UDC:004.056
Original scientific paper

IDENTIFICATION OF THE FREQUENCY AND THE INTENSITY OF THE THREATS IN THE FUNCTION OF DEVELOPMENT OF THE INFORMATION SYSTEM

Željko Hutinski, Miran Zlatović, Igor Balaban
University of Zagreb,Faculty of Organization and Informatics, Varaždin, Croatia
{ zeljko.hutinski, miran.zlatovic, igor.balaban}@foi.hr

Abstract: *In the process of development of the security system of the information system, the risk assessment is the foundation for selection of the security measures. The reduction of the level of risk and the amount of costs depend upon the adequate selection of the security measures. The quality of the risk assessment depends upon the adequate assessment of the form and the intensity of the threats. If the forms of threats are not monitored in the business system, it should make its own threat assessment, or use experience of others. The best, but also the most time-consuming solution is to develop own security system, while the fastest way is to use experience of others. However, there is the problem of migration of some other solution to our own system. Depending upon the question whether we are adopting the experiences of domestic or foreign business systems, the question of the applicability to the system from the different business environment becomes relevant. This happens because of the significant differences in the form and intensity of threats in certain local environments or different branches of industry.*

Keywords: *security threats, risk assessment, threat monitoring, security measures.*

1. INTRODUCTION

In the less developed and obsolete business systems, it is a common occurrence that the significance of the information system security is perceived as unimportant, or it is utterly neglected. The development of the information system security is in high correlation with the dependence of the managerial structures of the business system upon the data from the information system in the process of making business decisions. Therefore, from the point of security, very often only partial solution are selected, related to the security of only one component of the information system, while other components are neglected. Partial solutions of the information system security often are copy of solutions of the others. In this, sources, frequency and form of the risks and threats to that particular business system are not taken into account. If a system uses any model of development of the information system, it is most important to correctly establish the structure of

the threats, because it is the only way to create a system of protective measures in adequate manner [6].

Information security should be viewed as an investment. In this context, investing in the security can be viewed as the decrease of the direct costs, and simultaneously as the prevention of the possible losses. Vulnerability of an information system, and therefore business system (in proportion with the dependence of the business system upon the information system) stems from the vulnerability of its integral parts, which means that the potential intruders may use this vulnerability and endanger the integrity of the business system.

One of the steps in the development of the security system of the information system, using the methods of ISO 17799:2000, is establishing the significance of particular contents for the functionality of the business system (critical resources and their value – relative or financial). Therefore it is necessary to establish, as precise as possible, the sources and forms of threats, with the goal of risk assessment and definition of the risk reducing measures. Based on this, countermeasures targeted to the risk reduction are selected. Since the business system environment is in constant flux, which is also true for its organizational structure, it is necessary to continuously question and monitor the efficiency of the countermeasures through time, so we will be able to practice risk management. As we have already mentioned, one of the key factors of well-chosen measures of the risk reduction is the accurate assessment of the form and intensity of the threats. This assessment can hardly be taken from other environments, since it is related to business industry, area of implementation, educational and cultural structure of the environment. Therefore it is necessary to develop assessment of form and intensity of threats for every business industry and business environment. Managing the informational and organizational security is a continuous process of monitoring, in which the established level of the system security is continuously measured, assessed and developed.

2. SIGNIFICANCE OF THE DEVELOPMENT OF INFORMATION SECURITY SYSTEM

Business subjects and their information systems are increasingly exposed to the security threats which stem from the increasing significance of data and information for the functionality and efficiency of the business system, as well as the explosive increase of the number of sources of hazards, including computer frauds, espionage, sabotage, vandalism, arson, flooding etc. Sources of hazards are becoming more widespread, more ambitious and more sophisticated. In the same time, because of their greater dependence upon technologically developed information systems and services, organizations are becoming more and more vulnerable to the various forms of security threats. Linking of the public and private networks and sharing of the information resources increase the hardships in conducting the control of access to the information assets. Tendency of movement toward the distributed informatics weakens the efficiency of the centralized and specialized controls, which also includes development and control of the security system within the business system.

The purpose of the information security is to ensure:

- Continuous functionality of a system,
- Non-changeability of the content without authorization
- Prevention of the non-authorized usage of the content
- Continuity of business operations and
- Reduction of the damage to the business through prevention and minimization of the effects of security incidents.

Information security management enables usage of the content for the larger number of users who are dislocated, without endangering the information and other assets of the business system. The protection of the information assets consists of three basic features [19]:

- **confidentiality** – protection of the sensitive information from non-authorized or accidental disclosure
- **integrity** – preservation of the information accuracy completeness
- **availability** – ensuring the availability of information and vital services to the authorized users when they need them

Along with the development of the security system, we also need to develop the system of documenting security threats and incidents. This is the base for the revision of the preliminary risk assessment, which does not necessarily reflect the real picture of the security. Risk and threat assessment ate only a part of a much larger process of establishing and maintaining information security system – this process does not start with the risk assessment, nor does it finish with it. It consists of several steps of the development of the security system which are shown in the figure 1. Figure was made on the base of the norm BS7799 (ISO 17799:2000) [2]:

1. Definition of the information security policy.
2. Definition of the scope of information security system – boundaries should be defined according with the characteristics of the business system, its location, value and technology.
3. Conducting adequate risk assessment – threats should be identified in relation to the business system assets, vulnerability of those assets to those threats, and possible effects of these threats upon the assets; also, the assessment of the levels of particular risks should be made.
4. Identification of the areas of risk which need to be managed, according to the security policy and required level of security.
5. Selection of the goals and security measures which have to be implemented in the business system, along with adequate explanations.
6. Preparation of the applicability statement – the selected security goals and measures should be documented, as well as the reasons for their selection. Also, reasons for non-selection of other measures should also be documented.

It is clearly visible from the recommended frame of management that the process of risk assessment is precluded by identification and evaluation of the business system assets, and that the final result of the risk assessment is the set of conclusions related to the levels of vulnerability of particular elements of the business system assets, which is used as the base for risk management. Through the process of risk management, selection of adequate security measures and mechanisms can be made, through which the defined information security policy will be realized.

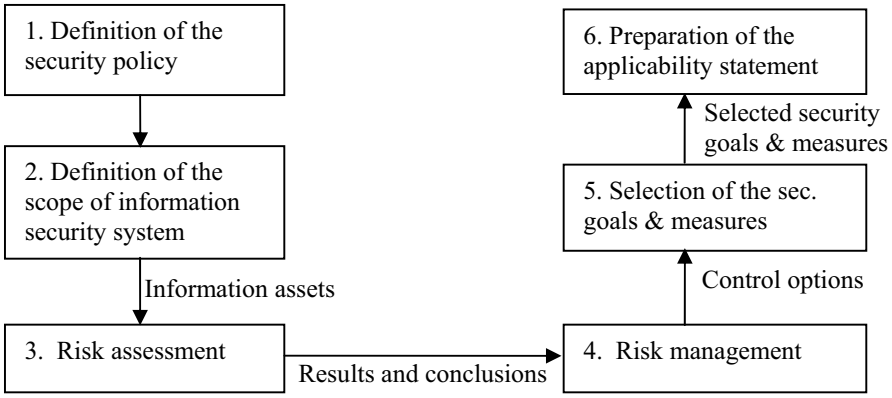

Figure 1. Frame for the managing of the information security system

3. RISK ASSESSMENT AS THE BASE FOR THE SECURITY MEASURES SELECTION

When the management of the business system for the first time encounters the need for development of the information security system, it should make a risk assessment. Generally speaking, it can be done in two ways: employees of the business system may assess the risk independently, or they can use experience of others. Use of other people's experience enables significantly faster development of the security system – in this, business system may use foreign or domestic solutions in the development of the security system of the business system. However, the applicability of transfer of the other people's solution into targeted business system is questionable. Differences in the business practice, because of which the use of experience of others is questionable, are not negligible within one country, and they are especially significant when taking solutions from foreign countries. Costs and time required for adaptation of foreign solutions to the condition and business operation of targeted business can be very high, so managers in every business system have to make careful assessment when deciding which approach is more acceptable in the security and cost relations.

3.1 INDEPENDENT RISK ASSESSMENT

Independent risk assessment can be conducted in two basic ways – using quantitative or qualitative methods of assessment. **Quantitative methods** of risk

assessment match the independent and objective numerical values (for example, financial values) to all components of the risk assessment process and to every potential level of loss. **Qualitative methods** of risk assessment are of more subjective nature, because they do not match the numerical values to the components of the risk assessment process, but express them through descriptive terms like “low/medium/high”, "important/moderately important/unimportant", etc. Each of these sets of methods has its own advantages and disadvantages [19]:

a) Quantitative methods

- *Advantages*
  - The results are based upon objective processes and metrics,
  - Great effort is put into the procedure of establishing the asset value,
  - They are convenient for *cost/benefit* analysis,
  - The results can be expressed in the form convenient for management (financial values, percentage, and probability).
- *Disadvantages*
  - Complex computations,
  - Good results can be achieved only with the support of specialized software tools and knowledge bases,
  - They require large quantity of preliminary activities,
  - User training is a demanding process,
  - Once the assessment commences, it is hard to change the direction of the process.

b) Qualitative methods

- *Advantages*
  - Computations are simple or non-existing
  - Matching financial values with the assets is not necessary,
  - Quantification of the threat frequency is not necessary,
  - It is easier to include the personnel not related to the security and technical operations into the process of evaluation,
  - Flexibility in the assessment process and in reporting.
- *Disadvantages*
  - Subjective nature of the assessment,
  - Results depend directly upon the quality of the risk management team,
  - Small effort is put into the establishing the asset value,
  - There is no base for *cost/benefit* analysis and risk reduction.

The base for the selection of the security measures during the development of security system in any business system is the real risk assessment. The process of risk assessment includes the following components [14]:

1. Identification of the information assets of the business system,
2. Knowledge about the value of the information assets of the business system,
3. Identification of the threats to the information assets of the business system,
4. Identification of the vulnerability of the information assets of the business system,
5. Identification of the existing and planned security measures,
6. Risk assessment.

3.1.1. Identification of the assets of the business system

The asset is something which is valued by the business system, therefore it should be protected. Adequate security and responsibility for the assets is the key for maintaining adequate protection of all assets of the business system. The notion of "assets" envelops [14]:

- **Information assets** – Databases and files, system documentation, user's manuals, training material, operative procedures, plans of continuity and rehabilitation
- **Paper assets** – contracts, guidelines, company documentation, documents containing important business results
- **Software assets** – application software, system software, development tools and auxiliary programs
- **Material assets** – computers and communication equipment, data storage media, and other technical equipment, furniture and offices.
- **Human resources** – employees, clients, subscribers
- **Image and reputation of the business system**

3.1.2. Knowledge about the value of the business system

Every component of the assets should be matched with the adequate value in the sense of its importance for the business operations. These values are usually expressed in the sense of potential consequences for the business operations, like loss of confidentiality, integrity and/or availability of the assets. To assess the potential damage consistently and to react in adequate manner, the assets should be measured on the scale of values. Every component of the assets and every potential loss (of confidentiality, integrity and availability) should be matched with its value – in quantitative or qualitative manner.

3.1.3. Identification of the threats to the assets of the business system

Depending upon the type of the information asset of the business system, the exposure to the various threats is different. A threat can cause undesired incidents, which may result in damage for the system and its assets. The damage may occur as the result of direct or indirect assault on the assets of the business system, for example, unauthorized usage, destruction, non-identified exchange, damage, unavailability or loss of content. Threats come from deliberate or accidental sources, and use the vulnerability of the system, applications or services used by organization, to damage the assets. After the identification of the threats, the probability of these threats should be assessed. In this, the following should be taken into account [14]:

- Frequency of the threat – how often it may occur (experience, statistic…)
- For the deliberate threats – motivation, required skills and resources which have to be available to the potential intruders, and the perception of attraction and vulnerability of particular component of the asset for the potential intruder
- For the accidental threats – geographical factors, like the vicinity of chemical industry or areas with the extreme weather conditions, are always present, and they may influence the human error and equipment failure.

3.1.4. Identification of the vulnerability of the business system assets

Vulnerabilities are weaknesses related to the business system assets. Security threats use the vulnerability and cause undesired incidents, which may result in non-authorized usage, loss or damage (change of the content) of the assets. Vulnerability does not cause damage by itself, it is only precondition for realization of some threat. It is important to assess the significance of particular vulnerability, i.e. how easily they could be exploited. In relation to this, the vulnerability can be classified in 3 or more levels, for example:

		Highly probable
Likely to occur		Likely to occur
Possible	or	Possible
Impossible		Unlikely to occur
		Impossible

The vulnerability should be assessed in relation to every threat which may exploit it in any way. For example, the system can be vulnerable to the covering of the user's identity and abuse of the resources. Such vulnerability may be highly probable if there is no user authentication [14].

3.1.5. Identification of the existing and planned security measures

Security measures identified during the risk assessment should be added to the already existing or planned measures. During the assessment of the measures for

risk reduction, it is important to take into account the already existing and planned measures, as to avoid unnecessary duplication of the security measures. During this phase, the insight can be reached that the existing or the planned measures are not justified. In this case, the decision should be made whether to remove the measures, to replace them with the more adequate measures, or leave them be because of the high costs. Besides, care should be taken that the security measures selected during the risk assessment can be harmonized with the existing and planned measures.

3.1.6. Risk assessment

The goal of this phase is to identify and assess the risks to which the business system and its assets are exposed, as to identify and chose adequate and justified security measures. The risks are function of the value of the endangered assets, probability for appearance of the threats which cause debilitating consequences for the business operations, easiness for exploiting the vulnerability, and all existing or planned security measures which can reduce the risks.

There are various techniques of risk assessment based upon the linking of the above mentioned factors, like [14]:

- Matrixes with values defined in advance,
- Ranking threats according to the measures of risk,
- Assessment of the frequency and possible debilitating consequences of the risk,
- Distinguishing between tolerable and non-tolerable risks, etc.

The above mentioned techniques are qualitative in nature and are based upon the use of tables and matrixes. Regardless to the selected technique of the risk assessment, the result should be formulated in the form of the list of measured risks for every consequence of the non-authorized disclosure, change and destruction of every individual part of the asset within the scope of the information security system.

3.2 EXPERIENCES OF OTHERS IN THE RISK ASSESSMENT

The data about the form and intensity of the threats can be reached through monitoring the functionality of the measures of risk reduction in the security system. This can be a long-term process, and the precondition for this is already developed and documented security system. When developing the security system for the first time, the organization may reach toward the experiences of others in the risk assessment. Such steps are most often taken from the following reasons:

- Lack of time and material resources for the comprehensive projecting and implementation of the security plan
- Lack of understanding of the basic concepts of risks and threats
- Lack of expertise or lack of team dedicated to the application of security measures, identification of risks and threats, and the development of the plans of analysis and implementation of the security mechanisms.

These are only some of the factors of unsuccessful application of the security system.

3.2.1. Methods of threat monitoring in the USA

If we decide to take over the experience and solutions of others, we need to know the conditions in which these solutions were applied. The statistics of form and intensity of threats should be tested before implementing those solutions in our environment, because various threats are represented differently in various environments. Extent of investment into IT security also differs in time and space. Researches for 2004 [17] have shown that, in USA, cca 50% of the business systems spends 1-5% of developmental funds for development of IT security. Also, cca 20% of them spends more than 6% of developmental funds, while the rest spends less than 1%.

Furthermore, the awareness of the harmfulness of the unauthorized usage of the computer systems is increasing. Educative and security measures have resulted in decrease of the number of such threats in the last few years. Despite the global decrease of the unauthorized usage of the computer systems, the relations of the number of incidents stemming from within and outside the business systems are shown in the following table.

Table 1: Number of security incidents in relation to the source [18]

Number of security incidents	*1-5*		*6-10*		*>10*		*Unknown*	
	2004	**2005**	**2004**	**2005**	**2004**	**2005**	**2004**	**2005**
Within	52%	47%	9%	10%	9%	8%	30%	35%
Outside	52%	46%	6%	7%	8%	3%	34%	44%

On the base of the data from the table 1, it is clear that the number of internal and external intrusions is similar, therefore it can be concluded that the additional measures of protection are required which in the equal proportion protect the system both from internal and external intrusions. Similarly, in 2005, the number of security incidents was not significantly different in relation to 2004, but there was an increase of the unknown incidents within the business system. The structure of the external and internal threats is different, and this also broadens the scope of the risk reduction measures, but also increases the costs.

If we want to study the types and forms of the threats in greater detail, we need to analyze them. Such analysis is one of the basics for setting the priorities in the selection of the security measures.

Table 2: Proportion and types of threats frequency [18]

Type of threat	***Year***						
	1999	**2000**	**2001**	**2002**	**2003**	**2004**	**2005**
Virus	90%	85%	95%	85%	82%	78%	74%
Internal cause of the network interferences	98%	79%	90%	78%	80%	59%	48%
Stealth of the portable computers	70%	60%	65%	55%	60%	49%	48%

Unauthorized access to the information	58%	70%	50%	38%	45%	37%	31%
System intrusion	30%	26%	41%	41%	37%	17%	15%
DOS assault	32%	28%	36%	41%	37%	39%	31%
Stealth of the information owned by the organization	26%	20%	26%	19%	20%	10%	6%
Sabotage	12%	17%	18%	5%	20%	5%	3%
Financial frauds	14%	11%	12%	12%	16%	8%	7%
Telecommunication frauds	18%	9%	8,5%	7%	8%	9%	9%

The protection from any security threat (like those listed in table 2) requires investment of certain financial resources from the total amount which the business system has available for the development of the IS. The number of security threats indicates that it is very hard to secure IS from all forms of threats with the limited financial resources – therefore, in the selection of the security measures, the greatest priority should be given to those measures which would yield the best results. The business system can influence the intensity of effect of particular forms of threats, therefore the largest part of the resources should be invested in countering the threats whose source lies in the internal weaknesses of the business system, like inadequate protection from the computer bugs, inadequate network infrastructure, badly adjusted access rights to the particular data and computer resources (which enables the intrusions into the system, and unauthorized access to the information, as well as the stealth of information) or irregular updating of the software support with the most recent security patches (which leads to the increase of vulnerability of the information system to DOS (Denial of Service) intrusions). From the data shown in the table 2, it is visible that the mentioned threats are also the most frequent ones. The last few years witnessed the decrease of the frequency of threats of all sorts, which is especially visible in 2005. This points to the increased concern related to the implementation and development of the security system.

Implementation of the direct measures for the protection from the above mentioned most frequent threats to the IS security will not be sufficient if these are not accompanied by the additional activities of the business system. On one side, it is necessary to continuously educate the employees about the security threats, their consequences and the way in which the effect of the threats can be eliminated, while on the other side there should exist a business policy (in the form of security policy and internal regulation books) which regulates and formalizes the security of IS. The optimal combination of educative and normative factors in the business system can have the influence on the significant decrease of the frequency of sabotage as the form of threat to the IS security.

The biggest financial losses were caused by the following threats, listed according to their frequency [18]:

Table 3: Impact of the threats on the financial losses

Year 2004	Year 2005
1. Viruses (39% of total losses) 2. DOS intrusions (19%) 3. Stealth of information owned by the organization (8%) 4. Internal cause to the network interference (7%) 5. Disruption of the wireless network (7%), etc.	1. Viruses (39% of total losses) 2. Unauthorized access to the information (24%) 3. Stealth of information owned by the organization (23%) 4. DOS intrusions (6%) 5. Internal cause to the network interference (5%), etc.

It is obvious from the table 3 that, within two years, the structure of threats has changed along with their frequency. In 2005 there was a high percentage of unauthorized access to the information, which was in most cases characterized by the companies as the internal threat. However, to be able to see more complete picture about the financial losses, it is also important to say that the absolute amount of the losses in 2004 [18] equaled 140 billion US dollars, while in 2005 that amount was reduced to 130 billions. This data suggests that the companies in USA use their limited IS development budgets for the development of the IS security in increasingly adequate manner.

The most frequently used security technologies for countering the threats are, as can be expected, related to the above mentioned list of threats, as is shown in the Figure 2:

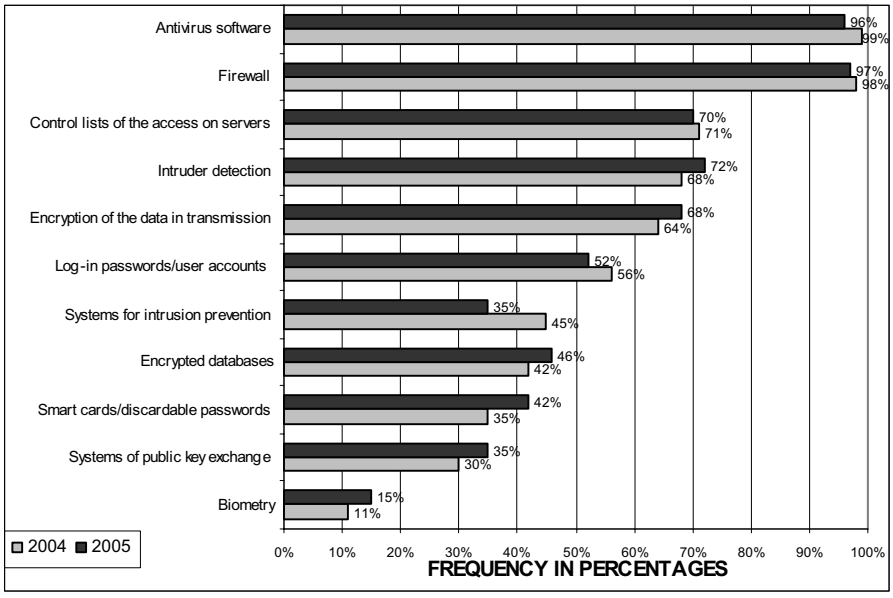

Figure 2. Usage of the security technologies [17],[18]

Besides being the most frequently used security technologies, antivirus software and firewall are also easiest for use. The firewall can be configured automatically, most often by the operational system (Windows XP SP2), while antivirus software is also very easy to install and use. Since the viruses, intrusions into the network systems and unauthorized accesses to the information are identified as the most frequent threats to the system, such frequent use of these two technologies is justified. Since these days witnessed increased use of the web-based technologies, it is necessary to use different control mechanisms and security controls (Figure 2). Namely, in 2005, the use of the wireless networks increased, as well as the access to the different services and systems through Internet, which changes the proportion of the impact of presupposed forms of threat in relation to 2004. In 2005, there was increased use of the systems for prevention of the intrusion, systems of the public key exchange, and the biometry. This does not mean that the traditional forms of threats, like computer viruses, should be neglected – this fact is confirmed by the consistent level of portion of the security technologies for prevention of such threats.

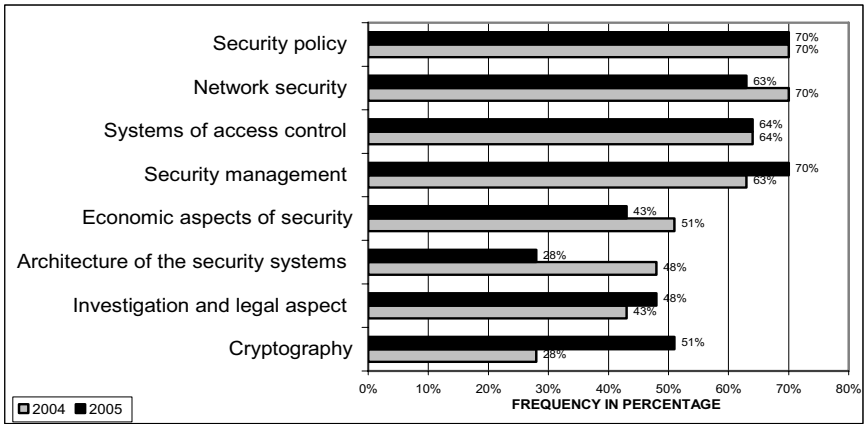

Figure 3. The importance of particular security segments [17],[18]

Different business systems in practice give different importance to the particular segments of security, as can be seen in the Figure 3. More and more of the networked computers justify the largest share of the network security which is realized and regulated through the security policy, both in the network and the individual computers. On the other hand, the importance which the respondents give to the cryptography had an important place in 2005. The review of the security incidents and possible «defense mechanisms» established that the cryptography offers very high level of protection, which justified increase of the use of this technology in 2005. Systems of the implementation of cryptography most often require additional engagement of the users and/or environment (PKI infrastructure, etc) or are implemented in other levels of protection (for example, security network protocols – https, ssh, etc.) and are executed in transparent manner for the user, so they are not aware of their presence. It should be emphasized here that, regarding the source [18] 87% of the companies conducts overview and revision of security and security policy, while 13% of the companies do not do it. Similarly, in 2005,

the proportion of the security segments changed significantly, so the biggest importance was given to the security policy, security management, systems of control access, network security and cryptography. They are followed by other mechanisms of protection, like legal regulative, economic aspects etc. It is obvious that the companies react actively to the changes in the structure of threats, by strengthening of the certain security segments and the use of adequate security technologies, which additionally supports the argument that the USA companies implement the measures for reduction of the risk from the assessed forms and intensity of threats to the business systems in more adequate manner.

3.2.2. Systems of threat monitoring in Europe

The last chapter has illustrated the picture of attacks in the last several years in USA. The situation related to the monitoring of risk and threats in Europe in somewhat more complex. On the level of particular countries, there are data available from many years of monitoring the intensity and frequency of particular threats, while there are no such data on the level of European Union. EU bodies have noticed the need for the systematic monitoring of the threats and the existence of the updated recommendations for management of the risks which are brought by the particular threats. With this purpose in mind, the ENISA (*European Network and Information Security Agency*) [5] was formed, but since the project of systematic monitoring of threats and risks is still in initial phases, there still are no detailed data comparable with those in USA. The awareness about the impossibility of development of the adequate protection of the information infrastructure without knowledge of the risk and threat profile already exists. Also, the problems which stand in the way of realization of the project of threats and risk assessment were noticed. [9]:

- Most of the informational infrastructure is private property; it crosses the borders of the particular states, and is intertwined among the companies.
- There are not enough initiatives for the protection which would be implemented in adequate manner.
- The companies hide real data about the threats, security incidents and costs,
- The governments are not prone to regulation of that problem, or are doing poor job in regulation.

The consensus was achieved related to the seven viewpoints important for the insurance of the critical information infrastructure [9]:

- **Protection is required** - critical information infrastructure is inherently vulnerable and the consequences of failure are high, thus requiring a high degree of protection.
- **Marketplace is insufficient** - the market alone will not provide sufficient protection because it lacks proper incentives, and technical solutions themselves are not perfect.

- **Government is inefficient** - regulation may not produce optimal results, since it may be inflexible to technical change and place the emphasis on compliance rather than security.
- **Information sharing** - to address the problem, it is imperative to understand the risks systems-wide, which necessitates information-sharing across firms and sectors, globally.
- **Insurance sector** - the insurance industry can facilitate the creation of a central point of information aggregation and risk assessment, and devise policies based on its findings.
- **Market for security** - the insurance industry's mechanisms of premiums, deductibles, and eligibility for coverage can incent best practices and create a "market" for security.
- **Government support** - government must actively support the process by serving as an observer, providing antitrust immunity, and encouraging limited disclosure of risks.

Recently, the work of the ENISA agency resulted in the set of suggestions for increase of the security related to the use of Internet [8]:

- Regular implementation of the security patches for software products,
- Use of anti-virus software,
- Use of the firewall (from personal to more complex),
- Browsing of the Internet with reduced (non-administrative) user authorization,
- Non-use of the active contents in web-browsers,
- Encryption of the important data, and
- Regular construction of the security data copies

If we compare these recommendations with the security technologies (Figure 2) which are used most frequently in USA according to [17] and [18], we can see significant level of overlapping.

On the other hand, United Kingdom has been monitoring omissions and penetrations in the information security for ten years on the national level. According to their data [1] for 2004 27% of the security incidents were manifested through accidental failure of the system and the data corruption, while 68% were malicious incidents.

One of the reasons for such high percentage was the change in the business environment. Today, the emphasis is placed upon the use of the technologies like e-mail (93%), Internet access (89%), remote system access (54%), wireless network (34%) etc. Network borders are spreading across the physical borders of the enterprises through the use of wireless networks and so-called PDA (Personal Digital Assistant) devices which enable the user mobility. By the development and adoption of new technologies, the organizations are trying to identify and eliminate threats, but generally speaking, these new technologies contribute to the fact that the number of the security incidents is still increasing.

The following figure shows the types and portions of the threats which the companies in United Kingdom faced until 2004:

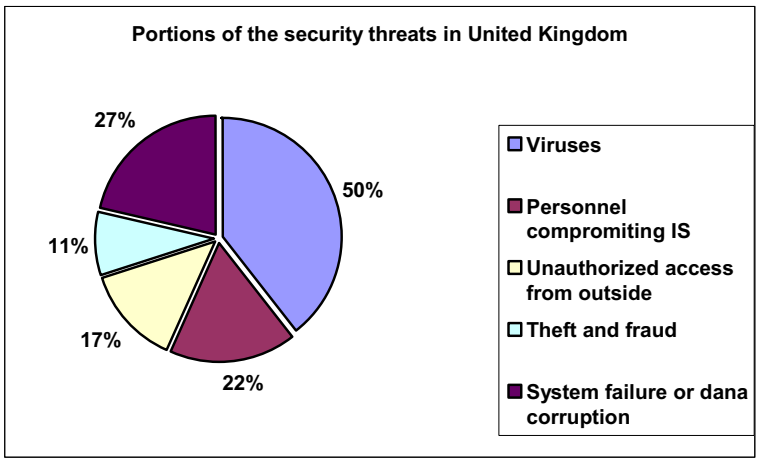

Figure 4. Types and portions of security threats in United Kingdom in relation to the source [1]

The above mentioned threats compared to the threats in USA point to their similar percentage on different continents, which supports the statement that the majority of the security incidents cannot be isolated and viewed as separate entities specific for a particular enterprise and particular area. This is confirmed by the increasing numbers of unwanted electronic mail, so called spam, from the companies worldwide.

Security mechanisms implemented in United Kingdom are not so different from those in USA. In the last few years, the greatest attention in the United Kingdom was given to the education of the employees, establishment of the security policy, and security investments. However, not enough attention is given to the security monitoring and revision, which would enable timely reactions to the identified forms of threats, and in such way eliminate, or at least reduce the costs of the security omissions. One of the omissions noticed was also inadequate investment in the security, which presently amounts to 3% of the IT budget, while reasonable investment should be 5% to 10% of the IT budget [1].

3.2.3. The situation in Republic of Croatia

In Republic of Croatia, the picture is rather different; the quality of the solutions in on significantly lower level. This environment struggles with the illegal purchase of the software, which is massively used in the big business systems. The awareness of the virus threats is present and widely spread, but the same cannot be said about the possibilities and methods of protection. The situation regarding this subject is also slowly developing in Republic of Croatia. However, some similar institutions have begun to appear also in Croatia. A service called Abuse was constituted at CARnet. Its goal is to record and process the information related to the computer security incidents and abuse of CARnet's resources, like:

spam, netiquette, viruses/worms/trojans, violation of the copyright, commercial use, unauthorized access, burglary, DoS, DDoS [10]. In this purpose, the form and system for reporting the incident was developed, which is documented, and which help the user to remove the threat.

The same or similar is the purpose of CERT (Computer Emergency Response Team), the national center for computer security established in 1996. Also, the attacks on the system which were observed are reported, and the service gathers and distributes security counsels, gives suggestions for application of the safety tools etc. According to the National Program of Information Security, CERT also takes over the function of the national center for information security [3], [12]. In such conditions, the domestic business systems face two possibilities: to apply experiences of others, or to develop their own system of monitoring the form, types and intensity of threats to the information system.

If we compare the results from the Table 2 with the results of the statistics shown in the Table 4 – the forms of threats for the last 12 months as reported by CARnet CERT, the significant difference of the reported threats is visible.

It is visible that the data are significantly different. This can be so due to the short period of monitoring, or due to the lack of knowledge of the users about the possibilities of reporting. However, it is certain that the structure of the intrusions is significantly different.

Table 4: Types and frequency of threats [13]

Type of threat	***%***
Virus/worm/Trojan	28
Port scanning	17
Undesired mail (spam)	10
Unreported	7
Attempt of unauthorized access	7
Violation of copyright	17
Denial of service	3
Unauthorized "root" access	3
Disfiguration of web sites	3
General unauthorized access	3
Distributed DoS	1

Unfortunately, this initiative for the systematic registration of the security incidents in Republic of Croatia was not long-lived. Extremely useful researches shown on the web site, which contained statistical data about the types and the frequency of the information security threats [13] do not exist any more in the moment of writing of this paper[1]. Inadequate substitution consists of one site of CARNet's Abuse service, on which there is just one graph (figure 5) with the total number of security incidents per months in 2005.

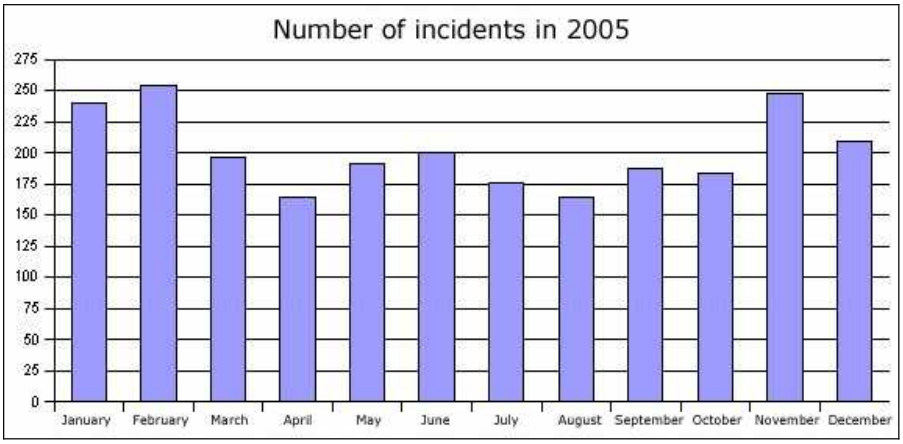

Figure 5. Number of security incidents in Republic of Croatia per months [11]

In such circumstances, the national business systems cannot rely on the services of the central body for following of the security incidents in Republic of Croatia. While the business systems in USA and certain European countries can use final results during the risk assessment in relation to the information security, the business systems in Croatia obviously do not have such possibility. If the situation remains unchanged, our business systems will have two possibilities: taking over the international experiences, or development of new system of risk and threat assessment.

4. CONCLUSION

The existing relevant data about the intensity of particular threats to the informational security relate mostly to the territories of USA [18] and United Kingdom [1], where threats and risks have been monitored systematically for many years. On the level of European Union, the need was perceived for the monitoring the threats and risks of the information security. The work of the ENISA agency [5] has set the foundations for systematic monitoring of the threats and risks, but the detailed statistical data from the long-time monitoring still do not exist, because the project of systematic monitoring is still in early phase.

One of the main problems of the development of security system in Republic of Croatia is the inadequate functionality of the CERT service, which presently does not provide adequately detailed information about the types and frequency of the computer threats to the public. According to the National program of information security [3] and the Plan of implementation of the national program of information security [4], the completely functional CERT service should have been established to the end of the third quartile of 2005, which was obviously not realized. Until the CERT service does not function in the planned manner, we can question the applicability of the data gathered from the foreign countries in the circumstances of the domestic environment. A research should be conducted which would identify proportions and frequency of threats to the information security in Republic of Croatia – only then will it be possible to compare domestic security circumstances in with those abroad, and to assess if it is convenient to apply their experiences and

solutions in the domestic environment or not. Any uncritical copying of the foreign experiences is presently too risky, because the risk and threats assessment is the base for development of the security system – bad foundations cannot support a successful system of information security.

REFERENCES:

[1] ***: *Information Security Breaches Survey 2004*, DTI, 2004., <http://www.pwc.com/images/gx/eng/about/svcs/grms/2004Technical_Report.pdf>, (1.12.2005)

[2] ***: *Information security management - Part 2: Specification for information security management systems*, British Standards Institution, London, 1998

[3] ***: *Nacionalni program informacijske sigurnosti u Republici Hrvatskoj*, Središnji državni ured za e-Hrvatsku, Stručna skupina za informacijsku sigurnost, Zagreb, ožujak 2005.

[4] ***: *Plan provedbe nacionalnog programa informacijske sigurnosti u Republici Hrvatskoj za 2005. godinu*, Središnji državni ured za e-Hrvatsku, Stručna skupina za informacijsku sigurnost, Zagreb, ožujak 2005.

[5] ***: *Risk preparedness in business in the field of network and information security*, European Network and Information Security Agency, <http://www.enisa.eu.int/studies/index_en.htm>, (10.6.2005)

[6] ***: *Sigurnost informacijskih sustava*, InfoTrend, <http://www.trend.hr/clanak.aspx?BrojID=35&KatID=5&ClanakID=443>, (25.03.2005)

[7] Barman S., Writing information security policies, New Riders Publishing, USA, 2002

[8] Bautsch M.: *Some Urgent Recommendations for Internet Security*, Stiftung Warentest, 2005, <http://www.enisa.eu.int/doc/word/

[9] recommendations_internet_security.doc>, (22.12.2005)

[10] Cukier K.: *Critical Information Infrastructure Protection*, Report of the 2005 Rueschlikon Conference on Information Policy, 5th annual Conference on Information Law and Policy for the Information Economy, Rueschlikon, Switzerland, 2005. <http://www.enisa.eu.int/doc/pdf/publications/56_r_05_report_online.pdf>, (22.12.2005)

[11] http://www.carnet.hr/abuse

[12] http://www.carnet.hr/abuse/broj_incidenata

[13] http://www.cert.hr/

[14] http://www.cert.hr/statistika.php?lang=hr

[15] Humphreys E. J., Moses R. H., Plate A. E.: *Guide to Risk Assessment and Risk Management*, British Standards Institution, London, 1998

[16] Killmeyer Tudor J., Information security architecture: an integrated approach to security in the organization, CRC Press, USA, 2001

[17] King C. M., Curtis, D.E., T. Ertem, O., Security architecture : design, deployment & operations, McGraw-Hill, USA, 2001

[18] Lawrence A. G., Martin, P. L, Lucyshyn, W., Richardson, R.: *2004 CSI/FBI Computer Crime and Security Survey*, 2004, <http://www.gocsi.com/

[19] forms/fbi/csi_fbi_survey.jhtml>, (18.05.2005)
[20] Lawrence A. G., Martin, P. L, Lucyshyn, W., Richardson, R.: *2005 CSI/FBI Computer Crime and Security Survey*, 2005, <http://www.usdoj.gov/
[21] criminal/cybercrime/FBI2005.pdf>, (1.12.2005)
[22] Peltier T. R.: *Information Security Risk Analysis*, Auerbach Publications, 2001.
[23] Tipton F. H., Krause, M., Information security management handbook – 5th edition, CRC Press, USA, 2004
[24] Vose D., Risk analysis: a quantitative guide – 2nd edition, John Wiley & Sons, London, 2000

Received: 18 November 2005
Accepted: 21 June 2006