Faculty of Economics, University of Niš, 16 October 2015

International Scientific Conference

CHALLENGES IN BUSINESS AND ECONOMICS: GROWTH, COMPETITIVENESS AND INNOVATIONS

THE STRATEGIES AND MEASURES FOR PROTECTION OF INFORMATION SYSTEMS

Slavoljub Milovanović*

Dušan Perović*

***Abstract**: Many organizations are functioning on a modern way. One of the reason is that implementation of information systems is huge. It helped many companies to progress on market and to make better decisions. Information systems had connected all main players on market, and cut many costs which companies had in past. With good information system, creating new ideas and solving problems is much easier. But information systems are also vulnerable on many circumstances. Sometimes they can produce big problems for companies and it takes a lot of time to bring everything to normal. The aim of this paper is to show how organizations can protect their information systems, where can problems arise and to see experience of some companies who are specialists for protection against cyber attacks.*

***Keywords**: information systems, security measures, strategies, levels of protection*

1. Introduction

Modern business world characterize dynamic in carrying out business tasks and solving their problems. Until just a century and a half it was unthinkable that technology will develop so it could change the life of all people. The invention of steam engine, as well as printing machine, steamships and locomotive have influenced the change in basic living habits of humans. Big industrial boom by the end of XVIII and on the beginning of XIX century enabled bigger trade between some regions and later even between different states and continents. At this way, many countries were given an opportunity to improve their economic performances. Period after the Second World War brought new trade relations were big corporations have started to make a huge impact on global economy. That period also brought bigger funds for many researches, which aim was to create new technology.

* University of Niš, Faculty of Economics, Serbia;
✉ smilovan@eknfak.ni.ac.rs bokaperovic@yahoo.com
UDC 007:004

One of the crucial moments in modern history was finding a microchip back in seventies. That helped to develop computers, that people have started to use for their business. All processes switched to automatic and workers only had to watch new processes and correct possible mistakes. Computers have important role in architecture, economy, math, medicine and many more sciences. Bigger use of Internet helped many companies to make huge profits and also to cut costs. One of the main tasks for companies in the future will be data management. It will be important to make a good selection from many data so companies can use them on a proper way. Data turn into information and that information can be crucial for doing business. Information system must be safe for use because these days there are many abuses of data which can make damage to information systems and finally companies themselves. Combination of internal and external factors that abuse information system must be carefully watched and stopped for further damages.

2. Information Systems Security Strategies

For organizations it is important to be well prepared for potential problems at their information systems. There must be some kind of behavior plan which represents possible ways for solution of information problems and also that plan must help organization to bring their business back to normal. Data security and use of data have to be one of the priority tasks for IT department. Employees at IT department must follow all data process so they can create a strategy for critical situations. Recovery has to be planned in a short time so everything can be brought back to normal. Later reactions cannot be effective if employees have not noticed problems momently.

Critical element of every security system is existing of a business continuity plan, also known as a disaster recovery plan. This plan identifies an organizations exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, while maintaining competitive advantage and value system integrity (Elliot et al., 1999., p.48). The purpose of a disaster recovery plan is to help employees to react properly after disasters and to try to bring business back to normal in a very short time. Restoring business is a hard task, but everyone in company must put efforts for finding a proper way of business without having any new problems.

There are few ways for restoring business and it includes some backup sites like: hot, warm and cold site. Hot site gives huge opportunities with its services, communication links and physical operations. All resources, telephone systems, applications and work stations duplicate for improving security of information systems. Warm site has almost every services like hot site has, but it does not includes some applications and work stations. It includes servers, but some basic needs for employees are not included such as improved tools of search or bigger space for data. Cold site offers basic services like building a room with heating, air conditioning and humidity control. No work station or improved hardware are offer by cold site. Good thing is that cold sites takes a care of some long time issues like building or renting high speed communication lines or installing high capacity power lines. Comparing to that buying or installing server does not take a very long time. Hot sites reduce most of the risks, but they are very expensive. Cold sites are cheaper than hot and warm sites, but they do not reduce risks at the same level. Final decision about backup sites will be made by managers, who know very well the capability of organization.

The Strategies and Measures for Protection of Information Systems

Many companies apply different types of controls for improving security of information system. Installing controls is necessary, but not enough powerful for security of information system. Employees responsible for security of information system must ask themselves regularly these kind of questions: Are all controls have been installed with a specific purpose? Are they enough effective? Is there a possibility to occur any security problem? How to react when security is in danger? To answer all these questions companies must implement Information System Auditing. Under Information System Auditing mean that all inputs, outputs and process inside a system must be carefully followed and react properly if there occur any error. There are two types of audit: internal and external. Internal audit is usually implemented by auditors from accountable and IT part of organizations. Internal auditors know very well all processes at the organization and they can easily correct potential errors. Internal auditors are usually controlled by external auditors. External audit is performed by an authorized audit company, which has obtained the license from the competent auditing institutions. In the context of information systems auditors observed potential hazards and methods of control checks conducted by the companies. Auditing analyze computer operations, the integrity of data, softwer applications, privacy and security terms, inputs and outputs, control cost and productiveness. Auditors often give guides to companies for making business more effective.

Auditing of the information system have three typical procedures: *1. auditing around computer; 2. auditing through computer; 3.auditing with computer*. Auditing around computer checks outputs and connects them with appropriate inputs. Auditors check if products or services had been made by using a specific computer or not. Auditing through computer look for all processes and data inside a computer. Logic path of operation is determined and then all data are tested inside system. Auditing with computer combine data and hardware of clients with data and hardware of companies. Auditors use simulation programs to find if data are truth. Simulations are good tool if auditors want to check regularity of doing business and find any possible abuse of data.

Public companies and their accountants and auditors have big responsibility for data security. Accounting ethics obliges accountants and auditors to do their job professionally and without any outside pressures. The aim of accounting is to show financial status of organization and auditors have to determine the validity of data which accountants had used in financial reports. Some elements of forensics must be included to see real truth. Financial sector of every organization must have responsibility for potential losses or abuses. Board of managers want to follow all processes inside the organization. This way, it would be easy to find weak links inside the company. Today many transactions go through communication networks and there is a slight possibility that some data can be intercepted and used for wrong actions. Hackers know that financial and assurance institutions have big funds, so they will always be one of the priority targets. In the past, attacks on banks had happened and because of that managers try to improve the security of information system.

Every part of organization must be prepared for any security problems. Marketing managers through electronic commerce collect data about clients and that gives them opportunity to create various product and services for them. Internet criminals know that organizations have some valuable data about their clients and they are finding ways to steal those data from company. Stealing data can cause big problems for companies such as bad

reputation in publics, lawsuits from customers and in the end losing customers to competitors. Companies often use CRM (Customer Relationship Management) operation to track customers and to create a good relation with them. Privacy terms must be improved and that is the main task for every company. Usually, customers give some personal data like numbers of credit cards and accounts which can be abused if they would fall in wrong hands. Organizations must think what data they do really need because too strong and too weak security cannot be the right solution. Balance between strong and weak security must be found. Financial sector is also in danger because they do all payments and know overall financial status of company.

HR (Human Resource) department also have important role in information system security. All across organization employees use computers and communication networks for doing business. But there is a one problem. No one can guarantee that every employee properly use computers. One of propositions is to install specific type of software which tracks how employees use computers and on that way every company can develop path of data. Everytime when there is some irregularity, managers can react quickly and find it. Today, IT department has a large impact on company business. IT department has a task to make all informational processes and technologies safe for use and their help is very valuable for other parts of company. Also, due to its role, IT department is probably the most critical part of every organization. When communication links failed, all attention will be switched to IT department. IT is very important and new investments in technologies are always precious. Without new technology all data processes will slow down by the time and company will have huge costs.

Many information systems have become vulnerable to external influences. The use of Internet without proper protection and manipulative wireless technologies represent the roots of the problem. There is a bigger use of tablets and mobile phones in business world and all these devices do not have good protection or upgrading of antivirus software is not effective enough. Another problem are hacker skills. During the investigation about hacker attacks true identity of hacker can be revealed, but investigators sometimes do not go deeper. Sometimes it is better to know more about hackers skill, especially how he got such a good knowledge about information security. This could help many institutions to upgrade their security systems and forecast possible attacks. Some hackers, after punishment, start regularly business in IT sector and their experience can help in future fight against cyber criminal. The support of company in doing security tasks is always welcome. Investment in education of IT experts can bring good results only if both sides have same intentions.

Information systems face numerous attacks that can be classified into ten specific types:

1. *Espionage* – individuals unauthorized access to organizations systems , follow data process and prepare illegal actions;
2. *Information extortion* – attackers threatened to steal data or they have already done that, so now they are blackmailing managers for money or some new data. In this kind of situation, organizations sometimes pay attackers just to keep the voice down and not to tell anyone for things that they have done to organization;
3. *Sabotage and vandalism* – this kind of attacks have aim to harm the reputation of company and to make company lose clients and money. In the past attacks were usually physical, but today they are usually virtual;

4. *Stealing of equipment* – attackers have figured out that all crucial information are located on many devices, so it is better to steal them and have a control of those information. Bigger capacity of devices means bigger security risk for companies;
5. *Identity theft* – attackers sometime use false ID to access the system. They steal employees personal documents so they can use them for illegal actions. When theft is discovered, first trail usually leads to company employees and there is a slight suspicion that they work for attackers;
6. *Preventing compromises to intellectual property* – some researchers spent whole life for inventing something. When they finally discover something, someone can abuse their inventions for criminal actions. The problem is that intellectual property often requires some digital sign, which hackers can abuse. In many states law does not cover digital signs at intellectual property and that is a big problem for researchers;
7. *Software attacks* – attackers put malicious software into organization system. These kind of attacks are profit oriented and it requires companies to upgrade their security, if they want to keep their data safe;
8. *Alien software* – this software had been installed on computers through process of duplicating data and methods. This software does not represent classical virus, but it can follow many data processes inside the system;
9. *Supervision control and the acquisition of data* – this attack cause damage to real world processes that are important for organization. All physical and transport processes have been monitored and after some period real attack happened.
10. *Cyberterrorism and cyberattacks* – these days this is the most often kind of attack. Many companies and institutions have been attacked this way and attackers usually leave some message after attacks. That message usually has usually a political sign.

Many organizations must improve risk management, if they want better security for data. Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations missions (Stoneburner et al., 2002., p.4). Sometimes organizations take over the risk and do not react at all, which is not a good for them. Another important thing for organizations is that they must find a proper balance between control processes. Too much control is not good because it can slow down other important processes in organizations. On the other hand, weak control cannot slow down processes, but it is not immune to outside attacks and possible abuses. Managers and IT sector must analyze all processes very carefully and then propose valuable solution for their security.

3. Measures for Protection of the Information Systems

The stability and security of information system are important for many companies and institutions. Information system can help organization to start and finish new business projects, analyze markets and bring better services to clients. Information systems contain numerous data bases, that can turn data into useful information which can later be used for doing some business. Information system has big influence to other parts of organization and they usually request them to transform so everything can function

normally. Global markets push information systems to change constantly and organizations who change by the time have a better chances to survive.

Development of information system has a huge influence on technological, economic and social part of organization (Milovanović, 2008., p.106). Technological part involves all automatic procedures and technology that company is using. For finishing tasks organizations use many tools, but changes at information systems can give advantage to different kind of tools. Changes must go in more effective direction and bring better results for organization. Many departments have IT experts who usually need additional knowledge from economy and law, if they want to understand business processes well. On that way, there will be better understanding for dealing problems. New organizational structure brings better coordination between different departments of company and also bigger addiction for information. The movement of information is very quick and it requires bigger attention. The path of information must be clear and because of that companies must find way to react quickly if there occur any problem. Information system can help employees to make decisions, but more important for employees is to recognize the significance of information system. All internal and external processes must be carefully watched and then employees will know which information to use.

Every information system is facing different kind of dangers, which can be caused by purpose or not. Sometimes natural disasters such as earthquakes, tsunamis and avalanches can put information system into disorder. With better connection between devices and appearance of wireless technology information systems had become vulnerable to different human actions. Some actions like data theft, unauthorized access, stealing hardware and inserting viruses into software are more often these days than natural disasters. Development of Internet had made much easier access to different documents, which can be abused. This can cause big material and financial loss for company. Also, reputation of company can be in danger. The presence of technological criminal is very wide. Stealing important documents and files can bring money to one side, but also can bring a terrible loss to the other side. Having crucial information is a big advantage to someone who have that information and has a big motivation to earn something. Many security services very carefully follow transfer of data so they can react properly on time. Systems are in big danger if protection is not good enough or if it reacts too late.

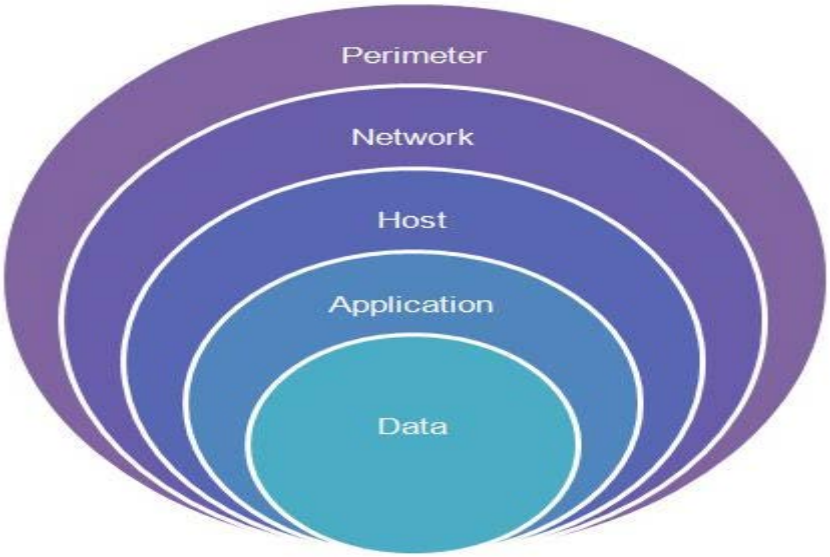
Due to low security, many organizations have started to implement certain kind of controls or defensive mechanisms. The aim of these controls is to protect all crucial parts of information system, which include hardware, software, data base and communication networks. Organizations have started to use more security levels for better protection. With security levels, every part of information system is covered so any possible attacks will be discovered immediately.

Defense-in-depth concept, presented on figure 1 encourages multiple-control levels. More controls are needed due to more cyber attacks. Hackers will always try to find a possible way to get company data and to avoid security system. With implementation of defense-in-depth concept companies have better chances to beat hackers and to maintain the security of information system.

When servers, inside the levels, locate a problem, they immediately send information to managing board and wait for further commands. Perimeters usually have firewalls which can block unknown users and their actions. They are the first level of

protection so they must be upgraded in certain period because that way company will stay immune to outside attacks. Networks and hosts are safe when perimeter is functioning well, but when they all are broken attackers can easily use applications to see needed information. Protocols between levels must be coordinated so employees can see the transfer of some data which are important for organization.

Figure 1: Defense-in-depth concept



*Source:*http://www.tech-wonders.com/2012/08/how-cyber-attackers-and-criminals-use.html

Organizations are implementing security controls due to possible abuse of data and unauthorized actions taken by individuals. With the help of security controls, problems can be easily discovered and they can give enough time for information systems to recover from attacks. For implementation of controls it is better for employees to be well educated, so they can see the importance of secured information system. Everyone in organization must have active role in improving security and everyday learning about new processes and procedures can be very valuable. To oversee the flow of data and to spot the weakest links, organizations can implement three types of controls: *physical, access and communication type of controls.*

Physical controls have role to prevent the unauthorized access to company documents. This type of control involve different kind of defense mechanisms such as walls, doors, fences, gates, alarms, guards, pressure and temperature sensors and movement detectors. The role of the guards is underestimated for two reasons. First, for someone their job is not interesting and not well-payed. Second, while they were doing their jobs, they could be distracted by other employees that can cause big security problems. The presence of guards is important and they were used more often than the other physical controls. One of better physical controls is limiting the access to certain documents or files. Users are allowed to access files only at certain time and on a certain way. On this ways users left trails which can help managing board to recognize users. With the help of physical controls, the number of unsuccessful logins can be lower and it can order employees to shut down

computers right after they finish their work. Computers can be set for automatic shut down after some period, if employees forget to shut them down.

Access controls can permit individuals to use data in case of unauthorized entries. Two majors functions of access controls are: identity check and verifying the permissions. Identity check or authentication confirms the identity of person who wants to access the information system. Users who want to access data first must pass identity check, which can identify true characteristics of users. On that way management board can see who access system, how long, how often and what do they really do. Applying identification of identity use following methods: *something the user is, something the user has, something the user does and something the user knows*.

Method something the user is represent biometric way of recognizing physical characteristics of users. Here many companies and institutions use fingerprint scans, palm scans, retina scans, iris recognition and facial recognition to identify users. Fingerprint scans, retina scans and iris recognition are most used by organizations and their implementation was very successful. For an example, new identification system in India helped many people to achieve some benefits. Fingerprint scans and iris recognition helped social services to identify ID of many citizens who live in slums to achieve food benefit. Aadahaar project in India revealed true identity of almost 1,2 billion citizens, who live in a very poor conditions. Police stations and city halls got modern equipment for discovering true identity of citizens. New technology was accepted very quickly by both sides and results showed that there were about over a half less abuses of citizens identity. Many people in India, now know their age number and also they can bring an evidence about place of their birth or a place where they reside. The capacity of data base is huge (20 petabytes) and every citizen document contains about 8 Mb of data.

Something the user has pay attention to use of regular ID card, smart cards and tokens. Regular ID or dumb card usually have a picture and a signature of owner. The similar thing is with most identity cards of citizens, who have their picture, signature and address written on card. Unlike the most regular ID, smart cards have a chip which contains important data of users. On this kind of card there are more information about holders and also e-commerce use a lot of smart cards. Tokens also digital display that represents a login number for employees to access the system. Login number changes with every new login, so it has a stronger protection. It is interesting that few banks in Serbia, have recently offered tokens for their clients who accepted tokens as a new non-cash mean of payment.

Something that user does uses voice or signature recognition to identify the true identity of users. At voice recognition, user can say a sentence that was previously recorded and approved by management. If two voices match, identification is successful. Similar thing is with signature recognition, only difference is that computer here check the signature. With authentic signature user can access to needed data. Something the user knows can identify users with the use of passwords or certain phrases. Passwords can be a big security problem, because many people use same password on different accounts and if their password is discovered on one account, other accounts will be in danger. Passwords are vulnerable to cyber attacks, so people must start to use improved passwords. These kind of passwords, have more letters, numbers, symbols and they are longer. They are hard to guess, and they must not contain some personal data like day of birth or a name of a pet. New passwords have to be much easier to remember, so one of suggestion is to use acronyms. For an example, password “dMp9I” is stronger password because it is an

acronym with number and letters of a different size. Also the use of a phrase is acceptable. “awakewithlove” is a kind of phrase that it is easy to remember and it has a meaning for user. Here can user also change the size of letters to make this password stronger.

Verifying the permissions or authorization can determine which privileges or rights after verifying the identity users have. Organizations have intern rules and procedures, so privileges depend on them. Authorization can allow users to login several times a day and use certain data. Here management can decide to allow employees to use data only for specific type of work or for work in general. Privileges can be time oriented or they can focus on a specific procedures. Also, organization make final decision about the access controls, but many of them implement multiple access controls. They combine smart cards with the voice recognition, or iris recognition and passwords. Multiple access controls can make security system stronger, but only question is will this be suitable for users? More security controls can sometimes make employees tasks more difficult, but with better protection company data are safer. When organizations want to built a stronger security system, they must first look at their capabilities and then decide how to improve security system.

Communication controls are the best way to secure the movement of data across organization network. This way, companies can easily control data and see if there are any problems which can stop further movement of data. Communication controls help organization to improve security system and to locate possible spots where can problems occur. Communication controls that organizations use are: firewalls, anti-malware systems, whitelisting and blacklisting, encryption, virtual private networks (VPNs), SSL protocol and employee monitoring system.

Firewalls help with movement of a specific type of data between Internet, virtual private networks and other kind of networks that companies use. Every data that enter company must first pass firewall. With firewalls, unauthorized logins of unknown users are blocked. Firewalls have a long specter of protection. They can follow data from house networks (private users networks) to company network. Firewalls usually follow company intern rules about security and every little troubleshoot will be quickly discovered. Organizations can use external and internal firewalls. External firewalls are located between the Internet and private networks. Internal firewalls are placed between private networks inside the organization. Between two firewalls is located the demilitarized zone (DMZ). Every message or data that passes external firewall directly goes to DMZ. Then, if all criteria are satisfied message will come to users inside the organization. Only problem for firewalls is that they are vulnerable if anti-virus system is not upgraded. Many viruses are evoluting very fast, so there must be good software for protection. If the protection is not good, viruses can break firewalls and make a huge damage to organizations. For companies, it is better to have anti-malware system. This way, companies can identify and eliminate all viruses. Today many famous organizations use software packages like Norton AntiVirus, McAfee VirusScan and Trend Micro PC-cillin for protection.

The biggest disadvantage of anti-virus software is that they all react right after attack had happened. They do not have any preventive role and because of that companies have started to use blacklisting and whitelisting. Blacklisting show what software and what actions should not organizations use. That is a some kind of directive and all employees must keep to following directions. Whitelisting suggest opposite things. It is a recommendation for using a specific kind of software or for doing particular actions. This

way only specific actions are recognized and employees must do everything what was named at whitelist. Organizations can also use encryption for sending messages inside the organization and prevent unauthorized activities. This is the best way for sending sensitive materials through laptops, mobile phones or tablets. Encryption involve files, folders or entire hard disc (Kerby, 2011.). With the help of encryptions data had become reasonable only to users who are receivers of messages. That way, thieves cannot understand full meaning of the message. For encryption clients use public and private key. One key is for making a code of message and the other key is for recoding. Public key can use everyone who have access to certain system, but only a few persons have private key. With private key receivers can see full message and understand the meaning of sent message. Sometimes intermediaries can be involved in this whole process and they approve digital certificate which confirm the authenticity of electronic document. At that point, receivers will be sure that they received valid message with data. Sony often uses help of company named Verisign for transactions with clients. Verisign can give digital certificate to all Sony document, which will later be sent to certain clients. On this way Sony usually makes arrangements with suppliers.

Virtual private networks (VPNs) are private networks that use public network (such as Internet) for accessing the information system of organization. VPNs have been built upon specific accounts, encryption and other techniques for improving the security of information system. Employees can connect to network from a remote devices and there is a bigger flexibility for users, because they can connect to network with their computers, tablets and even mobile phones. Security is improved, because every move of user can be known, so it is much easier to recognize any abuses of network. Tunneling represents important component of VPNs. With the help of tunneling data can be transfer from one to another protocol. Also, encryption is used for sending the data to appropriate users, without moving from a right direction. SSL protocol is encryptical standard which improves the security of data, especially one on banking or credit cards. Web servers and Internet browsers do coding and recoding of data. This operation requires the use of a specific URL address, titled with “https”, not anymore with “http”. That way better and secured connection had been established.

Many organizations use employee monitoring system (EMS) as a protection for information system. With EMS management board can have a closer look to all activities of employees. This way board can see how many hours are employees dedicated to work, how many hours do they spent on Internet and what do they do on Internet. EMS is good if companies want to improve the productivity of organizations. When employees are monitored, it is easy to discover weak spots at organization. In case of any dispute with any of employee EMS can bring evidence about activity of certain employee. Company named Vendors develops software for monitoring employees and their famous products are SpectorSoft and Websense. These software applications allow managers to have a closer look at the situation inside the organization and to help board in making an important decisions about work tasks. Only problem about EMS is the part about implementation. If organizations use EMS on a right way, it can help them to improve productivity. Employees in some situations can be on a huge pressure, but only if they work hard and effectively, they will not pay attention to EMS. Any abuse of EMS can harm the reputation of company, so managers must be very careful with this tool.

4. Fighting Against Botnets - FireEye

FireEye is one of the most effective and leading company in a fight against cybercriminal. This company provides services for numerous corporations, institutions and governments in more than 40 countries worldwide. FireEye has been following the lifecycle of many viruses and that helped them to develop software applications for further investigation and elimination of viruses. FireEye had participated in investigation of many cyber attacks such as:

- Aurora in 2009, where Chinese hackers planned to attack Google and other IT companies;
- Coreflood, a botnet which had stolen a millions of dollars from banking accounts of world famous banking corporations in 2000;
- ZeuS, a malware software which had stolen many identities of users worldwide for stealing money from accounts of many financial organizations.

FireEye proved as a powerful fighter against botnets. When hackers get into the computer system of a company they install servant code, which allows them to have full control of computers and company information system (Šoškić, 2006.). With control of information system, hackers have access to all data which they use for further criminal activities. At that situation companies are completely locked and any possible actions, without an assistance of IT experts can make things more worse. Fighters against cybercriminal usually have very huge experience behind them and know what to do. Some of the fighters against hackers, were hackers in a past which can help them to figure out the solution easily and quickly. FireEye has a lot of experienced IT experts, who have handled pressure very well and who worked for organizations that were usually a subject of a attack. This is big benefit for FireEye and all organizations who use their services.

Fighting against all sorts of abuse must first motivate companies to know something more about criminal activities. As we can see in table 1, source of threat could be hackers, computer criminals, terrorists, industrial espionage and insiders. Biggest problems companies have with hackers and computer criminals, but today terrorists and industrial espionage are more wide-spread among the other abuses. Insiders can be big problem for security in future. This kind of threat represent just a little danger, but activities that these persons do can be much bigger problem in future. Usually, hackers and computer criminal develop from insiders, so security companies such as FireEye must pay attention to insiders right on time, before they become chaotic.

One of the most known activities of FireEye was action against Rustock botnet. Rustock was powerful botnet that had sent spams to many e-mails worldwide. Spams had advertised fake drugs and cosmetics, but also Russian stocks, which was very interesting for potential clients. Rustock generated about 44 billion spam e-mails per day, and in period from 2007 to 2011 it illegally took over control of more than a million computers around the world. That helped Rustock to generate a huge profit.

Table 1: Human threats for information systems

Threat - Source	Motivation	Threat Actions
Hackers	Challenge	Hacking, social engineering, system intrusion, break-ins, unauthorized system access
	Ego	
	Rebellion	
Computer criminal	Destruction of information	Computer crime, fraudulent act, information bribery, spoofing, system intrusion
	Monetary gain	
	Illegal information disclosure	
Terrorist	Blackmail	Terrorism, information warfare, system attack, system penetration, system tampering
	Destruction	
	Revenge	
Industrial espionage	Competitive advantage	Economic exploitation, information theft, intrusion on personal privacy
	Economic advantage	
Insiders	Curiosity	Assault on employee, blackmail, computer abuse, fraud and theft, interception, malicious code, sale of personal information, system bugs, system sabotage
	Ego	
	Intelligence	
	Monetary gain	
	Revenge	

Source: Stoneburner et al., 2002.

For months, FireEye together with Microsoft and Pfeizer had been trying to set a plot. This union was a result of an abuse of Pfeizer logo in some spams, which made Pfeizer officials mad. During 2011. it has been discovered that Rustock had seven information centers in USA, with 96 servers. Later two more were found in Europe, Netherlands. Although operation had good results, Rustock found the way to survive. This time they attacked technical team of Microsoft. That attack had weakened technical team, but with much more difficulties they had found solution for this problem. If they did not react on time, all data would probably be lost. Attack was very strong, but it helped FireEye to analyze equipment carefully. It had been discovered that equipment was bought in Azerbaijan and that Rustock has two main servers in Moscow and St. Petersburgh. Forensic analysis discovered that Rustock earned first money through companies that never existed. Also on website www.webmoney.com Rustock use fake account under name Vladimir Alexandrovich Shergin to trick naive clients. Reviling of fake account helped police department to locate the place of criminals and they were later cought.

Microsoft had filled lawsuit on April 6, 2011 against Rustock botnet to the Federal court in Seattle. Soon was Russian minister of interior business informed about criminal activities of Rustock botnet and they received reports from Microsoft. At that time Microsoft announced reward for any information that could lead to discovering true identity of Rustock hackers. Meantime more Rustock hackers were discovered, but still about 600.000 computers are still under the control of Rustock botnet. New command centers and servers were discovered and every new trail leads to catching responsible persons. Security check worldwide for 2013 is presented in table 2.

Table 2: Security check worldwide for 2013

Attacks worldwide	Countries that suffered attack most	Institutions and organizations that were under attack	New viruses that were discovered
Total number of attacks: 39.504 Attacks that repeated on same targets: 4.192	USA, Great Britain, Israel, Canada, Japan, Switzerland	Banks, state administrations, consulting and marketing agencies, schools, police, military, telecommunication companies	DarkComet, LV, Gh0stRAT, Poison Ivy

Source: FireEye, Advanced Threat Report, 2013.

FireEye report showed that presence of unauthorized activities is still big. Interesting thing is that many of countries who had suffered attacks were initial creators of viruses and malware software. Among the organizations that were under attack number of companies from energetic and telecommunication sector are growing, which leads to new markets for cyber criminals. Predictions are, that in next few years the intensity of attack is going to be weaker, but organizations be more vulnerable to attacks. Proposition for them is to upgrade security system and look forward at new challenges that are in front of them. Companies from IT sector such as Google, Yahoo, and Apple must be very careful, because they are all becoming targets for cyber criminals. FireEye will always be there to fight against botnets and every other kind of cybercriminal, but they also need strong support for doing their job.

5. Conclusion

The question about security of information systems will be always present with new developments on global markets. Today business world is much different than two decades ago. People do business on Internet, communicate through different networks and improve their activities wireless. All that has advantages, but biggest problem is still security. There will always be someone who will try to trick people on Internet, use their personal data and generate profit for himself. Because of that companies are implementing strategies for security of information systems. Companies must be prepared for critical situations and implementation of disaster recovery plan can be useful. Also all departments must be involve in creating and implementing security strategy. Process of auditing is good, because it is first major step for discovering disadvantages of information technologies.

Organizations must implement measures for security of information system. It is better for them to have multiple system of controls, because security will be less problem. Most of companies and institutions use regular ID cards, voice or iris recognition, passwords and phrases to protect data. Employees must see the significance of controls and without their participation in whole process, everything will be worthless. Every security systems must be created upon company business and there is no place for employees habits. Sometimes it is better to involve capabilities of employees in whole security process, because they are important part of every organization.

There has to be bigger support for companies like FireEye. This kind of companies are unique and also very important for modern business. IT companies represent companies of future and IT sector is the fastest growing sector in the world. It can bring more profit for owners, so there is a slight possibility that they are going to be under attack in the future. Fighting against cyber criminals is a very long process, but all sides must be patient and careful if they want to achieve their goals. In the future, social networks will be one of the biggest threats for information systems, because there can be found a lot of interesting data for abuse. That is one of the reason to work more on security of information systems.

References

1. Elliot, D., Swartz, E. & B. Herbane (1999) Just waiting for the next big bang: business continuing planning in the UK finance sector, *Journal of Applied Management Studies*, 8(1): 43-60
2. FireEye (2013) *FireEye Advanced Threat Report: 2013*, Milpitas: FireEye
3. Jovanovic, R., Milovanovic, S. (2008) Upravljanje elektronskim poslovanjem preduzeca, Nis: Ekonomski fakultet
4. Kerby, F. (2011) *Understanding encryption*, Swansea: Sans Institute
5. Mayer, N. (2009) *Model-based Management of Information System Security Risk*, Namur: University of Namur
6. Milovanovic, S. (2008) *Upravljanje znanjem preduzeca*, Nis: Ekonomski fakultet
7. Soskic, R. (2006) Zlonamerno umrezavanje kao oblik zloupotrebe informacionih tehnologija, *Ziteh 06*: 1-13, Beograd: Udruzenje sudskih vestaka za informacione tehnologije
8. Stoneburner, G., Goguen, A. & A. Feringa (2002) *Risk Management Guide for Information Technology Systems*, Caithersburg: National Institute for Standards and Technology

STRATEGIJE I MERE ZAŠTITE INFORMACIONIH SISTEMA

Rezime: Mnoge poslovne organizacije posluju na savremeniji način, a kao jedan od razloga za takvo poslovanje jeste upotreba informacionih sistema. Zahvaljujući informacionim sistemima, kompanije ostvaruju bolju tržišnu poziciju, lakše donose poslovne odluke, povezuju se sa ostalim učesnicima i smanjuju troškove poslovanja. Dobar informacioni sistem doprinosi razvoju novih ideja, ali i lakšem rešavanju problema. Međutim informacioni sistemi su osetljivi deo preduzeća, zbog čega mogu prouzrokovati ogromne probleme. Cilj rada jeste da analizira načine na koje organizacije mogu da zaštite svoje informacione sisteme, kao i mesta unutar organizacija gde nastaju problemi. Takođe videćemo i iskustva kompanija koja se bave zaštitom informacionih sistema i borbom protiv sajber kriminala.

Ključne reči: informacioni sistemi, mere sigurnosti, strategije, nivoi zaštite