ECONOMIC THEMES (2019) 57(3): 351-364

DOI 10.2478/ethemes-2019-0020

INSTITUTIONAL MEASURES FOR INCREASING THE CYBER SECURITY FOR BUSINESS IN THE EUROPEAN UNION

Petar Čelik

Higher Educational Institution for Applied Studies for Entrepreneurship, Belgrade, Republic of Serbia

✉ *petarcelik@sbb.rs*

UDC
004.056.5
004:343.533

Review paper

Abstract: Numerous research and analytical studies envisage a new wave of disruptive innovations that will completely change the economic landscape, organization and business models in the short term, as well as ways of managing companies. This wave of innovation, followed by the use of new digital technologies, such as Big Data, mobile applications, social networking, robotics, 3D printing, nanotechnology, quantum informatics, cloud computing, etc., through various forms and modes of cyber vulnerability, contribute to reducing the ability to achieve effective protection, not only for companies and public services, but also for other services available to citizens. The current research preoccupation is focused on finding adequate solutions, in terms of protecting the digital economy and digital business from all modern threats and risks that the modern disruptive technologies carry along with. The thematic focus is on strengthening the institutional and operational capacities of existing and newly-formed specialized agencies, such as: ENISA, EC3 and EUROPOL, in order to provide an integrated institutional response to a wide range of hybrid and cyber threats. The final section of the paper presents an overview of comprehensive strategic, regulatory and institutional approach of the EU to cyber incidents and crises in the digital space.

Received: 08.05.2019
Accepted: 24.10.2019

Keywords: disruptive technologies, innovation, cyber security, incidents, crises, EU, agencies

JEL classification: D80, O34, O52

1. Introduction

The strategic environment of the EU in recent years is rapidly changing, due to global changes and the effects of various factors. The high intensity of changes, a wide range of accompanying and appearance forms and modalities greatly complicate the assessment of current and future trends. One of the most important

factors that generates the existing turbulent environment is the exponential growth of the use of digital technologies that enter all the spheres of social, business, public and private life. The second generation of digital technology, the so-called Industry 4.0, completely changes, not just the way businesses operate, or the work of public services, but the overall matrix of work, both of individuals and institutions and their interest organizations.

The use of modern disruptive technologies, at local, regional and global level, constantly generates new forms of abuse within the application of modern digital technologies, in all sectors of human activity and work. According to Eurostat data, based on Europol's analysis and statistics, cyber-attacks, incidents and cyber crises of wider scale are becoming numerous and more frequent, while from the aspect of prevention and digital forensics, these forms of endangerment, in addition to bearing the element of cross-bordering, are more difficult to discover and prevent in a timely manner, regardless of the available tools, techniques, instruments, strategies and operational procedures, which requires a systemic response created through the innovation of existing agendas (Europol Review, 2016, page 36).

Official reports of EU institutions and analytical and expert services show an increase in theft of business secrets, business information and personal data. In addition, incidents in cyberspace often cause the disrupted services, complicating the functioning of certain sectors of the infrastructure, resulting in significant economic losses in hundreds billions of dollars a year, in the form of direct and indirect damages and consequences, along with the disruption and discredit of the trust of citizens and businesses in the digital society. According to official statistics, cybercrime causes a loss of billions of euros a year in the EU, while the proliferation of various cyber threats requires additional financial investment in new cyber responses, i.e. mechanisms of cyber protection. (Special Eurobarometer 464a, 2017, p. 3)

Official statistics clearly show the trend that cybercrime in the EU, as well as in the surrounding countries, has a steady growth both in terms of volume and financial effect; however, it is difficult to give precise information considering this issue, since there are no relevant indicators of the overall state at the EU level. In fact, there are no fully standardized ways of collecting such statistics, so cyber-related incidents are often classified differently.

Currently, the most accurate data and analyses related to this issue keeps the European Center for Cybercrime, more commonly known as EC3, which operates within EUROPOL. Due to the aforementioned threats and risks to infrastructure, the financial sector, various economic sectors, as well as the freedom and rights of citizens, the European Union has intensified activities to reduce vulnerability from misuse of technological solutions and applications over recent years, and has increased the resistance to cyber-attacks through building and improving cyber

security models and systems, both at the national level of the Member States themselves and the supranational level of the Union. In this context, special attention is paid to detailed legal regulation of this issue, and then to the development and strengthening of, first of all, institutional, and then operational and organizational capacities of specialized agencies and professional services dealing with the protection of citizens' rights and freedoms, as well as economy and public administration in cyberspace, especially in the field of prevention and suppression of cyber incidents and crises.

2. Physiognomy and performance of cyber attacks

According to the findings of the Global Forensic Data Analyses Survey for 2016, done by Ernest & Young consulting, cyber risks and internal threats that involve theft, manipulation or data destruction, are the fastest growing business risks and major drivers of significant investments in forensic data analysis. This research has shown that companies, along with growing risks in different sectors and globally, increasingly use advanced forensic analysis in risk management and fraud-related cyber-attacks. In concluding the study, the authors suggest widespread use of forensic data analysis, which makes it an indispensable part of the proactive approach to risk management, in addition to strengthening corporate and general technological culture. (Ernst & Young, 2016)

Despite numerous and diverse regulatory interventions, conceptually strategic frameworks and certain positive results, the EU remains extremely sensitive to cyber-attacks and threats. According to the European Commission, attacks and incidents that occur in cyberspace can disrupt the unique digital market, and hence the economic and social life of the EU as a whole. Cyber-attacks in the event of the application of hybrid threats can be coordinated, linked and networked with other activities that have a subversive character, in order to destabilize the state or block political institutions. (COM 410 final, 2016, p. 2). The situation is similar in other regions of the world.

According to the latest Allianz risk barometer for 2019, in addition to the standstill in business, the leading risk for companies are cyber incidents. Statistically, 37% of respondents believe that cyber incidents are the main global business risk, as well as business congestion. The cybercrime losses, according to this survey, are drastically increasing and amount to about $ 600 billion a year, which is a significant increase from the $ 445 billion recorded in 2014. (Allianz Risk Barometer 2019, p. 9)

Table 1: The five biggest risks for small businesses with trends (<250m EUR of annual revenue)

Br.		%	2018	Trend
1.	Cyber incidents (e.g. cybercrime, IT failure / obsolescence, data breaches, penalties and offenses)	32%	2 (30%)	↑
2.	Changes in legislation and regulations (e.g. trade and tariff war, economic sanctions, anti-racism, Brexit, Euro Zone disintegration)	30 %	5 (22%)	↑
3.	Natural disasters (e.g. storms, floods, earthquakes)	27 %	3 (28%)	=
4.	Market development (e.g. volatility, intense competition / new market entry, mergers and acquisitions, market fluctuations	27 %	4 (27%)	=
5.	Business interruption (including supply chain disruption)	26 %	1 (33%)	↓

Source: Allianz Risk Barometer 2019, p. 22

Regarding the previous analysis, it is important to highlight the great concern of SMEs regarding cyber-attacks and data abuse, bearing in mind that this type of company has no strong and capable organization to respond adequately to, unlike big companies. This situation is confirmed by Volker Muench, Global Practice Leader, Utilities & Services, IT Communication, AGCS who points out that many small and medium enterprises have had data protection problems in the past period, but they have not always reported it to the authorities because of the fear of losing their market confidence and reputation, and therefore a possible loss of contract with clients. From the available data in the conducted research, a clear link can be established between the cyber business and the loss of market reputation, especially in this segment of economy.

Regarding the growing risks, companies with a high degree of digitized business must plan a large number of scenarios, which means identifying the reasons that distort the business, because they are the most vulnerable in today's networked society. Risks that distort business, or disruptive risks, can be physical, such as natural disasters, wars, etc., but also virtual with clear physical consequences as an interruption in the functioning of information systems, which can, again, be malicious or accidental.

Table 2: Causes of business interruption that most often raise fear for companies

Cyber incidents	Fire, Explosions	Natural Catastrophe	Suppliers and Business Processes Breakdown	Machine Breakdown
50%	40%	38%	28%	28%

Source: Allianz Risk Barometer 2019, p. 10

Breakdowns and losses of business (and processes) caused by these factors are becoming more and more complex, given the fact that supply chains are increasingly reliant on a larger number of smaller suppliers, especially when it comes to the industrial sector (automotive, electronics and pharmaceutical). Even an event like fire, in one of these industries could lead to serious losses due to the lack of built-in parts, according to Volker Muench, Global Practice Leader, Utilities & Services, IT Communication, AGCS.

In the previous period, we have seen serious losses from such events in the insurance sector. These losses exceed 1 billion euros ($ 1.1bn). With only one blaze, the entire factory can disappear, the entire production stops, causing the losses in the supply chain. Even the failure of the machines in production can have a similar effect.

Considering the vulnerability of digital business, one must bear in mind the circumstance that these risks may arise from their own business, but also from the business of suppliers, customers or suppliers of information services and resources. For these reasons, the company's management has the obligation to continuously monitor and analyze the situation in the cyber environment and, according to its needs and capabilities, (pre)assess the level of company vulnerability and then the level of necessary financial and other investments, in order to develop and improve preventive programs and profiling protection-operational responses. Modern approaches and solutions in the field of risk management, analytical tools, appropriate methodologies, procedures and innovative partnerships can significantly contribute to better understanding, mitigation and depreciation of the consequences of modern cyber-incidents and crises, and the reduction of losses thus generated. The practice has repeatedly confirmed that cyber risks and the risks of business downtime are interconnected and conditioned and that there is a high level of correlation between them. In fact, attacks by blackmail software (Ransomware) or accidental interruptions in the operation of information systems often lead to general business disturbances at the service bar, which creates large financial losses, whose amplitude varies widely between companies and sectors, depending on their degree of digitization.

3. Types and characteristics of cyber threats

However, in academic-professional circles, reference institutions and established publications, which in a narrower sense are specialized in dealing with cyber security issues, different, non-compliant typologies and classifications of cyber threats and risks (that have not become part of the EU acquis) can be found.

In addition to classic forms of cyber threats, (cybercrime, cyber terrorism, cyber spyware, cyber sabotage, cyber activism, etc.), experts in this field have started including new threats in the form of "Zero Day" threats, recycled threats, threats in the form of modification of existing code, combination of malware and social engineering, phishing attacks for theft of credentials, threats from social networks, advanced persistent threats, etc.

On this occasion, David Stupples, a professor from London City University and monitoring expert of virus insertion into software solutions, points out that the potential of all stakeholders in the field is very large, which in return calls for the need to develop and improve models for more efficient cyber defense and online counter attacks. (Stupples. D; 2015)

During a congressional hearing in 2014, former director of the US National Security Agency, Mike Rogers, pointed out that cyber warfare and threats that take place in cyberspace are everyday occurrences and that they can be easily recognized in the case of the Ukrainian and Syrian crisis. In addition, extensive activities are being intensively undertaken by all regional and global actors to strengthen their offensive and defensive components, which represent an extremely high risk, due to the existence of diametrically opposed strategic (and other) interests at the global level.

Serious security issues arise when cyber-attacks destroy or steal large databases and programs, as happened to the American company "Sony Pictures", or many other international companies, due to cyber-attacks by unknown players from an unknown location. The attacks of this type and of such proportions can endanger not only the lives and assets of companies and citizens, but also numerous critical infrastructures, such as nuclear and classical energy facilities, and cause disruptions in air, maritime, road and rail transport.

The availability of these infrastructures to malicious cyber groups and terrorist organizations is conditioned by their Internet connectivity at the national and global level, the international market for software and hardware traffic, where all stakeholders and subjects can easily and cheaply, but also at the expense of the victim, come up with an opportunity to bring on enormous damage and consequences, even those of a wider scale, despite a very small chance that they will be discovered and legally sanctioned, owing to the aforementioned legal voids and inconsistencies.

Analyst at London's Strategic Dialogue Institute, Rachel Briggs, warns that there is a real danger that terrorist groups, due to general availability of technological goods and services, as well as financial resources, will establish capacities and master the knowledge and techniques needed to run cyber or information warfare against anybody, regardless of its development. (Voice of America, 2015).

In its annual report, the European Network and Data Security Agency (ENISA) points out that most cyber-incidents are not reported nor disclosed for various reasons. Co-authors of this report warn that cyber incidents are usually the strictly guarded secret that leaves users, employers and lawmakers in the dark, regarding their frequency and the impact and causes of such a phenomenon. (ENISA; 2012) Deeper research in this field should show whether the source of insecurity is poor or insufficient protection of information systems or a human factor.

According to Verizon's report on personal data breach investigation for 2013, a total of 47,000 cyber incidents were reported and 621 incursions into databases, where at least 44 million documents were stolen (Constantin, L. Verizon, One in five data breaches are the result of cyber espionage, PC World, 2013).

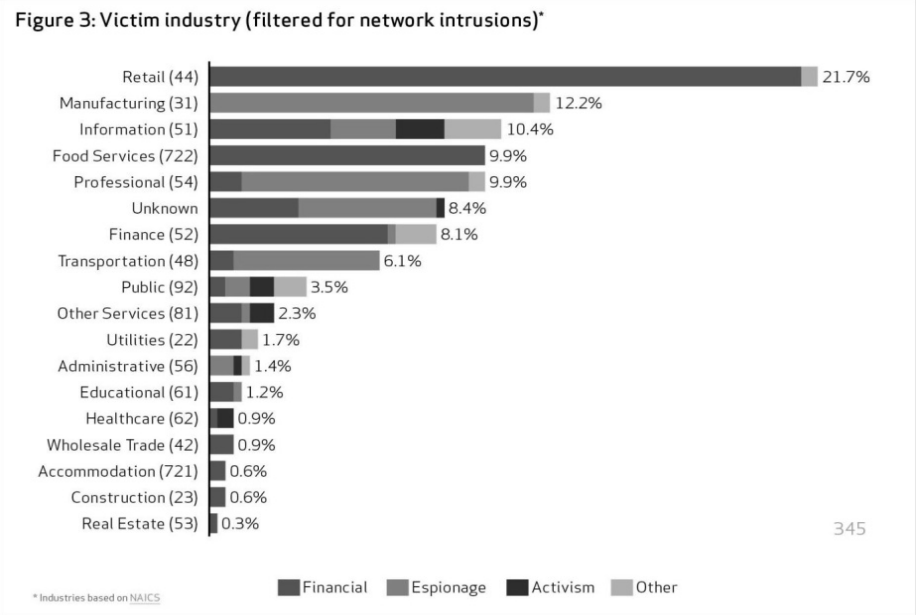
The state and development of cyber security, geopolitics and its trends have great significance and influence. Much attention has been paid in this regard to a study developed by McAfee and the Center for Strategic International Studies in the United States, which claims that cybercrime globally takes about $ 600 billion a year, with the figure rising due to increasing capabilities of hackers and the rise in the application and growth the crypto currencies' value. The study cites the epicenter of cybercrime in countries such as Russia, Vietnam, Brazil, India and North Korea, which are supposedly the most significant attackers against financial institutions, while China is the most active in cyber-spyware. (McAfee, 2014)

The so-called ransomware virus, which locks computers and their content and seeks redemption to unlock them, is on the list of the fastest-growing attacks, primarily due to the spread of real online stores offering pirated services. Hackers mostly use the same tools for data theft, identity, bank hacking or other offenses, relying on Bit Coin or other crypto currencies to remain anonymous in these financial transactions. The US administration recently reported that cybercrime in 2016 cost the United States between $ 57 billion and $ 109 billion, depending on direct or indirect costs and damages incurred.

In public debates and scientific discussions, there is a growing demand for the redefinition of cyber security policy and strategy, which in itself pulls or requires redesign of the existing cyber response model. However, in addition to improvement of the overall strategy and other security agenda, great attention is paid to the protective technological solutions that must keep up with the development of modern technological innovations and trends. If security incidents are inevitable, the consequences of cyber-attacks are certainly not. Namely, cyber

incursions are often the result of a lack of cyber readiness, early detection or timely response, in short, a lack of proactive measures. Analysts of the Verizon RISK team have come up with interesting information that even 95% of cyber spyware originates from China and that there is a whole hacker industry in this area (Figure 2).

Figure 2. Industrial branches - Victims of attack



Source: Constantin, L. Verizon, One in five data breaches are the result of cyber espionage, PC World, 2013

4. Regulatory scope of protection against cyber incidents in the EU

In order to bring closer and equate the criminal law of Member States in the area of attacks on information and communication systems, the European Parliament and the Council of the EU adopted a directive on attacks on information systems in early August 2013, which greatly facilitated not only cooperation between competent authorities, but also increased the capacity to react to such threats and risks. (Official Journal of the EU, L 218/8, 2013)

The establishment of minimum rules in this area is a starting point for numerous state authorities and specialized law enforcement agencies of Member States, as well as specialized EU-level agencies, such as EUROJUST, EUROPOL and its European Cybercrime Center, as well as the European Security Agency networks and data of ENISA.

The Directive clearly specifies activities that are identified as illegal access to the information system or some of its work, which are sanctioned by national legislation. In particular, criminal offenses that constitute unlawful interference with the system, through the entry, transmission, damage, deletion, destruction, alteration or concealment of computer data or the disabling of access to such data, are specially cited, with a reference to the prescribed sanctions for their perpetrators.

At the same time, Article 10 prescribes the responsibility of legal entities, if they in any way allowed the performance of any of these actions, while Article 11 prescribes a sanction for legal entities. The Directive, however, does not provide a typology of cyber-attacks on information systems, which in the criminal-legal sense and on the operational plan, represents a major disadvantage.

5. Reform of the cyber security regulatory framework in the EU

Along with the increase in the level and scope of digitization that has penetrated into all sectors of public life and socio-economic areas in recent years, the level of their cyber vulnerability is growing due to the exponential development of disruptive technologies and innovations on the one hand, and the increase in the vulnerability of these sectors and areas on the other.

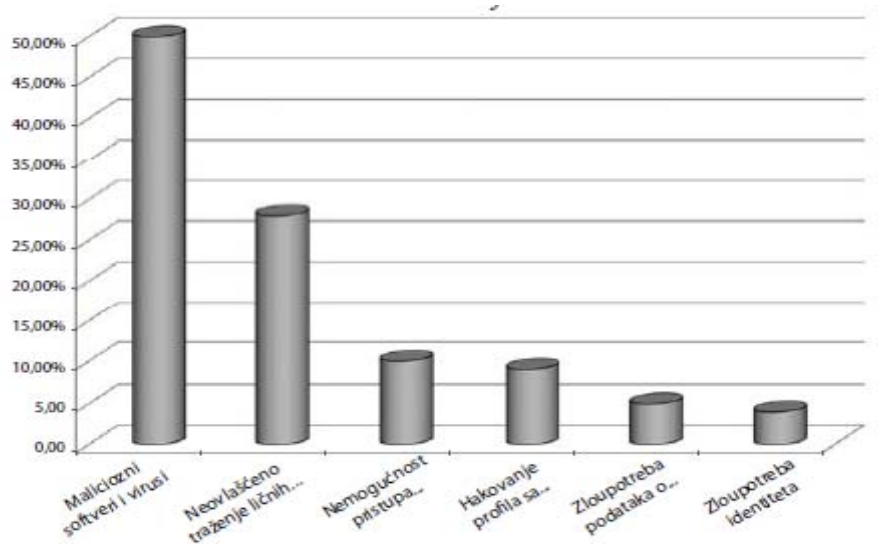
Numerous cyber-related incidents, such as theft of business secrets, business information, personal data, service disruption, and critical infrastructure sector troubles, almost daily cause economic losses that cost hundreds of billions of euros a year, as well as violating the trust of citizens and businesses in digital society and economy. In time, cyber incidents are increasing their frequency and impact, and from this aspect, they represent a great threat and risk in the operating of the network and information systems. Such incidents, if they have elements of intent to cause harmful consequences, "can endanger" the performance of economic activities, impair the trust of the users and, thereby, inflict enormous damage on the economy of the Union. (EU Directive 1148/2016, p.1)

From the above, it appears that cyber-crime in the EU is actually a crime without borders, which consists of criminal acts that involve attacks on information systems, in sense of interfering or disabling their functioning, and the various forms of online fraud and forgery, such as identity theft and malicious code, and the dissemination of illegal online content, such as child pornography etc. According to a Eurobarometer survey of June 2017, it is estimated that the cybercrime causes more than € 1 billion loss a year to the EU, with a remark that this drastically increases the pressure on the ability of police agencies to react due to additional engagement, unplanned resource spending, shifting focus, activity focus and other operational and organizational challenges, especially in the field of managing technical and human resources. (Special Eurobarometer 464a, 2017, p.5)

In order to review the state of cyber security, as well as the degree of cyber-crime towards EU citizens, a survey was conducted on behalf of the Directorate-General for Internal Affairs in 2014, on a sample of 27,868 respondents from different social and demographic groups. (Baltazarević, V. 2016: 244)

According to the research conducted, 79% of the citizens of Europe use the internet, 98% of the youngest age group use the Internet, as well as 91% of managers and 85% of administrative workers. The exposure to various forms of online crime is shown n Figure 3.

Figure 3: Exposure to various forms of online crime



Source: European Commission, Special Eurobarometer 423 Cyber security. Brussels. 2015

Despite all the positive results and efforts, the EU remains extremely vulnerable to cyber incidents and the cyber crisis. In the case of large-scale incidents and crises, this, according to the documents of the European Commission, could directly disrupt the functioning of a single digital market, indirectly both social and economic life as a whole.

In order to formalize a common, integrated and systemic response to rising cyber challenges, the EU has defined the approach in 2013 through coordinated policy on the adequate way of preventing and responding to cyber threats and attacks in the form of incidents and widespread crises.

As a result of this new approach in 2013, the European Parliament adopted the EU's cyber security strategy that sets out plans to address challenges in five priority areas:

- Achieving cyber resistance
- A drastic reduction in cyber crime
- Policy and capacity development for cyber defense
- Developing industrial and technological resources for cyber security and
- Establishing a coherent international cyber space policy for the EU

That same year, on August 12, the European Parliament and the EU Council adopted the Directive on attacks on information systems that set out minimum rules on the definition of criminal offenses and sanctions in the area of attacks on information systems. In addition, the competencies of the Member States to enforce the provisions of this Directive, as well as the ways of exchanging information between national police and judicial authorities in the EU area, are prescribed. By adopting this regulation, the process of comprehensive reform and completion of the regulatory framework in the field of cyber security in the EU area has begun.

During 2014 and 2015, the EU institutions, and above all, the European Commission (General Directorate for Migration and Home Affairs and the Communications Directorate), the EU Council, the European Economic and Social Committee and other EU expert bodies, conducted the strengthening of cyber security at the EU level, which implied the formation of new institutions within the Member States, as well as their networking at the supra-level. Among other things, an activity has been launched to establish special bodies for cyber security at the EU level, as well as develop programs for educating and informing citizens and businesses about this activity, and ultimately legally determining the company's obligations, in terms of developing a proactive approach to protecting against cyber-attacks, which implies safe and resistant information and communication technology and the ways of its application.

The key document marking a milestone in the legal regulation of this issue is the European Parliament and the Council Directive on the measures for a high level of common security of the network and information systems across the Union (L 194/1, 2016)

This document sets out the obligations of the member states to adopt national strategies for the security of the network and information systems, to establish an institutional body to support and facilitate strategic cooperation and information exchange among member states, i.e. form networks of teams ("the CSIRT network") to respond to computer-security incidents. The significance of cyber security for the future of the EU is best illustrated by the position expressed in the EU's Global Strategy for Foreign and Security Policy (2017), that EU security in the future depends on adapting and strengthening its ability to protect against cyber threats, while civil and military infrastructure also depend on the security of digital systems. Bearing in mind those facts, the European Commission, in cooperation with the High Representative of the Union for Foreign Affairs and Security Policy, adopted a joint document titled: Resistance, deterrence and defense: Strengthening the cyber security of the EU. (JOIN, 450 final, 2017)

The main purpose and goal of adopting this document is to ensure greater resilience, strategic independence and the EU's ability to develop and apply technologies and skills to enhance cyber security. To strengthen cyber resistance, a common and comprehensive approach is required, as alleged. In practice, this implies more robust and more efficient structures for the development of cyber security and a more effective response to cyber-attacks in Member States, but also in EU institutions and agencies. In this regard, the key priority of the reform of the legislative and institutional framework, in the field of cyber security, is the institutional strengthening of the EU Agency for Network and Information Security "ENISA", "EUROPOL", the Center for Cybercrime (EC3), the Intelligence Analysis Center "INTCEN", "CERT" teams at the level of the EU and the Member States themselves.

In order to establish the EU's resilience to cyber-attacks, and as a single market in the cyber security field, it is necessary that all relevant actors, that is, state bodies, economic operators, owners and operators of network infrastructure, focus all their activities on the next three priority areas:

- Security in key or high-risk areas, i.e. systems.
- Cyber security in digital products, networks, systems and services of wide use in the private and public sector for the purpose of defense and protection against attacks and implementation of regulatory obligations, e.g. e-mail encryption, firewall protection, and virtual private networks.
- Using "integrated security" methods in affordable, digital, interconnected broadband devices that make up the Internet of Things.

In the opinion of the EU institutions, the strongest instrument or risk-control tool in cyber security is a need for the introduction of stricter standards. In this regard, the Network and Information System Security Directive, better known as the "NIS" Directive, is the first legislative act in the field of cyber security that applies throughout the EU. The main objective of this act is to "increase resistance by improving national cyber security capabilities, strengthening the cooperation among Member States, and requiring companies in effective economic sectors to introduce effective practices and risk management rules, as well as to report serious incidents in cyberspace to competent national bodies. These obligations apply to three types of key Internet service providers: cloud computing, browser and internet markets. "(JOIN 450, final 2017)

Conclusion

Newer surveys in Member States or at the EU level, as well as numerous estimates of reference institutions, such as EUROPOL, ENISA, EUROBAROMETER and EUROSTAT, clearly show that cybercrime and fierce competition are the biggest threats to companies and public services. In the context of the above, a more subtle analytical explanation of both the current state and the trends started generating

two key reasons for the existing concern of cyber security. Namely, the causes of the current situation in cyberspace should be sought in a low level of awareness of the dangers and risks of cyber-attacks, both among decision makers, business users and public administrations, while IT security investments are still insufficient and often at the bottom the scale of priorities. Confronted with this challenge, the EU has recognized the need to strengthen the resilience of the EU's system and structure – to strengthen cyber culture and security through continuous innovation and adjustment of the regulatory framework. The improvement of institutional capacities at the Union level as a whole and the level of member states, and continuous monitoring, evaluation and control of organizational and operational responses to cyber challenges is also important. And finally, to establish a balance between available opportunities and the capacity for proactive performance on the one hand, and dynamic, complex and hard-to-predict cyber threats and risks, in the first place of their consequences and effects, on the other.

Since cybercrime, statistically, constantly and exponentially increases both in scope and financial impact, cyber security in the EU becomes extremely complex, organizationally, technically and financially very demanding, operatively diluted and structured, horizontally and vertically cross-linked, with a low level of manageability expressed, which also represents its weakest link in this security chain.

References

Baltezarević. V., Baltezarević. R. (2017) Zaštita privatnosti na internetu - Evropski model, *Megatrend revija*, Vol. 14, No 1. Beograd.

Constantin. L. (2013). Verizon: One in five data breaches are the result of cyberespionage, *PCWorld,* Preuzeto sa: https://www.pcworld.com/article/2036177/one-in-five-data-breaches-are-the-result-of-cyberespionage-verizon-says.html

Cyber Europe 2018: After action report, ENISA (2018), Grčka.

Definition of cyber security, Gaps and overlaps in standardisation, ENISA (2015), Grčka.

Direktiva EU 1148 (2016) *Službeni list EU*, L 194/1, Brisel.

Ernst & Young Global. (2016) Path to cyber resilience: Sense, resist, react, *EY's 19th Global Information Security Survey 2016-17*.

European Commission. (2017) Special Eurobarometer 464, *A Cyber Security*, Brisel.

Izveštaj Komisije o oceni Agencije Evropske unije za mrežnu i informacionu bezbednost, ENISA, (2017). Evropska komisija COM 478 final, Brisel.

Jačanje evropskog sistema sajber bezbednosti i podsticanje konkuretne i inovativne industrije sajber bezbednosti, Evropska komisija, (2016), COM 410 final, Brisel.

Neto gubici: procena troškova sajber kriminala na svetskom nivou, (2014), McAfee, Centar za strateške i međunarodne studije, Washington, D.C.

New Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. (2014). Washington, D.C., Center for Strategic and International studies.

Olmstead. K., Smith. A., (2017) *Americans and Cybersecurity*, Pew Research Center, Washington, D.C., Preuzeto sa http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

Otpornost, odvraćanje i odbrana: jačanje sajber bezbednosti EU, (2017). Evropska komisija, *JOIN 450 Final*, Brisel.

Reinforcing trust and security in the area of electronic communications and online services, ENISA, (2018) ISBN 978-92-9204-284-4, DOI 10.2824/015812, Grčka.

Rezolucija Evropskog parlamenta o borbi protiv sajber kriminala, *Službeni list EU*, C 346/29, 27.09.2018., Brisel.

Stupples. D. (2015). *Are we prepared for information warfare?*, University of London, London.

Threat landscape report 2017, 15 top cyber-threats and trends, ENISA (2018), Grčka.

Uredba EU o Agenciji Evropske unije za saradnju tela za izvršavanje zakonodavstva (EUROPOL), (2016) *Službeni list EU*, L 135/53, Brisel.

INSTITUCIONALNE MERE ZA POVEĆANJE SAJBER SIGURNOSTI POSLOVANJA U EVROPSKOJ UNIJI

Apstrakt: Brojna istraživanja i analitičke studije predviđaju novi talas razornih inovacija, koje će u kratkom roku potpuno promijeniti ekonomski krajolik, organizaciju i poslovne modele, kao i načine upravljanja kompanijama. Ovaj talas inovacija, praćen upotrebom novih digitalnih tehnologija, kao što su Big Data, mobilne aplikacije, društveno umrežavanje, robotika, 3D štampanje, nanotehnologija, kvantna informatika, *cloud computing*, itd. doprinosi smanjenju sposobnosti za postizanje efikasne zaštite, ne samo kompanija i javnih službi, već i drugih usluga koje su dostupne građanima. Sadašnja preokupacija istraživanja usmjerena je na pronalaženje adekvatnih rješenja, u smislu zaštite digitalne ekonomije i digitalnog poslovanja od svih modernih prijetnji i rizika koje moderne disruptivne tehnologije nose sa sobom. Tematski fokus je na jačanju institucionalnih i operativnih kapaciteta postojećih i novoformiranih specijalizovanih agencija, kao što su: ENISA, EC3 i EUROPOL, kako bi se osigurao integrisani institucionalni odgovor na širok spektar hibridnih i sajber prijetnji. U završnom delu rada, u vidu pregleda, daje se sveobuhvatan strateški, regulatorni i institucionalni pristup EU sajber incidentima i krizama u digitalnom prostoru.

Ključne reči: disruptivne tehnologije, inovacije, sajber bezbednost, incidenti, krize, EU, agencije