CHALLENGES AND VULNERABILITIES OF ANALYSING CYBERCRIME COSTS

Jūratė Kuklytė[1]

[1] *Vytautas Magnus University, Kaunas, Lithuania*

EUROPEAN JOURNAL OF BUSINESS SCIENCE AND TECHNOLOGY

Volume 3 Issue 2
ISSN 2336-6494
www.ejobsat.com

ABSTRACT

Recent studies have underlined a limited scope of research published with regard to the impact of cybercrimes, which is investigated by applying the scientific literature analysis and surveys. This paper focuses on in-depth research on cybercrime costs by analysing the information from selected online materials in order to reveal a research gap. To support the contributions of the research in the field, two methods, namely, literature review and statistical analysis were employed. The findings reveal that several interested parties such as independent IT companies, governmental and non-governmental institutions have conducted various surveys to identify the impact of cyberattacks. The main challenges and vulnerabilities of analysing cybercrime costs can be overcome by further investigations.

KEY WORDS

cybercrime cots, cyber attack, OLS regression

JEL CODES

M21, K24

1 INTRODUCTION

A rapid technological progress has enabled power imbalance and anonymity in electronic environment, which encourages cybercrime activities. Cybercriminals use various means of information and communication technologies (ICTs), networked computers, mobile telephones, bots, and other devices. In the effort to reduce computer-focused digital deviance (Reyns, 2010) and negative outcomes, it is essential for academics, practitioners and criminologists to understand the impact of cybercrimes. Bossler and Holt (2009) point out that individuals' cyber deviance and the absence of social guardianship have increased the chances of dataloss due to a malware infection, whereas physical guardianship (the usage of an antivirus

KUKLYTĖ, Jūratė. 2017. Challenges and Vulnerabilities of Analysing Cybercrime Costs. *European Journal of Business Science and Technology,* 3 (2): 81–89. ISSN 2336-6494,
DOI http://dx.doi.org/10.11118/ejobsat.v3i2.105.

software) has had no expected protective impact because of the lack of information.

In recent years, scientists as well as practitioners have shown an increased interest in cyber incidents and their effects. Cyber activities have been recognised as a destructive phenomenon in private and public enterprises (de Werra and Studer, 2017; Van Niekerk, 2016; Hills and Batchelor, 2015; Kawanaka et al., 2014; Ventre, 2013; Kim et al., 2011; Luo and Liao, 2009). Moreover, the major threat of cyberattacks, which have occurred in the last decade, has showed the vulnerabilities in cyber defence of the North Atlantic Treaty Organization (NATO), the European Union (EU), and the United Nations (UN). The number of studies in the field is sufficient, however, in order to shed light on the spread and the impact of cyberattacks and provide important information to policymakers and practitioners, a deeper analysis is necessary. Cybercrime entails a variety of costs for enterprises, e.g. system repair expenditure, compensations for customers, legal costs, lost revenues, and a reputational damage.

It should be noted that a viral spread of cybercrime has started increasing threats of digital challenges. It has motivated the interested parties to create prevention tools (Saxena et al., 2017), cyber security strategies (Miao and Li, 2017), and an intrusion detection system to reduce the number of cybercrimes. Nevertheless, when analyzing the effect of cyberattacks, some academics have highlighted extreme challenges related to the issue under discussion (Furnell et al., 2015; Leeuw and Leeuw, 2012; Musman et al., 2010; Fletcher, 2007).

It should be pointed out that many recently conducted studies measuring the economic effect of cybercrime costs in a contemporary workplace has remained ambiguous. The paper aims to contribute to in-depth research of cybercrime costs by analysing the information from selected online materials using the statistical package IBM SPSS version 20 and MS Excel 2012. The paper concludes with final remarks on the contributions of the research, its limitations and insights for future implications.

2 THEORETICAL BACKGROUND

Recent theoretical and practical advances have produced alternative views of forms, prevention and recovery costs of cybercrime (Ponemon Institute, 2016). In 2016, cybercrime cost the global economy more than $450 billion. Due to such a situation and an increasing operational risk, it is vital to understand the importance of the investment in the information security. Smith et al. (2011) estimated that cybercrime news story has a significant impact on the average stock price of companies in a short term.

Cybercrime costs are one of the biggest issues; however, they have been defined differently in the last decades. Center of Strategic and International Studies (2014) emphasizes three kinds of opportunity costs, which determine the losses after cyberattacks: (1) reduced investment in R&D, (2) risk averse behavior by businesses, and consumers that limit the Internet use, and (3) increased spending on the network defence. Ponemon institute (2016) divides internal cybercrime costs of organizations into three groups: (1) direct costs such as the main expense outlay to accomplish the given activity; (2) indirect costs such as time, effort and other organizational resources; (3) opportunity costs such as a negative reputation and lost opportunities. External costs include the loss of information assets, business disruption, equipment damage and revenue loss, which have been captured using shadow-costing methods. However, Jardine (2015) broaden the understanding of damage by operationalizing cyberattacks via: (1) the average cost per data breach; (2) overall organizational cost from data breaches; (3) the cost of detecting a data breach and escalating; (4) post-breach reaction costs; (5) lost business cost; and (6) victim notification costs.

Findlay (2015, pp. 4–5) emphasizes that measuring the degree of cybercrime harm addresses vulnerabilities – "analysts are required to postulate various scenarios of exploit and their immediate and secondary, or down-stream, impacts". Such harm is related to the cost (dollar value) of recovery procedures after data breaches. Immediate impact is defined as data loss, credibility, liability and intangible assets associated with financial or national security inferences.

3 METHODOLOGY AND DATA

In order to achieve the aim of the investigation, different methodological techniques were used. Firstly, the review of literature was done in order to create a unique dataset. To be more specific, information from previous researches carried out on behalf of governmental and non-governmental organizations and reports of independent IT companies and institutes were taken into consideration in this study. The search was accomplished in the scientific databases such as Web of Science, Scopus, JSTOR, Springers, Emerald, Science Direct, Sage, EBSCO, and Google Scholar. In addition, a snowballing technique was employed for the initial sample including relevant materials and the latest references. Thus, bibliometric review helped to reveal interests of Internet users, who search for specific keywords related to the impact of cyberattacks. The data of Google Trends was analysed.

Tab. 1: The type of selected materials

Type	Frequency	Percent	Cumulative percent
Articles	94	27.9	27.9
Scientific papers	1	0.3	28.2
Reports	217	64.4	92.6
Working papers	24	7.4	100.0
In total	337	100.0	

By reviewing a large number of published articles, reports and working papers from various scientific journals and online sources (Tab. 1), the research gap as well as challenges and vulnerabilities related to the analysis of cyberattacks were identified. To keep the research up-to-date, the recent materials were included and the collected data was analysed using statistical package IBM SPSS version 20 and MS Excel 2012. The collected data was used to develop a unique dataset for an empirical research analysing cybercrime costs.

Moreover, eight components or meta-clusters were chosen to estimate cybercrime costs using ordinary least squares (OLS) regression models. Based on a relative small sample and the violation of normality assumption of OLS regressions, the bias corrected and accelerated (BCa) bootstrapping technique was employed (Levi and Leighton Williams, 2013). Bootstrapping is a nonparametric resampling procedure to estimate the sampling distribution of an indirect effect (Bollen and Stine, 1990).

The investigation was based on the equation by cluster (Woolridge, 2006):

$$y_{gm} = \alpha + x_g\beta + z_{gm}\gamma + v_{gm}, \qquad (1)$$

where $m = 1, \ldots, M_g$ and $g = 1, \ldots, G$.

The estimation in the equation depends on the factor and effects of aggregate variables (β) or individual specific variables (γ). For the cluster sampling, it is important whether the vgm contains a group effect.

The first set of the meta-cluster consists of macroeconomic factors. The annual statistics from the World Bank database were taken into consideration in order to estimate GDP growth and growth of Internet users. The second set of items was collected by employing a snowballing technique to select relevant data and check if there is any bias among institutions. Two governmental companies, namely, the CSI and FBI were chosen as the control group. Another meta-cluster focused on the cybercrime costs: notification costs, data breach costs, privacy violations, stolen devices, thefts, opportunity costs, and phishing. The sets of predictor variables and the control group were regressed

and eight models were generated. In order to assert which set of variables was the most predictive in retaliation to each model, a sub-model analysis was conducted. R^2 statistic was used to evaluate the sub-models.

The hypothesis was made that the number of Internet users is significant in OLS regression. Kleiner et al. (2013) stated that Internet users are largely concentrated in North America and Western Europe. The Council of Europe Convention on Cybercrime and London Action Plan propose actions to develop global cyber security and policy initiatives. This study also suggests that the growth of Gross Domestic Product (GDP) has impact on cybercrime costs. The same hypothesis was applied for Microsoft researches in 2013.

4 RESULTS

To address the research gap, institutions which conduct surveys to measure the effect of cybercrime in different contexts and wide institutionalization were taken into account. The main contribution is that the analysis of cybercrime costs might be framed by specific institutions and authors, which provides directions or solutions to curtail cyber incidents (Tab. 2).

It could be unrealistically promising for a private sector to use services of independent IT firms such as Rand Corporation, IBM (sponsor investigation of Ponemon institute), Cisco (sponsor analysis of Government & Finance Divisions), PwC (sponsor surveys of HM Government), and others. It could be noted that private IT companies play the central role among relevant stakeholders because they have more capabilities or resources to conduct specialized surveys than any other actor (Tab. 2). There is also a difference in institutions influencing the understanding of the main factors that affect a control system and cyber security policy. While an institution is diffused in different cases of cybercrimes, the priorities are defined by stakeholders, the analysis focuses on governments and companies.

Tab. 3 shows the most common location of authors or institutions. Only one country, the USA, has more than 200 online materials, i.e. almost five times more materials than the United Kingdom, which is the second country in the list. It suggests that a few players have taken the lead in the empirical investigation of cybercrime costs, with the USA as the top-ranking country, which reflects the efforts to develop and implement a cyber security policy. This offers contributed identification of the used sample that should be investigated in depth through extensive econometric analysis in order to capture emerging trends. The lack of published reports in the world reveals another vulnerability.

Fig. 1 illustrates steep increases in the number of the selected online materials in 2003, 2013 and 2016. The main tendency is also obvious: most of scientific analyses, reports or working papers are published in the United Kingdom and the United States of America. This reveals the main vulnerability in the field of cybercrimes. The number of countries whose institutions focus on cyberattacks is very small; therefore, there is a great need for other countries to develop cyber security policy or create research institutes to curtail cyber incidents or analyze their impact on private and public sectors.

Cyberattacks gained interest in 1988. According to the NATO (2013), the Morris worm, which is one of the first recognised worm to affect the world's nascent cyber infrastructure, spread around computers largely in the US in 1988. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable. It was reported that 6000 computers were affected causing an estimated 10–100 million dollars for repair costs. This type of a cyberattack encouraged to develop methodology and create distributed denial-of-service (DDOS) attacks which were committed by MafiaBoy (Michael Calce) and targeted at

Tab. 2: Institutions which analyse the impact of cyber attacks

Institution	Frequency	Percent	Cumulative percent
Cardiff School of Social Science	7	2.1	2.1
CSI / FBI	12	3.6	5.6
Government & Finance Divisions (USA)	22	6.5	12.2
HM Government	8	2.4	14.5
Internet Crime Complaint Center (IC3)	58	17.2	31.8
Global Risk Specialists	1	0.3	32.0
Louisiana Technology University	34	10.1	42.1
University in Rock Hill	10	3.0	45.1
University of Plymouth	17	5.0	50.1
Norman Paterson School of International Affairs	25	7.4	57.6
Ponemon Institute	107	31.8	89.3
RAND Corporation	36	10.7	100.0
In total	337	100.0	

Tab. 3: Country institutions which analyse the impact of cyber attacks

Country	Frequency	Percent	Cumulative percent
The United Kingdom	57	27.9	20.2
World	11	2.3	3.3
The United States of America	269	69.8	100.0
In total	337	100.0	

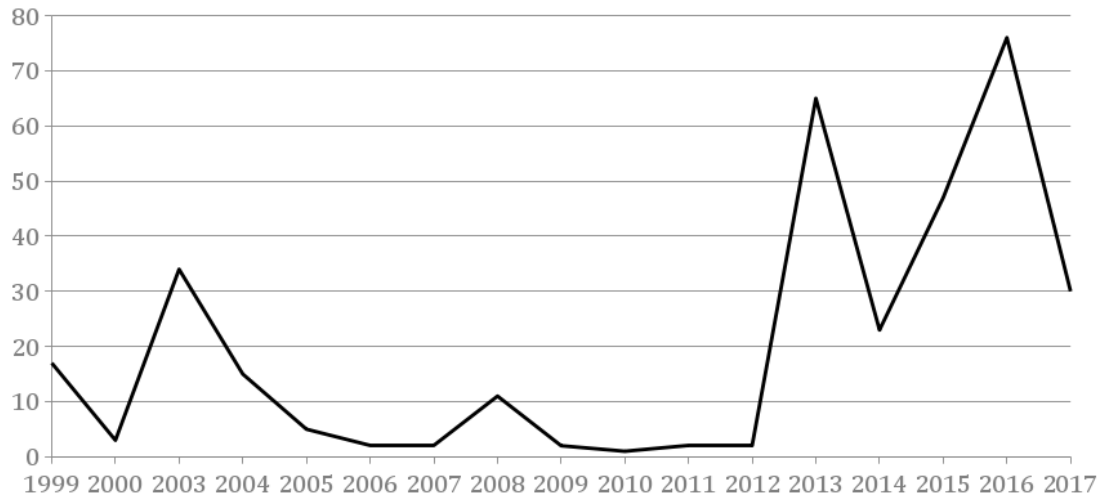

Fig. 1: The frequency of the selected materials 1999–2017

CNN, eBay, Amazon and Yahoo in 2000. It may have cost around 1.2 billion dollars for industry.

The reason for the increased interest in cyber security might have been due to various cyberattacks in 2012: hacking of the Vatican Websites, the theft of Michael Jackson's catalogue from Sony, and the leak which targeted Vector Inc., a Japanese computer selling firm, potentially affecting more than 260,000 users. Data Breaches (2012) stated that LulzSecReborn hacking group had initiated a massive information leak – of approximately 170,000 records from a military dating site (MilitarySingles.com) which might have cost over $33 Millions in 25 March, 2012. Kovacs (2012) announced that these hackers also had breached the website of CSS Corp, a global ICTs company, leaking the main domain's entire database in 27 March, 2012.

It was also revealed that an unknown group of cybercriminals had infiltrated multiple financial firms after phishing its targets with infected email attachments in 2013. The spread of massive attack was investigated by Kaspersky Lab, which stated that due to this attack at least "100 banks in 30 countries, including Russia, the US, Germany, China, and Ukraine, were affected. In many cases, criminals used their computer exploits to dispense cash from ATMs or transfer cash digitally to accounts they controlled" (Szoldra, 2015).

Following the above considerations, it can be pointed out that interest in ciberattacks has increased among members of the information society. Individuals are getting aware and are searching for more information which could help them to identify the effect of a digital deviance. Google trends reveal that the number of search queries for specific keywords such as "cyberattacks AND cybercrime costs" has been rapidly increasing (Fig. 2). The number of searches for information about the impact of cyberattacks has even doubled since 2016.

Based on the collected data, the sets of predictor variables and the control group were regressed (Tab. 4). The first hypothesis, that the growth of Internet users is significant, was approved, whereas the second hypothesis, that the GDP growth does not have impact on models of cybercrime costs, was rejected. There are no significant associations between the control group and other meta-clusters. What is more, the majority of determinants in meta-clusters of different models are statistically significant.

5 DISCUSSION AND CONCLUSIONS

The paper reveals that most authors and institutions are focused on technical detection and prevention of cyberattacks rather than taking evidence based view from the reports or collaborating with governmental institutions. Following new trends, cybercrimes are described as a destructive phenomenon – the highest threat for public and private institutions. To guide and align stakeholders' behaviour, investigations of cybercrime rely on the regulation and deliberate incentive structure of sponsorships.

Descriptive statistics lead to unique contributions since the analysis of reports of independent IT firms and cyber security institutes as well as scientific publications and working papers broaden our understanding of the analysis of cybercrime and its effect focusing on computer worms, viruses and other malware. It should be noted that this survey is limited to a statistical tool indicating only considerable subjectivity of the effect of cybercrimes. Nevertheless, Cashell et al. (2004) state that survey data is an objective way to measure the impact of cyber incidents on individual firms. Cavusoglu et al. (2004) argue that it is impossible to measure intangible costs and many companies underestimate the costs of security breaches. For this reason, the estimation of incidence reported by the CSI and FBI survey is much lower than the real price after cybercrimes.

The exponential growth in the selected online materials in 2003, 2013 and 2016 was also noticed. This may reflect the increased interest of IT companies and policy makers after the

Tab. 4: The clustered OLS regression

	1	2	3	4	5	6	7	8
GDP growth	−0.164	−0.204	−0.193	−0.178	−0.174	−0.208	−0.172	−0.166
	(−0.244)	(−0.249)	(−0.248)	(−0.246)	(−0.241)	(−0.251)	(−0.247)	(−0.254)
Growth of Internet users	0.001*	0.000	0.001*	0.001*	0.001*	0.001*	0.001*	0.000
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Sponsored by CSI	0.054	0.035	0.057	0.054	0.049	0.056	0.056	0.019
	(−0.048)	(−0.051)	(−0.046)	(−0.048)	(−0.052)	(−0.047)	(−0.046)	(−0.058)
Sponsored by IC3	0.476**	0.454**	0.473**	0.476**	0.480**	0.476**	0.474**	0.430**
	(−0.068)	(−0.071)	(−0.068)	(−0.068)	(−0.068)	(−0.068)	(−0.068)	(−0.074)
Sponsored by CISCO	0.507**	0.488**	0.510**	0.507**	0.503**	0.508**	0.510**	0.473**
	(−0.036)	(−0.038)	(−0.034)	(−0.036)	(−0.039)	(−0.035)	(−0.035)	(−0.043)
Sponsored by Global Risk Specialists	1.019**	1.001**	1.023**	1.020**	1.015**	1.021**	1.022**	0.986**
	(−0.037)	(−0.039)	(−0.035)	(−0.037)	(−0.041)	(−0.037)	(−0.036)	(−0.044)
Sponsored by PwC	0.593**	0.638**	0.590**	0.593**	0.597**	0.593**	0.590**	0.674**
	(−0.032)	(−0.037)	(−0.031)	(−0.032)	(−0.033)	(−0.031)	(−0.031)	(−0.047)
Sponsored by IBM	0.202**	0.202**	0.202**	0.211**	0.210**	0.206**	0.213**	0.216**
	(−0.039)	(−0.037)	(−0.039)	(−0.042)	(−0.040)	(−0.039)	(−0.041)	(−0.042)
Sponsored by universities	0.253**	0.244**	0.281**	0.254**	0.279**	0.260**	0.274**	0.339**
	(−0.078)	(−0.076)	(−0.077)	(−0.078)	(−0.089)	(−0.080)	(−0.075)	(−0.086)
Notification costs	0.399**							0.339**
	(−0.040)							(−0.045)
Data Breach Costs		−0.066**						−0.127**
		(−0.030)						(−0.043)
Privacy violations			−0.312**					−0.414**
			(−0.078)					(−0.092)
Stolen Devices				−0.151**				−0.201**
				(−0.030)				(−0.030)
Thefts					−0.334**			−0.413**
					(−0.094)			(−0.090)
Opportunity costs						−0.148*		−0.258**
						(−0.073)		(−0.077)
Phishing							−0.247**	−0.337**
							(−0.057)	(−0.090)
Constant	−0.123**	−0.100**	−0.119**	−0.123**	−0.127**	−0.121**	−0.120**	−0.077*
	(−0.034)	(−0.040)	(−0.033)	(−0.034)	(−0.035)	(−0.034)	(−0.033)	(−0.042)
Observations	326	326	326	326	326	326	326	326
R-squared	0.219	0.219	0.223	0.218	0.223	0.219	0.222	0.242

Note: The numbers in the parentheses indicate standard errors, * indicates a 10% significance level, ** indicates a 5% significance level.

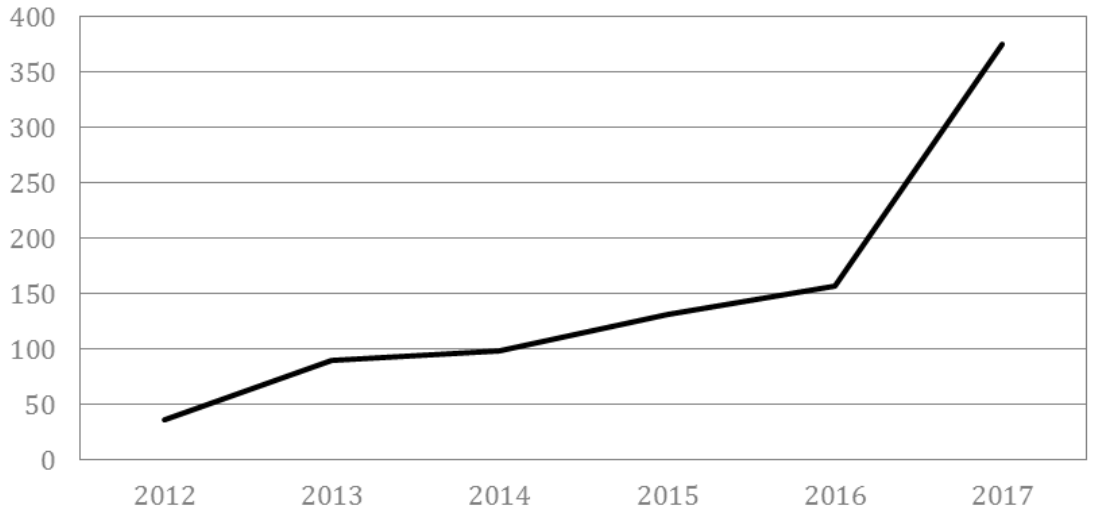

Fig. 2: The frequency of searching for specific keywords in 2012–2017

major cyberattacks in different countries. It is assumed that the sample of online materials can shed light on challenges and vulnerabilities of cyber incidents. This paper contributes to the understanding of the threat of cyberattacks by presenting interests, motivation and implication in different sectors.

Furthermore, the study reveals that the major vulnerability of the research in the field is the lack of information. This is illustrated by a limited number of institutions and scientific publications which analyse the costs of cybercrimes. Along similar lines, Cardenas et al. (2009) agree that researchers tend not to consider how cyberattacks affect the physical world because of limitations of control systems and technical challenges. Gol and Abur (2013) also add that state estimators are vulnerable to any existing critical measurements since their errors cannot be detected. Thus, by manipulating the number of critical measurements, the interested parties can bias results of the state estimation without being detected due to the lack of scientific publications and continuous research in this field.

The main limitation of the chosen methodology is randomised representativeness, which may cause the selection bias. It can be eliminated by further research, using different methodological techniques and analysing related macroeconomic factors. Moreover, instead of the GDP growth and the growth of Internet users other annual economic indicators can be used.

The empirical contributions provide the analysis of cybercrime costs and reveal the bias in this research field because of a limited number of institutions. Professionals and policy makers can use this information to manage the risk control of cyber security and reduce costs related to cybercrimes. There is a wide range of opportunities for future studies in this field as this issue can be addressed using multidisciplinary approach.

6 REFERENCES

Bollen, K. A. and Stine, R. 1990. Direct and Indirect Effects: Classical and Bootstrap Estimates of Variability. *Sociological Methodology*, 115–140.

Bossler, A. M. and Holt, T. J. 2009. On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, 3 (1), 400–420.

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A. and Sastry, S. 2009. Challenges for Securing Cyber Physical Systems. In *Workshop on Future Directions in Cyber-Physical Systems Security*, Vol. 5.

Cashell, B., Jackson, W. D., Jickling, M. and Webel, B. 2004. *The Economic Impact of Cyber-Attacks*. Congressional Research Service Documents. Washington DC. [online]. Available at: `http://www.au.af.mil/au/awc/awcgate/crs/rl32331.pdf`. [Accessed 2017, October 30].

Cavusoglu, H., Mishra, B. and Raghunathan, S. 2004. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9 (1), 69–104.

Center of Strategic and International Studies. 2014. *Net Losses: Estimating the Global Cost of Cybercrime*. [online]. Available at: `https://www.scribd.com/document/228803026/Rp-Economic-Impact-Cybercrime2`. [Accessed 2017, October 17].

Data Breaches. 2012. *Statement from ESingles about MilitarySingles.com*. [online]. Available at: `https://www.databreaches.net/update-statement-from-esingles-about-militarysingles-com/`. [Accessed 2017, October 30].

de Werra, J. and Studer, E. 2017. Regulating Cyber Security: What Civil Liability of Cyber Attacks? *Expert Focus*, 17 (8), 511–517.

Findlay, V. 2015. *Cyber-Threat Versus Cyber-Risk: Performing Adequate Analysis*. [online]. Available at: `https://www.researchgate.net/publication/276284211_Cyber-Threat_versus_Cyber-Risk_Performing_Adequate_Analysis`. [Accessed 2017, November 1].

Fletcher, N. 2007. Challenges for Regulating Financial Fraud in Cyberspace. *Journal of Financial Crime*, 14 (2), 190–207.

Furnell, S., Emm, D. and Papadaki, M. 2015. The Challenge of Measuring Cyber-Dependent Crime. *Computer Fraud & Security*, 10, 5–10.

Gol, M. and Abur, A. 2013. *Identifying Vulnerabilities of State Estimators Against Cyber-Attacks*. [online]. Available at: http://ieeexplore.ieee.org/abstract/document/6652124/. [Accessed 2017, November 1].

Hills, M. and Batchelor, G. 2015. Culturing Defensive Immunity: Hardening Psychological Targets Against Cyber Attack. In: Abouzakhar, N. (ed.). *Proceedings of The 14th European Conference on Cyber Warfare and Security ECCWS-2015*, pp. 95–103.

Jardine, E. 2015. *Global Cyberspace is Safer Than You Think: Real Trends in Cybercrime*. [online]. Available at: http://boletines.prisadigital.com/SSRN-id2634590.pdf. [Accessed 2017, October 29].

Kawanaka, T., Matsumaru, M. and Rokugawa, S. 2014. Software Measure in Cyber-Attacks on Production Control System. *Computers & Industrial Engineering*, 76, 378–386. DOI: https://doi.org/10.1016/j.cie.2014.08.008.

Kim, W., Jeong, O.-R., Kim, C. and So, J. 2011. The Dark Side of the Internet: Attacks, Costs and Responses. *Information Systems*, 36 (3), 675–705. DOI: https://doi.org/10.1016/j.is.2010.11.003.

Kleiner, A., Nicholas, P. and Sullivan, K. 2013. Linking Cybersecurity Policy and Performance. *Microsoft Trustworthy Computing*. [online]. Available at: http://www.ilsole24ore.com/pdf2010/SoleOnLine5/_Oggetti_Correlati/Documenti/Tecnologie/2013/02/SIR-Special-Edition-Security-Atlas-whitepaper.pdf. [Accessed 2017, October 30].

Kovacs, E. 2012. *CSS Corp Site Hacked by LulzSec, Database Leaked*. [online]. Available at: http://news.softpedia.com/news/CSS-Corp-Site-Hacked-by-LulzSec-Database-Leaked-261041.shtml. [Accessed 2017, October 30].

Leeuw, F. L. and Leeuw, B. 2012. Cyber Society and Digital Policies: Challenges to Evaluation? *Evaluation*, 18 (1), 111–127.

Levi, M. and Leighton Williams, M. 2013. Multi-agency Partnerships in Cybercrime Reduction: Mapping the UK Information Assurance Network Cooperation Space. *Information Management & Computer Security*, 21 (5), 420–443.

Luo, X. and Liao, O. 2009. Ransomware: A New Cyber Hijacking Threat to Enterprises. *Handbook of Research on Information Security and Assurance*. IGI Global, 1–6.

Miao, L. and Li, S. 2017. Cyber Security Based on Mean Field Game Model of the Defender: Attackerstrategies. *International Journal of Distributer Sensor Networks*, 13 (10), 1–8.

Musman, S., Temin, A., Tanner, M., Fox, D. and Pridemore, B. 2010. Evaluating the Impact of Cyber Attacks on Missions. In *International Conference on Cyber Warfare and Security*, p. 446. Academic Conferences International Limited.

NATO. 2013. *The History of Cyber Attacks – A Timeline*. [online]. Available at: https://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm. [Accessed 2017, October 30].

Ponemon Institute. 2016. *Cost of Cyber Crime Study & the Risk of Business Innovation*. [online]. Available at: https://saas.hpe.com/sites/default/files/assets/4AA6-8392ENW.pdf. [Accessed 2017, September 30].

Reyns, B. W. 2010. A Situational Crime Prevention Approach of Cyberstalking Victimization: Preventive Tactics for Internet Users and Online Place Managers. *Crime Prevention and Community Safety*, 12, 99–118.

Saxena, N., Chukwuka, V., Xiong, L. and Grijalva, S. 2017. CPSA: A Cyber-Physical Security Assessment Tool for Situational Awereness in Smart Grid. In *ACM CCS Workshop (CPS-SPC)*, Dallas, USA. [In press].

Smith, K. T., Smith, M. L. and Smith, J. L. 2011. Case Studies of Cybercrime and its Impact on Marketing Activity and Shareholder Value. *Academy of Marketing Studies Journal*, 15 (2), 67–81.

Szoldra, P. 2015. *The 9 Worst Cyber Attacks in 2015*. [online]. Available at: http://www.businessinsider.com/cyberattacks-2015-12/#hackers-breached-the-systems-of-the-health-insurer-anthem-inc-exposing-nearly-80-million-personal-records-1. [Accessed 2017, October 31].

Van Niekerk, B. 2016. Suppression of Cyber-Defences. In *IST-Africa Week Conference*, IEEE, pp. 1–12.

Ventre, D. 2013. *Cyberwar and Information Warfare*. John Wiley & Sons, Hoboken, NJ, USA.

Woolridge, J. M. 2006. *Cluster-Sample Methods in Applied Econometrics: An Extended Analysis*. [online]. Available at: http://econ.ucsb.edu/~doug/245a/Papers/Cluster%20Sample%20Methods%20in%20Applied%20Econometrics.pdf. [Accessed 2017, October 17].

AUTHOR'S ADDRESS

Jūratė Kuklytė, Department of Management, Faculty of Economics and Management, Vytautas Magnus University, S. Daukanto str. 28, Kaunas, 44246 Lithuania, e-mail: jurate.kuklyte@vdu.lt