romanian Economy", 4th Edition.* Orade, Romania 30 – 31 May 2008. Tom XVII 2008 – Volume II – Section: Economy and business administration. 163-168. ISSN – 1582–5450.

Gao, G.; Li, X.; Zhang B.; Xiao, W. 2011. Information Security Risk Assessment Based on Information Measure and Fuzzy Clustering, in *Journal of Software* 6(11): 2159–2166

Ginevičius, R.; Bivainis, J.; Melnikas, B.; Paliulis, N., Rutkauskas, A.V.; Staškevičius, J.A.; Pabedinskaitė, A.; Šečkutė, L.; Tamošiūnas, A. 2005. *Šiuolaikinis verslas: tobulinimo prioritetai*: Kolektyvinė monografija. Vilnius: Technika. 448 p. ISBN 9986-05-832-5.

Ginevičius, R.; Paliulis, N.K.; Chlivickas, E.; Merkevičius, J. 2006. *XXI amžiaus iššūkiai: organizacijų ir visuomenės pokyčiai:* Monografija. Vilnius: Technika. 548 p. ISBN 9955280573.

Gregg, M. 2007. CISA Exam Prep. Publisher: Pearson Certification. Print ISBN-10: 0-7897-3573-3, Print ISBN-13: 978-0-7897-3573-7. Pages 600.

ISACA 2002. *IS Auditing Procedure: P1 IS Risk Assessment Measurement* [online], [accessed 08 July 2012]. Available from Internet: < http://www.isaca.org/Knowledge-Center/Standards/Pages/IS-Auditing-Procedure-P1-IS-Risk-Assessment-Measurement1.aspx>.

ISACA 2009. RiskIT Brochure [online] [accessed 10 September 2012]. Available from Internet <http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx>.

LR statistikos departamentas, 2011. Informacinės technologijos Lietuvoje [online] [accessed 13 January 2011]. Available from internet: <http://www.stat.gov.lt/lt/catalog/pages_list/?id=1125>.

Munteanu, A. 2006. Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma, in Managing Information in the Digital Economy: Issues & Solution - Proceedings of the 6th International Business Information Management Association (IBIMA) Conference, 227–232.

PandaLabs. 2012. *Quarterly Report April – June 2012* [online], [accessed 10 September 2012]. Available from Internet: < http://press.pandasecurity.com/press-room/reports/>.

Sackmann, S., 2008. A Reference Model for Process-Oriented IT Risk Management, in *Proceedings of ECIS 2008*. p. 246. [online], [accessed 1 April 2012]. Available from Internet: <http://aisel.aisnet.org/ecis2008/246>.

Savić, A. 2008. Managing IT-Related Operational Risks, in Economic annals 53(176): 88–109. doi: 10.2298/EKA08760885

Smith, H.A; McKeen J.D. 2009. A Holistic Approach to Managing IT-based Risk, in *Communications of the Association for Information Systems*, Vol. 25, article 41. pp. 519–530.

Stoneburner, G.; Hayden, C.; Feringa, A. 2004. Engineering Principles for Information Technology Security, *NIST Special Publication 800-27 Rev A* June 2004.

Symantec Corporation 2007. IT Risk Management Report. [online] [accessed 22 August 2012] Available from Internet: <http://eval.symantec.com/mktginfo/enterprise/other_resources/ent-it_risk_management_report_02-2007.en-us.pdf>.

Symantec Corporation 2008. IT Risk Management Report 2: Myths and Realities, Volume 2 [online] [accessed 22 August 2012]. Available from Intenet: <http://eval.symantec.com/mktginfo/enterprise/other_resources/b-it_risk_management_report_2_01-2008_12818026.en-us.pdf >.

Tawileh, A.; Hilton, J.; McIntosh, S. 2007. Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. In *ISSE/SECURE 2007 Securing Electronic Business Processes*, 4: 331–339. http://dx.doi.org/10.1007/978-3-8348-9418-2_35

Taylor, D.; Glezen, G. 1988. *Auditing: Integrated Concepts and Procedures*. 4th Editon. New York: John Wiley & Sons. 845 p. ISBN-10: 0471856517.

Tchankova, L. 2002. Risk identification – basic stage in risk management, in *Enviromental Management and Health* 13(3): 290–297. http://dx.doi.org/10.1108/09566160210431088

Teilans, A.; Romanovs, A.; Merkuryev, Y.; Kleins, A.; Dorogovs, P.; Krasts, O. 2011. Functional modelling of IT risk assessment support system, *Economics and Management*, Nr. 16: 1061–1068. ISSN 1822-6515.

VITA 2006. Information Technology Risk Management Guideline, *ITRM Guideline SEC506-01, Appendix D – Risk Management Guideline Assessment Instructions* [online] [accessed 25 August 2012]. Available from Internet: <http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/unmanaged/library/RiskManagementGuideline.pdf>.

Westerman, G.; Hunter, R. 2007. *IT Risk. Turning Business Threats into Competitive Advantage*, Harvard Business School Press. 221 p. ISBN-10: 1422106667.

Withman, M.E. 2003. Enemy at the gate: threats to information security, in *Communications of the ACM* 46(8): 91–95. http://dx.doi.org/10.1145/859670.859675

Vida DAVIDAVIČIENĖ. Associate Professor at the Department of Business Technologies, Faculty of Business Management, Vilnius Gediminas Technical University. Research interests: e. business, e. marketing, business changes caused by ICT development, ICT in knowledge management.

Rasma JANELIŪNIENĖ. Master of Information technologies, Assistant at the Department of Information Technologies, Faculty of Fundamental Science, Vilnius Gediminas Technical University. Research interests: IT in business and public sector, IT audits.