VARSTVOSLOVJE, Journal of Criminal Justice and Security
year 13
no. 2
pp. 208-221

Information Security in Risk Management Systems: Slovenian Perspective

Igor Bernik, Kaja Prislan

Purpose:

Modern organizations are no longer able to operate and achieve their goals without information technology. The only stability in the modern world is change, and users adjust to them, as do the threats to information technology. Therefore, the only way to control threats to information security is to execute a process of risk management, which enables organizations to manage threats. This paper introduces various ways of managing information security threats and researches the existence of risk management systems in Slovenia.

Design/Methods/Approach:

The study focused on the research of the perception of information security risk management among Slovenian organizations. For this purpose, research has been conducted in different organizations. The results of this research revealed that threats to information security are largely not fully comprehended. Moreover, the structure of risk management systems depends completely on each individual organization. The problem is therefore the fact that there are as many systems as there are organizations. In theory, any information system must be examined thoroughly before risk management systems are established. It is important to know the weaknesses of the system, possible threats to it and ways of attack, and what consequences follow.

Findings:

Risks can be managed in different ways. Organizations choose mostly among the following approaches: (1) informal or unsystematic approach; (2) general approach, which provides the same protection mechanism for every organizational level; (3) exact approach, which refers to an analysis of the entire information system; (4) a combination of a general and an exact approach. When organizations choose their approach, they establish the control mechanisms. With these mechanisms it is possible to simply avoid risks, mitigate their consequences, accept a particular risk, or introduce adequate security mechanisms. Due to continual changes such systems must be constantly evaluated and improved. This means that systems must be constantly adjusted to new types of threats. By establishing a safe information system, organizations can consider different trends, recommendations and effective practices; for instance the ISO 27000 series of standards. In the process of managing information security, it is of great significance to establish a risk

management system, to be able to recognize the most exposed areas, and to protect them accordingly.

Research limitations/implications:

Research results cannot be generalized due to the relatively small number of companies interviewed.

Practical implications:

This paper represents a useful source of information for companies establishing information security risk management systems, and it represents the basis for further research.

Originality/Value:

Guidelines for establishing a secure information system and forms conclusions on how these guidelines are considered in practice are represented. The study has original value because it is based on a research of the current state of risk management procedures in different organizations. Organizations can consider different guidelines, recommendations and good practices for establishing their own effective information security. Findings show that defining management responsibility, identifying key vulnerabilities and securing them, are the three most significant elements in effective risk management and maintenance of information security.

UDC: 004.056(497.4)

Keywords: information system, management, security threats, risks, risk management, changes, Slovenia

Upravljanje tveganj v informacijski varnosti: pogledi Slovenije

Namen prispevka:

V sodobnem času organizacije ne morejo optimalno funkcionirati in dosegati zastavljenih ciljev brez informacijske tehnologije. Edina stalnica so spremembe, katerim se poleg uporabnikov prilagajajo tudi grožnje v informacijskem okolju. Iz tega sledi, da je vodenje procesa upravljanja s tveganji edini način obvladovanja in upravljanja omenjenih groženj. Predstavljamo načine in naravo upravljanja informacijske varnosti ter prikazujemo trenutno stanje omenjenih procesov v slovenskem prostoru.

Metode:

Prispevek se osredotoča na razumevanje informacijske varnosti in z njo povezanega sistema upravljanja s tveganji med slovenskimi organizacijami. V ta namen je bila izpeljana raziskava z usmerjenimi intervjuji v različnih slovenskih podjetjih. Rezultati kažejo, da grožnje informacijski varnosti v večini organizacij niso ustrezno razumljene, poleg tega pa je proces upravljanja s tveganji preveč odvisen od posamezne organizacije. Problem se kaže v tem, da poznamo toliko sistemov upravljanj s tveganji, kolikor imamo organizacij. Teoretično pa bi vsak informacijski sistem moral biti podvržen natančni analizi, preden se sistem upravljanja s tveganji vzpostavi in vpelje v organizacijsko strukturo. Poznavanje

organizacijskih ranljivosti, potencialnih groženj in posledic, ki bi ob njihovem uresničenju nastale, pa je pri tem ključnega pomena.

Ugotovitve:

S tveganji lahko upravljamo na različne načine, organizacije pa lahko v grobem izbirajo med štirimi različnimi pristopi: (1) neformalen ali nesistematičen pristop, (2) splošen pristop, s katerim se vzpostavlja enaka zaščita na različnih organizacijskih ravneh, (3) natančna analiza celotnega informacijskega premoženja, (4) kombinacija splošnega in natančnega pristopa. Ko organizacija izbere enega izmed pristopov mora vzpostaviti ustrezne kontrolne oz. zaščitne mehanizme, s katerimi se lahko tveganjem preprosto izogne, prenaša posledice na druga okolja, grožnje sprejema ali pa vpelje ustrezno stopnjo zaščite. Zaradi nenehnih sprememb, predvsem v informacijskem okolju, pa je potrebno vpeljane nadzorne mehanizme stalno ocenjevati in posodabljati, kar pomeni, da ga je potrebno nenehno prilagajati novim tipom groženj. Pri vzpostavljanju ustreznega in varnega informacijskega sistema si lahko organizacije pomagajo z različnimi priporočili in dobrimi praksami, med katere vsekakor uvrščamo serijo standardov ISO 27000. V procesu upravljanja s tveganji je ključnega pomena vzpostavitev sistema, ki je sposoben identificirati grožnjam najbolj izpostavljena območja in jih tudi ustrezno zavarovati.

Omejitve/uporabnost raziskave:

Rezultatov raziskave ne moremo posploševati, saj je število organizacij vključenih v raziskavo relativno majhno.

Praktična uporabnost:

Prispevek predstavlja uporaben vir informacij za podjetja, ki vzpostavljajo sisteme upravljanja z informacijsko varnostjo, prav tako pa predstavlja osnovo za nadaljnje raziskave.

Izvirnost/pomembnost prispevka:

Predstavljene so smernice pri vzpostavljanju sistema informacijske varnosti in ugotovitve, kako so te smernice uporabljene v praksi. Prispevek ima izvirno vrednost, ker je osnovan na raziskavi trenutnega stanja procesov upravljanja s tveganji v različnih organizacijah. Le-te lahko pri vpeljevanju učinkovite informacijske varnosti upoštevajo različne smernice, priporočila in uspešne prakse. Rezultati raziskave kažejo, da so razumevanje odgovornosti managementa, prepoznavanje ključnih ranljivosti in zaščita le-teh trije najpomembnejši elementi pri učinkovitem upravljanju s tveganji in vzdrževanju informacijske varnosti.

UDK: 004.056(497.4)

Ključne besede: informacijski sistem, management, varnostne grožnje, tveganja, spremembe upravljanja s tveganji, Slovenija

1 INTRODUCTION

In an era of hard competition organizations are prepared to spend large sums of money in order to get to data pertaining to competitive organization. Information, gained or destroyed by breaking into security systems, enables organizations to put a product on the market before the real owner of the product does. The damage

can be irreparable (Robinson, 1999). Knowledge is an asset, a part of the capital of an organization, therefore it is necessary to treat it carefully, protect it from misuse, and share it with the environment only under controlled circumstances (Podbregar, 2008).

Information security is one of the most essential aspects of successful operation of every modern organization. We can compare this with human life: a certain level of risk is always attached to any human activity, irrespective of its importance. In the digital era every organization strives to achieve its goals with the use of information systems. For this reason it is necessary for information systems to operate safely and undisturbed. Stoneburner, Gougen, and Feringa (2002) believe that the information field is the most exposed and vulnerable spot in an organizational structure. Organizations must therefore be thoroughly aware of every potential threat, otherwise consequences can be fatal to their existence.

2 DEFINITION AND PERCEPTION OF INFORMATION SECURITY RISK MANAGEMENT

There is no perfect protection against malicious attacks on data and information. The reason for this is the fact that even the most advanced security systems are targeted by more and more complicated threats. In order to protect themselves, organizations have to take all due precautions – their approach must be defensive and proactive (Podbregar, 2008). While planning an adequate level of security we have to ask ourselves: "Can lost information harm our organization and give our competitors an advantage?" (Robinson, 1999). If the answer is affirmative, precautions are inevitable. In order to provide an adequate level of security, an organization has to be able to manage a combination of threats. Managing information threats is achieved through a process of risk management that enables an organization to have relatively safe and stable operating conditions. The process of risk management depends completely on each individual organization. That is why there are as many ways of managing risks as there are organizations. There are four different approaches possible:

1. informal or technical approach without systematic/structural methods;
2. general approach, which refers to a choice of standardized protection mechanisms for every part of the information system;
3. exact analysis, which consists of identification and evaluation of information material, threats and their level of danger;
4. combined approach, which provides an exact analysis for the most exposed parts/systems, and a basic analysis for less vulnerable parts.

The fourth approach is the most useful (Trček, 2006). In theory, identification and evaluation of information material are necessary parts of the process of risk management. What follows is uncovering and evaluating threats with the help of past experiences, and identifying the weaknesses of information material, which could eventually be misused. Furthermore, calculating of the possibility of such an attack, and its consequences, are also necessary. An exact system analysis is therefore

inevitable in order to find the most appropriate mechanisms of protection for the information system. Such an analysis provides information for the management. The management makes decisions based on provided information. The main goal is to achieve a balance among risks and costs, which arise due to the implementation of preventive and protective measures (Sennewald, 2003). After analyzing the system, the organization chooses the most appropriate way for managing risks. Four basic strategies are possible (Whitman and Mattord, 2008):

1. avoidance: use of protection which excludes and decreases the remainder of uncontrolled risks;
2. transfer: transferring the risks to other areas or out of organizational existence;
3. mitigation: mitigating the damage in case of a successful attack;
4. approval: understanding consequences and admitting the risks without attempting 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 appear due to security incidents (Pfleeger, 1989).

The risk management system is a constant and cyclic process. It is used by leaders, managers and professional personnel to recognize the weaknesses in their information system, in order to ensure trust, integrity and accessibility of all components of the system (Whitman & Mattord, 2008). Even though the system's operation is explained thoroughly in theory, its type depends on various factors, such as the size of the organization, the interests of the management, how qualified the personnel is, and whether the organization is financially capable to establishing and maintaining such a system.

Organizations can introduce the ISO 27001 standard to aid them in designing a system that is the most appropriate for their organizational structure. The ISO 27001 standard is a means of providing information security. Organizations can also opt for a certificate which proves their perfection, proficiency and trust. This certificate recommends that the model PDCA (Plan, Do, Check, Act) should be used for adjusting to changes. The model PDCA includes four levels:

1. planning changes;
2. introducing changes;
3. checking effectiveness and reliability; and finally,
4. acting in ways to achieve improvement (Tague, 2004).

In the process of certification the management's liability for implementing a system of risk management, for recognizing critical areas, and providing adequate protection, is of great importance. The guidelines of the ISO 27002 standard (ISO 27000 Directory) can be useful when it comes to choosing the right mechanisms of protection. However, the guidelines of the ISO 27005 standard are more useful when an overview of the risk management system and exact system analysis is in question. Organizations choose the ISO 27001 certificate in order to provide higher levels of protection, to be more proficient, have greater credibility, and inspire

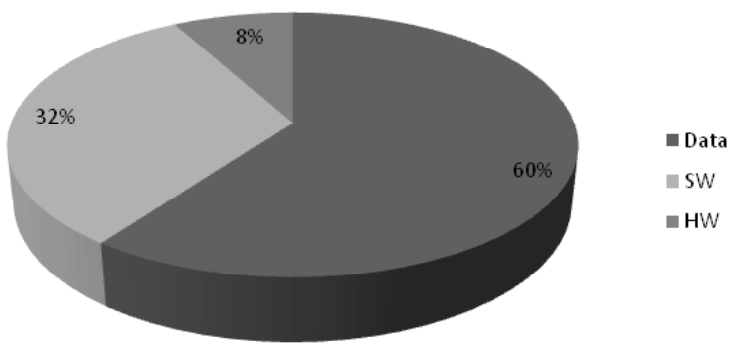
trust. Another reason, why organizations opt for the standard is that their business partners wish they did so. Some organizations follow the guidelines, even though they do not decide to acquire a certificate.

Many effective practices can make the process of managing risks easier. In theory, this process is very exhaustive, complicated and time-consuming. How organizations establish and oversee precautionary measures differs due to differences in (and the complexity of) organizational and informational structures. Our purpose was to discover how companies see themselves in a constantly hazardous environment, and how various threats influence their operation.

3 THE UNDERSTANDING OF INFORMATION SECURITY RISK MANAGEMENT

For the purposes of this study we performed in-depth interviews in 18 Slovenian organizations from different segments of the economy (a wide mix of companies from the private and public sector), which had from 15 to 50 employees (middle-sized companies in Slovenia). The study was carried out in the second part of 2010.

The majority of organizations included in the study (72.2 %) agreed that good competition and success in the global market can be achieved only with an information system of the best quality, which is directed towards the user. Moreover, organizations are not able to achieve their goals without an information system. Other organizations share the opinion that their information system represents an important part of their corporate structure, but that it is not essential for their operations. High dependence on information technology indicates the great significance of confidential, accessible information systems.



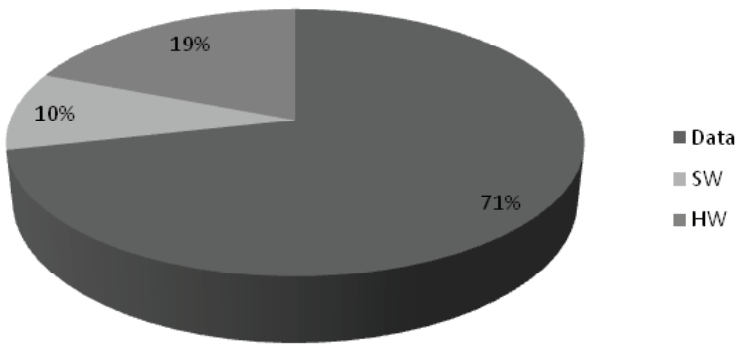
Graph 1: Information is the most important asset for corporate success.

A significant number of organizations (60 %) believe that data protection represents a critical point in successful operation. It is also surprising that some organizations responded that just hardware was important. That makes sense from the point of view of data protection and integrity. However, what really hinders

the success of an organization is data, but only according to a clear hypothesis that hardware and software provide everything needed for a stable, safe and effective information system.

Other problems, which affect success, are the ability to protect the most important elements, and oversee related costs. The highest operational and renewal costs appear at the data level. Why? After an attack, hardware and software can be replaced relatively quickly, but lost data, its retrieval, and other unexpected problems can lead to circumstances which hinder successful business operations. Data protection is the most difficult and expensive feat.

Graph 2: The most expensive IT assets to protect.



To protect their information assets companies take different measures, from the simplest to the most complicated. About 70 % of companies use the basic elements of data protection and information security. What is bothering is the fact that business insurance is in the first place. Why is protection needed, if damage can be prevented by taking such simple measures? The organizations in our study 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 these technical elements of information security are appropriate, this practice proves that there are still many other possibilities for improving information security. Improvement could be achieved at a relatively low cost, but with reliable solutions.

The answer to the question how to protect critical information, indicate, what we had presumed at the beginning of the study, and later proved. Each company has its own way of storing and protecting its critical information (e. g. security copies, double locations, filing, special servers, etc.). Even further analysis did not indicate that companies, similar in structure and size, use the same methods of storing critical information. The organizations in our study use basic and well-known protective measures dating from the time when information security issues were not so urgent: passwords, security copies, etc. Data protection with modern techniques and higher standards are used by 28 % of companies (continuous operating policy, SSL, TLS, digital certificate, etc).

How insufficient their risk management systems were, came to light through self- evaluation, made by the companies in our study. Only 35 % of the questioned

organizations evaluated their system as being good, the rest of them consider their system as being weak or inadequate. What is even more interesting is that, among the organizations with an inadequate risk management system, there are those whose information systems are connected to vitally important components. The management in these companies 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 risk management at the level of international standards. Why is this important? Information systems are part of global communications and enable global access. This means that risks also exist at the global level, and executing precautionary measures is nowadays no longer an option, but a necessity.

Every employee should be aware of information security issues. Technical services or external contracting parties, with strong support from the management, are the ones directly responsible for establishing and maintaining a company's information system. In the organizations, which were included in our study, information security is the responsibility of their technical staff, which are part of an IT department or service, the management, or the employee pool. When dealing with threats, it should be considered that the less obvious are the most dangerous. If the most common threats (viruses, software errors, etc.) can be managed simply and relatively inexpensively with the help of antivirus programs, firewalls, or appropriate data copying, there is still the biggest threat of all – the human factor. Users are most often the main threat to information systems due to their lack of knowledge and awareness of how important data confidentiality is for any corporation or organization. Unawareness of these issues is also evident in the most critical cases, because organizations consider that the worst threats are: viruses, system errors, break-ins, breakdowns, and temporary inaccessibility of the system. It is therefore necessary to change the perception of information security – from the technical aspect to the user's point of view.

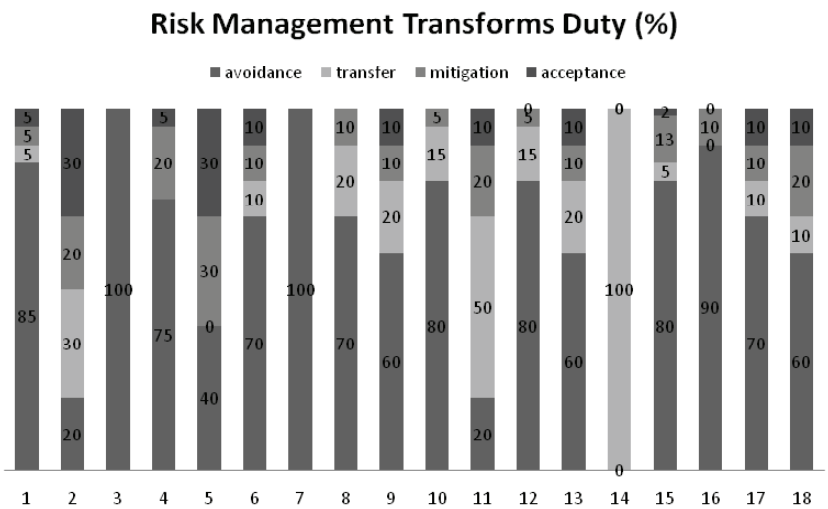
The scale of the most vulnerable information system elements is not surprising, if we take into consideration the previous answers. Software is listed as the most vulnerable element, followed by hardware, documentation and communications. Various answers and combinations of answers prove that the understanding of information security differs from company to company, and that this field is very wide. Awareness of system vulnerability is mostly limited to the system's operability, not from the business point of view. The most important asset of any business system is data which is the source of all knowledge necessary to aide the corporation's strategic fight against competitors. If data is lost, it is in effect transferred to the competition, which can take advantage of it: the competitor uses the data gained though someone's loss in combination with their own data, and thus gains knowledge and understanding of certain issues that were missing in their business system.

The organizations involved in this study listed loss of credibility among business partners and users as the biggest psychological consequence of a system breakdown. What follows are business loss, disgrace and bad feelings. Loss of credibility often also means loss of business. For that reason, corporations rarely publicly announce that they've experienced loss of data. It is therefore hard to

evaluate the risk factor and number of already misused systems in an environment. Consequently, the threats in the environment cannot be detected. Companies try to provide complete information security only when they are aware of their own security risk issues. That is not only insufficient, but also expensive and demanding.

When organizations were asked to evaluate the frequency of attacks, about half of them expressed the opinion that attacks on their information systems were rare; a quarter of them have not experienced any attack (or they just did not register); the remainder of them confirmed they were often the targets of attacks. However, evaluating the frequency of attacks is a problem in its self. Namely, the companies operate based on detected attacks, but many attacks are not detected at all. Unfortunately, undetected attacks represent the biggest threat – if you do not know of a problem, you cannot solve it. The companies most often list those attacks, which are the easiest to detect. However, regularly checking how the system operates, controlling unwanted data, and other hard to detect attacks were not mentioned. About a third of the organizations consider the damage resulting from an attack as acceptable, the other third as irreparable, a minority of them consider it as unnoticeable. Information security is an important part of our everyday life; information system security is the key factor of an organization's operation. Unfortunately, we became aware of it only when an actual attack on the information system occurs, e. g. when we lose data, or experience an integrity breach and an operational breakdown. Most organizations avoid risks as much as possible. This is obvious from their assessment of supervision. Deflection and mitigation of risks are not used very often, some organizations rather use risk approval.

Graph 3: Risk management transforms duty to match desired risk reduction.



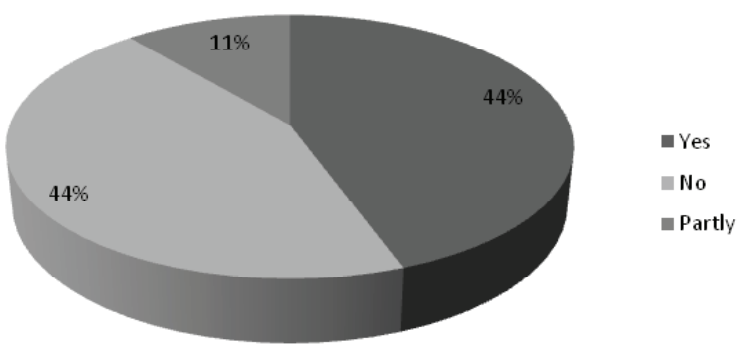
In general, companies are still not aware of the importance of information security, and therefore do not use the mechanisms to establish, supervise and

constantly improve it. Only half of the questioned organizations regularly improve their own information security systems, while the other half do so only, if necessary, or not at all. Therefore, companies are advised to begin with basic elements of information security (e. g. use of the PDCA cycle), and improve it up to the adequate level in regard to known risk factors.

To guarantee a high level of information security, all users of the information system must be included. They all have to strive to achieve the highest possible level of information system security. This is of great significance especially when a company decides to carry out business transactions with associated companies online. Employees usually have many suggestions for improvements (risk management, higher level of local security, regular system updates, improvement of communications, introduction of formal security policies, etc.), however minimal investments are necessary for the implementation of most measures. Investments are currently at a minimal level due to the financial crisis. For this reason, it is necessary to immediately start educating employees about potential threats, and teach them how to deal with information carefully. This can be done without a big investment, if management is efficient. This way security can improve, and funds can be channelled towards establishing a secure system instead of covering the costs generated by loss of data.

4 ISO 27000 – RISK MANAGEMENT BY STANDARD

One of the suggestions for improving information security is certification. In this regard, the ISO 27000 series of standards is the most efficient, checked and reliable. The ISO 27000 series of standards is intended for establishing information security and leading the process of risk management.



Graph 4: ISO27K guidelines accepted by company?

About 60 % of the questioned organizations consider guidelines of the ISO 27000 series of standards as a platform for maintaining safe information systems, while the remaining 40 % do not adhere to these guidelines. The ISO 27000 series of standards direct companies how to provide safe information systems in the process of risk management, but it also leaves them a wide margin for manoeuvring

and establishing their own level of security. More organizations could follow standard guidelines, even though certification is not compulsory. Introducing these guidelines and following them depends mostly on the awareness and willpower of the employees and their leadership. Only 15 % of the organizations, which were involved in our study, have acquired the ISO 270001 certificate. This is a relatively small part, if we take into consideration the seriousness of modern information threats and the necessity for providing sufficient protection. The ISO 270001 certificate is intended for providing information system security; it is thus a sign of trust, proficiency and perfection. The introduction of the certificate does not depend on the activities or size of an organization, but on other important factors. One of these factors is definitely a lack of knowledge about the advantages of the ISO standard; this is so, because it is still a process that is relatively new to Slovenian organizations.

Organizations that already have the ISO 270001 certificate, introduced it in the last four years, most of them in 2009. This means that organizations are still in the process of learning, and more of them will opt for the standard in the coming years.

The organizations questioned in the course of the study listed that contentment felt by users, employees, managers and business partners was the most important advantage of the ISO 270001 standard. This indicates that one of the reasons for introducing the standard is also that it is requested by business partners, because the formal certification means better credibility and trust. Even the users would probably rather see that the system is certified. Another advantage is the possibility that an organization can choose its own security level, a level, which it considers as adequate. The security level can be adjusted to an organization's activity and size, and individual segments 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 worsened or stagnated after long-lasting efforts to improve the standard.

Furthermore, after introducing the standard, business has also improved. The standard is a sign of quality and credibility, and business partners prefer to cooperate with companies, which can guarantee an efficient and stable information system. Better information security and successful business are therefore the direct consequences of the ISO 270001 standard and its certification.

Organizations without the standard (78 %) believe that the security of their system is adequate, so certification is not necessary. The other reason for not using the standard is the lack of financial means (true for 43 % of organizations without the ISO 27001). The process of certification generates some costs; however, these are repaid during the long-term high security level. Lack of information about the advantages and quality of the standard influences the decision whether to introducing it or not. Some organizations consider this standard to be inappropriate for their organizational structure, or they find themselves too small to taking such high-quality measures (13 %). A lack of adequately educated personnel is another obstacle in introducing the ISO 270001 standard. The reasons for avoiding the implementation of the standard are various, and they differ from organization to organization. To sum up: the decision to implement the standard and acquire a

certificate depends on the company's size, its organizational structure and financial resources.

In more than a half of the organizations without the ISO 270001 certificate employees believe that the decision to introduce it depends mostly on the willpower of the management. The decision made by the management depends on other factors mentioned before. The ISO 27001 standard will be introduced and certificated when the company will have enough financial resources and an adequate organizational structure, therefore, the introduction of the standard depends mostly on the willpower of the leadership, which further depends on other afore mentioned factors in the organizational structure.

Organizations have different opinions in regard to how necessary it is to have a certificate of standard in their informational structure. Almost half of them (47 %) believe they do not need it. The reasons for this can be that they have an adequately safe infrastructure (of the information system) and/or are not aware of the advantages and quality of the standard. The remainder of organizations believes they do need the standard. These organizations are probably more informed about the benefits that such a standard can bring, and they strive for a higher level of quality; for a more stable, credible and safer information system.

Organizations, which find standards beneficial and necessary, believe that safety would improve after an introduction of the ISO standard. We can therefore conclude that the level of awareness about the benefits of certification is high.

59 % of the organizations in our study do not intend to introduce and certificate the ISO 27001 standard in the future. Different reasons for such a decision were already stated, however, the main ones are probably the lack of financial means, and an adequate safety structure. Maybe this will change in the future due to new, progressive threats. Organizations, which expressed a need for the standard, have to be prepared for it. Preparations have to be made at the employees' level, as well as in the organizational structure. In order to achieve the purpose of the standard, the entire organization's sphere must be qualified.

5 CONCLUSION

An information system is a basic component of every organization, and it provides a support for achieving defined organizational goals. The success of an organization mostly depends on its information system. The quality of the information system therefore indicates the quality of the organization. The results of the research confirm this fact. Results indicate that the majority of organizations cannot achieve their defined goals without an adequate information system. The success of an organization also depends on how effectively it can protect and store its data. Organizations spend most of their financial resources to protect data and other material. To achieve this most organizations use standardized precautionary measures and mechanisms, while only a few of the most developed organizations take technically advanced measures. These measures do not depend on the size and structure of the organization, but on its needs and performance, which also determine the types of the information security system and risk management; and

the formalization of information security quality. The process of certification mostly depends on the willpower of the leadership, which makes its decision according to financial and human resources of the organization and a determined time frame. Only a few organizations have adequate resources to carry out the process of formalization. However, it should be taken into consideration that, from the long-term point of view, formalization leads to the minimization of costs in the event of a of security incident. Most of the organizations do not opt for formalization, and mostly use only one approach, due to their relatively weak performance in providing information security.

Many organizations use a combined approach, but the general and informal approaches are the methods of choice because they demand the least time, knowledge and financial resources. Economizing in this area is probably the reason why most organizations evaluate their information security system as weak or inadequate. However, improvement is possible, and organizations are aware of this. Unfortunately, they think that the most common and most obvious threats are the most dangerous, which means organizations are not aware how serious risks to their information security really are. Moreover, the human factor, which mostly drives these threats, is neglected. The consequences that follow an attack are considered to be shameful and cause loss of credibility. What follows is business loss, and for that reason organizations do not publicly admit how much damage they suffered. Consequently, attacks are supposedly rare, and organizations neglect threats that are not detected due to an inadequate security level. The security system detects only the most common threats that are also the least dangerous. This is why organizations believe, that the damage caused by these threats are mostly acceptable. In conclusion, it can be said that an inadequate level of security is the reason why organizations do not comprehend the seriousness and danger of modern threats, or they have wrong images of them. What could be immediately done in this area to prevent misconceptions, is educating employees, and making them aware of the dangers. This would lead to the improvement of information security. Instead of spending money to repair damages, money could be spent to introduce better types of security.

REFERENCES

ISO 27000 Directory. *The ISO27001 Certification Process*. Retrieved April 10, 2010, from http://www.27000.org/ismsprocess.htm

Pfleeger, C. P. (1989). *Security in Computing*. Englewood Cliffs: Prentice-Hall.

Podbregar, I. (2008). *Vohunska dejavnost in gospodarstvo*. Ljubljana: Fakulteta za varnostne vede.

Robinson, R. R. (1999). *Issues in Security Management: Thinking Critically about Security*. Woburn: Butterworth Heinemann.

Sennewald, C. A. (2003). *Effective Security Management* (4th ed.). Burlington: Elsevier Science.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of*

Standards and Technology. Retrieved November 25, 2009, from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Tague, N. R. (2004). *The Quality Toolbox* (2nd ed.). Retrieved April 10, 2010, from http://www.asq.org/learn-about-quality/project-planning-tools/overview/pdcacycle.html

Trček, D. (2006). *Managing Information Systems Security and Privacy*. Berlin: Springer.

Whitman, M. E, & Mattord, H. J. (2008). *Management of Information Security*. Boston: Course Technology Cengage Learning.

About the Authors:

Dr. Igor Bernik is Assistant Professor of Information Sciences and the head of Information Security department at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research fields are information system, information security and growing requirement for information security awareness.

Kaja Prislan is a graduate student at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. Her research interests include cyber crime and information security.