Risk Management with ISO 27000 standards in Information Security

KAJA PRISLAN, IGOR BERNIK
Faculty of Criminal Justice and Security
University of Maribor
Kotnikova 8, 1000 Ljubljana
SLOVENIA
igor.bernik@fvv.uni-mb.si  http://www.fvv.uni-mb.si

Abstract: Users need to adjust to constant changes, as do they need to manage threats to information technology. The only way of controlling the threats is executing a process of risk management which enables managing the threats. This article represents the ways of managing the threats, and researches the existence of risk management systems in practice. For this purpose, a research has been conducted among different organizations. The results of the research are revealing the problems of incomprehension of the threats. Moreover, a structure of risk management systems depends completely on each individual organization. The problem is therefore a fact that exist as many systems as organizations. The organizations choose mostly among following approaches: informal or unsystematic approach; general approach which provides the same protection mechanism for every organizational level; exact approach which refers to analysis of the entire information system; the combination of general and exact approach. When the organizations choose the approach, they establish the control mechanisms. With those mechanisms we can simply avoid the risks, mitigate the consequences, accept a particular risk, or introduce adequate security mechanisms. Due to continual changes, such system must be constantly evaluated and improved. In the process of managing the information security, it is of great significance to establish the risk management system, to be able to recognize the most exposed fields and to protect them accordingly.

Key-Words: security threats, risks, information system, management, ISO 27000, certification

1 Introduction

Information security is one of the most essential aspects of successful operation of every modern organization due to constant presence of risks by managing and leading the organization. We can compare that with human life: any human activity, irrespective of its importance, is always followed by a certain level of risk.

With adequate knowledge, time and finances, someone will do anything to disable the necessary part of security system. In era of hard competition among organizations, they are prepared to spend large volumes of finances in order to seize information material of the competitive organization. Information, gained or destroyed with breaking in security system, enables the organizations to put a product on the market before the real owner of the product. The damage can be irreparable [1]. Knowledge is therefore organization’s capital. It is necessary to treat it carefully, protect it from misuse, and share it with environment deliberately [2].

Every organization strives to achieve its aims with information system. For that reason, it is necessary for information system to operate safely and undisturbed. Stoneburner, Gougen and Feringa [3] believe that the information field is the most exposed and vulnerable spot in organizational structure. Organizations must therefore be aware of every potential threat thoroughly, otherwise, consequences can be fatal for their existence.

However, there is no perfect information protection against malicious attacks. The reason for that is a fact that the most improved security systems are threatened by more and more complicated threats. In order to protect themselves, they have to take all due precautions, from defensive to proactive approach [2]. By planning of adequate security level we have to ask ourselves: “Can information be harmful for organization and give priority to other organization, if the information is lost [1]?” If the answer is affirmative, precautions are inevitable. In order to provide adequate security level, the organization must be able to manage the threats. Managing the threats is achieved with process of risk management which contributes to relatively safe and stable operation of organization. Process of risk management depends completely on each individual organization. For that reason, exist as many ways of managing the risks as organizations. In theory, identification and evaluation of information material are necessary parts of the process of risk management [4]. What follows is finding and evaluating the threats with the help of past experiences, and identify the weaknesses of information material which could possibly be misused. Furthermore, calculating of possibilities for such attack and consequences is necessary as well. The exact system
analysis is therefore inevitable in order to find the most appropriate protection mechanisms for information system. Such analysis provides information for management. On the basis of information, the management makes decisions. The main aim is to provide balance among risks, and price for implementation of preventive and protective measures [5]. After system analysis, the organization chooses an appropriate way for managing the risks. Four basic strategies are possible [6]: (1) avoiding: use of protection which excludes and decreases the rest of uncontrolled risks, (2) transfer: transferring the risks to other areas or out of organizational existence, (3) mitigation: mitigating the damage in case of successful attack, (4) approval: understanding of consequences and admitting the risks without attempt of control or mitigation. As the system is established, it needs to be constantly checked, evaluated and improved. In order to examine system efficiency, we have to find out if the costs of introducing supervision are lower than annual costs which have appeared due to security incidents [7].

Risk management system is therefore constant and cyclic process. It is used by leadership, management and professional personnel for recognizing of weaknesses in information system, in order to provide trust, integrity and accessibility of all system’s components [6]. Even though the system’s operation is explained thoroughly in theory, its type depends on various factors, such as size of the organizations, management’s interest, qualified personnel and financial capability for establishing and keeping such system.

2 Formulation
The organizations can therefore introduce the international security standards for easier establishing of the most appropriate system for their organizational structure. The standards advices model PDCA (Plan, Do, Check, Act) for adjusting to changes. Model PDCA includes for levels: planning of change, introducing it, checking its effectiveness and reliability, and finally, acting in a way to make an improvement [8]. In process certification is of great significance management’s liability for establishing of the risk management system, recognizing critical fields and providing adequate protection. The organizations decide for the ISO 27001 or former standardization and maybe certificate in order to provide higher protection level, to improve a proficiency, credibility, and trust. Another reason can simply be a wish or requirement of business partners. Some organizations follow the standards guidelines, however, they do not decide for formal certification.

Many effective practices can make the process of managing the risks easier. In theory, the process is very exhaustive, complicated and time-consuming. The ways of establishing and leading of precautionary measures differ among the organizations due to differences and complexity of organizational and informational structures. For that reason, we decided to do an overview of the systems in different Slovenian organizations. A sample consisted of 20 organizations, from the smallest to the biggest ones. The interviews gave us information on the factors which influence the ways of protecting information systems. Furthermore, our purpose was also to discover how the companies see themselves in the sphere of constant hazards, and how those hazards influence their operation.

3 Results
The most organizations (70%) agree that good competition and success in the global market can be achieved only with quality information system which is directed to a user. Moreover, the organizations are not able to achieve worked-out goals without information system. High dependence on information technology indicates the great significance of confidential, accessible information systems.

The important part of the organizations (60%) believe that data protection represents a critical point for successful operation. It is a surprising fact that some organizations listed hardware of information system as important as well. That makes sense from the point of view of data protection and integrity. However, what disables success of organization is data protection, but only according to clear hypothesis that hardware and software provide everything for stabile, safe and effective information system.

For protecting their information asset the companies take different measures, form the simplest to the most complicated. About 70% of the companies use the basic elements of data protecting and providing information security. What bothers is a fact that the business security is on the first place. Why the protection is needed, if the damage can be prevented with taking simple measures? Here are listed some simple and inexpensive measures which are being used rarely: servers with security copies, regular filing, adequate password use, providing hardware operation, etc. Despite the belief that technical elements of information security are appropriate, the practice proves there are still many possibilities for improving information security. Improvement could be achieved with relatively low costs and reliable solutions. By additional checking we found out that some of the listed measures are taken in some companies; however,
they are not used in connection to system security, but as integrity part of the entire information system due to long-term usage of the measures. It is very positive that those measures are used at all. Namely, it indicates improvement in the field of awareness of the problems regarding to information security from the view of protection and keeping access to data sources in information systems.

The answers to the questions about the ways of keeping of critical information indicate what we have presumed before and then proved. Each company has its own way of keeping the critical information and adequate protection (security copies, double locations, filing, special servers, etc.). Even the further analysis does not indicate that companies, similar in structure and size, use the same approaches of keeping critical information.

The organizations participating in the research choose very different approaches by managing the risks in the field of information security. In general, the companies decide for only one approach (the combined approach is used by only a third of the questioned). We can therefore assume that the companies do not examine information security issues in their entirety. What also makes concerns is that 5% of the questioned organizations do not manage the risks at all.

Furthermore, an evaluation of the risk management system proves the inadequate approach too. Only 35% of the questioned organizations evaluated its system as a good one, the rest of them consider their system as weak or inadequate. What is more, among the organizations with inadequate risk management system are those whose information systems are connected to life-important components. The company’s management does not put enough effort into providing information security in its entirety. Consequently, appropriate support, solutions, and employees’ responsibility are lacking. Moreover, only a few companies execute the risk management at the level of international standards. Why? Information systems are part of the global communication and enable the global access. Therefore, the risks exist also at the global level, and executing the precautionary measures is nowadays not just a need but a necessity.

Every employee in the company should be aware of the information security issues. For establishing, operating and keeping the system are responsible technical services or external contracting parties with strong support of the management. In the questioned organizations, information security is a responsibility of technical staff which belongs to informatics department or service, to the management, or to the employees.

By dealing with threats, we should consider that the less obvious are the most dangerous. If we manage the most common threats (viruses, software errors) simply and relatively inexpensively with help of the antivirus programs, firewalls or appropriate data copying, it can still appear the biggest threat – human factor. We are mostly the main reason for threatening information system due to lack of knowledge and awareness what meaning have confidential data for business system.

Unawareness of the issues can also be seen in the case of the most critical threats because the organizations consider those only as viruses, system errors and break-ins, breakdowns and inaccessibility of system. It is therefore necessary to change the aspect of understanding information security – from the technical aspect to the “user’s” one. Namely, it is simply considered that the most harmful threats derive from the software. However, we should be aware that in modern systems, the software is activated only when the user activates it with an access to harmful websites, or unsecure opening of the harmed files, etc. Moreover, it is being forgotten that employees often uncritically transfer information into environment.

The scale of the most vulnerable information system components is not surprising, if we take into consideration the previous answers. Software is listed as the most vulnerable, than hardware, documentation and communications. Various answers and combinations of answers prove that understanding of information security differs in each company, and that this field is very wide. Awareness of system vulnerability is mostly seen from the system operation, not from the business point of view. The most important value of the business system are data from which derives all necessary knowledge for competition which takes advantage of it: the competitive companies use the lost data in the combination with their own data, and in this way gain knowledge and understanding of the issues that lacks in our business system.

A quarter of the questioned organizations are convinced of the unlikely consequences in the case of the error or loss of important information. The error or a gap in protection of information system would probably not cause death of the personnel which is responsible for information security.

The organizations listed loss of credibility among business partners and users as the biggest psychological consequence of the system breakdown. What follows are business loss, disgrace and bad mood. Credibility loss
often means also business loss. For that reason, business subjects in the case of data loss mostly does not spread that into public. It is therefore hard to evaluate real hazard state and number of already misused systems in one environment. Consequently, the threats in that environment cannot be identified, and the companies try to provide entire information security only with the awareness of their own issues. That is not only insufficient, but also expensive and demanding.

By evaluating the frequency of attacks, almost half of the questioned organizations share the opinion that the attacks on their information systems are rare; a quarter of them have not experienced the attack at all, and the rest of them are more often the targets of the attack. However, the evaluating the frequency of attacks is an issue. Namely, the companies operate based on the detected attacks, but many attacks are not detected at all. Unfortunately, undetected attacks represent the biggest threat – if you do not know the issue, you cannot solve it.

By assessment of damage caused by the attack is different. More than third of the organizations consider the damage as acceptable, the other third as irreparable, and the smallest part consider it as unnoticeable. Information security is an important part of our everyday life, and the information system security the essential aspect of organization’s operation. Unfortunately, we became aware of it only when the actual attack on information system, data loss, integrity breakdown and end of operating occur.

Most of the organizations avoid the risks as much as possible which is seen from the assessment of supervision. Transfer and easing of the risks are not used very often, and some organizations use risk approval.

In general, the companies are still not aware of the meaning of information security, and therefore do not use the mechanisms for establishing, supervising and improving of it. Only half of the questioned organizations improves their own information security system regularly, while the other half only if necessary, or not at all. Therefore, the companies are advised to begin with basic elements of information security (use of PDCA cycle), and improve it to the adequate level regarding the known risk factors.

For providing high level of information security, all users of information system must be included, the employees and external users. The employees are those who mostly warn of need for improvement, then users, information scientists, associate companies and auditors. All of them have to strive for safe information system and high level of information system security. This is of great significance especially when the companies decide to establish online business with associate companies.

The employees have many suggestions for improvement (risk management, higher local security level, regular system updates, improving communication, introducing of formal security policy, etc.), however, for the most of the measures minimal investments are necessary which are currently lacking due to the current economic crises. For this reason, it is necessary to immediately start making employees aware of the potential threats, and teach them how to deal with information carefully. This measure can be taken with minimal investment, if the management is efficient. In this way, security can improve, and instead of investing into abolition of consequences after data loss, finances can be spent for establishing of lacking security system. One of the suggestions for improving information security is also certification. In this field, ISO 27000 series of standards are the most efficient, checked and reliable. ISO 27000 series of standards are intended only for establishing of information security and leading the process of risk management.

Most of the questioned organizations (60%) consider guidelines of the ISO 27000 series of standards by providing of safe information systems, while the rest 40% do not introduce those guidelines. ISO 27000 series of standards directs the companies how to provide safe information system in the process of risk management, but it also let them a wide margin for maneuver for establishing their own security level. More organizations could follow those guidelines regarding the fact that the process of certification is not necessary. Introducing the guidelines and following them depends mostly on awareness and willpower of the employees and the leadership. Only 15% of the organizations have introduced ISO 270001 certificate which is very small part if we take into consideration seriousness of modern information threats and necessity for establishing sufficient protection. ISO 270001 certificate is intended for providing information system security, and is a sign of trust, proficiency and perfection. The introduction of the certificate does not depend on activity or size of organization, but on other important factors. One of those is definitely lack of knowledge on it advantages because it is relatively new process in Slovenian organizations. Organizations which already have ISO 270001 certificate, have introduced it in the last four years, the most of them in 2009. That means the organizations are still in learning process, therefore, increase of introducing it is probably going to occur in the following years.
The questioned organizations list a better contentment of the users, employees, leadership and business partners as the most important advantage of the ISO 270001 standard. That indicates that one of the reasons for introducing it is also a request of business partners because the formal certification means better credibility and trust. Moreover, the users probably also rather decide for certified system. Another advantage is also a possibility for organization to choose its own security level which it considers as adequate. Security level can be adjusted to organization’s activity and size, and individual fields can be protected according to their vulnerability.

The security level has increased since the ISO 270001 standard has been introduced. Actually, it would be surprising if safety would worsen or stagnate after long-lasting efforts for improving of the standard. Furthermore, after introducing the standard, business has also improved. Namely, the standard is a sign of quality and credibility, and business partners rather dice for cooperation with companies which have a guarantee for efficient and stable information system. More efficient security and more successful business are therefore the consequences of the ISO 270001 standard and its certification.

The organizations without the standard believe that the security of their system is sufficient enough, so the certification is not necessary. The other reason for not using the standard is the lack of financial means. The process of certification causes some costs; however, these are repaid during the long-term high security level. Lack of information on advantages and quality of the standard influences a decision for introducing it. Some organizations consider this standard as inappropriate for their organizational structure, or they find themselves too small for taking such high-quality measures. Another restriction by introducing the ISO 270001 standard is a lack of adequate personnel. The reasons for avoiding the standard are therefore different, and they vary form organization to organization. To sum up, a decision for introduction and certification of the standard depends on the company’s size, organizational structure and financial resources.

More than a half of the organizations without the ISO 270001 certificate believe that a decision for introducing it mostly depends on the willpower of the management. The decision of the management than depends on other factors mentioned before. The ISO 27001 standard will be introduced and certificated when the company will have enough financial resources and adequate organizational structure. Therefore, the introduction of the standard depends mostly on the willpower of the leadership which further depends on other factors in organizational structure mentioned before.

The organizations share different opinions on a necessity of the certificate in their informational structure. Almost a half of them (47%) believe they do not need it. The reasons for that are adequate safety infrastructure of information system and lack of awareness of advantages and quality of it. The rest of the organizations believe they would need the standard. Those organizations are probably more informed of benefits that such standard can bring, and they strive for more quality, more stable, more credible and safer information system.

The organizations which find such standard beneficial and necessary believe that safety would improve after an introduction of the standard. The organizations who have actually introduced the ISO 270001 standard agreed with it according to their own experiences. We can therefore see that level of awareness of benefits of certification is high. However, some other organizations find the standard as unnecessary, and are not aware of the benefits. Beside lack of information and awareness, the reason for such opinion could also be adequate or the highest possible level of information system security. However, that is less possible due to continuous changes in information environment which make difficult to follow the threats and update information system.

Most of the questioned organizations (59%) do not intend to introduce and certificate the ISO 27001 standard in the future. The reasons were already stated, however, on the first place are probably a lack of financial means and adequate safety structure. Maybe this will change in the future due to new, progressive threats. The organizations which expressed a need for the standard have to be prepared for it. They need preparations at the level of employees as well as at the level of organizational structure. In order to achieve a purpose of the standard, the entire organization’s sphere must be qualified.

4 Conclusion

Information system is a basic component of every organization, and provides a support for achieving worked-out goals. The success of organizations mostly depends on their information system. Quality of such system therefore indicates quality of organization. This fact is also proved by the research results. The results indicate that the most of the organizations cannot achieve their worked-out goals without information system. Furthermore, success of organizations depends also on successfully protected and saved data. The organizations spend most of their financial resources for
data protection. For protecting data and other material most of the organizations use standardized precautionary measures and mechanisms, while only a few of the most developed organizations take technically improved measures. Those measures do not depend on size and structure of organization, but on its needs and performance which also determine a type of information security system, the risk management, and formalizing of information security quality. The process of certification mostly depends on willpower of the leadership which makes its decision according to financial, personnel and time abilities of organization. Only a few organizations have adequate resources for formalization. However, it should be taken into consideration that from the long-term point of view formalization leads to decreasing the costs in case of security incident. Most of the organizations do not decide for formalization, and mostly use only one approach due to their relatively weak performance for providing information security.

Many organizations use a combined approach, while general and informal approach is taking the first place because they demand the least time, knowledge and financial resources. Economizing in this field has probably caused that the most organizations evaluate their information security system as weak or inadequate. However, good improvement can be done in this field, and organizations are aware of it. Unfortunately, they consider the most often and the most obvious threats as the most dangerous, which mean the organizations, are not aware of seriousness of the risk in the field of information security. Moreover, the human factor which mostly activates the threats is neglected. The consequences caused by the attack are considered as shame and credibility loss. What follows is business loss, and for that reason the organizations do not spread the amount of damage into public. Consequently, the attacks are supposedly rare, and the organizations neglect the threats that are not detected due to inadequate security level. Security system therefore detects only the most common threats which are also the least dangerous. For that reason, the organizations believe the damage caused by the threat is mostly acceptable. To conclude, inadequate security level is a reason for incomprehension and wrong images of seriousness and danger of modern threats. What could be immediately done in this field to prevent that is educating and making the employees and the users aware of it. This would lead to improvement of information security. Instead of spending financial means for repairing the damage, the finances could be spent for introducing of better security types.

References: