Cyber Security Challenges in Digital Economy

Mario Spremić, *Member, IAENG*, Alen Šimunic

***Abstract*—In recent decades the nature of IT security incidents have changed, from isolated attacks on information systems to intentional, targeted and sophisticated cyber threats at individual, institutional or even national level. Interconnected capabilities of digital technologies bring many benefits, but also introduce a host of new vulnerabilities with far reaching implications. Even so it is common to use both terms interchangeably, cyber security differ from information security. In this paper we discussed about the shift from information to cyber security, mainly as the change of paradigm in protection from ongoing attacks. While in information security era it was enough to conduct basic protection from 'common' attacks, in cyber security era organisations need to implement smart, innovative and efficient controls to detect and prevent advanced and emerging cyber attacks. Cyber security activities should no longer be solely the responsibility of IT departments or assigned individuals (CISOs or similar), but institution-wide efforts with all employees engaged. As digital technologies are strategically aligned with business strategy, the same should be done with cyber security. We have conducted a preliminary research on how mature are security controls in large companies in Croatia related to important or critical national infrastructure. We came out to conclusion that basic protection is efficient, but there are still rooms for improvements in taking a collective ambition towards holistic cyber security governance and applying more advanced controls.**

***Index Terms*— cyber security, basic and advanced cyber threats, digital transformation, preliminary research, important or critical national infrastructure**

I. Introduction

COINED by visionary researcher Don Tapscott in 1995 in a book called "The Digital Economy: Promise and Peril in the Age of Networked Intelligence", digital economy refers to new business models, markets, goods and services, especially those based on digital technologies as a basic business infrastructure [21]. The concept of digital economy is based on integration and simultaneous application of different, independently developed and ready-to-use digital technologies. Bharadway [3] define digital technologies as combinations of information, computing, communication, and connectivity technologies and argue that exponential advancements in price/performance capability of computing, storage, bandwidth, and software applications are driving the next generation of digital technologies to be delivered through cloud computing.

If aligned with strategic objectives and used simultaneously, different, independently developed and ready-to-use digital technologies - such as cloud computing, mobile technology, sensors, Internet of Things (IoT), big data, cognitive technologies (AI), augmented reality (AR), robotics, addictive manufacturing (3D printing), drones and others - have the ability to extract information form physical devices (data on sensors about condition of physical device), disseminate it quickly (using mobile technologies), store it on cloud, analyse it instantly (using big data and advanced analytics), thus, integrating products, services and processes, and making disrupting impact on established business models [19].

While information technology (IT) initiatives are more internally focused, mainly with the objective of aligning with current business process, digital technologies are externally oriented, connecting devices, enabling excellent digital services and enhanced customer experience. Digital transformation has become high priority on leadership agendas and recent researches (Bonnet et.al. [4]) illustrates that nearly 90% of business leaders in the U.S. and U.K. expect IT and digital technologies to make an increasing strategic contribution to their overall business in the coming decade. On the other hand, these initiatives will expose them to wide range of new risks - cyber security risks. As companies are increasingly using novel digital technologies to foster innovation, the nature of IT security incidents is changing and prevailing to more externally oriented and sophisticated threats (cyber incidents).

Although, characteristics of information system (IS) security incidents and associated risks have dramatically changed in recent decades, it seems that IS and underlying IT and digital technologies are still mistakenly regarded as a separate organization of the business and thus a separate risk, control and security environment. While since 10 or 15 years ago an IS security incident could cause minor 'technical' problems, today we are faced with wide range of advanced, intentional cyber attacks that may cause massive incidents, large direct and indirect costs and affect corporation's competitive position and strategic goals [20]. PricewaterhouseCoopers survey [16] showed that companies that experienced cyber security related incidents lost an average of 2.1% of its value with an average loss of over 1.6 billion USD per incident. In addition to impact on companies, due to interconnectivity of digital technologies, cyber security incidents can have very negative impact on individuals (phishing attacks, identity theft) and at national and state level (state-sponsored attacks, organize crime groups, exploiting vulnerabilities on 'smart' devices to gain access to data, control systems, or critical national infrastructure), which was not so likely to happen some 15 years ago, in so called 'information security' era.

F. A. Mario Spremic is full professor at Faculty of Economics and Business Zagreb, Department of Informatics, University of Zagreb, Kennedy's sq 6, 10000 Zagreb. CROATIA (e-mail: mspremic@efzg.hr)

Alen Simunic is student at Faculty of Economics and Business Zagreb, Department of Informatics, University of Zagreb, Kennedy's sq 6, 10000 Zagreb. CROATIA (e-mail: asimunic2@net.efzg.hr)

World Economic Forum [25] recently rates a large-scale breach of cyber security as one of the five most serious risks facing the world today. It is estimated [6] that the scale of the threat is expanding drastically: by 2021, the global cost of cyber security breaches will reach US$6 trillion by some estimates, double the total for 2015.

In this paper we will give an overview of changing nature of security incidents, prevailing from 'internal' IT mode (‘common’ attacks and IT incidents) to 'externally' oriented digital environment (advanced and emerging cyber attacks). We will explain the differences between information security and cyber security and discuss about how to protect from ongoing cyber threats. As cyber incidents are targeted, sophisticated and difficult to detect and prevent, we need more holistic approach in governing them [20]. The main objective in managing cyber security is to carefully design and implement basic protection to prevent common attacks, but also, innovative, smart and sophisticated security controls to detect and respond to advanced and emerging threats. In order to evaluate the efficiency of these controls, we will conduct a preliminary research on a sample of large companies in Croatia. Even the sample is small (nine large organisations), we used it for the preliminary research, as they represent companies related to important or critical national infrastructure, employing on average 2.707 people, and having an average income over 260 million EUR. In our research we have combined survey questionnaire and structured in-depth interviews with the experts responsible for information / cyber security.

II. INFORMATION SECURITY VS CYBER SECURITY

Interconnected nature of many digital technologies and important or critical infrastructure systems has introduced a host of new vulnerabilities with far-reaching implications. Even so it is common to use both terms interchangeably, cyber security is a part of information security, as term 'cyber' is often use too broadly, mainly due to the increasingly complex nature of information in the digital age [13]. In practice, cyber security addresses primarily those types of attack, breach or incident that are targeted, sophisticated and difficult to detect or manage. Contrary to information security, cyber security is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace [26]. ISACA [13] defined cyber security as the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems. The main focus of cyber security is related to designing and implementing effective controls which will help protect enterprises and individuals from intentional attacks, breaches, incidents and consequences.

In the last 15 years numerous issues have occurred that affect the shift from information security to cyber security, such as:

- increased internal threats (internal ‘wiki-leaks’ incidents, data breaches, malicious attacks from within),
- emerging technologies, namely digital technologies which are externally oriented and enable inter-connectivity of devices that constantly interact (cloud computing, sensors and IoT - Internet of Things, cognitive technologies - AI, mobile technology, social media, etc.),
- increased external threats (malware, ransomware, data breach, interconnected devices, IoT devices, cyber war, state sponsored attacks. For example, Ponemon Institute [22] estimated that direct costs of data breach in 2017 were 3,62 million USD, while ISACA [12] revealed that a single data breach costs - direct and indirect expenses - around 5,5, million USD),
- huge data proliferation (volume of data transmitted over interconnected systems are doubling every 20 months, mobile Internet data is doubling every year [18]),
- extensive use of mobile devices and social media networks and increasingly mobile workforce (if not managed properly, BYOD - bring your own device means ‘bring your own risks’),
- strong regulation at international and national domain in the area of IS security and data privacy. For example, 65 countries have their own data protection law [18], GDPR – General Data Protection Regulation is due in full implementation on May 2018.

Cyber security incidents can have very negative impact on many levels (individual, institutional, organisational, corporate, national), causing direct financial and other damages (downtime, inability to implement business processes, data breach, etc.) and indirect effects (legal obligations, lost privacy, stolen identity, regulatory penalties, loss of reputation and bad public image). Many organisations still do not have sound policies to manage this [10], [14], [20].

For example, in July 2015, Chris Valasek and Charlie Müller hacked Jeep Cherokee car while someone was driving it on a highway. Vulnerabilities in car info-entertainment system, which is an integral part of every modern car, have enabled hackers to take remote control of the vehicle, using smart phone and while seating on their sofa. The epilogue was recall of 1,4 million cars, repairs, customer claims, reputation risks, regulatory provisions, etc [18]. In July 2017 there was a massive cyber incident in Sweden[1] – a breach of very confidential data stored at cloud computing environment, exposure of national secrets, major international scandal, threat to national security, government crisis, resignation of ministers. In June 2017 disruption of British Airways information system caused over 100 flights from London airports being cancelled, making direct financial loss estimated at 114 million EUR[2]. In May 2017 WannaCry ransomware affected many services worldwide: National Health Service in UK, Renault stopped production at factories throughout France, Deutsche Bahn had problems displaying train lines on train stations, Maersk - container traffic worldwide was very difficult, etc[3].

Even short analysis of described examples and case

[1] The Local.se (2017): Sweden targeted in global cyber attack, https://www.thelocal.se/20170405/sweden-targeted-in-global-cyber-attack-cloud-hopper-apt10

[2] The Guardian (2017): https://www.theguardian.com/business/2017/may/28/british-airways-cyber-attack-unlikely-amid-scramble-to-resume-flights-on-sunday

[3] The Verve (2017): https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries

studies suggest that such cyber threats are not isolated incidents, but very carefully planned and targeted to achieve a precisely defined goal. Apart from many benefits, the notion of digital economy also bring a lot of concerns, especially in cyber security area, mainly due to the fact that literally everyone (any individual, companies of all sizes, operating in any industry, institutions, states, etc.) might be a target of cyber attack. Cyber incidents have a carefully planned 'life cycle', consisting of the following phases [18]:

- 'sniffing', 'exploring', vulnerability analysis,
- assessment of identified vulnerabilities and preparation of ‘test’ attack,
- ‘test’ (experiential) cyber attack,
- analysis of test attack results, 'learning' about security controls which should detect and prevent the attack,
- cyber attack ‘improvements’,
- next test attack,
- major attack (well prepared) with the specific objective.

Therefore, we can conclude that main objective in managing cyber security is to carefully design and apply basic, sophisticated and smart, but effective and efficient security controls to address common, advanced and emerging threats to information stored in information systems supported by digital technologies.

III. Managing cyber security by implementing effective controls: preliminary research findings

According to ENISA [8] Threat Landscape Report, main trends in cyber security in 2017 were:

- increasing complexity of attacks and sophistication of malicious actions in cyberspace,
- malicious infrastructures continue their transformation towards multipurpose configurable functions including anonymization,
- encryption and detection evasion,
- monetization of cybercrime is becoming the main motive of threat agents, in particular cyber-criminals,
- state-sponsored actors are one of the most omnipresent malicious agents in cyberspace,
- cyber-war is entering dynamically and finally,
- skills and capabilities are the main concerns for organisations.

Top threats in 2017 were malware, web based attacks, web application attacks, phishing, spam, denial of service, ransomware, botnets, insider threats and physical manipulation/damage/theft/loss of devices [8].

On the other hand, cyber incidents are not happening due to any kind of 'accident' or 'bad luck', but due to poor management of information systems and insufficient competencies in cyber security. Every information system has many embedded IT controls, which are enabling its non-disrupted, accurate, reliable and effective work. The more effective basic and advanced controls which are detecting and preventing all cyber threats an organisation implement, it is less likely to be exposed to cyber risks, or will be exposed to lower risk level. Therefore, in order to successfully manage cyber risks, it is very important to constantly evaluate how effective security controls are [20]. ISACA [13] revealed that 97% of cyber-attacks could be prevented if institutions had effective controls. Security controls are applied to detect and/or prevent unwanted events or processes in information system (unauthorized use, inaccurate data, ineffective processes, wrong algorithms or faulty system inputs etc.) or problems from external environment (external attacks, faulty data transmission, natural disasters, etc.).

A. *Research methodology and sample*

We have learned from previous research findings that companies associated with important or critical national infrastructure might be exposed to cyber threats, and would like to investigate what control mechanisms are in place to mitigate them. National infrastructure (or NI for short) refers to the complex, underlying delivery and support systems for all large-scale services considered absolutely essential to a nation [1]. These services include power control networks, providers of telecommunication services, public transport services, financial institutions, military support and similar services widely available to public. However, not all national infrastructure is referred to as a “critical” national infrastructure (or CNI for short). CNI of USA is defined as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters [9]. UK Government defines CNI as those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life [23]. NI put an emphasis on wide impact on national security, while CNI is more related to public security and safety and focused on events leading to severe damage in public lifestyle. Therefore, CNI is a subset of all systems that together form a country’s NI. Most countries strive to protect their cyberspace by first formulating their cyber security strategies [2]. These strategies usually include some guidelines on how to implement cyber security issues in each NI or CNI institution. While Croatia has established national cyber security strategy [7], there is still no measurement of impact of cyber security events to NI or CNI. In addition, cyber security strategies of companies related to NI or CNI still remain unknown.

In this paper we have conducted a preliminary research on how large companies in Croatia, namely companies which are associated with NI (important national infrastructure) or CNI (critical national infrastructure), are managing cyber security. As there were no similar researches, we have specifically investigated which controls are in place to mitigate cyber threats and to what extent they are effective. To address the research objective, firstly we draw a survey questionnaire to be able to collect general information about cyber security issues. The questionnaire is in line with researches we relate to in previous chapters [8], [13], [14]. To increase research validity, it was pilot tested by cyber security professionals (research experts with international certifications in the field). Then we narrowed our focus to nine selected companies and finally conducted series of comprehensive and in-depth interviews with people responsible for cyber security. Interview transcripts were selected and reviewed by two independent researchers.

Sample for our research include nine large companies operating in Croatia, with average number of 2.707 employees and average yearly income of 1,9 billion HRK (around 260 million EUR). These companies cover many industries related with NI or CNI, as they operate in financial sector (2 of them), insurance (2), IT (1), energy (1), food and agriculture (1), telecommunication (1) and other (health fund 1). In total, there are 421 large companies in Croatia (by Croatian regulations, large are companies with over 250 employees), but there are just 25 of them with over 2.500 employees. In that light, we may find this sample representative, as it covers almost all companies in the country of that size, which are related either to NI or CNI. In this paper we will use this sample for preliminary research, while in the future, we are planning to conduct a separate, more comprehensive research on much larger sample, covering many industries and organisations of all sizes. Profile of sampled companies is shown in table 1.

Table 1. All sampled companies are related to critical national infrastructure

Profile of sampled companies	
Average number of employees	2.707
Average income	260 million EUR
Industry profile	
Financial industry (banks)	2 (22,11%)
Insurance	2 (22,11%)
IT	1 (11,11%)
Energy	1 (11,11%)
Food and agriculture	1 (11,11%)
Telecommunication	1 (11,11%)
Other (health services	1 (11,11%)
Responsibility for IT/cyber security	
Board member	2
C-suite executive level	4
CISO	2
Cyber security advisor	1

All sampled companies have a person specifically responsible for cyber security: 2 of them are Board members, 4 directly report to CEO, in two companies that responsibility is assigned to CISO (Chief Information Security Officer) who directly reports to CEO and Supervisory board and one company have an autonomous cyber security advisor. All of them continuously evaluate the effectiveness of security controls and regularly report on cyber security to highest executive levels (predominantly on monthly, quarterly basis, or twice a year). As EY 2017 Global Information Security Survey [10] revealed that 63% of organisations still have the cyber security function reporting into IT, and only 50% report to Board regularly, we may found the controls in the sampled companies matured and effective.

Almost all sampled companies are obliged to follow cyber security regulations, either at national or international level. Majority of them spend around 1% of total income for cyber security and all have key internal acts like IT security or cyber security policy in place. Also, as C-suite level executives are well informed about cyber risks and regular IT security audits are taking place, we can conclude that key organisational controls are effective and efficient. On the other hand, even there are companies in our sample where cyber security was mentioned in organisation's strategies, these issues are not in heart of C-suite level interest as they still assume cyber security is solely the responsibility of IT departments or assigned individuals (CISO and similar). In that light, cyber security is still not a core part of business strategy and culture, and companies should engage more employees around it, take more collective ambition toward cyber security management and implement more integrated and holistic cyber security vision.

Table 2 shows that average grade for threats is relatively low (from 2,22 to 3,22 on 1-5 scale), which might imply that sampled companies either underestimate cyber threats or are very confident that controls to mitigate them are mature and efficient. ISACA report on State of Cyber security 2017 [14] revealed IoT is replacing mobile as the emerging area of concern, which is not the case here, mainly due to the fact that our sample is consisted of companies not so related to digital transformation issues, but with critical national infrastructure. As these researches are hardly comparable, our findings might be useful as preliminary information on various cyber security issues.

Table 2. Cyber threats

Major cyber threats (on 1 to 5 scale, 1 minimum, 5 maximum)	
Employees and their behaviour	3,22
Disruptive technologies (IoT, mobile, cloud, byod)	3,00
Cyber criminal	2,78
Organisational issues (culture, awareness, policies)	2,56
Compliance with regulations	2,22
How likely is that following threats will happen?	
Loss of mobile devices	3,67
Phishing attacks	3,11
Malware attacks	3,00
Social engineering	2,44
Dana breach	2,33
External attacks (DDoS, sql injection, ..)	2,11
Internal attacks	2,00

Finally, our respondents find controls implemented to mitigate these threats very mature and efficient (average grades ranging from 4,22 to 4,33 on 1-5 scale). They highly rate both technical (4,33), organisational (4,22) and physical (4,22) controls. Major problems associated with IT/cyber security by our research respondents are: employees not aware of the cyber security issues (2,89, on a 1-5 scale), insufficient education (2,89), insufficient employees technical skills and business competencies (both 2,22), lack of competent experts (2,22) ineffective preventive and detective controls (1,89).

As ENISA 2017 report revealed [8], top threats in 2017 were malware, web based attacks, web application attacks, phishing, spam, denial of service, ransomware, botnets, insider threats and physical manipulation/damage/theft/loss of devices. As depicted in table 3., our respondents are very confident that security controls will prevent and detect major cyber threats, which is very important for any organisation, especially for those related to critical national infrastructure.

Table 3. Effectiveness of controls

How effective are controls to detect and prevent cyber threats? (1 to 5 scale, 1 minimum, 5 maximum)?	
Web base attacks	4,22
Malware	4,22
Internal fraud	3,89
Internal attacks	3,78
Identity theft	3,44
Data breach	3,33
Loss of mobile devices	3,22

IV. Conclusion

Most organizations in all sectors of industry, commerce and government are fundamentally dependent on their information systems (IS) and would quickly cease to function should the technology (preferably information technology – IT and recently novel digital technologies) that underpins their activities ever come to halt [20]. Although, characteristics of IS security incidents and associated risks have dramatically changed in recent decades, from isolated incidents in 'information security era' to sophisticated cyber attacks which are exploiting vulnerabilities of inter-connected systems in 'cyber security era', it seems that cyber security is still the sole responsibility of the IT departments. In addition to 'common' IT incidents which should be mitigated by basic security controls, today we are faced with advanced and emerging cyber attacks, which need to be detected and prevented with smart, innovative and efficient controls.

We gave the overview of digital technologies and explained how its external focus and inter-connecting features are affecting the shift from information to cyber security issues. We argued about the differences between these two terms, which are often used interchangeably, and concluded that main focus of cyber security is related to designing and implementing smart and sophisticated, but still effective controls which will help protect enterprises and individuals from intentional, advanced attacks, breaches, incidents and consequences.

Finally, we have conducted a preliminary research on how large companies in Croatia, which are associated with important (NI) or critical national infrastructure (CNI) are managing cyber security. It was our specific interest to investigate how mature and effective are basic and advanced controls to mitigate cyber threats. Our research was based on a survey questionnaire followed by in-depth interviews with experts responsible for IT/cyber security. Nine sampled companies are covering wide range of industries, employing 2.707 people on average, have large budgets and all are engaged in providing important (NI) or critical national infrastructure (CNI), which made them interesting for our research. Furthermore, there are 25 companies of that size in the country, which make our sample of nine organisations relevant, especially due to the fact this is a preliminary research. We can conclude that companies associated with important or critical national infrastructure in Croatia have very efficient basic organizational and technical controls. In addition, our research revealed that our respondents were very confident that security controls will prevent and detect major cyber threats such as web based attacks, malware, phishing, insider threats, ransomware, identity theft, data breaches and loss of mobile devices. All this considerations are very important for any organisation, especially for those associated with important (NI) or critical national infrastructure (CNI).

Majority of sampled organisations spend around 1% of total income for cyber security, all of them have key internal policies in place and C-suite level executives are well informed about cyber risks, mainly through monthly or quarterly reports. As people responsible for cyber security report directly to CEOs, we can conclude that key organisational controls are effective. On the other hand, even there is increased awareness about cyber security, these issues are still not a core part of business strategy and culture. Our research revealed that highest executives (C-suite level executives) still assume cyber security is solely the responsibility of IT departments or assigned individuals (CISO and similar). In that light, companies should take more holistic and collective ambition toward cyber security management. Cyber security should be the responsibility of every employee and even of the people in the ecosystem of the organisation [10]. We can conclude that sampled companies are lagging behind in applying more advanced and sophisticated controls.

Our respondents find controls implemented to mitigate regular cyber threats very efficient (average grades ranging from 4,22 for organisational to 4,33 for technical controls on 1-5 scale). On the other hand, major problems with cyber security are evaluated with low relatively grades: employees not aware of the cyber security issues (2,89, on a 1-5 scale), insufficient education (2,89), insufficient employees technical skills and business competencies (both 2,22), lack of competent experts (2,22) ineffective preventive and detective controls (1,89). This might imply that sampled companies either underestimate cyber threats or are very confident that controls to mitigate them are effective and efficient.

Although this paper extends the existing body of knowledge, there are limitations of this preliminary research. Since we were focused on large companies in Croatia related to important or critical national infrastructure, the sample itself were small (nine companies), but representative. Research results could not be generalized for a single industry, and is not comparable to many other surveys, but might be a guideline for future work. Our plan for the future is to use this preliminary findings to conduct a separate, more focused and comprehensive research on much larger sample, covering many industries and organisations of all sizes.

References

[1] Amoroso, E.G. (2010): Cyber attacks: Protecting national infrastructure, Bh, Elsevier.

[2] Atoum I, Otoom A., Abu Ali A. (2014): A holistic cyber security implementation framework, Information Management & Computer Security Vol. 22 No. 3, 2014 pp. 251-264.

[3] Bharadwaj, A., El Sawy, O., Pavlou, P.A., Venkatraman, N., Digital business strategy: toward a next generation of insights, *MIS Quarterly* Vol. 37, No. 2, June 2013, pp 471-482,

[4] Bonnet, D., Ferraris, P., Westerman, G. and McAfee, A., Talking 'bout a Revolution, *Digital Transformation Review* Vol 2, No 1., 2012, pp. 17-33.

[5] Cheng, Y., Groysberg, B. (2017): Why Boards Aren't Dealing with Cyberthreats, Harvard Business Review, https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats

[6] Cybersecurity Ventures (2017): Cybercrime Report 2017 Edition.

[7] Cyber Security Strategy of The Republic of Croatia, October 2015 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf

[8] European Union Agency for Network and Information Security - ENISA (2018): Threat Landscape Report 2017, January, 2018.

[9] Executive Order no. 13636 (2013), Improving Critical Infrastructure Cybersecurity, DCPD-201300091, 2013

[10] EY (2017): Global Information Security Survey, December 2017.

[11] International Telecommunication Union – ITU (2017): Global Cyber Security Index, December 2017.

[12] ISACA (2012): Extracting Value from Information Chaos: Why Good Governance Makes Good Sense, CobiT 5, ISACA, Rolling Meadows, Illinois,USA

[13] ISACA (2015): Global Cyber Security Status Report, ISACA, Rolling Meadows, Illinois, USA.

[14] ISACA (2017): State of Cyber Security 2017, ISACA, Rolling Meadows, Illinois,USA

[15] Klahr, R., Shah, J.N., Sheriffs, P, et. al (2017): Cyber Security Breaches Survey 2017, UK Department for Media, Culture and Sport, https://www.gov.uk/government/publications/cyber-security-breaches-survey-2017

[16] PricewaterhouseCoopers (2015): Global State of Information Security, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/key-findings.html

[17] Siponen, M.T., Oinas-Kukkonen, H. (2007) "A review of information security issues and respective research contributions", The Database for Advances in Information Systems, Vol.38 No.1 pp 60-81.

[18] Spremić, M. (2018): Enterprise information system in digital economoy, Faculty of Economics and Business, Zagreb, Croatia.

[19] Spremić, M. (2017): Governing Digital Technology – how Mature IT Governance can help in Digital Transformation?. *International Journal of Economics and Management Systems*, **2**, 214-223.

[20] Spremić, M. (2013): Holistic approach to governing information system security, Lecture Notes in Engineering and Computer Science, Volume 2 LNECS, 2013, Pages 1242-1247

[21] Tapscott D., *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*, McGraw-Hill, 1995.

[22] The Ponemon Institute (2017): Cost of Data Breach Study, June 2017.

[23] UK Cabinet Office (2010): Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards, March 2010

[24] Werlinger, R., Hawkey, K., Beznosov, K. (2009) "An integrated view of human, organizational, and technological challenges of IT security management", Information Management & Computer Security, Vol. 17 Iss: 1, pp.4 – 19

[25] World Economics Forum (2017): Global Risk Report 2017.

[26] Von Solms, B. (2006) "Information security – the fourth wave", Computers & Security, Vol.25 No.3 pp165-8