VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 16 no. 2 pp. 128–147

Efficiency of Corporate Security Systems in Managing Information Threats: An Overview of the Current Situation

Kaja Prislan

Purpose:

Information security should be a strategic goal of every responsible and safety-conscious organisation that wants to follow current security and technological trends. The purpose of this paper is to summarize the corporate practices in addressing IT risks, to explain the benefits of a comprehensive approach to information security as a business function, and to improve understanding of the current issues associated with its management.

Design/Methods/Approach:

Topics presented in this paper were analysed using descriptive and qualitative analysis of international reports and surveys. The findings obtained using the comparative method and their synthesis are supported by other research in this area.

Findings:

Due to the large volume of information assets, sophisticated IT threats and the heterogeneous nature of security factors, the efficiency of information security is very difficult to achieve. It has been observed that many organisations are at an early stage in developing a comprehensive approach to information security, since, in practice, they are still dealing with the problems of the past, yet they are very consistent with tracking user trends. This disproportionate situation represents a major security challenge for an organisation's management.

Practical Implications:

The findings of this research are useful for the further analysis and evaluation of information security and victimization of cybercrime, and are also applicable to facilitating strategic planning and decision making.

Originality/Value:

Based on the review of the current corporate state, this paper presents baseline information and security situations in the business environment and evaluates the efficiency of information security as a business tool. Based on the results, contemporary security challenges and organisational guidelines for the future were identified.

UDC: 004.056

Keywords: information security, corporate security, efficiency, management, security challenges

Učinkovitost sistema korporativne varnosti pri upravljanju informacijskih groženj: pregled trenutnega stanja

Namen prispevka:

Informacijska varnost mora biti cilj vsake organizacije, ki želi odgovorno slediti tehnološkim trendom. Namen prispevka je analizirati prakso organizacij pri soočanju z informacijskimi tveganji, pojasniti prednosti celovite ureditve informacijske varnosti kot poslovne funkcije in izboljšati razumevanje aktualnih problemov, povezanih z njenim upravljanjem.

Metode:

Uporabljena je deskriptivna metoda in vsebinska analiza mednarodnih poročil in raziskav, povezanih z informacijsko varnostjo. Ugotovitve pridobljene s komparativno metodo in zaključki so podprti z drugimi strokovnimi viri.

Ugotovitve:

Zaradi velikega obsega informacijskega premoženja, sofisticiranih informacijskih groženj in heterogene narave varnostnih dejavnikov je učinkovitost informacijske varnosti težko uresničljiv cilj. Ugotavljamo, da je veliko organizacij pri celoviti obravnavi informacijske varnosti šele na začetni stopnji, saj se v praksi podjetja še vedno ukvarjajo z zastarelimi problemi, medtem ko je sledenje uporabniškim trendom zelo aktualno. Takšno stanje predstavlja velik izziv za management organizacij.

Praktična uporabnost:

Ugotovitve prispevka so uporabne na znanstveno-raziskovalnem področju oz. ravni analiziranja in ocenjevanja informacijske varnosti, viktimizacije ter upravljavskem nivoju, za lažje strateško načrtovanje in sprejemanje odločitev.

Izvirnost/pomembnost prispevka:

Prispevek s pregledom stanja predstavlja izhodiščno informacijskovarnostno situacijo v poslovnem okolju in podaja oceno razvitosti ter učinkovitosti informacijske varnosti kot poslovne funkcije. Na podlagi analize rezultatov so identificirani tudi sodobni varnostni izzivi in organizacijske smernice za prihodnost.

UDK: 004.056

Ključne besede: informacijska varnost, korporativna varnost, učinkovitost, upravljanje, varnostni izzivi

1 INTRODUCTION

The widespread availability of electronic devices and global connectivity are changing the concepts of social life and business operations. The success of our personal and professional life depends on the information available, on which we base our decisions. However, due to information overload, we are not able to make rational decisions without the use of electronic devices which make it possible to collect and process the information. On the one hand, contemporary information and communication technology [ICT] has made it easier to meet some basic human needs, such as maintaining social life, acquiring knowledge, being informed and productive, etc. On the other hand, it has entirely shaken the foundations of some basic assumptions about security and capability of maintaining social order as well as national security. According to Bernik (2014), military, political and economic powers that create a stairway to success of societies have become dependent on information power and information advantage.

Business entities have also followed the trend of changing power and concepts of success. Consequently, organisations are not able to cope with the rapid business pace and changes without the use of electronic devices and the internet. In order to operate successfully in times of aggressive competition, they must prove flexible, innovative and be able to develop production processes. Therefore, the organisations seek to update existing ICT and extend the amount of information they manage. That improves business operations, though it poses serious information security risks at the same time. Expert discussions and information security studies presented in this paper increasingly emphasize that cybercrime is becoming more organised and focused on the big-data environments.[1] In comparison to the conventional types of deviant behaviour, this kind of crime threatens business security in a different way. Before the exponential development and widespread use of technology, confidential and important business information was relatively less exposed to the risks of unauthorized use. Contemporary threat landscape has become highly uncertain which makes efficient information security an important business advantage. Namely, due to continuous technological changes and innovations, business entities have to constantly be ready to respond properly in case of a confidentiality breach.

1.1 Predictions

Current expert and research reports prove that information security as a business function and an organisational process, is becoming a serious topic of discussion. In addition to the expert reports in this field, much research, market analysis, and reports of international communities deal with this topic as well. The major future predictions for development of information security and threats are highlighted in the following paragraphs:

1 *Companies produce, store and process huge amount of information which is difficult to handle due to the lack of its transparency and extremely large quantities.*

- **Increased number of cybercrime cases**: In terms of information security and cybercrime, the last decade has been marked by exponential development and misuse of ICT. Cybercrime is the major security issue of the 21st century, as it has exceeded conventional crime, meaning it is more common in comparison to conventional violence-related and financial crime (Comprehensive study on cybercrime, 2013).[2, 3]
- **Increased number of state-supported cyber attacks**: At the state level, the number of targeted cyber attacks is expected to increase. Furthermore, the attacks on critical infrastructures are in sight, since it is an important aspect of national sovereignty and functioning of societies. Therefore, the critical infrastructure protection should become a priority in the eyes of states and major operators. Organisations must also be prepared to respond to such attacks, since they can be indirect victims in case of collateral damage (Internet security threat report,[4] 2013).
- **Increased number of threats and risks in cloud computing services**: Cloud computing has become an inevitable part of the internet and corporate infrastructure. Since cyber threats tend to focus on the locations where the big data is stored, cloud computing services are expected to be a future target, as well (ENISA threat landscape 2013 – Overview of current and emerging cyber-threats,[5] 2013; Internet security threat report, 2013).
- **Development of mobile-platform-related threats**: The increased use of mobile devices in the work environment has resulted in evolving new forms of threats and redirecting cybercriminals to the mobile media. Mobile devices are changing the conventional concepts of corporate structure and are causing revolution in the areas of mobile applications in terms of their use and capability. The use of applications has paved the way to easier and faster gathering of the big data; however, this process is more difficult to control. Since mobile platforms will remain the main area of the future innovations, organisations which follow the trend are expected to face a series of challenges (ENISA threat landscape 2013 – Overview of current and emerging cyber-threats, 2013; Internet security threat report, 2013).

2 *For example: e-mail abuse, phishing attacks and identity theft became the most common forms of crime, comparing to those long considered the most widespread problem (e.g. burglary, robbery and car-jacking) (Comprehensive study on cybercrime, 2013).*

3 *Research conducted by UNODC about the state of cybercrime in the 69 Member States of the United Nations. Data was collected in 40 companies, 16 academic institutions and 11 government institutions, while the meta-analysis of 500 publicly available documents was conducted as well. The study highlights the problem of collecting e-evidence, while solution can be seen in the new multilateral legal instruments.*

4 *The report includes an analysis of the IT incidents detected by Symantec's Global Intelligence Network, which records thousands of incidents per second in 157 different countries. In addition to incidents, the research covered 5,291 technological vulnerabilities detected in 2012. The results have shown that perpetrators are using new and innovative techniques, while migrating from classical stationary to mobile, virtual and social platforms.*

5 *Survey performed by ENISA, includes the analysis of 250 public documents and research on the topic of cybercrime. The purpose of the research was the identification of current trends in the field of information security with the aim to predict the future challenges. The results of the analysis showed that the major issue are less common forms of organized and sophisticated attacks that cause serious consequences.*

- **Threat migration to social media**: In recent years, social network sites which enable constant connectivity and knowledge sharing have become social psychological phenomena, and are expected to integrate into individual lives and corporate environments even more in the future. The most problematic is a tendency towards combining social media, mobile platforms and electronic payment system services which the perpetrators are expected to misuse, since they already optimize their operating techniques (Internet security threat report, 2013).
- **Internet of things and interconnection of devices**: Nearly all human needs and the ways of meeting them are somehow technology based. Communication services and electronic devices, which are part of our everyday life, are a great springboard for development of innovations (e.g. e-medical services, smart homes, electronic transportation and electronic cars, industrial control and energetic systems, live stream, etc.). Internet exceeds the limits and capabilities of computers and mobile devices which results in so called micro-digitalisation of organisations (Gartner, 2013).

Considering user trends and development of cybercrime, the future predictions are relatively reasonable. Cybercrime is expected to evolve hand-in-hand with developing science and ICT. If these predictions are right, mobile platforms and applications will continue to be the main source of innovations, whereas internet and information threats will continue to spread to the parts of personal life and business that have not been part of the network so far. According to the UNODC (Comprehensive study on cybercrime, 2013), such information threat development is driven by current socio-economic situation. Namely, people and organisations have gone viral and became connected during strong economic and demographic transformations, growing inequality among social classes, and strong belt tightening in the private sector. Lower financial liquidity of countries and organisations has had major impacts on crime and security situation.

1.2 The Nature of Information Security

In order to explain security trends, it has to be taken into consideration that the security of corporate structures is a very heterogeneous area and information security still plays a supportive role in it, despite its importance. Information security must be flexible and multidisciplinary, since it must ensure business continuity without threatening its functionality. Therefore, the efficiency of information security depends on the level of an organizations management capabilities. According to the Global state of information security survey (Defending yesterday: Key findings from the global state of information security survey, 2014), organisations which seek to be efficient and leaders in the field of information security have to meet three basic conditions:

- **Employing staff in charge of information security**: An organisation has to employ security management staff with adequate management

knowledge, whereas the board of directors must show appropriate support to the management staff regarding their authority and decisions.

- **Adopting detailed information security strategy**: The management staff has to adopt detailed information security strategic plan which must be approved by the board of directors. The strategic plan clearly defines objectives and purposes as well as responsibilities of ensuring information security.
- **Analysing the importance of information resources and assessing the efficiency of security measures:** An organisation has to periodically assess information security risks and evaluate the results of security controls. That makes it clear which parts of the information systems fail to ensure business continuity and which information is important for gaining information advantage. Such analyses also give insights into the efficiency of other conditions listed above.

Inadequate assessments of current situations or the lack of information on this issue can lead to wrong and irrational decisions resulting in inefficient information security. Stewart (2012) describes an optimal security situation in which all organisations first identify their security needs and then allocate the appropriate financial and human resources for managing those needs. Therefore, being acquainted with actual risk situations and information needs is one of the most important conditions for efficient information security. This is extremely difficult due to the specific nature of information security and cybercrime. Despite many available measuring instruments and accessible resources, there are still some methodological questions and practical limitations.

The most difficult task of every researcher is ensuring reliable results in assessing information security. The cybercrime situation is different from the conventional crime issues (e.g. violence-related crime) where more detected criminal offences result in a higher level of crime. Malicious information threats are specific deviances which do not necessarily lead to detection and reporting of incidents. On the one hand, a great number of cybercrime reports may demonstrate a stronger willingness of victims to report detected incidents or higher levels of information security in terms of better detection systems. On the other hand, the low level of reported or detected information incidents does not necessarily reflect high security levels, but incapability of detecting incidents or unwillingness to report them. Since organisations rarely report incidents and police statistics are an unreliable source of information (Comprehensive study on cybercrime, 2013; Goel & Shawky, 2009), business studies can be considered as the satisfying alternative for examining current situation. However, generalizing and explaining the results of such researches require caution due to unrepresentative samples.

2 METHODS

Similar to the general and overall corporate security, ensuring information security is not solely a technical issue, which should be considered while managing information risks. It is a multi-level discipline, which, in addition to the

technical tasks, includes organisational, management, user, strategic, legal and administrative tasks. Information security is a process that needs to live, develop and adapt; however, that requires a systematic and analytical approach.

In order to get an insight into current information security situation and define future challenges in this field, studies assessing the information threat situation in organisations were analysed and compared. The presented studies are international and up-to-date (majority of them published at the latest in 2012), and their findings have been confirmed by other independent professional sources. Detailed analysis of the research results shows that the most common research questions deal with examining the risk level, damages caused by actual incidents, and their impact on performing business operations. Unlike previous research, those which are up-to-date tend to focus on network attacks, social-media-related risks, mobile technology, cloud computing and outsourcing. Other important research topics include: (1) information security organisation, planning and strategy, (2) general management efficiency and feeling of satisfaction with information security (self-perception), (3) board of directors' support and investments, (4) employee information security awareness, (5) compliance with legal regulations, (6) current security controls in use, and (7) business continuity. With regards to these topics, analysis and findings are presented in the following section.

3 INFORMATION SECURITY SITUATION ANALYSIS

Despite the alarming predictions about the future development of information threats, there is one even more alarming finding: The majority of information threats that organisations currently face are occasional and basic in nature. Although this may not seem problematic, considering the fact that the least sophisticated threats can still bypass existing security controls, it actually demonstrates the unpreparedness for the emerging targeted threats. Stagnation of information security is problematic because the simplest forms of incidents are already causing major consequences which will be even greater in future. For example, researchers found that more than one-third of information incidents lead to disclosure of confidential information (Global corporate IT security risks, 2013), which in turn results in the loss of reputation, productivity and business opportunities. Confidentiality breaches, if not managed properly, could also lead to severe financial consequences and business illiquidity. Researchers note that smaller organisations suffer losses of tens of thousands, and perhaps hundreds of thousands of euros due to the event of severe information incidents, while in large corporations financial consequences are incomparably higher (Comprehensive study on cybercrime, 2013; Information security breaches survey, 2013). These and other findings suggest that existing security mechanisms should be immediately upgraded while considering the main corporate risk factors (structure, size, business model, links and partners, amount of technology and information, incident impact, etc.).

The results presented here can raise awareness and knowledge about the consequences of ineffective security systems which makes them important

for different target groups. First and foremost, they should be interesting for smaller organizations, because they are currently the most vulnerable part of the inter-organizational links. Their false sense of security can lead into deeper business insecurity, higher failure rate and greater information risks to connected third parties. Also, companies that are part of the public sector or the development industry, could use the analysis highlights in assessing the contemporary threat landscape. Clear presentation of the results is intended for security professionals, management and leadership, since their awareness is key to long-term effectiveness of corporate information security. Although most results are logical, they clearly show that saving at the expense of information security undermines all other security and business efforts.

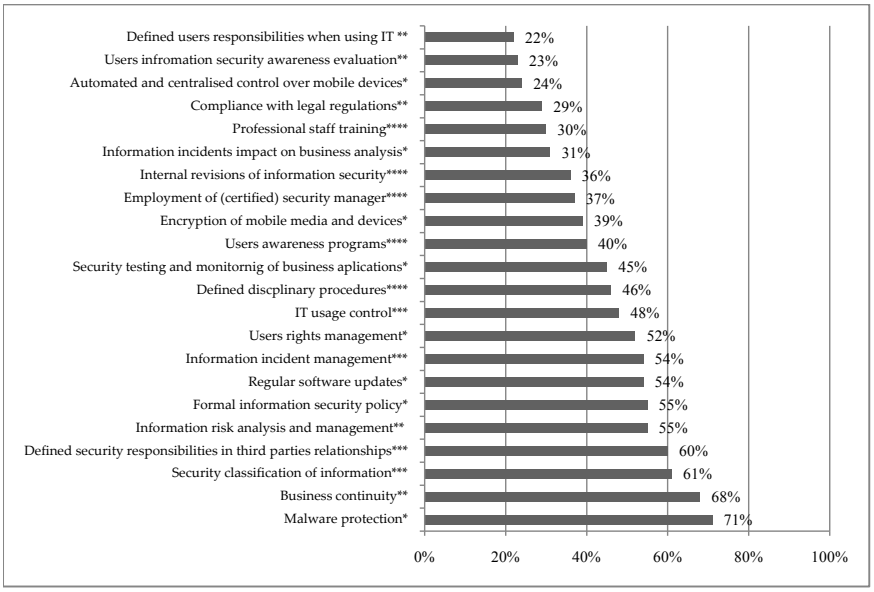
3.1 Current State of Information Security

In The Global state of information security survey (Defending yesterday …, 2014),[6] the opinions of organisations regarding the level of their efficiency in information security were analysed. More than two-thirds of respondents (74 percent) share the opinion that their organisation is efficient, about half of respondents consider themselves as the leading organisations in the field, whereas 11 percent of respondents are reactive rather than proactive in facing cybercrime-related issues. They do not develop a strategy and are inefficient. However, those opinions turned out not to reflect the actual situation. Considering various criteria, only 17 percent of respondents turned out to be leaders in this field. According to other research (Security effectiveness framework study, 2010), small organisations have the least efficient and the riskiest information security, as well as organisations which do not develop security management. In general, approximately 35 percent of organisations are inefficient, whereas the largest barrier to information security efficiency is the lack of awareness of management inefficiency and information vulnerability.

On the other hand, large organisations and the most threatened business activities tend to be more successful in information security planning and achieving its efficiency. There are two reasons why this finding makes sense. Large organisations have more expertise, resources available and experiences with actual incidents, whereas small organisations may have an impression they are less vulnerable due to their size (Comprehensive study on cybercrime, 2013). Figure 1 below shows the results of four studies on the corporate practices in the field of information security. The results indicate that general development of information security is still in relatively initial phases, since the majority of organisations do not adopt some basic security measures.

6 *International research performed by PwC has focused on measuring the state of information security in various business sectors. It was conducted among 9,600 respondents from 115 different countries. The conclusion of the research is that organizations are improving the security situation, but in doing so they are still not effective, nor do they follow the evolution of cyber threats. The results showed that the number of incidents is increasing steadily as well as financial loss caused by those incidents. Generally, organizations still use outdated security measures.*

Figure 1: Information security practices[7]



According to the data presented above, organisations first and foremost focus on regulating software and physical security measures. The results indicate that software protection, which includes antivirus programmes and firewalls, is the most developed security measure, followed by the physical measures for securing corporate capital and ensuring business continuity. Moreover, organisations have grown more aware of the importance of information confidentiality, since a relatively high percentage of organisations manages information resources in terms of resource classification and security during downloading and storing. On the other hand, staff management measures, such as raising employee awareness, staff training and control over ICT use, are less regulated and developed. Compliance with legal regulations is considered an insufficient condition for achieving information security; therefore, it is not a primary concern of organisations anymore (TMT global security study, 2013).[8]

According to the organisations' reports, the major barrier to information security management is the lack of financial means for information infrastructure. Despite growing attention to security, the budget for ensuring information security remains the same or insufficient in average (Defending yesterday …, 2014; TMT Global Security Study, 2013). Due to the lack of resources, many organisations fail to realize their information security plans and policy in practice (Global corporate

7 **Global corporate IT security risks (2013), **Information security breaches survey (2013), ***Defending yesterday … (2014), ****TMT global security study, (2013).*

8 *International research conducted by Deloitte analysed the practice of information security in technology, media and telecommunications sectors. 122 organizations in 37 different countries were included. The main findings highlight the changing motivations of organizations in managing information security. Improving confidence among customers and good security posture in the market are the basic advantages of information security, while compliance is no longer a top priority.*

IT security risks, 2013).[9] Namely, decisions on investments in information security are made by a board of directors; however, the leadership often considers only the financial benefits (Pironti, 2007) and therefore connects the security with costs involved. Concrete benefits of investments into information security are indirect and long term and therefore difficult to measure, and it is hard to assess to what extent an organisation has benefited from preventing attacks by unknown threats. And if a threat is prevented due to security, it might be assumed that the threat did not even exist (Burton & Stewart, 2009). In recent years, organisations allocate more resources to information security management; however, investments are still disproportional with regards to the growing use of ICT and evolution of threats.[10]

3.2 Cybercrime

Research proves that cyber attacks and misuse of information represent a common threat to many organisations, yet they do not address this issue properly. According to various studies (Data breach investigation report, 2013; Defending yesterday …, 2014; ENISA threat landscape …, 2013; Fourth annual cost of cyber crime study, 2013; Global corporate IT security risks, 2013; The impact of cybercrime on business, 2012;[11] Internet security threat report, 2013):

- In the past year, 91 percent of organisations were victims of information breaches;
- Approximately 66 attempts and 1,4 successful cyber attacks happens in a given week;
- The most common form of information threats are network attacks which exploit approximately 20 the most known information vulnerabilities;
- More than 70 percent of information incidents happen to be less or unsophisticated;
- 75 percent of incidents are opportunistic and 25 percent are organised; 66 percent of those incidents are detected several months after an actual attack and nearly 70 percent are detected by third parties; and
- External security incident solving takes approximately 27 days, whereas dealing with the internal incidents takes approximately 53 days.

9 *A survey conducted by Kaspersky Lab on the state of IT security. The sample consisted of 2,895 experts from 24 different countries. The purpose was to analyse their practices in addressing information risks and expectations for the future. The main finding is that cyber threats are a multi-level problem; for that reason, the surface treatment is the wrong approach.*

10 *Studies indicate that companies will have to invest more money in information security; at least a third of finances intended for IT, while in practice they are investing 4–16 percent of IT finances (Information security breaches survey, 2013; Defending yesterday …, 2014).*

11 *International research by Ponemon Institute has analysed the opinions of 2,616 security experts from five different countries on current practices in information security. The survey focused on the qualitative analysis of five different cyber threats: botnets, APTs, DOS attacks, malware and social engineering. The study notes that threats as we knew them no longer exist, because the perpetrators are merging into well-organised criminal groups that follow trends of online communication, mobile technology and cloud.*

According to the findings, organisations mostly deal with less complex information security risks. The majority of risks were opportunistic, meaning they resulted from current circumstances and the lack of basic security measures. This is a troublesome issue, since incapability to ensure protection against basic forms of threats means high vulnerability to more serious threats. Inefficient dealing with basic information security risks raises even more concerns, since 25–35 percent of security incidents cause disclosure or loss of confidential information; more than half of those cases lead to the loss of business reputation and one-third to the loss of important business opportunities and partners (Defending yesterday …, 2014; Global corporate IT security risks, 2013).[12]

According to one of the business research studies, information threats arise mostly from the external corporate environment (Data breach investigation report, 2013). Moreover, the research Internet security threat report (2013) found that the number of network attacks has increased by one-third as compared to the previous year, and that the most common source of cyber attacks are hackers. Other perpetrators might be contractors, suppliers and competitive organisations with financial and espionage motives (Defending yesterday …, 2014). The most common external threat is a malicious code, followed by information system penetration, social engineering, phishing attacks and cases of causing unavailability (e.g. the DOS attacks) (Comprehensive study on cybercrime, 2013; Data breach investigation report, 2013;[13] Global corporate IT security risks, 2013).

In addition to the external threats, information security risks arising from the internal corporate environment should not be neglected. Internal information threats arise from inadequate user behaviour and management decisions, from failure to act or negligence of a specific issue. Therefore, technology performance and information confidentiality depend on the behaviour of employees. The internal threats reflect mostly in the vulnerability of software and applications. That is a consequence of inappropriate maintenance (e.g., security updates) or the lack of understanding of technological innovations which organisations use in order to improve their production processes. Other internal information threats are user threats, which occur in the form of unauthorised data disclosure and negligent use of ICT (Global corporate IT security risks, 2013). A high number of cyber threats is also a consequence of insufficient user knowledge, low employee motivation or dissatisfaction. More than two-thirds of organisations that participated in the TMT global security study (2013) and Data breach investigation report (2013) consider employees as the most important information resource and, consequently, the lack of employee awareness as high information vulnerability. The most common targets of external threats are internal sources;

12 *Analysis highlights the following information as the most important and vulnerable: information about customers, employees, intellectual property, financial statements and financial data, organisational strategy, development and marketing plans, administrator and user rights.*

13 *The research conducted by Verizon, has been carried out in collaboration with 19 organisations (research and scientific institutions, law enforcement agencies, organisations responding to cyber incidents). Information base of 47,000 and 621 incidents of cyber intrusions in 29 different countries was made in the process. The study notes that the new age IT incidents are heterogeneous problem, so one-dimensional characterization, does not capture their complexity. The research concludes that all organizations are potential target of cyber threats, so "Assume you're breached" mentality must prevail.*

beside servers and network, accountants, system administrators, executives and board of directors, marketing and advertising staff are also exploited (Data breach investigation report, 2013; Internet security threat report, 2013).

Generally, all types of organisations deal with external and internal information security threats. However, the comparative graph (Figure 2) below indicates differences in types of threats affecting various types of organisations. Large organisations deal with more incidents on an annual basis (Internet security threat report, 2013) and are mostly exposed to more serious and sophisticated forms of threats (e.g. cyber espionage, DOS attacks, information system penetrations, misuse of confidential information), whereas small organisations are exposed to less serious forms of threats (e.g. viruses, Trojan horses, worms, phishing attacks). Other research also proves that small organisations are the most common target of unsophisticated malicious software or cybercriminals with financial motive (ENISA threat landscape …, 2013).[14]

Although findings indicate that large organisations are more exposed to information risks, small organisations still remain highly threatened. In comparison to small organisations, the larger ones are better protected against cybercrime and employ more experts from this field which results in better knowledge and understanding of information security issues. Therefore, simple threats are not overly troublesome for them, although they more often face organised and dangerous criminals. On the other hand, small organisations are often the target of opportunistic cybercriminals who quickly detect poor and inadequate protection (Internet security threat report, 2013), and spread the word about their findings, which can lead into multiplying threats. The interesting fact is that the targeted attacks equally focus on both small and large organisations (Figure 2) which makes sense. Small and vulnerable organisations represent an entry point to the systems of large organisations in the chain of suppliers/partners and are therefore attractive for wired cybercriminals.

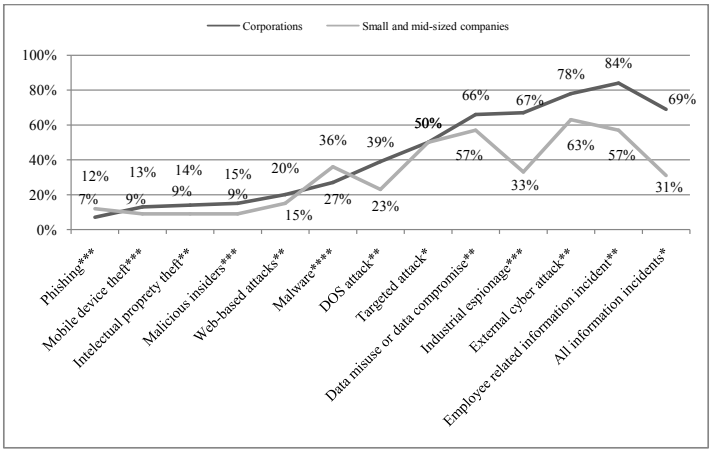


Figure 2: Information threat comparison by organizational size[15]

14 *59 percent of incidents happen in large organisations, 31 percent in the small ones, and the rest percentage in those organisations, which employ 251–1500 people (Internet security threat report, 2013).*

15 **Internet security threat report (2013), **Information security breaches survey (2013), ***The impact of cybercrime on business (2012), ****Comprehensive study on cybercrime (2013).*

In order to determine the most threatened corporate profile, some other factors, besides the size of the organisation, should be taken into consideration, such as the type of business activity and business sector. According to the Data breach investigation report (2013), Fourth annual cost of cyber crime study (2013),[16] The global state of information security survey (Defending yesterday …, 2014), Information security breaches survey (2013),[17] and Internet security threat report (2013), the most exposed to risks are large production facilities and public sector organisations which manage critical services. Those are first and foremost financial institutions (e.g., banks, insurance companies), healthcare services and the pharmaceutical industry, professional services and counselling (e.g. legal, architectural, medical counselling, revisions and system controls) and organisations in the field of ICT development (automobile industry, computer and information science, telecommunications).

Information threat situation analysis in the corporate environment proved that each and every organisation can be the target of a malicious incident. The majority of information threats are not serious, but the incidents are not dealt with within an appropriate response time. Organisations are most commonly challenged by external threats, especially network attacks and malicious software. With regards to internal information risk management, organisations should first and foremost focus on updating software and access control as well as on raising employee awareness. But users and networks are not the only targets of cybercriminals. It is necessary to emphasize that other corporate elements, which are results of micro-digitalisation, enable access from the external to the internal corporate environment.

3.3 Cloud Computing, Outsourcing and Mobile Media

As organisations tend to follow technological trends, they often make false decisions that lead to increased information vulnerability. The question of information security efficiency often coincides with the dilemma of transferring the responsibility for information security to the third professional subjects (so-called outsourcing of security functions), transferring information to the cloud and integrating mobile technology and applications into work processes.

In times of evolving threats and increasing demands for efficient information security, security management departments often decide to outsource. A growing number of organisations use services of cloud computing and exploit

16 *The survey conducted by Ponemon Institute covered 234 companies, 1,935 security professionals and 1,372 security incidents. The results showed that cybercrime is a threat which represents a high financial risk. According to the findings, the annual damage caused by cyber attacks varies between three hundred thousand and tens of millions of dollars per organisation. With that said, the damage depends on the size, business activities and security controls in use.*

17 *A survey conducted by PwC which has analysed the state of information security in British companies. The sample covered 1,402 respondents across different business sectors. The results of analysis showed that cybercrime is an important threat to small businesses which are forced to deal with problems that have long been considered the concern of large corporations. Due to the indifference, many of the small businesses are unprepared to tackle modern information security challenges.*

its advantages, therefore, outsourcing of computer capabilities and security is becoming very common corporate practice (Information security breaches survey, 2013). By outsourcing, some risks are transferred to third parties; however, at the same time, other vulnerabilities arise. Transfer of security functions from the corporate environment to the external one might result in decreasing the number of in-house employees that are responsible for ensuring information security. That makes organisations even more vulnerable, since they have less professional knowledge available and less control over threats. Regarding the transfer of services and computer capabilities, cloud computing appears to be troublesome in terms of its security, since it stores a large number of personal and confidential information.

Current use of cloud computing refers mostly to storing information on the network. Organisations also tend to outsource other services, such as website management, business mail management, payment and accounting services and business applications (Defending yesterday …, 2014; Information security breaches survey, 2013; TMT global security study, 2013). According to the latest McAfee report (McAfee, 2014), cyber attacks are increasingly focusing on business applications used by employees, the majority of which are not checked and approved by a security management department. When an organisation transfers its applications and information to the cloud, it loses security control over their operation and use. The service providers may offer those applications and information on the remote and unknown platforms, which can result in sharing and distributing confidential information in ways organisations are not able to understand and control. Such cases raise a question where information is actually stored and which formal-national regulations apply to information governance (TMT global security study, 2013). Furthermore, service providers often store and manage personal and confidential information of several clients at the same time on the same platform which attracts cybercriminals even more, since they can misuse more information in one place (Internet security threat report, 2013).

In the global online environment, a security incident in one organisation can influence information security in all of its partner organisations. Therefore, information security in the external environment also plays an important role. If organisations decide to cooperate with outsourcing service providers, they need to take care of the control and responsibility aspects of such services. Most importantly, a strict policy should be adopted regulating who is allowed to access the cloud information and under what circumstances, where the information is stored, who is in charge of the information and what is happening with the information during storage.

In addition to cloud computing, the major future security challenge for organisations is mobile technology which is one of the most vulnerable elements of organizational structure (Sjouwerman, 2012). Simple and widespread use gives the impression of a low risk level; therefore, the mobile technology protection has not been sufficiently adapted (Fighting to close the gap, 2012). Recently, the so-called BYOD trend ("Bring your own device") has exponentially increased which made insufficient protections even weaker. The term applies to integrating personal mobile devices, usually used in private life, into the corporate and

work environment for the business purposes. This results in an increase in an organization's vulnerability and, consequently, chances of information misuse. The most complex issues are expected to arise when employees will start to use their personal mobile devices to access business information via cloud computing services. The previous year analysis showed that the evolution of malicious threats and vulnerabilities in mobile media was more intensive and rapid in comparison to the evolution of threats focused on stationary devices. Just in the second half of 2013, the number of malicious threats has increased by one-third (McAfee, 2014).

Considering all those facts, the use of cloud computing services in combination with the use of mobile devices in the work environment, brings new information security challenges and risks which should be of primary concern to management in the near future. Since organisations try to follow security trends and technical innovations, vulnerabilities increase. Therefore, the decisions on changes and integration of new systems into a corporate structure have to be based on justifiable reasons. Negligence of security issues raises even more concerns, regarding the fact that, beside relatively known information threats, there are also well organised cybercriminals that use unpredictable and complex techniques for achieving their objectives.

3.4 Organised Cybercrime

Development of organized and structured cybercrime is the consequence of the increased interconnection of organisations, their mobility, information outsourcing and similar business and user trends which opened new canals for cybercriminals and created vulnerabilities as well as opportunities for attacks (The impact of cybercrime on business, 2012). Sophisticated cyber attacks are usually not carried out by individuals, but are the matter of wide social motivation, such as industrial and state espionage, information warfare, "hacktivism", terrorism and organised criminal underworld activities. Unlike opportunistic cybercriminals, such organised groups are well funded and highly motivated; they carefully set their goals, choose their targets in advance and employ competent hackers. The attacks are well planned and systematic—a great deal of time and means are used for gathering information and victim profiling which increases chances for performing a successful attack. According to the Data breach investigation report (2013) and Internet security threat report (2013), the organised crime groups with financial motive and state-supported espionage activities with military, economic or political motives prevail in this field. Both usually focus on large inter-organisational structures with massive amounts of information.

Cyber attacks caused by such groups are rarely isolated cases, but rather belong to an organised action and consist of various threats. That kind of cyber occurrences are called APTs (advanced persistent threats). And when an attack is focused on a specific target or victim (e.g. a specific organisation), it is called a targeted attack. The research indicate that targeted attacks are skyrocketing, and since they are hybrid threats they are the most sophisticated and troublesome types of cybercrime. Targeted attacks were initially financially motivated and

focused on the private sector, but now they happen to be increasingly politically and socially motivated (McAfee, 2014).

Another important form of organised cybercrime that poses a threat to the confidential information is "hacktivism" which combines social or political activism with hacking. The protesters and activists who used to block access to a certain location, building or physically disable business operation of a certain organisation now use the denial-of-service (DOS) attacks for the same purposes (Data breach investigation report, 2013). Such attacks overload the components of network infrastructures and disable their operation. In 2013, 25–40 percent of organisations were victims of DOS attacks (Information security breaches survey, 2013; TMT global security study, 2013) which resulted in the blockage of websites, postal and communication systems, as well as in general disruption of business operations that usually lasted up to six working days (Information security breaches survey, 2013). In order to redirect a victim's attention, the DOS attacks frequently occur in combination with other cybercrime techniques. The cybercriminals first perform the DOS attack and force an organisation to deal with the incident. During the organisation's focus on incident solving, they try to carry out other system penetrations from the background which the organisation is not able to detect because it still deals with the first incident (Internet security threat report, 2013).

To sum up with regards to the trends described, mobility, information sharing and interconnection of corporate structures cause organised cybercrime to grow. By using reverse engineering, new, less known and resilient cybercrime techniques evolve. Cybercrime tends to develop to such an extent that reactive responding to attacks and trying to mitigate the impact of attacks will not be sufficient for managing information risks anymore. To conclude, the review and analysis of studies reveal that saving money at the cost of security and ignorant behaviour are dangerous and risky approaches that threaten the success, productivity and competitiveness of organisations.

4 CONCLUSION

As organisations decide to regulate or update their information security measures, they need to understand that negligence of information security may cause higher costs than its maintenance. While it is true that initial planning and establishing information security is more difficult in comparison to its maintenance, it should be kept in mind that the impacts of efficient security pay off in the long term. On the basis of the prior research and expertise in the security field, a wide range of measures that appear to be the most efficient in practice is offered in the following list:

- Automated intelligent systems for threat detection and prevention (IDS, IPS);
- Mobile devices management, user policy and encryption;
- Advanced network and access control (UTM, NGFW);
- Risk management: assessment of information capital, vulnerability and threats;

- Processes and systems for preventing information loss and information recovery;
- Cryptography of mobile devices and information during communication or transferring;
- User rights management and system access control;
- Automated updating and security testing of applications and software;
- Efficient firewalls and prompt antivirus programs at all entry points,
- The list of authorised and unauthorised software and electronic devices;
- Professional staff training and competencies assessment;
- Separation of system and security roles and responsibilities, the control over the use of administrator rights;
- The control over users' insight with the need-to-know policy;
- Ensuring trailing and audit trail maintenance;
- Crisis management: response plans for the most important risks;
- Penetration tests: assessment of organisation's defence capabilities.

Currently, those measures listed are the most recommended and efficient security controls, and include not only technical security demands, but also other aspects of security management. However, it has to be taken into consideration that each individual measure does not ensure efficient information security. In order to be able to manage threats proactively, combining measures and multi-level protection are needed.

After planning and adopting changes, users have the greatest impact on information security efficiency; therefore, user management is the field that needs to be given more attention in practice. It depends on the security-aware and motivated users whether the plan and the rules adopted will indeed be considered in practice. Here are some recommendations for directing organisational behaviour and establishing strong security culture among employees:

- **Raising user awareness**: Regular seminars need to be organised for people who use ICT or manage confidential information at work. The seminars must be adjusted to user knowledge and situations (threats, vulnerabilities, rules) that are typical for a specific organisation. Moreover, the users must be acquainted with reasons for adopting rules and dangers that might occur if they do not act according to the rules.
- **Professional training of expert staff**: Since ICT and threats constantly change and develop, professional training of employees must be provided as well. Useless management and old-fashioned management techniques can be a huge barrier to the efficiency of information security and technology. A good way to follow security trends is by attending professional conferences and informal trainings.
- **Confidentiality statements and agreements**: User obligations and responsibilities need to be well defined and formal regulations for dealing with confidentiality breaches specifically outlined. By signing a confidentiality agreement, employees accept the risks and assure they understand what their responsibilities are as well as bind to protection of confidentiality. On the other hand, organisations need to clearly define what kind of behaviour is forbidden.

- **Motivating employees**: Any change adopted may bring disapproval and rejection among employees, especially if current processes are in use for a long period of time. Resistance to change is very common in technology fields and when restrictive rules are adopted. In order to integrate information security into the organisational culture and employee ethics, the needs of employees and their feedbacks on control functionality must be taken into consideration. Furthermore, while implementing restrictive rules, organisations need to respect the right to privacy and integrity.
- **Regular security meetings**: Information security must be discussed within the entire hierarchical pyramid. Management in the organisation should regularly report on innovations and current issues, help users to manage everyday dilemmas and encourage them to behave in accordance with the policies. Management should also inform board of directors about security needs and lobby for attention and financial means.

According to the given recommendations for regulating information security, it is clear that information security is very heterogeneous field which covers the variety of processes. Since technology changes on a daily basis, it is of great importance for organisations to choose services and devices rationally and carefully. Every change adopted by organisations also brings some negative impacts and vulnerabilities, therefore, they should adopt only such measures and follow only such trends they really need. Organisations must justify their decisions with concrete information and bear in mind their actual security needs.

The wide and macro aspect of information security issues need to be emphasized as well. In order to properly govern cybercrime, organisations need to design strong security architecture that goes beyond organisational boundaries. Most importantly, new and better cooperation methods between private and public sector must be adopted. Such cooperation must be based on mutual trust and sharing of responsibility. Organisations and both sectors must establish long-term partnerships that are beneficial in terms of helping in case of actual incidents and exchanging of information on threats, risks, trends, development, good practices and experiences regarding preventing measures. Such strategic partnerships and coordinated cooperation involving organisations that encourage each other rather than compete, would strongly contribute to better information security situation, improve understanding of the nature of cyber threats as well as raise general awareness.

REFERENCES

Bernik, I. (2014). *Cybercrime and cyber warfare*. London: Wiley.

Burton, S., & Stewart, S. (2009). *Security implications of the global financial crisis*. Austin: Stratfor Global Intelligence. Retrieved from http://www.stratfor.com/weekly/20090304_security_implications_global_financial_crisis

Comprehensive study on cybercrime. (2013). New York: United Nations Office on Drugs and Crime. Retrieved from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Data breach investigation report. (2013). New York: Verizon. Retrieved from http://www.verizonenterprise.com/DBIR/2013/

Defending yesterday: Key findings from the global state of information security survey 2014. (2014). London: Price Waterhouse Coopers. Retrieved from http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

ENISA *threat landscape 2013 – Overview of current and emerging cyber-threats*. (2013). Heraklion: European Union Agency for Network and Information Security. Retrieved from http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

Fighting to close the gap. (2012). London: Ernst & Young. Retrieved from http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf

Fourth annual cost of cyber crime study: Global. (2013). Traverse City: Ponemon Institute. Retrieved from http://www.hpenterprisesecurity.com/register/2013-fourth-annual-cost-of-cyber-crime-study-global

Gartner. (2013). *Gartner identifies the top 10 strategic technology trends for 2014*. Retrieved from http://www.gartner.com/newsroom/id/2603623

Global corporate IT security risks: 2013. (2013). Moscow: Kaspersky Lab. Retrieved from http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

Goel, S., & Shawky, H. A. (2009). Estimating market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404–410.

The impact of cybercrime on business. (2012). Traverse City: Ponemon Institute. Retrieved from http://www.checkpoint.com/products/downloads/whitepapers/ponemon-cybercrime-2012.pdf

Information security breaches survey. (2013). London: UK Department for Business Innovation & Skills. Retrieved from http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf

Internet security threat report. (2013). Mountain View: Symantec Corporation. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

McAfee. (2014). *McAfee Labs 2014 threats predictions*. Retrieved from http://www.mcafee.com/uk/resources/reports/rp-threats-predictions-2014.pdf

Pironti, J. P. (2007). Developing metrics for effective information security governance. *ISACA Journal*, 7(2), 1–5.

Security effectiveness framework study. (2010). Traverse City: Ponemon Institute. Retrieved from http://h71028.www7.hp.com/enterprise/downloads/software/Security%20Effectiveness%20Framework%20Study.pdf

Sjouwerman, S. (December 10, 2012). 2013 security prediction. *Cyberheist News*, 2(54). Retrieved from http://blog.knowbe4.com/cyberheistnews-vol2-53/

Stewart, A. (2012). Can spending on information security be justified? *Information Management & Computer Security, 20*(4), 312–326.

TMT global security study. (2013). New York: Deloitte. Retrieved from https://www2.deloitte.com/content/www/global/en/pages/technology-media-and-telecommunications/articles/2013-tmt-global-securitystudy.html

About the Author:

Kaja Prislan, MA in Criminal Justice and Ph.D. student at Faculty of Criminal Justice and Security, University of Maribor.