**MYKOLAS ROMERIS UNIVERSITY**

**BUSINESS AND MEDIA SCHOOL**

**VIKTORIJA GRIGOROVIČ**

Electronic Business Management

# CYBER CRIMES: ANALYSIS OF REASONS AND EFFECTS FOR BUSINESS ORGANIZATIONS

**Master thesis**

**Supervisor -**

**Prof. Dr. Vida Davidavičienė**

**Vilnius, 2016**

**MYKOLAS ROMERIS UNIVERSITY**
**BUSINESS AND MEDIA SCHOOL**

# CYBER CRIMES: ANALYSIS OF REASONS AND EFFECTS FOR BUSINESS ORGANIZATIONS

**Electronic Business Management Master Thesis**
**Study program 621N20018**

**Supervisor**
**Prof. Dr. Vida Davidavičienė**
**2016 12**

**Performed by**
**EBMmfs4-01**
**V. Grigorovič**
**2016 12**

**Vilnius, 2016**

# CONTENT

# LIST OF TABLES

# LIST OF FIGURES

# LIST OF ANNEXES

# ABBREVIATIONS

CaaS - Crime-as-a Service

CEO - Chief Executive Officer

CFO - Chief Financial Officer

DDoS - Distributed Denial of Service

EU – European Union

ICT - Information and Communications Technology

ISO - International Organization for Standardization

ISPs – Internet Service Providers

NIST - National Institute of Standards and Technology

PCI DSS – Payment Card Industry Security Standard

PwC - PricewaterhouseCoopers

RATs - Remote Access Tools

URL - Uniform Resource Locator

# INTRODUCTION

**Novelty and relevance of the topic.** The rapid growth of the Internet is extremely important in many fields. It affects and facilitates nearly every aspect of modern life. Considering the benefits and opportunities provided in cyber world many companies have moved or expanded their businesses to the e. environment. However, cyber space provides tremendous opportunities for criminals as well.

Cyber crime is a fast-growing area of crime. New trends in cyber crime are emerging all the time, with estimated costs to the global economy running to billions of dollars. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide. (INTERPOL)

Cyber crime is a significantly growing way of stealing, threatening and blackmailing organizations all over the world. Not only it disturbs business processes but also affects the confidence that customers, professionals and government demonstrate towards the organization. This can have direct impact on financial results of organization and even lead to a bankrupt. (Putte and Verhelst, 2013)

Extracting value from the computers of unsuspecting companies and government agencies is a important business for criminals. The scope of the damage to the victims ranges from reputational risk, loss of customer trust, financial penalties, disturb of business processes, costs of remediation and repair to greater competition arising from the stolen information. (Sentonas, 2014)

Since most cybercrimes are transnational in nature, cooperation among law enforcement institution, organizations and individuals has a significant impact in cyber crimes prevention.

**The problem.** Although cyber crime is an increasing issue for the business, many companies do not evaluate properly the challenges and risks associated with cyber crimes and impact on the business.

**The object of the research** – the cyber crimes and prevention measures against them.

**The purpose of the research** – to analyze the reasons and effects of cyber crimes on business organizations.

**The objectives of the research:**

1) To overview the main characteristics of cyber crimes (the concept, types and prevention measures).
2) To compare the cyber crimes trends in EU and the US.

3) To perform the qualitative study of experts regarding the strategies for preventing and handling cyber crimes challenges.

**The methods used in master thesis:**

1) Analytical method. Different articles, various reports and online sources were analyzed in order to overview the main characteristics of the cyber crimes.
2) Comparative method. Major cyber crimes trends were compared in two regions – European Union and United States of America.
3) Structured interview method. Cyber security experts were interviewed in order to find out their opinion and insights regarding cyber crime challenges and strategies used to manage cyber risk.
4) Descriptive statistical method. Some results are systematized, described in detail and graphically visualized.
5) Method of the generalization. All used literature, various reports and other documents were summarized; conclusions and recommendations were formulated.

**The structure of master thesis.** The master thesis consists of three main chapters. In the first chapter major characteristics of cyber crimes (the concept, types and prevention measures) are analyzed. In the second chapter current cyber crimes trends in European Union are overviewed in details and compared with tendencies in the United States. The third section provides the experts' interview analysis regarding the strategies for handling and preventing challenges of cyber crimes. At the end of the research conclusions and recommendations are provided.

# I. THEORETICAL ASPECTS OF CYBER CRIMES

The aim of this chapter is to provide a holistic view on the concept and classification of cyber crimes. Moreover, it will be presented the main challenges, caused by cyber crimes and prevention measures, which can be used to manage cyber crime risk.

## 1.1. The concept and characteristics of cyber crimes

Nowadays the importance of Internet is well recognized globally. Many business processes moved and are conducted fully or partially on the Internet. Despite of all of advantages and benefits caused by these developments, there are also risks related to the usage of technology with purpose to harm and exploit other individuals, agencies and/or organizations. Such exploitation of cyberspace for the purpose of accessing unauthorized or secure information, spying, disabling of networks and stealing data as well as money is termed as cyber crime (Uma and Padmavathi, 2013). Karamchand Gandhi (2012) describes cyber crime as "activity in which computers or computer networks are a tool, a target or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. Cyber crime mainly consists of unauthorized access to computer systems data alteration, data destruction, theft of intellectual property". According to Menon and Siew (2012) "cyber crime is comprising diverse offences in which either the computer or network is the target of the criminal activity, such as hacking and malware, or where it is the tool used to commit the crime, such as child pornography and identity fraud". Joseph (2006) defined a cyber crime as "a crime committed on the Internet using the computer as either a tool or a targeted victim". When the individual is the main target of cyber crime, the computer can be considered as the tool rather than the target. In this case, human weaknesses are generally exploited. The crimes using the computer as a target, requires the technical knowledge of the perpetrators. However, all cyber crimes involve both the computer and the person behind it as a victim.

Goderdzishvili (2010) provided the following features of cyber attacks:

- Harmonized process. Synchronization of the steps involved to steal the information leads attackers to achieve what they expect. The hackers will get their result in time, in step and in their line.

- Organized form of the methods. The usage of logically organized methods leads attackers to get more efficient results.
- Enormous. The attacks are usually large scale and causing high data and/or financial loss.
- Regimented. The attacks are regimented with perfect sequence of actions.
- Not spontaneous. Attacks that occur deliberate are very careful planned in order to cause maximum damage.
- Demanding time and resources. Attacks are usually planned in advance and require time and money resources.

These characteristics are followed by attackers in order to achieve their aims. Usually, the main targets of cyber criminals are the data or information of governmental organizations' websites, financial institutions websites, online discussions forums, news and media websites and/or military/defense networks. The main motivations of cyber attacks are as follows (Uma and Padmavathi, 2013):

- Obstruction of information. The main aim of the attacker is to block the access of authorized user to the important information of any organization or government offices when there is a need for particular data or information.
- Counter international cyber security measures. The main purposes of any major cyber attacks are to challenge and defeat the measures initiated by the international cyber security community to reduce or prevent cyber attack.
- Retardation of decision making process. Cyber attackers may aim to cripple and damage important organizations' processes.
- Denial in providing public services. By blocking the authorized users from accessing the information of any organization or from government relating to public services the attackers can cause disruption in domains such as banking, railway and airline services, stock markets.
- Abatement of public confidence. Due to hacking or stealing of the information there is a substantial loss of confidence among the public about the trustworthiness or security of an organization.
- Denigrating the reputation of the country. Due to technological developments every country has competencies which enhances its prestige among various countries and this could be seriously undermined if a large scale cyber attacks is able to penetrate the countries networks.

Based on the motivation cyber criminals can be divided in the following categories (Saini and et. al., 2012):

- Crackers. These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.
- Hackers. These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.
- Pranksters. These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.
- Career criminals. These individuals earn part or all of their income from crime.
- Cyber terrorists. These individuals use computer network tools to shut down or damage critical national infrastructures (e.g., energy, transportation, government operations). Based on the political, religious or ideological aims, the main purpose is to bring actions that result in disabling or deleting critical infrastructure data or information.
- Cyber bulls. Cyber bullying is any harassment that occurs via the Internet. The main ways of cyber bullying are vicious forum posts, name calling in chat rooms, posting fake profiles on web sites, cruel email messages and etc.
- Salami attackers. Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed, e.g. a bank employee inserts a program into bank‘s servers, which deducts a small amount from the account of every customer.

To sum up, the growth and ubiquitous of Internet provides opportunities not only for fair businessmen but also creates environment for the criminals. Any player of cyber space can become victim of cyber crime: from the governmental institution to the single individual. The cyber criminals have very different motives to commit a crime. Based on the aims of attackers different level of damage can be achieved.

## 1.2. Classification of cyber crimes

There are various cyber crimes classifications provided by different sources. INTERPOL emphasizes that law enforcement generally makes a distinction between two main types of cyber crimes:

- Advanced cyber crime – sophisticated attacks against computer hardware and software;

- Cyber-enabled crime – “traditional” crimes, which can be increased in their scale or reach by use of computer, computer networks or other forms of information communications technology, such as crimes against children, financial crimes, terrorism and etc.

Saini and et. al. (2012) provided the following categories of cyber crimes based on target:

1) **Data crime.** The target of this crime is illegal access to information, data modification or/and data stealing. This crime can be divided in three main forms:
   - Data interception. The target of this attack is information gathering. The attacker is usually passive and simply observes regular communication and reads the content, however, in some instances the attacker may attempt to influence the nature of the data transmitted. The data collected might be used to support later attack.
   - Data modification. The malicious third party can perpetrate a computer crime by tampering with data as it moves between sites. During the attack an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. For instance, the Euros amount of a banking transaction would be changed in transit stage from €100 to €10,000.
   - Data theft covers illegally copied or taken information from a business or an individual. Usually, this is user’s information such as passwords, social security numbers, credit card information, other confidential personal or corporate information.
2) **Network crime.** The target of this crime is inferring the Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data.
3) **Access crime** can be divided into two categories:
   - Unauthorized access. The purpose of this activity is to use a computer or network without permission. Usually, computer crackers aim to steal computer resources or corrupt a computer's data.
   - Virus dissemination describes the process when the malicious software, such as worms, Trojan horse and others, attaches itself to other software and destroys the system of the victim.
4) **Related crimes** cover “traditional” crimes which are moved to the online environment such as computer forgery or fraud, cyber sex, cyber defamation and others related offenses.

Other authors provide the following types of cyber crimes:

- **Cyber stalking** or **cyber-bullying** is use of the Internet or other electronic means to stalk someone. Stalking generally involves harassing or threatening behavior such as following a person, appearing at a person's home or place of business, making harassing phone calls,

leaving written messages or objects, or vandalizing a person's property. Cyber stalking can take many forms, including: harassment, embarrassment and humiliation of the victim; emptying bank accounts or other economic control such as ruining the victim's credit score; harassing family, friends and employers to isolate the victim. A true cyber stalker's intent is to harm their intended victim using the anonymity and untraceable distance of technology. (Bocij, 2004)

- **Hacking** is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them (Erickson, 2008). In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems (Franceschetti and Grossi, 2008). Hacking is most commonly associated with malicious programming attacks on the Internet and other networks.
- **Phishing** is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information such as passwords, credit card, social security or bank account number that will be used for identity theft. Recipients are directed to a fraudulent copy of institution's website when they click on the links on the email to enter their information, and in that way they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account or other confident information. (Milhorn, 2007).
- **Online scams or fraud** are dishonest schemes that seek to take advantage of unsuspecting people to gain a benefit (such as money, or access to personal details). Common types of online scams include unexpected prize scams (f.e. lottery scams, travel scams and etc.); dating or romance scams; jobs and investment scams and others scam types. (Australian Cybercrime Online Reporting Network (ACORN))
- **Bot networks.** This is a cyber crime, when perpetrators remotely take control of computers without the users realizing it. Computers get linked to Bot Networks when users unknowingly download malicious codes sent as e-mail attachments. The affected computers can work together whenever the malicious code within them get activated, and those who are behind the Bot Networks attacks get the computing powers of thousands of systems at their disposal. Bot networks create unique problems for organizations because they can be remotely upgraded with new exploits very quickly and this could help attackers avoid security efforts. (Byrne, 2007)
- **Online trading scam** involves scammers targeting people or businesses who buy, sell or trade online. There are different schemes used by online trading scammers such as: (ACORN)

- advertise products for sale at cheap prices, and once purchased the products never arrive;
- target small businesses and attempt to bill them for a particular service – usually a listing or advertisement – which the business never asked for;
- take advantage of natural disasters by impersonating charities requesting donations;
- claim victim's computer is infected with a virus and request remote access to fix the problem and etc.

- During **social engineering attacks** websites are infected by a malicious code by SQL injection so that any user entering will also be infected or the content of these websites might be altered (Uma and Padmavathi, 2013). Social engineering fraud refers to the scams used by criminals to trick, deceive and manipulate their victims into giving out confidential information and funds. Criminals exploit a person's trust in order to find out their banking details, passwords or other personal data. Scams are usually carried out online (by email or through social networking sites). An instance of such crime is CEO/Manager fraud when fraudsters gather publicly available information about the company to be targeted. They find out details of the Head of the company, and those managers and employees who are authorized to handle cash transfers. The criminals use this data in order to impersonate the head of company and coerce employees into making an urgent and high-value cash transfer to a designated bank account. (INTERPOL)

There are many others types of cyber crimes such cyber terrorism, cyber espionage or even cyber war, which can bring damage not only to single individual or the company, but also national security could be affected. To summarize, the variety of cyber crimes types shows that there are many different ways to harm and interrupt individuals' or companies' private data. Each of the crimes costs more or less for the victims. Therefore, it is very important for individuals as well as for businesses to know possible techniques used by cyber criminals and take measures to prevent them.

## 1.3. Challenges and impacts of cyber crimes

The volume and complexity of cyber crimes are increasing very fast as the technology is growing very rapidly. Cyber crime identification and investigation is becoming a very complicated task and this leads to the range of challenges related with the key features of cyber crime.

First, and perhaps the most significant, is the non-territorial or borderless nature of cyber crimes. Cyberspace, by its nature, ignores territorial boundaries. This borderless nature of the virtual world, in which some of the most dangerous criminals operate, creates tremendous

challenges for the law enforcement authorities. Cyber crime investigations often require that evidence be traced, collected and preserved in more than one country. The challenge in prosecuting transnational crimes is to ensure that the collective efforts of law enforcement bodies are effectively coordinated with the legal proceedings being commenced in the most appropriate jurisdiction. (Hodgson, 2008)

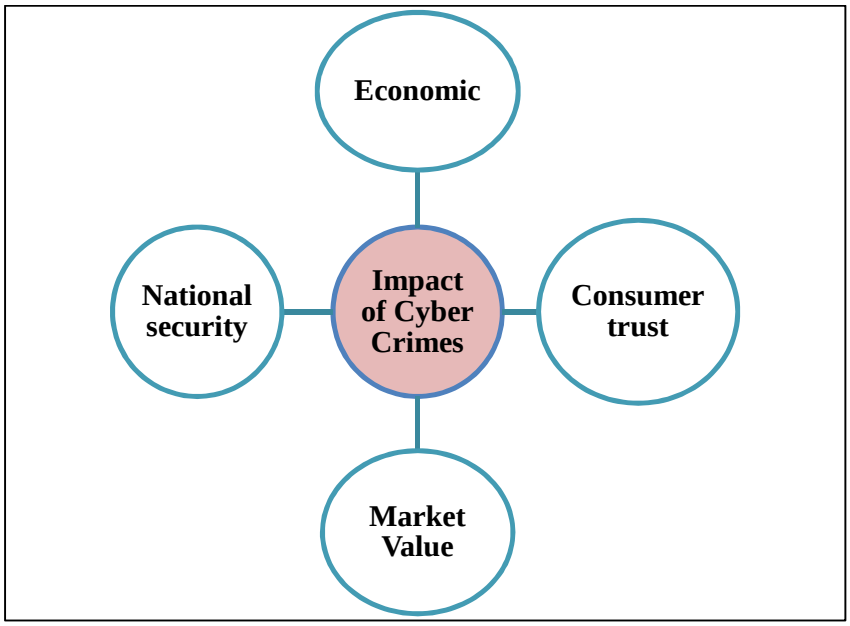
Second, rapidly evolving and ever changing nature of cyber crimes poses many challenges for law enforcers. The law and its procedures must react fast to these changes and adapt and keep pace with the changing cyber crimes. (Menon and Siew, 2012)

The third characteristic of cybercrimes is the fact that these crimes are very often profit driven (Gottschalk, 2010). The amounts involved can be staggering. The unprecedented scale at which criminal proceeds across jurisdictions further means that effective asset recovery will increasingly depend on mechanisms to ensure collaboration and coordination among different national agencies. (Menon and Siew, 2012)

Poonia (2014) provides the following list of potential challenges related to cyber crimes:

- lack of awareness and the culture of cyber security, at individual as well as organizational level;
- lack of trained and qualified workforce to implement the counter measures;
- the speed of cyber technology changes always beats the progress of governmental sector so that they are not able to identify the origin of these cyber-crimes;
- security forces and law enforcement personnel are not equipped to address high-tech crimes;
- present protocols are not self sufficient, which identifies the investigative responsibility for crimes that stretch internationally;
- budgets for security purpose by the government especially for the training of law enforcement, security personnel's and investigators in ICT are less as compare to other crimes.

As today's consumer has become increasingly dependent on computers and networks, the risk of being targeted of cyber crime is very high. When it is done, cyber crime creates high impact on different subjects. Figure 1 introduces the schematic structure of the main areas which are significantly influenced by cyber crimes.




**Source:** prepared by author using H. Saini and et. al. (2012)

**Figure 1.** The main areas influenced by cyber crimes

One of the fields that suffer due to cyber crimes is economy. Since it increases its reliance on the Internet and cyber space, it is exposed to the threats caused by cyber criminals. The variety of operations is performed via Internet such as purchases using credit card; different bank transactions, stocks trade and etc. All instances of cyber fraud in the mentioned operations impact the financial state of the affected business unit and hence the economy. In addition, productivity is another important concern. Attacks from worms, viruses and others malicious software take productive time away from the user: machines could perform more slowly; servers might be inaccessible; networks might be jammed, and so on. These instances of attacks affect the overall productivity of the user and the organization. Due to such issues a considerable part of e-commerce revenue is lost. Moreover, the disruption of international financial markets could be one of the risks since the modern economy spans multiple countries and time zones. Such interdependence of the world's economic system means that a disruption in one region of the world will have effects on other regions as well. The overall monetary impact of cyber crime on society and government are unknown. Some estimates are that viruses and worms cause damages into the billions of dollars a year. (Saini and et. al., 2012)

To keep consumer trust is one of the most challenging and important tasks for each business. Once it is lost, it very difficult and often impossible to gain it back. On the one hand, if companies' functionalities are disturbed due to cyber attack and this has customer service impact,

the external customer sees it as a negative aspect of the organization. Moreover, if customer becomes defrauded while visiting webpage which was concerned by cyber attackers, he might lose confidence not only in the particular site but also in the Internet and its strengths overall. Consumer perception can be just as powerful (or damaging) as fact. User's concern over the credibility of an e-business in terms of being unsafe or cluttered makes a shopper reluctant to transact business. Even the slightest perception of security risk or amateurish commerce seriously compromises potential business. (Saini and et. al., 2012)

In addition to the loss of the customers' confidence, if it is perceived that the business unit might be vulnerable to cybercrime, such vulnerability may lead to a decrease in the market value of the company due to legitimate concerns of financial analysts, investors, and creditors (Smith and et.al., 2010).

The fourth, and probably the most important area, influenced by the cyber crimes, is national security. Modern military of most of the countries depends heavily on advanced computers. One of the challenges for governments is the information warfare, including network attack and exploitation. Information warfare can easily spread malware, causing networks to crash and spread misinformation. In addition, it can be low-cost, highly effective and provide deniability to the attacker. Terrorists and criminals use information technology to plan and execute their criminal activities. Due to advanced communication technology people do not need be in one country to organize such crime. (Saini and et. al., 2012)

To sum up, the main challenges concerning cyber crimes are tightly related with their main features such as borderless, rapidly changing and profit driven nature. There are four main areas which are mostly impacted by the activities of cyber criminals: economic, consumer trust, market value and national security. Cyber crimes cost for companies billions of dollars annually in stolen assets and lost business. They can totally disrupt a company's activities and ruin customers' trust. Moreover, not only consumers or companies are vulnerable to cybercrime, but also national security stands at the risk while facing criminal activities in cyber space.

## 1.4. Prevention measurements against cyber crimes

Cyber crimes represent really huge challenges for single individual, business managers and certainly for governmental institutions. Cyber crime is an increasingly common way of stealing, threatening and blackmailing not only individuals but also organizations all over the world. There are many preventive measures which can be taken to tackle root causes of cyber crimes. The general overview of main actions against cyber crimes are presented in Table 1.

**Table 1**. Main actions against cyber crimes on different levels

| Individual level | Company level | National level |
|---|---|---|
| • Keep the computer system up to date;<br>• Secure configuration of the system;<br>• Choose a strong password and protect it;<br>• Keep firewall turned on;<br>• Install or update antivirus software;<br>• Protect personal information;<br>• Read the fine print on website privacy policies;<br>• Review financial statements regularly;<br>• Investigate online dealer on Internet;<br>• Turn off computer | • Establish the cyber security policies and procedures, which include guidelines for investigation of and recovery from cybercrimes after they occur;<br>• Implement training programs and disseminate the information on latest threats within the organization;<br>• Maintain multiple intrusion detection technology;<br>• Investments into qualified cyber security professionals;<br>• Active partnership with other organizations, sharing initiatives and reporting of cyber crime;<br>• Timely and cooperative response to threats and attacks;<br>• Demonstrating an appropriate standard of diligence to auditors, regulators and stakeholders, which should reduce business exposure to regulatory or legal sanctions;<br>• Continuous risk assessment, development and implementation of risk management strategy in terms of cyber security; | • Centralized coordination at regional and interregional levels, to streamline the fight against cybercrime;<br>• Active partnerships with ISPs, Internet security organizations and online financial services;<br>• Collaboration with the private sector, to proactively identify features of future communications technologies liable to criminal exploitation;<br>• Encouraging and enabling the reporting of cyber crime;<br>• Active targeting of the proceeds of cyber crime in collaboration with the financial sector;<br>• Developing insight into the behavior of the cybercriminal by means of intelligence analysis, criminological research and profiling techniques;<br>• Sharing the best practice;<br>• Awareness raising on individual and corporate user responsibility. |

Table 1 continued on the next page

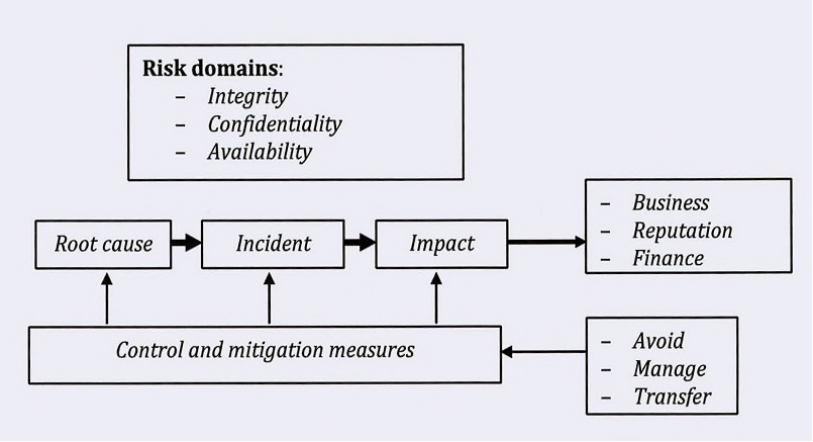
Table 1 continued from the previous page

| Individual level | Company level | National level |
|---|---|---|
| | • Continuous systems testing which encompasses the resistance to threats and ability to minimise and mitigate the damage caused by successful attacks;<br>• Educating and encouraging customers and suppliers to improve their own cyber security. | |

**Source:** prepared by the author using R.Wainwright (2010), K.T.Smith and et.al. (2010), Kratchman and et al. (2008), R. Borum and et.al. (2014), OECD (2002), FBI, Europol (2011), National Crime Prevention Council (2012), NCA (2016) information

According to the information from Table 1, we can conclude that the major means in the fight against cyber crime is not only criminals' catching and fining. Investment in prevention and protection initiatives is the essential measure and can guard from damage caused by cyber crimes.

Putte and Verhelst (2013) suggested organizations to use general risk model in order to manage the risk related to cyber crimes. The model is shown in Figure 2.




**Source:** Putte and Verhelst (2013)

**Figure 2.** The risk management model

The figure shows three main risk domains: (Putte and Verhelst (2013))

1) Confidentiality is the assurance of documents and data privacy. Disclosure to unauthorized entities, for example, using unauthorized network sniffing, is a confidentiality violation.
2) Integrity. Document and data integrity is ensuring that the information has not been altered during transmission, from origin to recipient, and during storage.
3) Availability is being sure of the timely and reliable access to documents and data services for authorized users when required.

The cyber risk analysis is possible in two ways:

- Looking upstream, when reputational, financial or impact on business processes is already known, means trying to find out what the possible root causes might be or, after the incident has occurred or what the root causes were;
- Looking downstream means trying to see what impact can be expected during and after the incident predicting different scenarios.

In the each step control and mitigation measures should be indicated which would help avoid, manage or transfer the risk associated with cyber crimes. The identification of relationship between root causes, the underlying reasons of incident and the possible impact on business could support organization in better cyber risk management.

The National Institute of Standards and Technology (NIST) provided the Framework, which is a voluntary risk-based compilation of guidelines that aims to help organizations identify, implement, and improve their cyber security practises. The Framework is organized by five continuous functions: identify, protect, detect, respond and recover (see Figure 3).

| Functions | Definition | Categories |
|---|---|---|
| Identify | An understanding of how to manage cybersecurity risks to systems, assets, data, and capabilities | Asset management, business environment, governance, risk assessment, risk management strategy |
| Protect | The controls and safeguards necessary to protect or deter cybersecurity threats | Access control, awareness and training, data security, data protection processes, maintenance, protective technologies |
| Detect | Continuous monitoring to provide proactive and real-time alerts of cybersecurity-related events | Anomalies and events, continuous monitoring, detection processes |
| Respond | Incident-response activities | Response planning, communications, analysis, mitigation, improvements |
| Recover | Business continuity plans to maintain resilience and recover capabilities after a cyber breach | Recovery planning, improvements, communications |

**Source:** NIST (2014)

**Figure 3.** Core functions of effective cyber security

The Framework provides an assessment mechanism that enables organizations to determine their current cyber security capabilities, set individual goals for a target state and establish a plan for improving and maintaining cyber security programs. A guiding principle of the Framework is collaboration to share information and improve cyber security practices and threat intelligence. The Framework describes the continuous cycle of business processes that constitute effective cyber security. It also aims to deliver such benefits as effective collaboration and communication of security posture with executives and industry organizations, as well as potential future improvements in legal exposure and even assistance with regulatory compliance. However, it is important to note that there is no one-size-fits-all solution for cyber security, and the government cannot provide comprehensive, prescriptive guidelines for all entities across industries. (Guinn and et.al., 2014).

In summary, the prevention measurements against cyber crimes should be taken on all levels: individual, company's and national. The enhanced partnership and information sharing among all actors is essential factor in the fight against cyber crimes. For the organizations, one of the main measures in cyber crime prevention is ensuring that cyber risk management strategy is in place and is aligned with overall business strategy.

# II. THE PRESENTATION AND THE COMPARISON OF CYBER CRIMES TRENDS IN EUROPEAN UNION AND UNITED STATES

The aims of this chapter are to overview the cyber crimes tendencies within European Union and compare them to the United States of America. Cyber crime trends will be analyzed and compared considering to following aspects:

- main types of cyber crimes and their impact on business;
- volumes of key cyber crimes;
- major challenges for law enforcement institutions.

## 2.1. The overview of cyber crimes tendencies in the EU

The main source used to analyze trends in EU was 2015 Internet Organised Crime Threat Assessment (IOCTA) prepared by the European Cyber crime Centre (EC3) at Europol. On 28th of September IOCTA 2016 was published. However, many of key threats remain largely unchanged from the previous report.

IOCTA (2015) shows that cyber crime is becoming more aggressive and confrontational and there is a growing trend of aggression in many cyber-attacks. The Crime-as-a Service (CaaS) business model, which grants easy access to criminal products and services, enables a broad base of unskilled, entry level cybercriminals to launch attacks of a scale and scope disproportionate to their technical capability and asymmetric in terms of risks, costs and profits.

The sphere of cyber crime encompasses an extremely diverse range of criminality. In the context of ‘pure’ cyber crime, malware predictably persists as a key threat. Ransomware attacks have grown in terms of scale and impact and almost unanimously represent one of the primary threats encountered by EU businesses and citizens as reported by law enforcement. Information stealing malware, such as banking Trojans, and the criminal use of Remote Access Tools (RATs) also feature heavily in law enforcement investigations. Banking malware remains a common threat for citizens and the financial sector, generating sizeable profits for cybercriminals. A coordinated effort between law enforcement, the financial sector and the Internet security industry will be required in order to effectively tackle this problem. This will necessitate better sharing of banking malware samples and criminal intelligence, particularly relating to enabling factors such as money mules.

The number and frequency of publically disclosed data breaches is dramatically increasing, highlighting both a change in attitude by industry and that data is still a key target and commodity for cybercriminals. Such breaches, particularly when sensitive personal data is disclosed, inevitably lead to secondary offences as the data is used for fraud and extortion. According to the Breach Level Index, more than 3.6 billion data records have been exposed since 2013 when the index began benchmarking publicly disclosed data breaches. In 2015 malicious outsiders were the leading source of these breaches, accounting 58% of breaches, while identity theft remained the primary type of breach, accounting for 53% of data breaches. In terms of geographic regions, 77% of all data breach incidents occurred in North America, with 59% of all compromised records happening in the United States. Europe accounted for 12% of overall breach incidents, followed by the Asia Pacific region at 8%. (Gemalto, 2016)

While it is possible for organizations to invest in technological means to protect themselves, the human element will always remain as an unpredictable variable and a potential vulnerability. Social engineering is a common and effective tool used for anything from complex multi-stage attacks to fraud. Indeed, CEO fraud – where the attackers conduct detailed research on selected victims and their behavior before initiating the scam – presents itself as a prominent emerging threat which can result in large losses for those affected.

It should be noted that the majority of reported attacks are neither sophisticated nor advanced. While it is true that in some areas cybercriminals demonstrate a high degree of sophistication in the tools, tactics and processes they employ, many forms of attack work because of a lack of digital hygiene, a lack of security by design and a lack of user awareness. (IOCTA, 2016)

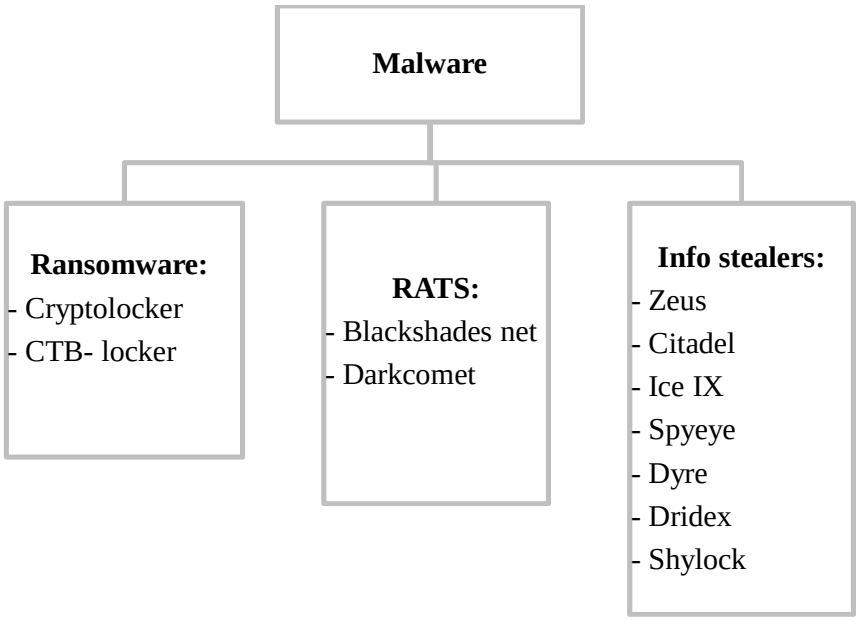
It is a common axiom that technology, and cyber crime with it, develops so fast that law enforcement cannot keep up. The lack of digital hygiene and security awareness of citizens and businesses contributes to the long lifecycle and continued sales of exploit kits and other basic products through CaaS models, bringing opportunities and gain to the criminal masses. Furthermore, a key driver of innovation within cyber crime may be law enforcement itself. Every law enforcement success provides impetus for criminals to innovate and target harden with the aim of preventing or mitigating further detection and disruption of their activities. Overall, where genuine innovation exists in technology, criminals will rapidly seek ways to exploit it for criminal gain.

## 2.2. Main cyber crime threats within EU

Europol's European Cyber crime Centre annual report (2015) presents several threats areas within cyber crime. In the next sub-chapters the main focus will be on the following threats: malware, social engineering, data breaches and network attacks.

### 2.2.1. Malware

According to IOCTA (2015) malware remains one of the key threat areas within cyber crime. The maps provided below highlight EU countries where different malware accidents were reported. Although IOCTA does not provide exact ranges for number of reports, the brighter color notes the higher number of reports in particular country. The malware identified as the current threats across the EU by EU law enforcement can be divided into three categories based on their primary functionality – ransomware, Remote Access Tools (RATs) and info stealers. Figure 4 introduces the schematic structure of the malware classification.



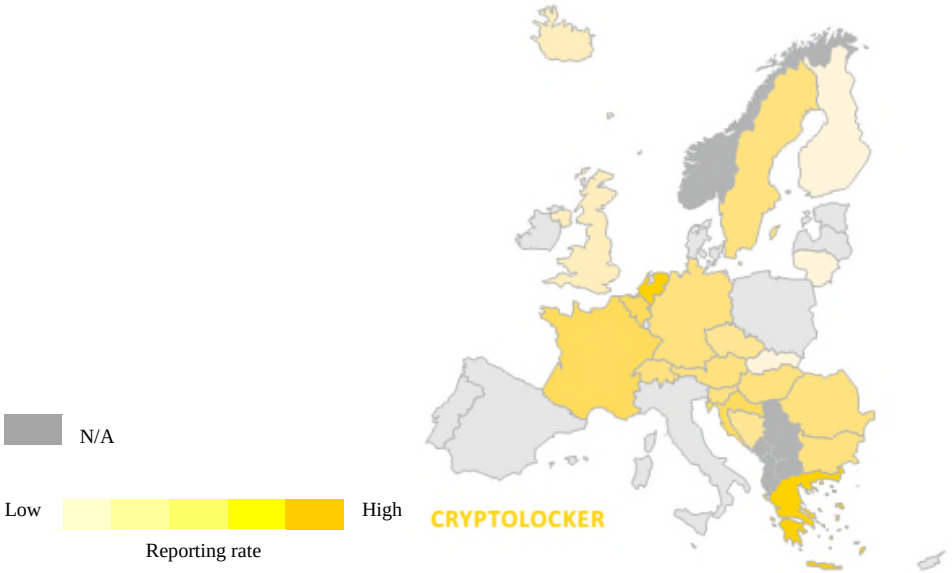

**Source:** prepared by author using IOACTA (2015)

**Figure 4.** Malware classification

Ransomware remains a top threat for EU law enforcement in year 2015 as well as in 2016. Almost two-thirds of EU Member States are conducting investigations regarding these

malware attacks. Police accounts ransomware for a significant proportion of reported incidents. This may be due to an increased probability of victim reporting or it being easier for victims to recognize and describe. Ransomware installs covertly on a victim's computer, executes a cryptovirology attack that adversely affects it, and demands a ransompayment to decrypt it or not publish it. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse and display a message requesting payment to unlock it. More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. (Mehmood, 2016)

CryptoLocker is identified as the top malware threat affecting EU citizens in terms of volume of attacks and impact on the victim. It is also considered as one of the fastest growing malware threats. First appearing in September 2013, CryptoLocker is believed to have infected over 250.000 computers and obtained over 24 million euro in ransom within its first two months. CryptoLocker is also a notable threat amongst EU financial institutions. Figure 5 shows the geographical concentration of this ransomware.

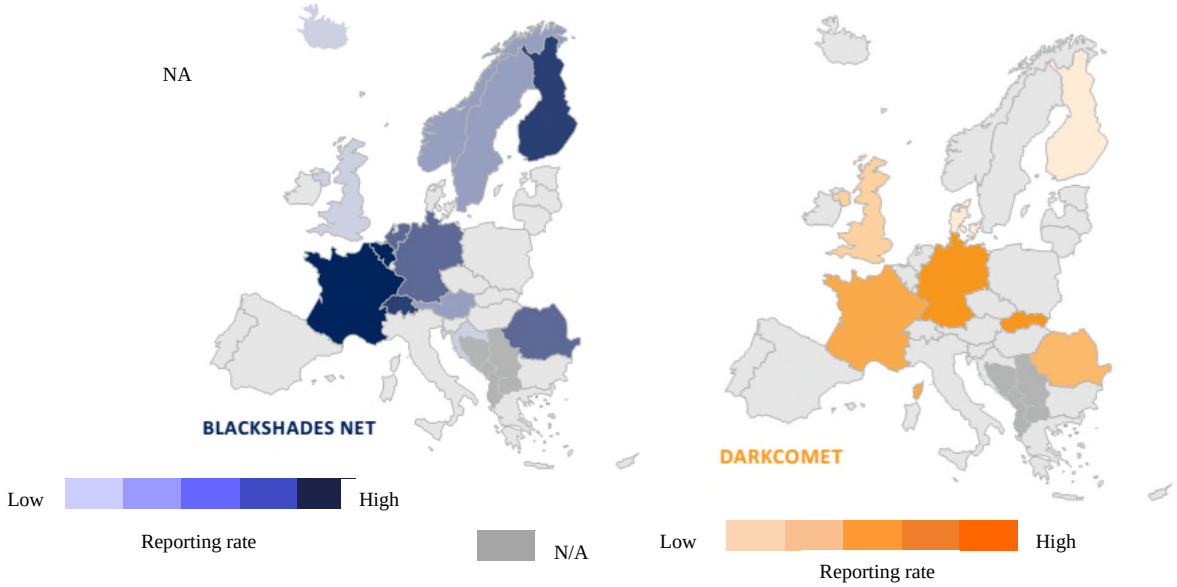



**Source:** IOCTA (2015)

**Figure 5.** CryptoLocker spread across EU

Remote Access Tools (RATs) exist as legitimate tools used to access a third party system, typically for technical support or administrative reasons. These tools can give a user remote access and control over a system, the level of which is usually determined by the system owner. Variants of these tools have been adapted for malicious purposes making use of either standard or

enhanced capabilities to carry out activities such as accessing microphones and webcams, installing (or uninstalling) applications (including more malware), key logging, editing/viewing/moving files, and providing live remote desktop viewing, all without the victims knowledge or permission. RATs provide cybercriminals with unlimited access to infected endpoints and are used to steal information through manual operation of the endpoint on behalf of the victim. Using the victim's access privileges, they can access and steal sensitive business and personal data including intellectual property or personally identifiable information. Figure 6 presents the spread of two RATs widely used for criminal purposes.



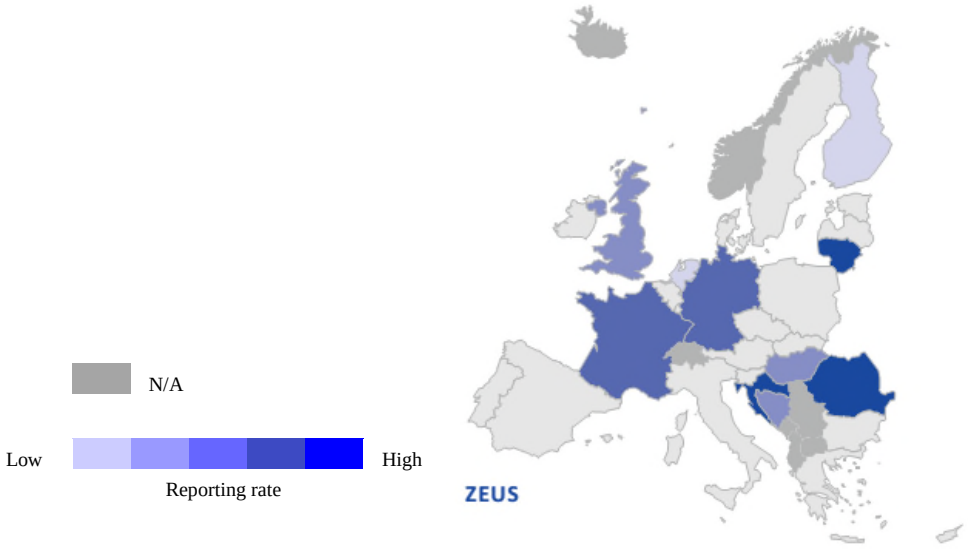

**Source:** IOCTA (2015)

**Figure 6.** Blackshades.net and Darkcomet spread across EU

The majority of malware is designed with the intent of stealing data. Banking Trojans, malware designed to harvest login credentials or manipulate transactions from online banking, remain one of the top malware threats.

One of the well known info stealers, Zeus, has been created to steal private data from the infected systems, such as system information, passwords, banking credentials or other financial details and it can be customized to gather banking details in specific countries and by using various methods. Using the retrieved information, cybercriminals log into banking accounts and make unauthorized money transfers through a complex network of computers. First appearing in 2006, Zeus is one of most significant pieces of malware to date and represents a considerable threat today.

A number of cyber crime groups have adapted the source code to produce their own variants. Figure 7 presents the distribution of Zeus across EU.




**Source:** IOCTA (2015)

**Figure 7.** Zeus spread across EU

In June 2015, a joint investigation team consisting of investigators and judicial authorities from six European countries, supported by Europol and Eurojust, arrested a Ukrainian cyber crime group who were developing and distributing the Zeus malware and cashing-out the proceeds of their crimes. The group had tens of thousands of victims and caused over 2 million euro in damages.

One of the most common methods of malware distribution is by malicious email attachment and the most productive way to reach the wide range of potial victims is via spam. Another common way of malware spread are exploit kits – programs or scripts which exploit vulnerabilities in programs or applications to download malware onto vulnerable machines. As more consumers move to mobile devices for their financial services such as banking, mobile payments and etc., the effectiveness and impact of mobile malware will increase.

Although the recent experiences and investigative focus of European law enforcement suggests that the top malware threats (Zeus, Blackshades) are steadily in decline due to discontinued development and support by the developers (either voluntarily or as a result of their

arrest), a new generation of malware is becoming more prominent in law enforcement investigations.

In order to develop the trend of successful multijurisdictional operations targeting cyber crime groups, law enforcement should continue pro-actively share criminal intelligence related to cyber crimes with other EU Member States and build or maintain relationships with private industry. Moreover, adequate resources should be given to prevention strategies in order to raise awareness of cyber crime and increase standards in online safety and information security, which should include awareness in relation to mobile devices.

### 2.2.2. Social engineering attacks

Social engineering has developed into one of the most prevalent attacks and one of the hardest to defend against. Increasing Internet access in developing countries has led to higher numbers of innovative yet technically unskilled attackers with access to a greater number of victims. Human factor is often the weakest link in the company's security chain. The lack of employees' security awareness and skills can leave a company open to attack despite of all investments into securing their networks and systems. Two main forms of social engineering attacks are phishing and CEO fraud.

In 2014, the majority of EU Member States indicated that the amount of phishing has either stabilized or increased in their jurisdiction. This trend was substantiated by financial institutions where almost every major business indicated that it was targeted by a phishing campaign. Additional security measures adopted by banks have become increasingly successful in identifying fraudulent transactions related to phishing attacks although this in itself has resulted in increased costs due to investment into proactive monitoring capability. In 2015, as a result of these proactive measures, some institutions noted a decrease in the number of phishing attacks for high-value transfers and have observed fraudsters moving to high-volume low-value based attacks instead. Phishing traditionally occurred on a larger scale in widely spoken languages such as English. Phishing attacks often originate from countries sharing the same language (e.g. French victims targeted by offenders from French-speaking North African countries). Nevertheless, some smaller EU countries have also observed a notable increase in localized phishing. The quality of phishing has improved due to professional web design and translation services. Moreover, phishing is not limited to desktop users. Phishing smartphone apps, particularly on the Android platform, often slip through the Google Play review process. These malicious apps collect credentials and other information and deliver it to the attackers. These applications are often downloaded from

trusted locations and the phishing website is accessed from the app so that users do not see the malicious URL. (IOCTA, 2016)

While companies can invest in secure technology tools which in turn requires criminals to innovate their own technical capability, it is harder to upgrade the “human firewall”. Training in cyber security awareness can be provided and safe practice encouraged but is harder to enforce. According to Verizon Data Breach Investigations report (2015), 23% of recipients who receive a phishing message will open it and a further 11% will continue to open any attachments. For untargeted attacks, the primary way to distribute phishing emails is via spam. Moreover, attackers are gradually shifting their activities to alternative distribution channels such as social media.

CEO fraud scheme involves an attacker impersonating the CEO or CFO of the company. The attacker will contact (usually via email or telephone) an employee targeted for their access and request an urgent transaction into a bank account under the attacker’s control. Branches of multinational companies are often targeted, as employees working for regional cells do not usually personally know senior management in the holding company and may be fearful of losing their job if they do not obey their ultimate boss. The scam does not require advanced technical knowledge as everything the attacker needs to know can be found online. Organization charts and other information available from the company website, business registers and professional social networks provide the attacker with actionable intelligence. Several EU Member countries as well as financial institutions reported an increase in CEO fraud which is now leading to significant losses for individual companies. IOCTA (2016) confirms that CEO fraud has evolved into a key threat as a growing number of businesses are targeted by organized groups of professional fraudsters.

Since the growing volume of communication and social networking apps provide further access to potential victims, it is predicted that the number of social engineering attacks via mobile devices and social media platforms will increase further. Moreover, smaller, more compact screen sizes and reduced readability increase the likelihood of potential victims inadvertently clicking on a link.

All in all, it is very important for organizations to improve their employees’ awareness and skills of cyber security and threats related to social engineering attacks. Law enforcement should also continue to share information with and via Europol in order to identify the campaigns which are having the greatest impact. It is advisable for law enforcement organizations to establish and maintain working relationships with both global and national webmail providers to promote the lawful exchange of information relating to criminals abusing those services.

### 2.2.3. Data breaches and network attacks

According to IOCTA (2015), almost 75% of Member States indicated that they had investigated some form of data breach or network intrusion. Over one third of EU law enforcement agencies identified network intrusions as an increasing threat. In 2015, compared to previous year, it has been an increase in the level of network incidents reporting to and subsequent involvement of law enforcement in such investigations. Not all network intrusions lead to the leakage of data or theft of intellectual property. The defacement of business or private websites was one of the most commonly reported cyber-attacks within EU law enforcement.

Table 2 shows some of the data breaches from the first half of 2016 that had impact on the EU. The breaches originate either from within the EU, or from outside the EU, but involve significant numbers of EU citizens. In this context, a breach is defined as an incident that results in the confirmed disclosure of data to an unauthorized party. (Verizon, 2016)

**Table 2**. Data breaches statistics

| **Organization** | **Industry** | **Country** | **Source of breach** | **Number of records compromised (thousands)** | **Type of data compromised** |
|---|---|---|---|---|---|
| Fling | Adult | Globally | Malicious outsider | 40.000 | Email address, passwords, IP address, date of birth, sexual preferences |
| T Mobile | Telecoms | Czech Republic | Malicious insider | 1.500 | Undisclosed |
| Kiddicare | Retail | UK | Malicious outsider | 794 | Name, address, email address, telephone number |
| Nulled.io | Criminal | Globally | Unknown | 474 | Username, email address, IP address, hashed password, personal messages |
| Kinoptic | Technology | Globally | Accidental loss | 198 | Username, email address, hashed password |
| Rosebutt Board | Adult | UK | Malicious outsider | 107 | Username, email address, IP address, hashed password |
| Postbank, Commerzbank and Landesbank Berlin | Finance | Germany | Malicious outsider | 85 | Credit card data |
| Swiss People's party | Government | Switzerland | Malicious outsider | 50 | Name, email address |
| Islamic State Human Resources and Recruiting | Military | Globally | Malicious insider | 22 | Name, address, telephone number, place of birth |

**Source:** Breach Level Index (2016)

The majority of data breaches occurred as a result of compromised credentials (typically those with administrator rights), with the rest largely made up of phishing attacks. 25% of breaches were as a result of crimeware, 20% the result of insider misuse and 15% as a consequence of physical theft or loss. Almost one third were additionally as a result of miscellaneous human errors, such as sending sensitive information to the wrong recipient or accidentally publishing sensitive data to public servers. (Verizon, 2016).

In 2016, companies that store financial credentials remain a key target for financially motivated cybercriminals carrying out network attacks and data breaches. As such, the accommodation and retail sectors are common targets. However, there is a growing trend in the compromise of further data types for other purposes, such as medical records. (IOCTA, 2016)

One of the most considerable threats highlighted by approximately half of the Member States are Distributed Denial of Service (DDoS) attacks, attempts to make an online service unavailable by overwhelming it with traffic from multiple sources. This confirmed by security industry reports documenting hundreds of DDoS attacks per day. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information. Three-quarters of attacks last less than four hours, suggesting that this is sufficient time for an attacker to either achieve their goal or to realize their attack was successfully mitigated. DDoS extortion attacks have become a well-established criminal enterprise. These attacks further benefit from availability of DDoS capable malware and increasing popularity of pseudonymous payment mechanisms. DDoS attacks continue to grow in intensity and complexity in 2016. (IOCTA, 2016).

In 2015, European law enforcement agencies noted the positive trend change in the reporting of incidents related to network intrusion or data breach. Historically, law enforcement has not been the first port of call when an organization has been the victim of a network intrusion or data breach. The reasoning behind this is likely a combination of the belief that law enforcement would be either unwilling or unable to investigate the crime and/or a lack of confidence in law enforcement's ability to handle the investigation with the appropriate level of discretion. However, the number of breaches being both reported to law enforcement and publically disclosed increased. Part of this may be a change in thinking amongst the private sector. Prior to 2014, publicizing a data breach would have significant reputational damage. Recently, it was realized that more frequent engagement with law enforcement and timely, clear and confident message to customers and stakeholders as part of an effective communication strategy can do much to maintain confidence in an organization and prevent rampant speculation by the media.

## 2.3. Major cyber crime challenges for EU law enforcement institutions

One of the aims of IOCTA (2015) report is to evaluate the strengths and weaknesses of EU law enforcement agencies in terms of cyber crime investigations and provide recommendations for the improvement areas. According to the report, law enforcement has convincingly demonstrated its competence in dealing with cyber crime and has achieved great successes in the 2015. The effect of the positive results is witnessed in stronger willingness of partners from law enforcement, the private sector and academia to contribute and cooperate. The growing reporting of data breaches by financial sector and e-commerce companies contributes to the better performance as well. However, several disturbing areas were identified:

- the lack of judicial cooperation possibilities with several countries outside the EU (Eastern European States, including Russia and countries in Southeast Asia);
- inefficient information exchange processes, in particular with private sector parties;
- unclear or unaligned legal frameworks within the EU, in particular in regard to the application of various reluctant measures, undercover work, data retention, online detection, operational involvement of private sector partners in takedowns and the lack of regulation of virtual currencies;
- challenges related to the Cloud:
  - access to data – including determining the location of and timely and lawful access to evidence, determining the relevant legislation;
  - training and education – specifically in terms of establishing and maintaining the necessary skills;
  - privacy and data protection issues linked to a lack of control over data and the risk of data breaches, criminal abuse;
  - cross-border / international cooperation issues linked to inadequate legislation.

Overall, cyber crime investigations are often complex and resource intensive. Therefore, law enforcement must be granted the latitude it requires in order to conduct long-term, comprehensive investigations for maximum impact without undue pressure to obtain rapid results or arrests. The fight against cyber crime must encompass more than catching criminals. Investment in prevention and protection initiatives is also essential and can guard against many facets of cyber crime. With the increasing adoption of the Cloud computing services, law enforcement needs to invest in developing and maintaining the necessary skills, knowledge and technical capability to investigate Cloud-related crimes. Moreover, law enforcement must continue and expand initiatives to share knowledge, expertise and best practice on dealing with cyber crimes. It is essential for law

enforcement to develop working relationships with the financial sector including banks, payments industry, money transfer agents, virtual currency scheme operators and exchangers. The collaboration with the private sector and academia is also very important in order to explore investigative and research opportunities related to emerging technologies such as artificial intelligence. IOCTA (2016) suggests that law enforcement, policy makers, legislators, academia and training providers need to become even more adaptive and agile in addressing the phenomenon. Existing frameworks, programs and tools are often too slow and bureaucratic to allow for a timely and effective response. Rather than multiple partners investing in and developing the same highly specialized skill-sets and expertise, perhaps a more effective, high-level model would be for law enforcement and relevant partners to focus on distinct core competencies. In order to minimize unnecessary overlap and duplication of efforts by connecting existing initiatives and partnerships, the development of a 'cyber-security ecosystem' is needed at EU level and beyond to identify all the relevant partners and stakeholders, map out networks, identify interfaces and links to legal and regulatory frameworks, facilitate easier capacity building and visualize opportunities for the further strengthening of cyber security in the EU.

## 2.4. The overview of common cyber crimes tendencies in the US

In 2015, PwC conducted Cyber crime Survey, which included more than 500 executives of US businesses, law enforcement services, and government agencies. There were evaluated trends in the frequency and impact of cyber crime incidents, cyber security threats, information security spending, and the risks of third-party business partners in private and public organizations. The 2015 US State of Cyber crime Survey report is the main source for the cyber crime tendencies overview in the US. Additionally, FBI and other sources were used as well.

According to PwC report cyber security incidents in US are not only increasing in number, they are also becoming progressively destructive and target a broadening array of information and attack vectors. It's clear that adversaries continue to advance their threats, techniques, and targets. They are investing in technologies, sharing intelligence, and training their crews to attack with purpose and competence.

According to FBI, the cyber crime threat is incredibly serious and growing. Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated. The critical infrastructure of the US, including both private and public sector networks, are targeted by adversaries. American companies are targeted for trade secrets and other sensitive corporate data, and universities for their cutting-edge research and development.

PwC survey results showed that the most-frequently types of cyber crimes are usually committed by external threat actors, those who are not employees or third-party partners with trusted access to networks and data. Particularly worrisome are phishing campaigns, which are comparatively easy to initiate and can rapidly spread across an organization, targeting top executives as well as employees and managers. Almost one-third (31%) of respondents said they had been hit by a phishing attack in 2014, making it one of the most frequent types of incidents.

Distributed denial of service (DDoS) attacks are becoming increasingly potent and are one of the most frequent types of cyber security incidents, cited by 18% of survey respondents in 2015. DDoS assaults most often result in damage to reputation, but they also can put businesses at risk by disrupting e-commerce and other business processes.

Ransomware is becoming more sophisticated and commonplace. The FBI (2015) warned that this type of attack, in which adversaries take control of a company's data until it pays a ransom, is on the rise. In 2014, 13% of Cyber crime Survey respondents said they had been a victim of ransomware.

Another cyber crime, wire fraud, is becoming more prominent and costly. According to FBI and the Internet Crime Complaint (2015), global wire fraud cost businesses $215 million during a 14-month period, with US companies representing 84% of those financial losses. It's a crime that frequently begins with phishing campaigns that often target top executives

The FBI highlights two key priorities in terms of cyber crime threat: ramsomware and computer and network intrusions.

**Ransomware attacks** target different organizations such as hospitals, school districts, state and local governments, law enforcement agencies, businesses and etc. The inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation. Ransomware attacks are not only proliferating, they're becoming more sophisticated. Several years ago, ransomware was normally delivered through spam e-mails, but because e-mail systems got better at filtering out spam, cyber criminals turned to spear phishing e-mails targeting specific individuals. In newer instances of ransomware, some cyber criminals are bypassing the need for an individual to click on a link by seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers. When the data is infected, the criminals usually demands for a ransom payment in bitcoins because of the anonymity this virtual currency provides. However, the FBI doesn't support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee an organization that it will get its data back—there have been cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens

current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. Additionally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals such as terrorism activities and etc. In order to prevent the ransomware attacks the organizations should consistently provide awareness training for employees and also robust technical prevention controls. Moreover, solid business continuity plan should be created in the event of a ransomware attack.

Another threat, which has a very huge impact on businesses, **computer and network intrusions** take down vital systems, disrupting and even disabling the work of hospitals, banks, and "911" services around the US country. Behind such attacks stand different groups such as "computer geeks" looking for bragging rights, businesses trying to gain an upper hand in the marketplace by hacking competitor websites, rings of criminals wanting to steal personal information and sell it on black markets, even spies and terrorists looking to rob the nation of vital information or launch cyber strikes.

The recent rash of security incidents may be convincing companies to step up their investments in cyber security. The Cyber crime Survey indicated that industries that have been impacted by high-profile cyber attacks were more likely to significantly boost information security investments.

The 2015 US State of Cyber crime Survey report emphasizes the importance of information sharing as the effective measure in the prevention and fight against cyber crimes. Sharing reliable, actionable, and timely intelligence advances situational awareness of threats, defense agility, informed decision-making, and rapid notification to affected customers and businesses as well as regulatory bodies. It's also a relatively inexpensive way to gain a bigger picture of threats facing an organization. Organizations engaged in information sharing related to cyber security risks and incidents play an invaluable role in the collective cyber security of the United States. However, many companies have found it challenging to develop effective Information Sharing and Analysis Organizations (ISAOs). In response, President Obama issued the 2015 Executive Order 13691 directing the Department of Homeland Security (DHS) to encourage the development of ISAOs. Many industry observers anticipate that the president's executive order will boost participation in information-sharing initiatives. Membership in ISAOs will be more flexible, enabling businesses and public-sector agencies to share information specific to individual industries as well as intelligence related to geographies, issues, events, or threats. A key roadblock to information sharing is a lack of a unified framework, platform, and data standards. Therefore, Department of Homeland Security and others are working to promote specific, standardized message and communication formats.

PwC survey showed that despite the fact that 69% of respondents are investing in cyber security technologies more than any other spending category, employee training and awareness continues to be a critical component of cyber security. Only half of survey respondents said they conduct periodic security awareness and training programs, and the same number offer security training for new employees. Companies that implement new technologies without updating processes and providing employee training will very likely not realize the full value of their spending. To be truly effective, a cyber security program must carefully balance technology capabilities with redesigned processes and staff training skills.

It's clear that the threats, techniques, and targets of adversaries continue to evolve. Businesses must keep up with the capabilities of their adversaries. Staying abreast of threats may require that organizations redirect limited resources to initiatives that deliver the greatest return. These can include enhanced threat analytics capabilities, prioritizing security of the most critical assets, performing simulations to improve response capabilities across the organization, and stepping up security awareness efforts. Organizations should also be prepared to share information on cyber security threats and response tactics proactively. Moreover, organizations must summon the vision, determination, skills, and resources to build a risk-based cyber security program that can quickly detect, respond to, and limit fast-moving threats.

## 2.5. Comparison of main cyber crimes trends in EU and the US

The fast and reliable ICT infrastructure found in much of Europe is exploited by cybercriminals to host malicious content and launch attacks on targets both inside and outside of Europe. The EU hosts approximately 13% of global malicious URLs (i.e. online resources that contain redirects to exploits or host exploits themselves). The Netherlands accounts for the most significant proportion of this figure. Germany, the UK, the Netherlands and France feature as significant hosts for both C&C infrastructure and phishing domains globally. Italy, Germany, the Netherlands and Spain are also some of the top sources for global spam. Additionally, Spain is consistently one of the top 10 global sources of DDoS, accounting for between 6-7% of global attacks. France, Germany, Italy and the UK have the highest malware infection rates and the highest proportions of bots found within the EU. In terms of EU law enforcement activity, approximately one half of EU Member States identified infrastructure or suspects in the Netherlands, Germany or the United Kingdom in the course of their investigations. Moreover, approximately one third found links to Austria, Belgium, Bulgaria, the Czech Republic, France, Hungary, Italy, Latvia, Poland, Romania and Spain. (Trend Micro and Symantec reports, 2015)

According to Symantec Internet Security Threat report (2015), the US hosts over 45% of the world's phishing domains and remains one of the world's top spam producers. The United States is home to a comparatively high proportion of global bots, harboring between 16% and 20% of all bots worldwide. In addition, in 2014 almost one third of PoS malware and over 40% of all ransomware detections were in the United States. 20 EU Member States had investigations where criminal infrastructures or suspected offenders were located in the United States.

Table 3 provides summary of main trends in European Union in comparison to the United States of America.

**Table 3**. Comparison of main cyber crimes trends in EU and the US

| | **European Union** | **United States of America** |
|---|---|---|
| **Most frequent cyber crimes** | Malware (ransomware, RATs, info stealers);<br>Data breaches and network attacks (DDoS attacks);<br>Social engineering attacks (phishing and CEO fraud). | Ransomware attacks;<br>DDoS attacks;<br>Phishing attacks;<br>Computer and network intrusions. |
| **Volumes of key cyber crimes and damage for business** | 12% of all data breach incidents<br>$929 billion damage for companies | 59% of all data breach incidents<br>$1.07 billion damage for companies<br>hosts almost a half of the world's phishing domains |
| **Major challenges for law enforcement institutions** | Lack of judicial cooperation possibilities with several countries outside the EU;<br>Inefficient information exchange processes;<br>Unclear or unaligned legal frameworks within the EU.<br>Challenges related to the Cloud. | Lack of information sharing;<br>Challenges related to the Cloud;<br>Inefficient international collaboration. |

**Source:** prepared by the author

All in all, the cyber crimes overview shows similar trends in Europe as well as in the US. Since cyber crimes are considered as global issue, the trends in both regions are comparable. Ransomware attacks remain top malware threat in both regions. Data breaches, network intrusions, different fraud attacks are main focus areas for EU and the US law enforcement institutions. In terms of cyber crimes volumes, the U.S. outruns European countries: 59% of all data breach incidents occurred United States, while Europe accounted for 12% of overall breach incidents in 2015; the US hosts almost a half of the world's phishing domains and remains one of the world's top spam producers. As a highly competitive, English-speaking community, the US environment attracts many fledgling cybercriminals. Cyber crime causes about billions of US dollars damage every year for business in European Union as well as in the United States. Europol as well as FBI highlight the importance of international collaboration and information sharing among law enforcement institutions, business organizations, academia and other units in order to have effective fight against cyber criminals.

# III. QUALITATIVE STUDY OF THE STRATEGIES FOR HANDLING AND PREVENTING CYBER CRIMES

## 3.1. Research methodology

**Issue of the research.** Cybercrime is a significant threat for the business organization all over the world. However, many companies still lack the information and measures for risk evaluation and effective management of challenges caused by cybercrimes.

**The object of the research.** The cyber crimes and prevention measures against them.

**Goal of the research.** Based on the experts' knowledge and opinion to figure out the main challenges and strategies used to manage risk associated with cyber crimes.

**The tasks of the research:**

- To identify the main cyber crimes threats for the companies from experts' point of view;
- To find out companies' strengths and weaknesses in terms of cyber risk management;
- To figure out experts' opinion regarding effectiveness of cyber crimes prevention measures suggested in scientific literature;
- To disclose experts' evaluation of the external guidelines for cyber risk management;
- To identify legal regulation development areas based on the experts' opinion.

**The qualitative research method** – experts' opinion survey by structured interview or questionnaire form. This method was chosen in order to dig deeper into the problem, while the quantitative research is focused on the extent and spread of the phenomenon (Baley, 1995). Qualitative research allows obtaining various information, broadening the issue and analyzing it in a broader context. Interview is considered as one of the most effective qualitative research methods, which provides detailed answers, especially to open questions (Tidikis, 2003). Of all the types of interviews the expert interview was selected. The interview was carried out according to formulated questions and respondents were asked by the same procedure.

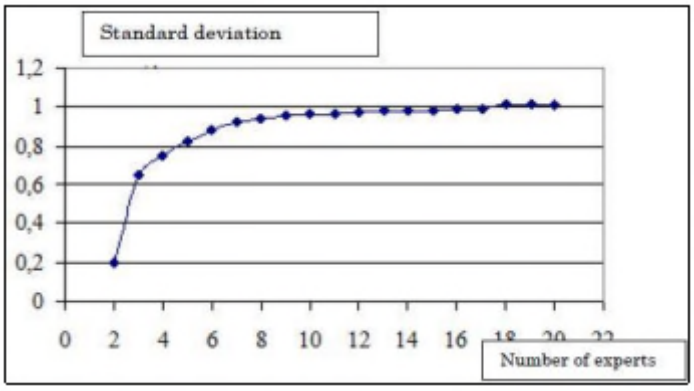
The questionnaire was made accordance with the **principles of drawing up the questionnaire**. The objective of the research was introduced; respondents were familiar with the issue of the research. It was noted that the questionnaire is aimed to find out the experts' insights about the main challenges and strategies used to manage risk associated with cyber crimes. The answers are submitted as the personal opinion and evaluation. The questionnaire indicates major explanations and instructions on how to fill in a certain part of the questionnaire.

### 3.1.1. Organization of the research

The problem of a sample size in quantitative research has been analyzed sufficiently. However, it is hard to determine what sample size should be held in qualitative research. The sample size depends on phenomenon details of the research, strategy of the research, informativeness of collected data and method of data collection. Applying interview, the proposed sample size is from five to thirty people, in this case eleven respondents have been chosen. Qualitative research findings are more closely related to the investigators' analytical capacity and testing of selected cases informativeness than the sample size of the problem (Bitinas, Rupšienė & Žydžiūnaitė, 2008). As a result, the sample size problem is not that much important by applying qualitative research method.

The experts have been chosen based on their professional area. The main selection criterion was that the expert would be related to cyber security field. The information was gathered based on recommendations and using the Internet. After selecting the experts, they were contacted personally. The researcher was presented to the experts as well as the problem of the research and the goal. Most of the experts wanted to stay anonymous without disclosing names of companies they are working in, but it was agreed to specify work experience and company's sector. In order to keep the anonymity, the experts are named with letters such as Expert A, Expert B and etc.

The survey was carried out between October 12 and November 4, 2016. The questionnaire was sent to eleven experts, assuming that not all answers will be received. All in all, three of the respondents did not provide the answers due to tight work schedule and lack of time. However, opinions of eight experts were analyzed. Moreover, the accuracy of decision and evaluation is sufficiently high when the number of experts reaches eight. Therefore, this number of experts is enough to obtain accurate information (see Figure 8).




**Source:** Baležentis & Žalimaitė, 2011, p. 25

**Figure 8.** Experts' evaluation standard deviation dependence on the number of experts

The graph illustrates the methodological assumptions set out in classical test theory. According to this graph, aggregate decision reliability and decision-makers number connects fast fading nonlinear connection. In the modules of aggregated experts' evaluation which are connected with equal weights, small groups of experts' decisions and evaluations accuracy do not descend to large group of experts' accuracy of decisions and evaluation (Baležentis & Žalimaitė, 2011).

The questionnaire consists of eleven questions: six of them are open-ended nature, four partly open and one was closed question. The questions were prepared based on the theoretical part of master thesis. The logical structure of the questionnaire is provided in the Annex 2.

### 3.1.2. Characteristics of survey respondents

In the **first** question, respondents were asked to describe their work experience and main responsibilities. The following eight respondents have answered the questionnaire:

- **Expert A** - Chief Information Security Officer, 12 years of experience. Field of activity - payments services. Main functions: risk management; deployment and management of information security management system; information security policy development; business continuity plan development; coordination of CERT team.
- **Expert B** - Chief of Critical Information Infrastructure Protection Branch, 25 years of experience in a defense sector, in a field of information security, intelligence and cyber defense. Field of activity – governmental institution. Main function - cyber security strategy creation and implementation.
- **Expert C** – Information Security Specialist, 3 years of experience. Main functions – cyber risk evaluation and management; business continuity plan development. Field of activity - state-owned enterprise, which provides services related to agriculture information management systems.
- **Expert D** – IT support Executive, 3 years of experience. Main function – coordination of the customers in terms of ensuring secure IT solutions. Field of activity – IT services.
- **Expert E** - Information Security Consultant, 5 years of experience. Main functions – support for project to identify gaps and advise how, they could be covered from security point of view; verification of solutions, implemented during the project, from security point of view. Field of activity – banking services.
- **Expert F** – Lead Information Security Engineer, 11 years of experience. Main functions – coordination of building and maintaining security systems; development of technical

solutions and new security tools; creation and development of information security strategy. Field of activity – banking services.

- **Expert G** – Senior Information Security Analyst, 5 years of experience. Main functions - establish plans and protocols to protect digital files and information systems; maintain data and monitor security access; plan, implement and upgrade security measures and controls; analyze security breaches to determine their root cause. Field of activity – money transfers services.
- **Expert H** – Information Security Manager, 13 years of experience. Main functions - developing, maintaining monitoring compliance of information security policy and procedures; security risk analysis and risk management; management of internal audits on information security processes, controls and systems. Field of activity – financial services.

Overall, all respondents are responsible for ensuring information security at the company on different levels. Some of them have more experience and see the broader view of the company in terms of cyber security management; others are more focused on specific functions in whole cyber security assurance process.

## 3.2. Data analysis

In the **second question**, respondents were asked to mark most frequent cyber crimes against business companies with possibility to add their own options. Figure 9 shows how experts' choices were distributed.

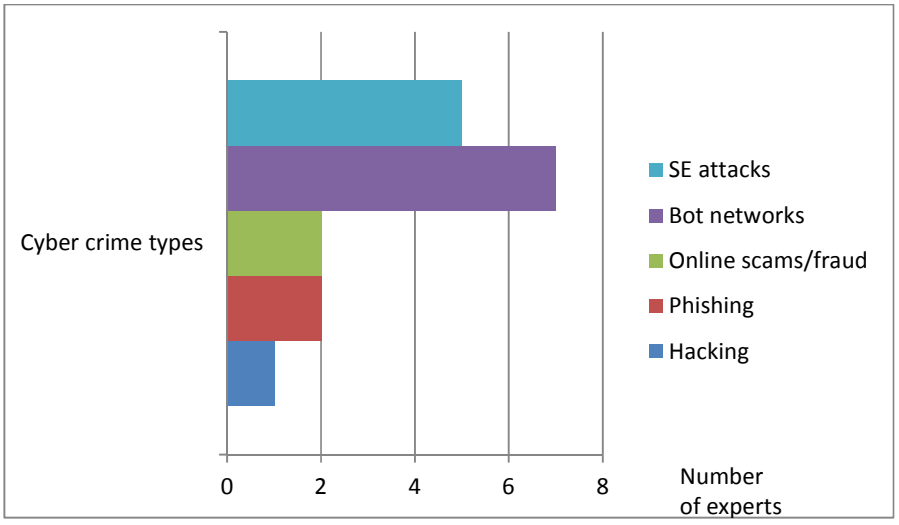



**Figure 9.** Most frequent cyber crimes against business companies

According to experts, the most frequent cyber crimes against companies are bot networks and social engineering attacks. None of the experts has chosen cyber stalking and online trading scam, which possibly are more complex and rare attacks. Expert A provided some additional comments regarding these types of cyber crimes. According to him, bot networks attacks (spam emails, DDoS attacks) are able to compromise many systems at the same time, usually they target even different companies and spread malicious software to several users' computers, and therefore, those attacks are one of the biggest online threats today. Meanwhile, social engineering attacks target the particular company and are one of the most dangerous cyber crimes. Since the target of such attacks is an employee of the company, the damage for the company can be very significant (sensitive information loss, financial damage and etc.). Hacking is more complex and rare attack and usually targets also the specific company. Phishing attacks seeks for sensitive information such as usernames, passwords and credit card details and for this purpose often targets private consumers.

To sum up second question, based on the experts' opinion the most frequent attacks against companies are bot networks and social engineering attacks. Bot networks are automated attacks, which target several systems at the same time, while social engineering attacks focus on specific company and target is a person.

**Third question:** How would you describe the main threats for the companies in terms of cyber crime?

- Expert A claims that threats caused by cyber crime tightly depend on the type and activity of the company. Overall, main threats are *"confidential data loss and disturbance of the processes or services provided to customers, which might lead to reputational as well as financial losses. The human factor is a part in security chain which is most difficult to control for any company. Therefore, it is very important to provide limited access for confidential information."*
- Expert B: *"Main cyber threat goes from the inside of the company: lack of understanding of cyber threat and lack of budget of prevention capabilities."*
- Expert C listed such cyber crime threats as *"sensitive information loss or theft, denial of service, misuse of confidential data, illegal access to the databases".*
- Expert D: *"In my experience main cyber crime threats such as information loss or misuse, identity theft, processes disturbance appear due to non existing security policy in the company and human errors."*
- Expert E provided two main categories of the cyber crime threats:

- *"Data leakage – when organization classified data (customer details; organization secrets) are stolen by organized criminal groups and later used to compromise organizations or their customers.*
- *Deny of Service – when organization provided service are not accessible to organization customers."*

- Expert F: *"Main threats can be assumed to be the ones that would mean loss of revenue and have an impact on customers."*
- Expert G: *"Main threats in terms of cyber crimes for the any organization are the following: lack of cyber security policy and recovery plan; human factor as the weakest link for information loss; lack of "Bring Your Own Device" policy."*
- Expert H: *"Main cyber crime threats are related to systems intrusions or human mistakes and can lead to a loss of confidential information. When that happens, the organization can lose revenue and may even face fines from regulatory agencies for failing to protect data."*

In summary, the main threats for the business caused by cyber crimes can be defined as confidential data loss and/or disturbance of services. The organization might face these threats due to lack of cyber security policy and recovery plan, unawareness or intentional actions of employees, lack of investments into cyber security and other factors. The consequences can have very significant impact on the organization such as reputational or/and financial losses.

In the **fourth question** experts were asked to evaluate their current company's strengths and weaknesses in terms of cyber risk management. Figure 10 shows the results of evaluation (S – strength, W – weakness).

| **Factor** | **Experts** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** |
| Cyber security policies and procedures | S | S | S | S | S | S | S | S |
| Cyber security training programs | S | S | S | S | W | W | S | S |
| Qualified cyber security professionals | S | S | S | S | S | S | S | S |
| Active partnership with other organizations, sharing initiatives and reporting of cyber crime | S | S | W | W | S | S | W | W |
| Timely response to threats and attacks | S | S | W | S | S | S | S | S |
| Continuous risk assessment, development and implementation of cyber risk management strategy | S | S | S | S | W | W | S | S |
| Continuous systems testing | S | S | W | S | W | W | S | S |
| Customers' education | S | S | S | S | W | S | W | S |
| Technology security level | S | S | S | S | W | S | S | S |

**Figure 10.** Evaluation of strengths and weakness in terms of cyber risk management

In summary, results show that two experts A and B evaluated their current companies as very strong and developed in terms of cyber security management. Two factors were identified as most frequent weaknesses of the evaluated companies: active partnership with other organizations, sharing initiatives and reporting of cyber crime and continuous systems testing. Main reason for no partnership with other organizations might be that companies usually are not willing to disclose any incidents they face and to solve issues within the organization without spreading the information further. In order to continuously test the systems, organization requires additionally to fund the testing, which is not priority costs for some companies. All experts agreed that their companies have cyber security policies and procedures and qualified cyber security professionals in place, which are very important factors in order to effectively manage cyber risk.

In the **fifth question** experts were asked to evaluate effectiveness of the measures in cyber crime prevention used on national level as well as on company level according to the evaluation assessment scale from -2 to 2 (2 means “most effective”, 1 – “effective”, 0 – “neutral ”, -1 – “ineffective”, -2 – “most ineffective”). Figure 11 presents the results of cyber crime prevention measures on national level evaluation.

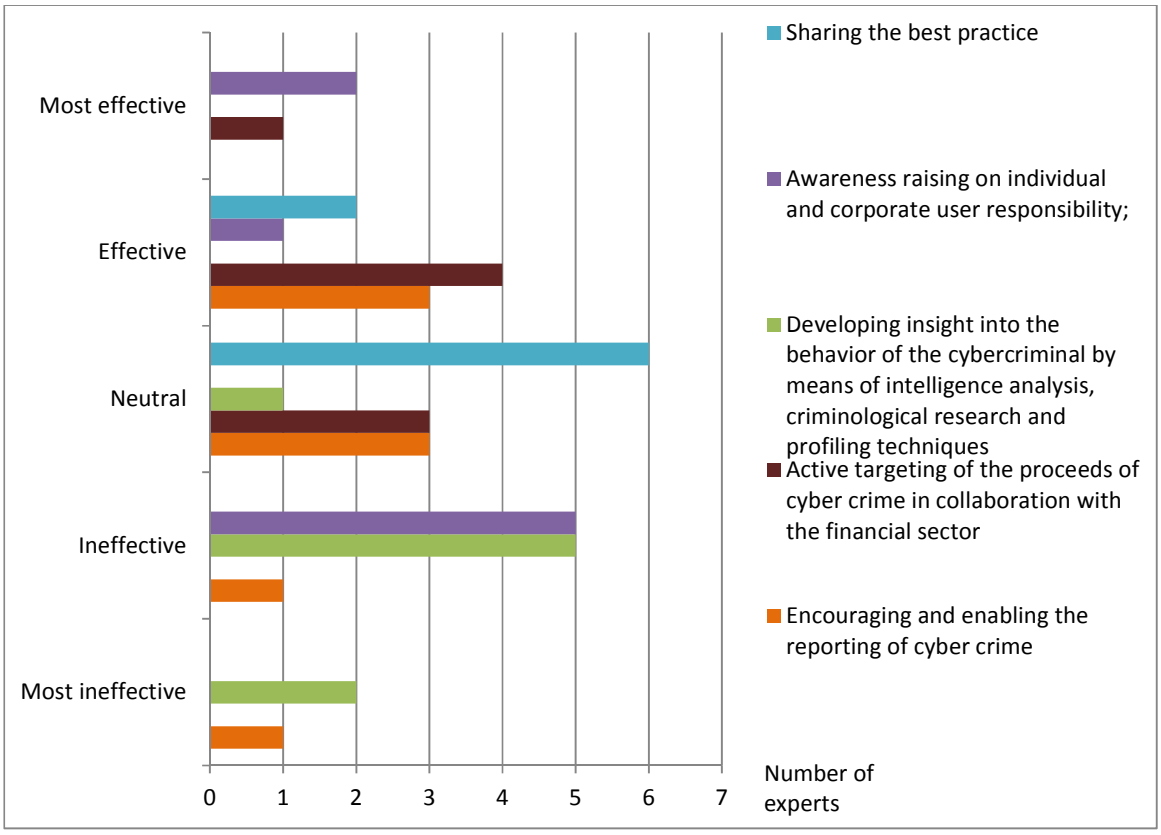



**Figure 11.** Evaluation of cyber crime prevention measures on national level

Results show that more than half of the experts (5 out of 8) have an opinion that two suggested cyber crime prevention measures (developing insight into the behavior of the cybercriminal by means of intelligence analysis, criminological research and profiling techniques and awareness raising on individual and corporate user responsibility) are not working on national level and, therefore, they were evaluated as ineffective. Sharing the best practice was evaluated as neutral by the majority of the respondents (6 out of 8). According to Expert A, institutions might share some important information regarding cyber crimes among each other but usually this information is not accessible for financial institutions and other companies. More than half of experts (5 out of 8) think that active targeting of the proceeds of cyber crime in collaboration with the financial sector is effectively working on national level. Experts had a different opinion regarding encouraging and enabling the reporting of cyber crime: evaluations vary from "most ineffective" till "effective".

Figure 12 presents the results of cyber crime prevention measures on company level evaluation.

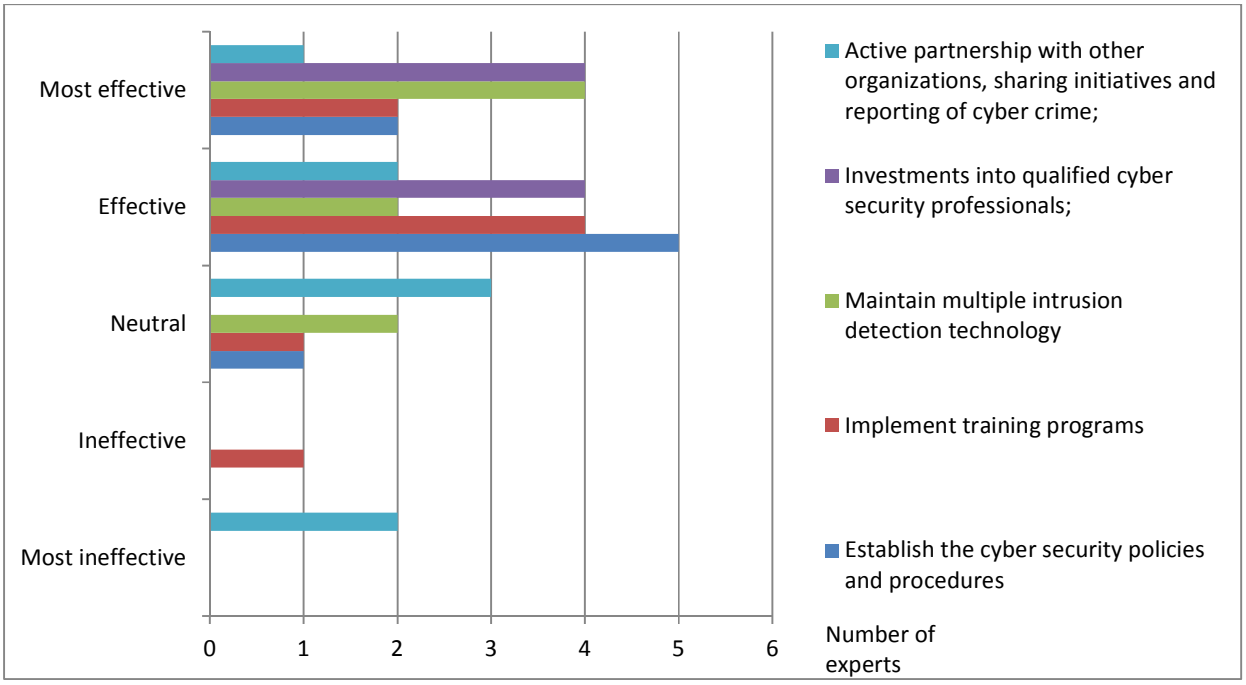



Figure 12 continued on the next page

Figure 12 continued from the previous page

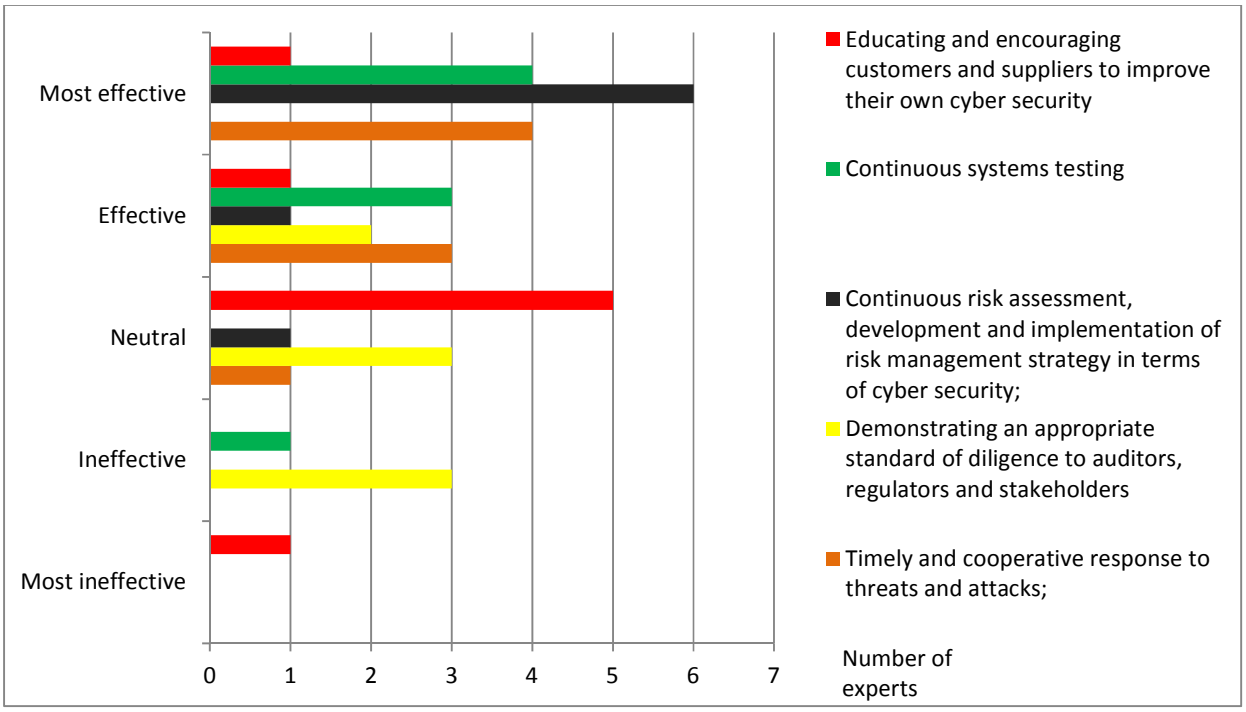



**Figure 12.** Evaluation of cyber crime prevention measures on company level

More than half of experts evaluated the following measures as effective or most effective which are used by companies in prevention of cyber crimes:

- Investments into qualified cyber security professionals (8 out of 8).
- Establish the cyber security policies and procedures, which include guidelines for investigation of and recovery from cybercrimes after they occur (7 out of 8);
- Timely and cooperative response to threats and attacks (7 out of 8);
- Continuous risk assessment, development and implementation of risk management strategy in terms of cyber security (7 out of 8);
- Continuous systems testing which encompasses the resistance to threats and ability to minimize and mitigate the damage caused by successful attacks (7 out of 8);
- Maintain multiple intrusion detection technology (6 out of 8);
- Implement training programs and disseminate the information on latest threats within the organization (5 out of 8).

None of the measures listed in Figure 12 was evaluated as ineffective or most ineffective by the half or more experts. However, communication in terms of cyber threats to the external stakeholders such as customers, auditors, regulators and other organizations has to be

improved in order to manage cyber risk in more efficient way. Moreover, some experts noted that these measures are usually used by large companies from financial or IT sector, small and medium enterprises often do not focus on cyber security at all due to lack of awareness and financial resources.

**Sixth question:** What are the main reasons, from your perspective, why some companies still do not focus enough on cyber crimes risks?

- Expert A states that the lack of financial recourses is a primary reason for small and medium enterprises not to focus on cyber security. *"Unfortunately, usually the investments into cyber security impact the higher price of services which would reduce the competitiveness of the company or it even can be thrown out of the market."* Larger companies, which do not focus enough on cyber security, usually do not evaluate properly the risks and potential damage caused by cyber crime. The attitude usually start to change after some significant losses caused by any cyber attack.
- Expert B identified three main reasons:
  - *"Cyber risks are evaluated as low;*
  - *Cyber security is not in same line of defense as other disciplines (physical, personnel, industrial security, etc.);*
  - *Lack of evidence of big losses in a larger segment of the companies (by size and turnover)."*
- Expert C noted that only few companies include in their budget plan expenses for cyber security. According to him, the main reason is a lack of managers' awareness about the importance of cyber security and possible cyber crime threats.
- Expert D: *"Usually companies think that they are safe and that the cybercrimes are happening only to large companies. Moreover, the complex cyber security solutions are too expensive for small and medium enterprises."*
- Expert E: "*Lack of information about possible cyber crimes damage/impact."*
- Expert F: *"Primarily because losses and/or fines are much lower than the cost of mitigating controls to prevent the attacks, especially for small companies."*
- Expert G: *"Smaller companies usually lack resources to mitigate cyber crime risks. They focus primarily on investments into product, services, marketing strategies and etc. Since SMEs often do not evaluate the importance of cyber security, cybercriminals use them as a gateway into larger organizations they have business relationship with. Therefore, education and information sharing on the cyber crimes threats are very important factors as well."*

- Expert H identified that companies which do not focus enough on cyber crime risks usually lack "*actionable vision or understanding within the organization about the significance of cyber risks management. It has to be clearly communicated that safeguarding intellectual property, financial information, and company's reputation is a crucial part of business strategy.*"

To sum up sixth question, based on the experts' insights the main barriers for effective cyber security are lack of financial resources; failure to understand possible damage and losses caused by cyber crimes; inappropriate evaluation of cyber crimes risks; lack of cyber security strategy and prioritization from leadership; gaps in external as well as internal communication about the importance of cyber security.

In the **seventh question** experts were asked if they would recommend for business organizations to use NIST Framework (see Figure 3) or would they suggest any additional or totally different steps for the cyber risk evaluation and management framework. All nine experts were familiar with this model and they all recommended using it for business organizations as basic guidelines to identify, implement and improve their cyber security practises. According to experts, each company should adapt this model and expand it considering the specifics of business activities, potential risks and etc. Moreover, Expert C suggested that some metrics and scales could be introduced for risk evaluation, but this should be done by each company individually. All in all, the opinion of experts coincides with the view of scientists that there is no one-size-fits-all solution for cyber security management, and business organizations might use the Framework as recommendation adjusting it to the business needs.

**Eighth question:** What development areas do you see on legal regulation side? What can be improved from law enforcement perspective in fight against cyber crimes?

This question was answered by four experts in details:

Experts A and C provided similar opinion that in Lithuania responsibilities of institutions involved in cyber security regulation are not clear defined and distinguished. Institutions responsible for cyber security policy formatting, implementation and control have to be clearly determined. Expert A added that it should be one institution responsible for fast response to cyber attacks instead of complicated bureaucratic system. From his point of view, the police is missing instructions and knowledge how to handle cyber crimes in efficient and faster way. Moreover, according to expert A, Lithuanian court practice shows that articles related to cybercrime under the Criminal Code of the Republic of Lithuania are still not applied in practice. Instead, articles related to fraud are being applied to crimes conducted in e-environment.

Expert B: *"Taking into account the fact that cyber crimes are committed by differently motivated actors and the most incidents are coming from online internet connection, the state internet infrastructure should be regulated better: implemented mechanism of elastic balancing of internet volumes within ISP's, activities of actors (infrastructure owners, ISPs, web application engineering subjects) should be regulated by the minimal cyber security requirements, i.e. the responsibilities should be divided and set by law to all players in the chain."*

Expert F: *"First off responsibility for company management has to be increased. For example, the US, after major attacks and incidents of neglect have changed laws making the managing director personally responsible for security and clarity of financial data (audits in general focus on integrity of systems doing the processing and now reviewing each reporting line) and imposing fines and jail sentences. Adding this across businesses including governmental institutions would increase cyber security significantly. At the same time law enforcement requires more control to ensure that they are not bypassing laws and have sufficient evidence of wrongdoing before gaining access to data through call/data interception and investigation."*

Overall, experts identified several areas which could be improved on legal regulation side. Those would include responsibilities of institutions involved in cyber security regulation should be clearly defined and distinguished. Furthermore, fast response to cyber attacks is missing from law enforcement side. Finally, responsibility of companies' management as well as of ISPs should be increased introducing mandatory cyber security requirements.

**Ninth question:** Do you cooperate with other organizations in sharing best practices or other information related to cyber crimes? If yes, please select the units you are in partnership with.

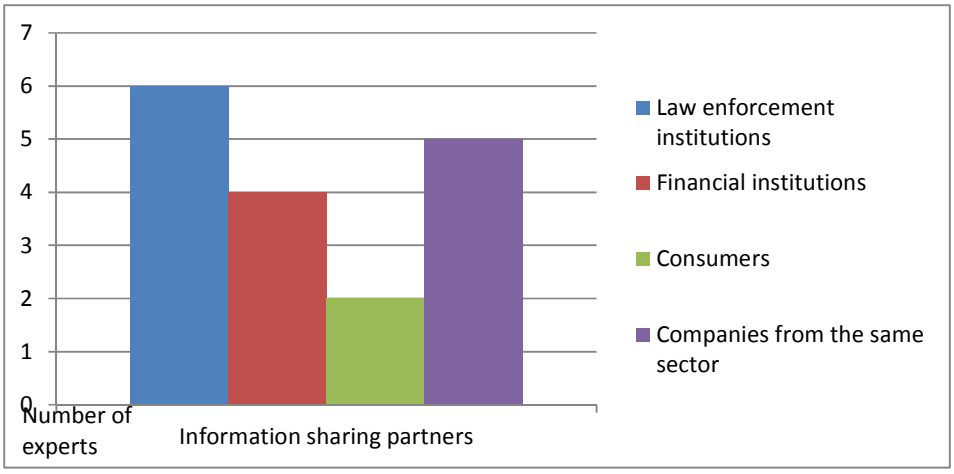



**Figure 13.** Partners for best practices sharing

Figure 13 shows that more than half experts' companies tend to share information regarding cyber crimes threats and trends with law enforcement institutions and other companies from the same sector. However, only 2 of 8 respondents stated that their companies share best practice with consumers. Business organizations might avoid to share information with customers regarding cyber incidents in order not to frighten them and do not lose clients, but on the other hand customer may lack education in cyber security field which could lead the company again to reputational risk. Therefore, it is very important to develop and promote best practices sharing culture among all stakeholders.

In the **tenth question** experts were asked if they have to use any external guidelines for cyber risk management in the company they work for. The experts identified the following external sources which are used for cyber risk management:

- ISO/IEC 27032:2012, which provides guidance for improving the state of cyber security and mainly covers information security, network security, internet security, and critical information infrastructure protection aspects. In particular this International Standard provides technical guidance for addressing common cyber security risks, including social engineering attacks, hacking, malware attacks and etc.
- ISO 31000:2009, which provides principles and generic guidelines on risk management.
- ISO/IEC 27005:2011, which coverts information technology, security techniques and information security risk management topics.
- PCI DSS (Payment Card Industry Data Security Standard), which is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. The PCI DSS specifies and elaborates on six major objectives: build and maintain a secure network; protect cardholder data; maintain a vulnerability management program; implement strong access control measures; regularly monitor and test networks; maintain an information security policy.
- NIST Framework.

All of these sources provided by the experts are used by the companies as recommendations and guidelines while creating internal cyber security policies and procedures. The exception is only the PCI Standard which applies to any organization, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data.

In the **eleventh question** experts were asked to provide examples of cyber attacks if they have faced any during their work experience. 6 of 8 experts provided the following examples presented in Table 4.

**Table 4**. Examples of cyber crimes

| | |
|---|---|
| | |
| **Type of cyber crime** | Defacement of web sites |
| **Damage for the company** | Reputational |
| **Main measures which solved the issues** | Set of procedural and technical measures which are implemented at corporate level |
| **Lessons learned** | Re-gain the control over the process |
| | |
| **Type of cyber crime** | DDoS attacks |
| **Damage for the company** | No losses |
| **Main measures which solved the issues** | Well prepared counter-measures |
| **Lessons learned** | N/A |
| | |
| **Type of cyber crime** | Phishing attack |
| **Damage for the company (please select)** | Business processes restriction |
| **Main measures which solved the issues** | Recovery plan and fast actions |
| **Lessons learned** | Training for new hires during onboarding stage has to be provided. |
| | |
| **Type of cyber crime** | DDoS attacks |
| **Damage for the company (please select)** | Business processes restriction |
| **Main measures which solved the issues** | Deployment of security measures against DDos attacks |
| **Lessons learned** | N/A |
| | |
| **Type of cyber crime** | Hacking of testing system |
| **Damage for the company (please select)** | No losses |
| **Main measures which solved the issues** | N/A |
| **Lessons learned** | Additional actions was introduced: coordination of actions among involved parties during, refreshment training for employees regarding strong passwords creation |
| | |
| **Type of cyber crime** | Social engineering attack |
| **Damage for the company (please select)** | No losses |
| **Main measures which solved the issues** | Awareness of employee who was targeted and following the cyber risk management procedure |
| **Lessons learned** | Promotion of information and best practices sharing |

**Source:** prepared by the author based on the information received from experts

Table 4 shows that even two experts have faced DDoS attacks in their experience, other experts provided different examples of cyber crimes which were analyzed in previous chapters. Two cyber attacks caused business processes restriction and one – reputational damage for the companies. In order to solve the issues triggered by cyber incidents organizations usually follow an internal company's procedure and adjust counter measures against cyber criminals. Finally, cyber attacks reveal for the company gaps in cyber risk management process (f.e. lack of training, weak control mechanism, need for actions coordination and information sharing promotion), which organization should focus on.

## 3.3. Results of data analysis

- According to the experts, the most frequent attacks against companies are bot networks and social engineering attacks. Bot networks are automated attacks, which target several systems at the same time, while social engineering attacks focus on specific company and target is a person.
- Confidential data loss and/or disturbance of services were identified by experts as main threats for business caused by cyber crimes. The organization might face these threats mainly due to lack of cyber security policy and recovery plan, unawareness or intentional actions of employees and/or lack of investments into cyber security. The consequences can have very significant impact on business such as reputational or/and financial losses.
- Two experts evaluated their current companies as very strong and developed in terms of cyber security management. Other respondents identified partnership with other organizations and continuous systems testing as most frequent weaknesses of the evaluated business organizations. Main reason for no partnership with other organizations might be that companies usually are not willing to disclose any incidents they face and solve issues within the organization without spreading the information further. In order to continuously test the systems, organization requires dedicating additional funds for the testing, which is not a priority costs for some companies.
- More than half of experts think that cyber crime prevention measures such as awareness raising on individual or corporate user responsibility and developing insight into the behavior of the cybercriminal by means of intelligence analysis, criminological research and profiling techniques are not working properly on national level. Meanwhile, active targeting of the proceeds of cyber crime in collaboration with the financial sector was evaluated by five experts as effective measure applied on national level.

- Most of cyber crime prevention measures, which are used on a company level, were evaluated as “effective” or “most effective” by the majority of experts. All experts agreed that investment into qualified cyber security professionals contributes to effective cyber crime prevention. However, communication in terms of cyber threats to the external stakeholders has to be improved in order to manage cyber risk in more efficient way.
- Considering experts’ insights, main barriers for effective cyber security management are the following: lack of financial resources; lack of understanding of possible damage and losses caused by cyber crimes; inappropriate evaluation of cyber crimes risks; lack of cyber security strategy and prioritization from leadership; gaps in external as well as internal communication about the importance of cyber security.
- All nine experts were familiar with NIST Framework they all would recommend to use it for business organizations as basic guidelines to identify, implement and improve their cyber security practises. According to experts, each company should adapt this model and expand it considering the specifics of business activities, potential risks and etc.
- Experts identified several areas which could be improved on legal regulation side. First of all, responsibilities of institutions, involved in cyber security regulation, should be clearly defined and distinguished. Secondly, fast response to cyber attacks is missing from law enforcement side. Finally, responsibility of companies’ management as well as of ISPs should be increased introducing mandatory cyber security requirements.
- Experts revealed that companies tend to share information regarding cyber crimes threats with law enforcement institutions and other companies from the same sector. However, there is a lack of sharing best practices with consumers.
- Experts identified different external sources (f.e. ISO International Standards) which are used by organizations as recommendations and guidelines while creating internal cyber security policies and procedures.
- Cyber crimes examples provided by experts showed that in order to solve the issues triggered by cyber incidents organizations usually follow an internal company’s procedure and adjust counter measures against cyber criminals. Moreover, cyber attacks identify for the company gaps in cyber risk management process (f.e. lack of training, weak control mechanism, need for actions coordination and information sharing promotion), which organization should focus on.

# CONCLUSIONS AND RECOMMENDATIONS

1. The growth and ubiquitous of Internet provides opportunities not only for fair business creation and development but also creates environment for the criminals. Any player of cyber space can become victim of cyber crime: from the governmental institution to the single individual. The cyber criminals have very different motives to commit a crime. Based on the aims of attackers different level of damage can be achieved. The variety of cyber crimes types shows that there are many different ways to harm and interrupt private and confident data, which usually leads to losses for individual as well as for business. Main challenges concerning cyber crimes are tightly related with their main features such as borderless, rapidly changing and profit driven nature. There are four main areas which are mostly impacted by the activities of cyber criminals: economic, consumer trust, market value and national security. Cyber crimes cost for companies billions of dollars annually in stolen assets and lost business. They can totally disrupt a company's activities and ruin customers' trust. Moreover, not only consumers or companies are vulnerable to cybercrime, but also national security stands at the risk while facing criminal activities in cyber space. Prevention measurements against cyber crimes should be taken on all levels: individual, company's and national. The enhanced partnership and information sharing among all actors is essential factor in the fight against cyber crimes. For the organizations, one of the main measures in cyber crime prevention is ensuring that cyber risk management strategy is in place and is aligned with overall business strategy.
2. Since cyber crimes are considered as global issue, the trends in Europe and the US are comparable. Ransomware attacks remain top malware threat in both regions. Data breaches, network intrusions, different fraud attacks are main focus areas for EU and the US law enforcement institutions. In terms of cyber crimes volumes, the U.S. outruns European countries. Main challenges for law enforcement institutions in both regions are inefficient international collaboration and information exchange as well as different challenges related to the Cloud. Europol as well as FBI highlight the importance of international cooperation and information sharing among law enforcement institutions, business organizations, academia and other units in order to have effective fight against cyber criminals.
3. Qualitative study of experts showed that most of the large companies in financial and IT sector have implemented cyber risks management strategy. According to the experts main barriers for effective cyber security management are lack of financial resources; not understanding of possible damage caused by cyber crimes; lack prioritization from

leadership; gaps in external as well as internal communication about the importance of cyber security. All experts agreed that investment into qualified cyber security professionals contributes to effective cyber crime prevention. Although a majority of cyber crimes measures suggested in scientific literature are effectively applied on the company's level, communication regarding cyber crime threats among stakeholders has to be improved in order to manage cyber risk in more efficient way. Cyber crimes examples provided by experts showed that in order to solve the issues triggered by cyber incidents organizations usually follow an internal company's procedure and adjust counter measures against cyber criminals. Moreover, cyber attacks identify for the company gaps in cyber risk management process, which organization should focus on.

**Recommendations:**

- While handling cyber crime challenges, business organizations should identify their weaknesses in terms of cyber risk management and put efforts to improve these areas.
- Cyber security management has to be prioritized and promoted by leadership on company level. Moreover, this field has to be important not only for the financial or IT organizations but also for all others sectors as manufacturing, educational, medical and etc.
- On the national level, responsibilities of institutions, involved in cyber security regulation, should be clearly defined and distinguished. Moreover, respective governmental institutions should more focus on awareness raising on individual or corporate user responsibility.
- Finally, information and best practice sharing is one of the improvement areas for public institutions as well as for private business companies in order to better fight against cyber criminals.

# LIST OF REFERENCES


1. Australian Cybercrime Online Reporting Network. Attacks on Computer systems. Retrieved from: https://www.acorn.gov.au/learn-about-cybercrime/attacks-computer-systems (date of access: August 25, 2016)
2. Australian Cybercrime Online Reporting Network. Cyber bullying. Retrieved from: https://www.acorn.gov.au/learn-about-cybercrime/cyber-bullying (date of access: August 25, 2016)
3. Australian Cybercrime Online Reporting Network. Email spam and phishing. Retrieved from: https://www.acorn.gov.au/learn-about-cybercrime/email-spam-and-phishing (date of access: August 25, 2016)
4. Australian Cybercrime Online Reporting Network. Online scams or fraud. Retrieved from: https://www.acorn.gov.au/learn-about-cybercrime/online-scams-or-fraud (date of access: August 25, 2016)
5. Australian Cybercrime Online Reporting Network. Online Trading Issues. Retrieved from: https://www.acorn.gov.au/learn-about-cybercrime/online-trading-issues (date of access: August 25, 2016)
6. Atoum, I. and et. al. (2014). A holistic cyber security implementation framework. Journal of Information and Computer Security, Volume 22, Number 3, p. 251 – 264.
7. Bailey, W. G. (1995). The Encyclopedia of Police Science. New York: State University of New York.
8. Baležentis, A. & Žalimaitė, M. (2011). Ekspertinių vertinimų taikymas inovacijų plėtros veiksnių analizėje: Lietuvos inovatyvių įmonių vertinimas. Vadybos mokslas ir studijos – kaimo verslų ir jų infrastruktūros plėtrai, 3 (27). P. 23-31.
9. Beard, Ch. and et. al. (July, 2015). US cybersecurity: Progress stalled. Key findings from the 2015. US State of Cybercrime Survey. Retrieved from http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-cybercrime-survey-2015.html (date of access: September 5, 2016)
10. Bocij, P. (2004). Cyber stalking – harassment in the Internet age and how to protect your family. Library of Congress Cataloging in Publication Data. ISBN: 0-275-98118-5.
11. Borum, R. and et. al. (2014). Journal of Information and Computer Security, Volume 23, Number 3, p. 317 – 332.
12. Breach Level Index. Data breach database. Retrieved from http://www.breachlevelindex.com/data-breach-database (date of access: October 10, 2016)

13. Byrne, G. (2007). Botnets- the killer web app. Syngress Publishing Inc. ISBN: 1-59749-135-7.
14. Department of Homeland Security. Information Sharing and Analysis Organizations (ISAOs). Retrieved from https://www.dhs.gov/isao. (date of access: October 13, 2016)
15. Erickson, J. (2008). Hacking – the art of exploitation. William Pollock Publishers, 2nd Edition. ISBN: 1-59327-144-1.
16. Europol (January, 2011). Cyber crime presents a major challenge for law enforcement. Retrieved from: https://www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law-enforcement-523 (date of access: August 26, 2016)
17. Europol's European Cybercrime Centre (EC3) (September, 2015). The Internet Organized Crime Threat Assesment (IOCTA). Retrieved from: https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015 (date of access: September 3, 2016)
18. Europol's European Cybercrime Centre (EC3) (September, 2016). The Internet Organized Crime Threat Assesment (IOCTA). Retrieved from https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016 (date of access: October 10, 2016)
19. Federal Bureau of Investigations. Cyber crime. Retrieved from: https://www.fbi.gov/investigate/cyber (date of access: August 20, 2016)
20. Federal Bureau of Investigations. Internet Fraud. Retrieved from: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud (date of access: August 20, 2016)
21. Federal Bureau of Investigations (April, 2016). Incidents of Ransomware on the Rise. Retrieved from https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise. (date of access: October 16, 2016)
22. Franceschetti, G. and Grossi, M. (2008). Homeland security – technology challenges from sensing and encrypting to mining and modeling. Library of Congress, U.S. ISBN: 978-59693-289-0.
23. Gemalto (February, 2016). Gemalto releases findings of 2015 Breach Level Index. Retrieved from http://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-2015-Breach-Level-Index.aspx (date of access: September 10, 2016)
24. Gottschalk, P. (2010). Categories of financial crime. Journal of Financial Crime, Volume 17, Number 4, p. 441 – 458.
25. Goderdzishvili, N. (November, 2010). Legal assessment of cyber attacks on Georgia. Data Exchange Agency Ministry of Justice of Georgia.

26. Guinn, J. and et. al. (May, 2014). Why you should adopt the NIST cyber security framework. Retrieved from http://www.pwc.com/us/en/increasing-it-effectiveness/publications/adopt-the-nist.html (date of access: August 30, 2016)
27. Hodgson, T.W. (2008). From famine to feast: the prosecution of multi-jurisdictional financial crime in the electronic age. Journal of Financial Crime, Volume 15, Number 3, p. 320 – 327.
28. Infosec Institute (November, 2013). 2013 – The impact of cyber crime. Retrieved from: http://resources.infosecinstitute.com/2013-impact-cybercrime/ (date of access: August 20, 2016)
29. Interpol. Cybercrime. Retrieved from: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (date of access: August 14, 2016)
30. Interpol. Online Safety. Retrieved from: http://www.interpol.int/Crime-areas/Cybercrime/Online-safety (date of access: August 14, 2016)
31. Joseph, A.E. (June, 2006). Cybercrime definition. Computer Crime Research center. Retrieved from: http://www.crime-research.org/articles/joseph06/ (date of access: September 5, 2016)
32. Karamchand Gandhi, V. (2012). An overview study of cyber crimes in Internet. Journal of Information Engineering and Applications, Volume 2, Number 1.
33. Kratchman, S. and et al. (2008). The Perpetration and Prevention of Cybercrimes. Internal Auditing, Volume 23, Number 2, p. 3-12.
34. Lavorgna, A. (2015). Organised crime goes online: realities and challenges. Journal of Money Laundering Control, Volume 18, Issue 2, p. 153-168.
35. Mcguire, M. and Dowling, S. (October, 2013). Cyber crime: a review of the evidence. Research Report 75. Chapter 2: Cyber enabled crimes – fraud and theft.
36. Mehmood, Sh. (April, 2016). Enterprise survival guide for ransomware attacks. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-ransomware-attacks-36962 (date of access: September 14, 2016)
37. Menon, S. and Siew, T. G. (2012). Key challenges in tackling economic and cyber crimes: Creating a multilateral platform for international co-operation. Journal of Money Laundering Control, Volume 15, Issue 3, p. 243 – 256.
38. Milhorn, H.T. (2007). Cyber crime – how to avoid becoming a victim. Universal Publishers. ISBN: 1-58112-954-8.
39. Moyer, J. and Rudasill L. (2004). Cyber security, cyber attack and the development of governmental response: the librarian's view. New Library World, Volume 105, Issue 7/8, p. 248 – 255.

40. National Crime Prevention Council (2012). Cyber Crimes. Retrieved from http://www.ncpc.org/resources/files/pdf/internet-safety/13020-Cybercrimes-revSPR.pdf (date of access: August 12, 2016)
41. National Crime Agency (July, 2016). Cyber Crime Assessment 2016. Retrieved from http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file (date of access: August 12, 2016)
42. OECD guidelines for the security of information systems and networks: towards a culture of security. (2002). Retrieved from: http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm (date of access: August 29, 2016)
43. Poonia, A.S. (2014). Cyber Crime: Challenges and its Classification. International Journal of Emerging Trends & Technology in Computer Science, Volume 3, Issue 6, p. 119 – 121.
44. Putte. D. V. and Verhelst, M. (2013). Cyber crime: Can a standard risk analysis help in the challenges facing business continuity managers? Journal of Business Continuity & Emergency Planning, Volume 7, Number 2, p. 126 – 137.
45. Saini, H. and et. al. (2012). Cyber crimes and their impacts: a review. International Journal of Engineering Research and Applications, Volume 2, Issue 2, p. 202-209.
46. Sentonas, M. (March, 2014). The Economic Impact of Cyber Crime and Cyber Espionage. Security Solutions Magazine. Retrieved from http://www.matthewaid.com/post/79863382147/the-economic-impact-of-cyber-crime-and-cyber (date of access: August 30, 2016)
47. Smith, K.T. and et. al. (2011). Case studies of cybercrime and its impact on marketing activity and shareholder value. Academy of Marketing Studies Journal.
48. Statista (2016). IC3: total damage caused by reported cyber crime 2001-2015. Retrieved from https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/ (date of access: October 25, 2016)
49. Symantec (April, 2015). Internet Security Threat Report, Volume 20. Retrieved from https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf (date of access: September 4, 2016)
50. The National Institute of Standards and Technology (February, 2014). Framework for Improving Critical Infrastructure Cybersecurity.
51. Tidikis, R. (2003). Socialinių mokslų tyrimų metodologija. Vilnius: Lietuvos teisės universiteto leidybos centras.

52. Trend Micro (2015), Annual Security Roundup. Retrieved from https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf (date of access: September 4, 2016)
53. Uma, M. and Padmavathi, G. (2013). A survey on various cyber attacks and their classification. International Journal of Network Security, Volume 15, Number 5, p. 390 – 396.
54. U.S. Agency of International development. Cyber crime: it's impact on government, society and the prosecutor.
55. Verizon (2016). Data breach investigation report. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/ (date of access: September 10, 2016)
56. Vijayan, J. (April, 2010). Targeted cyber attacks testing IT managers.
57. Wainwright, R. (2010). Dealing with cyber crime – challenges and solutions. Global Economic Symposium. Retrieved from http://www.global-economic-symposium.org/knowledgebase/the-global-polity/cybercrime-cybersecurity-and-the-future-of-the-internet/proposals/dealing-with-cyber-crime-2013-challenges-and-solutions (date of access: August 30, 2016)
58. William, L. and Tafoya, L. (November, 2011). Cyber terror. FBI Law Enforcement Bulletin. Retrieved from: https://leb.fbi.gov/2011/november/cyber-terror (date of access: August 27, 2016)

**Grigorovič V.** Cyber Crimes: Analysis of Reasons and Effects for Business Organizations / Master's Thesis of Electronic Business Management program. Supervisor Prof. Dr. V. Davidavičienė – Vilnius: Mykolas Romeris University, Business and Media School, 2016. – 69 p.

## SUMMARY

The rapid growth of the Internet provides not only tremendous opportunities for business development, but also it opens new possibilities for cyber criminals. New trends in cyber crime are emerging all the time, with estimated costs to the global economy running to billions of dollars. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities without any borders and cause serious damage to victims worldwide. The problem of the research is that many companies do not evaluate properly the challenges and risks associated with cyber crimes and impact on the business. The object of study - cyber crimes and prevention measures against them. The goal of the research - to analyze the reasons and effects of cyber crimes on business organizations. In order to achieve the goal the following objectives were determined: to overview the main characteristics of cyber crimes (the concept, types and prevention measures); to compare the cyber crimes trends in EU and the US; to perform the qualitative study of experts regarding the strategies for preventing and handling cyber crimes challenges. The following methods were applied in master thesis: analytical method, comparative method, structured interview method, descriptive statistical method, method of the generalization.

After the analysis of theoretical aspects and qualitative study results, main cyber crime challenges were identified. Moreover, the drawbacks of cyber risk management have been determined and the solutions proposed for gaps filling. The comparison of cyber crime trends in EU and US showed the similar tendencies in both regions. Master thesis results were presented during Compliance conference at Western Union on 28th of November, 2016.

The master thesis consists of three chapters. In the first section the cyber crimes concept and main types are analyzed and overview of prevention measures is provided. In the second chapter current cyber crimes trends in European Union are analyzed and compared with tendencies in the United States. In the third section results of experts' interview concerning the topic of strategies for cyber crimes preventing and handling are presented.

**Key words:** cyber crimes, cyber risk management, cyber security.

**Grigorovič V.** Kibernetiniai nusikaltimai: priežasčių ir poveikio verslo organizacijoms analizė / Magistro baigiamasis darbas. Vadovė prof. dr. V. Davidavičienė – Vilnius: Mykolo Romerio universitetas, Verslo ir medijų mokykla, 2016. – 69 p.

## SANTRAUKA

Spartus interneto vystymasis atveria naujas galimybes ne tik verslo plėtrai, bet ir sukuria palankią aplinką kibernetiniams nusikaltimams. Specialistai skaičiuoja, kad kibernetiniai nusikaltimai globaliai ekonomikai kasmet atsieina milijardus dolerių. Vis daugiau nusikaltėlių pasinaudoja tokiomis interneto savybėmis kaip greitis, lankstumas ir anonimiškumas tam, kad be ribų galėtų įvykdyti nusikalstamas veiklas ir tokiu būdu sukelti žalą pasauliniu mastu. Šiame darbe yra iškeliama problema, kad daugelis verslo organizacijų tinkamai neįvertina kibernetinių nusikaltimų keliamų grėsmių ir jų poveikio verslui. Šio tyrimo objektas – kibernetiniai nusikaltimai ir jų prevencijos priemonės, o pagrindinis darbo tikslas – išanalizuoti kibernetinių nusikaltimų priežastis ir poveikį verslo organizacijoms. Siekiant užsibrėžto tikslo, buvo iškelti tokie uždaviniai: apžvelgti pagrindines kibernetinių nusikaltimų charakteristikas (koncepciją, rūšis ir prevencijos priemones); palyginti kibernetinių nusikaltimų tendencijas ES ir JAV; atlikti kokybinį ekspertų nuomonės tyrimą, kuris padėtų nustatyti strategijas taikomas kibernetinių nusikaltimų prevencijai ir valdymui. Atliekant tyrimą buvo taikomi šie metodai: mokslinės literatūros analizė, palyginimo metodas, struktūrizuoto interviu metodas, aprašomosios statistikos ir apibendrinimo metodai.

Apibendrinus teorinės dalies aspektus bei kokybinio tyrimo rezultatus, buvo nustatytos pagrindinės grėsmės ir iššūkiai susiję su kibernetiniais nusikaltimais. Taip pat, buvo apibrėžti kibernetinės rizikos valdymo proceso trūkumai ir pateikti pasiūlymai šiems trūkumams mažinti arba šalinti. Palyginus kibernetinių nusikaltinimų situaciją ES ir JAV, buvo nustatytos panašios tendencijos abiejuose regionuose. Šio darbo rezultatai buvo pristatyti „Western Union“ organizuojamoje konferencijoje 2016 m. lapkričio 28 dieną.

Šis magistro baigiamasis darbas susideda iš trijų dalių: pirmoje dalyje pateikiama kibernetinių nusikaltimų koncepcija bei rūšys ir apžvelgiamos šių nusikaltimų prevencijos priemonės; antroje dalyje yra analizuojamos kibernetinių nusikaltimų tendencijos Europos Sąjungoje ir pateikiamas palyginimas su situacija JAV; trečioje dalyje pateikiami kokybinio tyrimo rezultatai, kurio metu buvo klausiama ekspertų nuomonės dėl strategijų taikomų verslo organizacijose kibernetinių nusikaltimų prevencijai ir valdymui.

**Raktiniai žodžiai:** kibernetiniai nusikaltimai, kibernetinės rizikos valdymas, kibernetinis saugumas.

# LIST OF ANNEXES

**Annex 1**. The questionnaire of the survey

Good afternoon.

I am Electronic Business Management, masters' degree student at Mykolas Romeris, together with Middlesex University and I conduct a research of *"Cyber crimes reasons and effects for business organizations"*.

Although cyber crime is an increasing issue for the business, many companies still lack the information and measures for evaluation and effective management of cyber crime risks. The aim of the survey is to figure out the main challenges and strategies used to manage risk associated with cyber crimes. The survey is anonymous and the data will be used in a master's thesis. Please provide the generalized experience from the experts' point of view.

Thank you in advance for the answers.

1. Please shortly describe your work experience and main responsibilities in the risk management field.
2. From your perspective, what are the most frequent cyber crimes against business companies? (please mark)
   - **a)** Cyber stalking
   - **b)** Hacking
   - **c)** Phishing
   - **d)** Online scams or fraud
   - **e)** Bot networks
   - **f)** Online trading scam
   - **g)** Social engineering attacks (e.g. CEO fraud)
   - **h)** Other (please indicate)
3. How would you describe the main threats for the companies in terms of cyber crime?
4. Please mark the factors which are strengths or weaknesses in terms of cyber risk management <u>in your current (previous) company</u> (f.e. if the company takes effective measures to educate customers in cyber security field," Customers' education" would be marked as strength). Please feel free to indicate any other factors which are not listed here.

| Factor | Strength | Weakness |
|---|---|---|
| Cyber security policies and procedures | | |
| Cyber security training programs | | |
| Qualified cyber security professionals | | |
| Active partnership with other organizations, sharing initiatives and reporting of cyber crime | | |
| Timely response to threats and attacks | | |
| Continuous risk assessment, development and implementation of cyber risk management strategy | | |
| Continuous systems testing | | |
| Customers' education | | |
| Technology security level | | |
| | | |
| | | |
| | | |

5. Please evaluate the effectiveness of the following measures in cyber crime prevention on national level as well as on company level according to the evaluation assessment scale from -2 to 2 (2 means "most effective", 1 – "effective", 0 – "neutral ", -1 – "ineffective", -2 – "most ineffective"). Please feel free to indicate any other measures which are not listed here.

| Measures on national level | -2 | -1 | 0 | 1 | 2 |
|---|---|---|---|---|---|
| Encouraging and enabling the reporting of cyber crime; | | | | | |
| Active targeting of the proceeds of cyber crime in collaboration with the financial sector; | | | | | |
| Developing insight into the behavior of the cybercriminal by means of intelligence analysis, criminological research and profiling techniques; | | | | | |
| Awareness raising on individual and corporate user responsibility; | | | | | |
| Sharing the best practice. | | | | | |

| **Measures on company level** | **-2** | **-1** | **0** | **1** | **2** |
|---|---|---|---|---|---|
| Establish the cyber security policies and procedures, which include guidelines for investigation of and recovery from cybercrimes after they occur; | | | | | |
| Implement training programs and disseminate the information on latest threats within the organization; | | | | | |
| Maintain multiple intrusion detection technology | | | | | |
| Investments into qualified cyber security professionals; | | | | | |
| Active partnership with other organizations, sharing initiatives and reporting of cyber crime; | | | | | |
| Timely and cooperative response to threats and attacks; | | | | | |
| Demonstrating an appropriate standard of diligence to auditors, regulators and stakeholders, which should reduce business exposure to regulatory or legal sanctions; | | | | | |
| Continuous risk assessment, development and implementation of risk management strategy in terms of cyber security; | | | | | |
| Continuous systems testing which encompasses the resistance to threats and ability to minimise and mitigate the damage caused by successful attacks; | | | | | |
| Educating and encouraging customers and suppliers to improve their own cyber security. | | | | | |

6. What are the main reasons, from your perspective, why some companies still do not focus enough on cyber crimes risks?
7. The National Institute of Standards and Technology (NIST) provided the Framework, which is a voluntary risk-based compilation of guidelines that aims to help organizations identify, implement, and improve their practises (see Figure 1). Do you recommend for business organizations to use this model? Would you suggest any additional or totally different steps for the cyber risk evaluation and management framework?

| Functions | Definition | Categories |
|---|---|---|
| Identify | An understanding of how to manage cybersecurity risks to systems, assets, data, and capabilities | Asset management, business environment, governance, risk assessment, risk management strategy |
| Protect | The controls and safeguards necessary to protect or deter cybersecurity threats | Access control, awareness and training, data security, data protection processes, maintenance, protective technologies |
| Detect | Continuous monitoring to provide proactive and real-time alerts of cybersecurity-related events | Anomalies and events, continuous monitoring, detection processes |
| Respond | Incident-response activities | Response planning, communications, analysis, mitigation, improvements |
| Recover | Business continuity plans to maintain resilience and recover capabilities after a cyber breach | Recovery planning, improvements, communications |

**Figure 1.** Core functions of effective cyber security

8. What development areas do you see on legal regulation side? What can be improved from law enforcement perspective in fight against cyber crimes?
9. Does a company you are working in cooperate with other organizations in sharing best practices or other information related to cyber crimes? If yes, please select the units you are in partnership with:
   a) Law enforcement institutions;
   b) Financial institutions;
   c) Consumers;
   d) Companies from the same sector;
   e) Other (please indicate)
   f) No, we do not share any information.
10. Does the company you work for uses any external guidelines for cyber risk management (f.e. NIST, OECD and etc.). If yes, can please provide the names of external sources.
11. During your work experience have you faced any cyber attack against the company? If yes, could you please provide the following information:

| Question | Answer |
|---|---|
| a) Type of cyber crime | |
| b) Damage for the company (please select) | - Reputational<br>- Financial<br>- Business processes restriction<br>- Loss of market value<br>- Loss of market value of consumer's trust<br>- Other (please indicate) |
| c) Main measures which solved the issues | |
| d) Lessons learned | |

**Annex 2**. Logical structure of the questionnaire