Editors

Damir Boras

Nives Mikelic Preradovic

Francisco Moya

Mohamed Roushdy

Abdel-Badeeh M. Salem

Associate Editor

Nadja Damij

Recent Advances in Information Science

Proceedings of the 7th European Computing Conference (ECC '13)

Dubrovnik, Croatia, June 25-27, 2013

Scientific Sponsors

Recent Advances in Computer Engineering Series | 13

Recent Advances in Information Science

RECENT ADVANCES in INFORMATION SCIENCE

Proceedings of the 7th European Computing Conference (ECC '13)

Dubrovnik, Croatia
June 25-27, 2013

Scientific Sponsors:

University of Dubrovnik

Ain Shams University

University of Zagreb

Sarajevo School of Science and Technology

Recent Advances in Computer Engineering Series | 13

ISSN: 1790-5109
ISBN: 978-960-474-304-9

RECENT ADVANCES in INFORMATION SCIENCE

Proceedings of the 7th European Computing Conference (ECC '13)

Dubrovnik, Croatia
June 25-27, 2013

Published by WSEAS Press
www.wseas.org

All papers of the present volume were peer reviewed by no less that two independent reviewers. Acceptance was granted when both reviewers' recommendations were positive.
See also: http://www.worldses.org/review/index.html

ISSN: 1790-5109
ISBN: 978-960-474-304-9

Role of Managers in Safety Risk Management in Integration Information Systems

LJERKA LUIĆ
Faculty of Humanities and Social Sciences
University of Zagreb
Ivana Lučića 3, 10000 Zagreb
CROATIA
Karlovac University of Applied Sciences
Trg J.J. Strossmayera 9, Karlovac
CROATIA
ljerka.luic@b4b.hr, ljerka.luic@vuka.hr

Abstract: - Today, almost all organisations create and use in their business electronic data and documents which are created both within and outside the organisation. A vast quantity of information which is thus being used and replaced may be processed in a timely and quality way only by integrated information systems (IIS) by fulfilling three basic safety requirements: confidentiality, integrity and availability. Various risks may impact and do impact the fact that information system is not always safe. While at the beginning of development of IT systems, safety was taken care of only by IT experts, today the efficient protection of IIS systems is unthinkable without the active role of top managers of all profiles. A thesis expanded in this paper is that the efficient management of safety risks is proportional to the amount of active participation of top management in the process of implementing safety, indicating that knowledge of information safety is an unavoidable component of manger's knowledge.

Key-Words: - information safety, integrated information system, top management, safety risks

1 Introduction

In today's business environment, information-communication technologies (ICT) play a significant role, and integrated information systems (IIS) become crucial for business success, therefore it is important to consider all safety risks which may impact their safety and consistency. Some of these risks may be partially prevented by preventive activities so that they do not appear, some may be only partially impacted, while the appearance of other risks such as natural disasters are often out of human control. Whatever the way in which these risks appear, the damage they can create to IIS system of one or more networked organisations can have a large negative impact on their business.

Information safety implies the state of confidentiality, integrity and availability of data created and/or used in electronic form, and which is achieved by applying specified norms on information safety, and organisational support for planning, implementation, verification and processing of these norms. In this paper, information safety has been considered from the point of view of concentric circles in which the central circle is made of risks which directly impact electronic data, then there are circles in which risks are viewed from the point of view of disruption of integrity of data, while the outer circle is based on risks significant for operative business running of an organisation and the role of top management in the process of its management.

What are the ways in which safety of IIS system may be threatened, how to protect it and what top managers in an organisation are to know in order to actively participate in the process of management of safety risks – were crucial questions in the process of defining research problems and setting a hypothesis that the efficient management of safety risks is proportional to the amount of active participation of top management in the process of implementing protection. Results of descriptive analysis of relevant sources indicate that the importance of knowledge on information safety is an unavoidable component of manager's knowledge, and indicates further implementation of research aimed at detecting metrics relevant for the evaluation of maturity of top managers as holders of management of risk safety in integrated information systems.

ISBN: 978-960-474-304-9

2 Safety risks in IIS systems

At the time of global businesses that we witness, more than ever in business history, by having timely knowledge of information, people become more successful in their work and their creativity, it prevents accidents, bad solutions and bad decision, it neutralises mistakes, and decreases the impact of unforeseen situations. The value of accurate and timely information may be measured as gold, both figuratively and literally, and increasingly becomes a means of trade. As soon as a piece of information has obtained sufficient value, it has become a target of theft, forgery, and by further development of ICT technologies and IIS systems, it has become a basis for market combat regardless of the field of business. Due to all of the above, it is necessary to consider all aspects of safety risks in the context of information safety of IIS systems with the goal to make them maximally protected, and business transactions of an organisation unquestionable.

The safety of IIS systems is based on fulfilling three basic safety requirements: (1) *confidentiality* – data and other resources may be accessed only by authorised users, (2) *integrity* – data or programmes may be modified only by authorised users, and (3) *availability* – data, programmes and other information resources must be available whenever it is requested by authorised users. IIS system which is composed of six basic parts: physical part (*hardware*), programme part (*software*), users (*lifeware*), data sources and data bases (*dataware*), communication solutions (*netware*) and organisational procedures (*orgware*) may influence differently the fulfilment or non-fulfilment of all three safety requirements [1]. Safety breakthrough may occur in any component respectively or it may impact several of them, therefore it is important to consider all sources and forms of safety threats.

2.1 Sources of threats vs. safety

Risks which may threaten the safety of IIS system have been considered from the point of view of four possible sources of threat: (1) nature, (2) by human, intentionally, (3) by human, unintentionally, (4) technical malfunction. It is unquestionable that the said risks are not equal by their destructive properties, nor by the probability of their appearance, and that there are other risks which have not been taken into consideration in the context of this paper. When determining which risk has been more destructive and whose appearance is more probable, it is important to match it with the importance of IIS for each respective organisation and in this regard, to decide what and which measures of protection are to be applied, and to secure maximum support of top management in this process.

2.1.1 Nature

Natural occurrences may cause a series of unforeseen risks that will significantly render more difficult to plan, protect and recover IIS systems within respective, as well as networked organisations. Destructive natural disasters may directly cause damage on information equipment, and they can also have a secondary effect on communication channels and threat integration links of IIS, which may additionally impact the recovery of business, and even have larger consequences from direct, primary effect of the source of threat [2].

2.1.2 By human, intentionally

Source of threat caused by human intention refers to software programmes which have been created with the goal to inflict damage or some other unwanted action on individual computers, ICT systems or IIS systems as a whole. Malicious software (*malware*) may inflict damage on critical parts of IIS system, may cause large financial damage and, what is immeasurable and the worst of all, they may shatter, and even destroy the confidence into information and business system of an organisation as a whole [3].

2.1.3 By human, unintentionally

The analysis in regard to what part of caused damage of a user was made due to the lack of knowledge, and what part of damage was caused by malicious intention - is not the object of this paper. However, we consider it is worthwhile to mention the fact that a significant part of safety risks is caused either by the lack of knowledge or by inattention, which has to be taken into account as a significant source of threat to information safety of IIS systems, and which is normally used by large number of key and end users.

2.1.4 Technical malfunction

Technical malfunction as a source of threat of information security is primarily viewed as irregularity in the work within electronic assembly or electro-mechanical components (disks, tapes) of a computer system whose reversal to a previous working condition requires a repair or a replacement of affected parts. Risk from loss of data caused by technical malfunction may occur due to several reasons, of which the most represented are

ISBN: 978-960-474-304-9

malfunctions in the work of hardware, then theft of information equipment and the destruction of a building in which hardware is located, regardless of the cause of destruction [4].

2.2 Protection

Protection of IIS system implies the application of a series of measures which secure the wanted level of functionality of integrated information system in conditions in which supposed forms of risks have appeared. Before applying any mode of protection of IIS system, the desired and possible level of protection is to be set in place, it has to be determined which parts of IIS system are critical for the organisation, what is the probability of appearance of a risk and other parameters which impact the safety. After such analysis has been made, a selection of adequate measures for the protection of IIS systems is to be made which is suitable for the organisation in question.

The analysis of relevant sources leads to the conclusion that the majority of experts for information safety has a divided opinion that the best safety protection of IIS system is an educated user. This is an additional reason for further dealing with this topic in this paper and to restate that the knowledge of information safety is to be an unavoidable component of manager's knowledge.

2.2.1 Education of users

The primary goal of education of all users of IIS systems (key and end users, both internal and external) is to be directed at awareness of the sources of threat and safety risks so that in the course of performing their working tasks, they may observe and timely and validly react; and even more so, so that those with a higher level of knowledge may personally contribute to securing information safety of an organisation. It needs to be emphasised that the term «all users» includes real users who come into contact with IIS system, regardless of whether they work in an organisation or whether they are interested third parties. Also, all users are to be familiar with possible consequences for IIS system if safety policy and safety procedures are not implemented or are implemented partially or if there is a safety incident in any way.

As previously emphasised, all levels of users are to be educated, form those who have rudimentary information literacy, to more advanced users and information experts, and to all members of top management, since their active role in the risk management has been evaluated as proportional to their participation in the said process.

3 Role of managers in safety risk management

The safety of electronic data and the protection of information systems have long been considered as an exclusive right, but also an obligation of information experts. By taking into consideration the fact that it concerns tasks which primarily require specific knowledge in the field of ICT technologies, often inaccessible to larger number of employees, other users have not been adequately trained, nor included in the said process. With the increase of the use of computers in business practice, first standards and policies relating to the safe work with computers and data stored in IT systems have began to be introduced, while the safety has ceased to be an exclusive right and obligation of information experts only.

3.1 Manager's responsibility

Modern, top managers, regardless of the field they work in, know very well that information system makes the core of a business system, and integrated information system is, so to speak, a nerve system of an organisation without whose assistance it is practically impossible to manage it. In order for ICT technologies to be applied in business, top management needs to have basic knowledge for its use and application, so that it may adequately evaluate required investments and match them for other users. By building IIS systems, the need to secure their safety increases. Safety risks become ever more important and security incidents have a growing impact on business results. All of the above requires an increased level of information safety which implies further investment and of which the decision is made by top management of an organisation. IIS systems require significant investment, enable organisations to increase their profits and competitive advantage, while at the same time, it is not certain if there will be any return of invested funds. They are also burdened with project management of which the application of ICT technology is only a part. Most frequently, planning to build IIS systems leaves little margins for unforeseen expenditures so that each safety incident may have a very negative impact on the entire system, and therefore, it is extremely important that top management is actively involved in the entire procedure of safety risk management. It goes without saying that top management will not be able to directly implement safety protection, but it shall decide on what safety measures shall be applied, and shall approve their financing.

ISBN: 978-960-474-304-9

From the above said, it may be concluded that top management must be familiarised with all threats and risks to IIS systems, and the modes for their defence. It is however clear that this is by far not enough in order to protect IT system efficiently. Before any consideration of how to protect IIS system, each manager must be well familiarised with the system itself, must analyse business processes in the system and based on that, has to consider potential risks in order to define priorities for their removal.

3.2 Implementation costs

One of the main criteria in decision-making of top management in any organisation is the return of profits and the impact of business decisions on the stability of business. Implementing safety solutions and protection plan for IIS system has its price which decreases profits. Having this in mind, the question arises how to obtain support which is necessary for implementing protection plan and to have the top management react in an adequate way.

This particularly refers to funds that need to be allocated for the reaction plan in case of security incidents and which are not small, while doing everything that can be done and hoping that the need to spend these funds will never rise. Top management is to have a clear image in their mind that costs and implementation of safety policy are not insignificant, but it also has to be aware that in case a safety incident arises, the costs will be even larger without those safety solutions in place.

As IIS systems today have become very complex, it is practically impossible to catch up with all modifications, advancement, new possibilities and upgrades that are occurring and which impact the safety of a system. Therefore, it is important to include all members of top management so that in a relatively short time period, they may conduct a quality analysis of safety of the entire IIS system, with all its interdependences it has [5].

4 Synergy of IT and business management

In conditions when IIS systems become more important, and even a decisive part of business running, the protection from safety risks is even more important and requires a synergy approach to IT and business managers. The mere awareness of protection of IIS systems is not enough to develop successful protection.

This requires high level of knowledge and experience from various fields, and the capacity to make timely decisions. It is necessary to know the risks to which IIS system is exposed and how each of them may impact the safety of the system as a whole.

From all of the above, it is obvious that for the management of safety risks, a large amount of knowledge is required. Various studies have shown that managers, if they are included in a project from its very beginning, they will significantly contribute to its realisation, as they have a sense of control, and feel as if the project is theirs [6].

All of this confirms the initially presented hypothesis that the efficiency of a safety risk management is proportional to the amount of active participation of top management in the process of implementing protection and indicates the significance of the knowledge of information safety as an irreplaceable component of manger's knowledge.

5 Conclusion

In business world, especially today, having the right information at the right time with required knowledge to use this information means competence. The task of IIS system in business running of an organisation is that at the request of a right person at the right time, it delivers the right piece of information.

In this task, today's IIS systems use ICT capacities for processing large amounts of information in a very short period of time and displaying processed results. As a consequence, there is an increasing amount of information, even those which are vital for an organisation, that exist only in electronic form. Along with advantages that ICT application brings, there are also bad sides – and this is the increasing exposure of IIS systems to safety risks.

Defence and protection of IIS systems in previously described conditions is no longer an exclusive care of information experts, and shall continue to decrease in the future. Instead, it shall become an integral part of business plans and strategies of an organisation, an object of synergy work between IT and business managers.

The awareness of the fact that protection of information system is not a one-time task, but a continual follow-up of modifications, adjustment and perfection – requires a permanent education of all users, and notably of top management as the stability of an organisation depends on them.

ISBN: 978-960-474-304-9

6 Acknowledgements

Publication of this paper was supported by Faculty of Humanities and Social Sciences, University of Zagreb and by scientific project *Optimization and Risk Management in Information Systems* (No. 036-0361983-3137) of the Croatian Ministry of Science, Education and Sports, to which the author of the article are grateful for big support.

References:

[1] M. Spremić, *Management and e-Business*, Narodne novine, 2004, p. 28.

[2] P. Gregory, *IT Disaster Recovery Planning for Dummies*, Wiley Publishing, 2008, p. 285.

[3] OECD, *Computer Viruses and Other Malicious Software - A Threat to the Internet Economy*, OECD, 2009, p. 12.

[4] D. Cougias, *The Backup Book Disaster Recovery from Desktop to Data Center*, Schaser-Vartan Books, 2003, p. 429.

[5] P. Gregory, *IT Disaster Recovery Planning for Dummies*, Wiley Publishing, 2008, p. 52.

[6] S. Snedaker, *Business Continuity & Disaster Recovery for IT Professionals*, Syngress Publishing, 2007, p. 72