Cybercrime: The Cost of Investments into Protection

VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 16 no. 2 pp. 105–116

Igor Bernik

Purpose:

This paper focuses on investments in protection of organisations against cybercrime. Current research points to enormous financial losses suffered by countries, organisations and individuals due to the impact of criminal offences committed in cyberspace. A detailed overview shows that such losses are fictitious and that the largest share of costs is generated by investments into protection, which, however, is not omnipotent. At the same time, practitioners in the field of cyberspace security find that awareness rising among personnel is a much more efficient and inexpensive method of protection enabling a higher level of security in cyberspace and individual organisations.

Design/Methods/Approach:

The author adapted the cost model of cybercrime by examining data regarding costs and losses inflicted by cybercrime available in different reports and documents drafted by global organisations and governments and analysing the true causes of such losses.

Findings:

The cost model presented in this paper considers the main causes of losses in a comprehensive manner and indicates guidelines for the protection of organisations. However, the provision of greater security in cyberspace is not only a technical, organisational and personnel problem, but ever more often also a political problem, as it is related to the regulation of cyberspace. The costs related to this problem are increasing, since no one endeavours to tackle it.

Practical Implications:

By becoming familiar with the causes and the cost model, organisations may find it easier to decide to invest into protection against attacks from cyberspace and improve their own efficiency with lower costs.

Originality/Value:

This paper presents the impacts of cybercrime on organisations from the point of view of costs and not from the point of view of technical experts in organisations, which are mostly responsible for the implementation of information systems' protection. Therefore, the analysis of the issue provides management with the possibility to better understand individual problems, thus enabling it to take appropriate positions and support more efficient solutions or methods of protection.

UDC: 004.056

Keywords: cyberspace, cybercrime, investments, protection, costs

Kibernetska kriminaliteta: cena investicije v zaščito

Namen prispevka:

Prispevek prikazuje investicije v zaščito organizacij pred kibernetsko kriminaliteto. Aktualne raziskave kažejo oz. predstavljajo enormne finančne izgube držav, organizacij in posameznikov zaradi vpliva kriminalitete v kibernetskem prostoru. Podrobnejši pregled pokaže, da so te izgube fiktivne in da se večina stroškov skriva v investicijah v zaščito, ki pa ni vsemogočna, hkrati pa praktiki varnosti kibernetskega prostora ugotavljajo, da je ozaveščanje osebja učinkovitejša in cenejša zaščita ter ima večji vpliv na varnost kibernetskega prostora in organizacij.

Metode:

Z analizo stroškov in izgub zaradi kibernetske kriminalitete, predstavljenih skozi različna poročila globalnih študij in vladnih dokumentov, ter dejanskih vzrokov za izgube predstavljamo adaptirani stroškovni model kibernetske kriminalitete.

Ugotovitve:

Predstavljeni stroškovni model celovito obravnava glavne vzroke izgub in nakazuje smernice zaščite organizacij. Zagotavljanje višje varnosti kibernetskega prostora pa ni zgolj tehnični, organizacijski in problem osebja, pač pa zaradi regulacije kibernetskega prostora tudi vse bolj politični problem. Ker pa se nihče globalno ne loti reševanja problema, stroški le naraščajo.

Praktična uporabnost:

Organizacije se s poznavanjem vzrokov in stroškovnega modela lažje odločajo za ustrezna vlaganja v zaščito pred napadi iz kibernetskega prostora in izboljšajo lastno učinkovitost z manjšimi stroški.

Izvirnost/pomembnost prispevka:

Zaradi predstavitve vpliva kibernetske kriminalitete na organizacije iz stroškovnega in ne vidika tehnične stroke v organizacijah, ki so večinoma odgovorna za izvedbo zaščite informacijskih sistemov, je razumevanje bližje managementu, s čimer zavzame ustrezna stališča in zaradi boljšega razumevanja podpira učinkovitejše zaščite oz. rešitve.

UDK: 004.056

Ključne besede: kibernetski prostor, kibernetska kriminaliteta, investicije, zaščita, cena

1 INTRODUCTION

When analysing modern ways in which organisations operate, it quickly becomes obvious that classic, paper-based transactions were replaced by the use of information and communication technologies (ICT) and the exchange of information in cyberspace, »as nearly all types of private and public sector organisations have turned to electronic rather than physical informational exchanges in order to improve their efficiencies and service delivery« (Wall, 2013: 107). Hence, the need to protect ICT and provide for an appropriate, secure and protected information exchange is increasing on a daily basis. Information security is affected by external factors present in global cyberspace and internal threats, which may be directly linked to employees' aspirations to abuse company information for different reasons. In addition, an indirect abuse committed by employees may also occur.

The costs of attacks on and abuse of a system are much lower than the costs of a system's comprehensive protection. The majority of measures, which were implemented on the technical and organisational levels in the past few years, and investments into employees aimed to better protect ICT systems and information wealth, were not successful in terms of closing the aforementioned gap. This is why perpetrators of cybercrime are able to achieve extremely high levels of profitability by their actions. In addition, the gap has, in many ways, increased even further due to technological advances and the introduction of new, mainly mobile, technologies. At the same time, scientific journals and news programmes report on cybercrime on a daily basis, which leads one to believe that this is an extremely dangerous phenomenon requiring thorough protection.

Computer Weekly (Ashford, 2013) states that costs of cybercrime for UK businesses average 3.7 million EUR per year. This conclusion is based on findings published in the *Fourth Annual Cost of Cybercrime Study* conducted by Ponemon Institute and sponsored by HP (Ponemon, 2013). The same study also notes that costs for businesses that are victims of internet-based attacks have risen 78 percent per year, on average, over the past four years. The losses in terms of personal information, intellectual property and system damage are staggering enough. But now, the average cost of cleaning up after a successful attack has passed the 0.8 million EUR mark. This, however, does not include the cost of customer lawsuits against companies whose systems have been breached.

Meanwhile, Symantec's 2013 *Norton Report* (Norton, 2013) notes that the overall number of victims of online attacks has actually decreased, which may be attributed to higher levels of awareness regarding different threats and more prudent behaviour of advanced users. On the other hand, the average cost per victim has risen by 50 percent (Cost per cybercrime victim …, 2013). Trilling (Norton, 2013) adds that »today's cybercriminals are using more sophisticated attacks, such as ransomware and spear-phishing, which yield them more money per attack than ever before«. It is clear that the period marked by users' naivety and greed has not yet come to an end, while at the same time the number of new users of cyberspace is still dramatically increasing. The number of naïve users who believe that they can easily make large sums of money, thus remains relatively

high. They obviously believe that lines, such as »I want to give you 1 million because I like your face«, represent their ticket to a carefree future. However, their hope is most often transformed into misery and despair. This is particularly true in cases of abuse committed by employees and the loss of business data. In dealing with offenders and the investigation of cybercrime, it is observed that there is much talk about the losses caused by it; however, only a few articles and studies deal with its actual costs. Data regarding most losses are obtained on the basis of statistical surveys among companies (Symantec, Ponemon, McAfee, etc.) or those affected. In fact, only a few previous scientific publications (addressed in Anderson et al., 2012) considered the problem of calculating the actual costs that cybercrime poses at different levels in detail: at the level of an individual, an organisation or a country.

2 METHODS

Many studies and documents (Alperovitch, 2011; McAfee, 2013; Norton, 2013; Ponemon, 2011, 2012, 2013; SOCTA, 2013; United Nations Office on Drugs and Crime, 2010) examine the costs and losses caused by cybercrime. Some works estimate the overall costs; others evaluate the costs of individual countries, while individual documents even assess losses of certain organisations regardless of their size and technological development. Anderson, Bohme, Clayton, and Moore (2008) assessed security economics and the internal markets already in 2008 and prepared an analysis based on security economics of the practical problems in network and information security that the European Union faces. It analysed fifteen policy proposals that should make an appropriate next step in tackling the problems. In May 2013, the U.S. Commission on Intellectual Property Theft reported that private studies tend to underestimate the impact of Computer Network Exploitation (CNE) information theft and found that the scale of CNE enabled intellectual property theft was »unprecedented« and amounted to "hundreds of billions of dollars per year, on the order of the size of U.S. exports to Asia" (The National Bereau of Asian Research, 2013). In July 2013, McAfee and CSIS[1] (McAfee, 2013) estimated that cybercrime and cyber espionage result in costs ranging from 250 billion to 0.8 trillion EUR; the staggering equivalent of 0.4% to 1.4% of Gross Domestic Product. For the United States, this amounts to 60-120 billion EUR a year. On the basis of the aforementioned studies and starting points, this paper presents an adapted cost model, which outlines comprehensive investments into the protection of organisations against cybercrime.

The selection of a method of protection and the amount of investments into cyber security depends on the individual organisation. Certain approaches were already discussed in previously published papers (e.g. Bernik & Meško, 2011; Bernik & Prislan, 2013), and in addition, a number of other sources also considerd the aforementioned issues from different perspectives. However, the fact that they can be evaluated on the basis of the model presented in this paper, is common to all. Protection against cybercrime will become ever more important due to recent

1 *Center for Strategic and International Studies.*

developments succinctly described by Krebs (2014): »I think we're going to hear a lot about these breaches over the next year… It just looks like some of the guys involved in this activity have compromised a ridiculous number of companies.«

3 COST OF CYBERCRIME

Notwithstanding the above-mentioned research studies, none of them actually presented the general model of calculating the cost of cybercrime until now. Therefore, the best experts in the field of (cyber)crime decided to devise a model entitled »Measuring the Cost of Cybercrime« and published it in a paper authored by Anderson et al. (2012:[2] 1), whereby the introduction states: »We present what we believe to be the first systematic study of the costs of cybercrime … For each of the main categories of cybercrime we set out what is and is not known of the direct costs, indirect costs and defence costs – both to the UK and to the world as a whole.« In this study, the authors carefully distinguish between traditional crime that is now carried out in cyberspace (e.g. tax fraud or deception by selling products related to well-being, health improvement, etc.), and traditional crime, in which the perpetrators' method of operation changed significantly due to the possibility of abuse in cyberspace (credit card fraud) and new types of crime that have been developing with the expansion of the internet. They thus use the cyberspace platform for committing criminal offences (mostly through the use of botnets[3]) that enable an indirect commission of crime. The costs are divided into direct and indirect costs, whereby direct costs or amounts are usually small, almost minimal, and do not cause severe harm to victims of cybercrime.

Indirect costs and defence costs in the field of cybercrime are very high and significantly higher in comparison to classic crime. For example, in order to combat spam alone, produce (anti)spam software, and provide education, billions of dollars are spent every year. The fact is that we, as a society, are very ineffective in the fight against cybercrime. Criminals, on the other hand, impose disproportionately high costs on the society, which mainly happens due to the global nature of cybercrime and strong external influences. Therefore, experts who prepared the above mentioned model (Anderson et al., 2012: 1) offer the following response: »As for the more direct question of what should be done, our figures suggest that we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail.«

In practice, the term cybercrime is applied to three categories of criminal activities:

- traditional forms of crime, such as fraud or forgery, though in a cybercrime context, relate specifically to crimes committed over electronic communication networks and information systems;

2 *Updated version also published in Anderson et al. (2013).*

3 *A botnet is a collection of compromised computers connected to the Internet, through which attacks are carried out.*

- the publication of illegal content over electronic media (i.e. child sexual abuse material or incitement to racial hatred);
- crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking.

One of the models of cost calculation, which relies on the following categories, has previously been proposed in a Detica report (Detica, 2011):

- costs in anticipation of cybercrime, which include individual and organisational security measures, insurance costs and costs associated with gaining compliance to required IT standards;
- costs as a consequence of cybercrime, which take into account direct losses to individuals and companies, and indirect losses arising from reduced commercial exploitation of IP and opportunity costs through weakened competitiveness;
- costs in response to cybercrime, such as compensation payments to victims of identity theft, regulatory fines from industry bodies and indirect costs associated with legal or forensic issues;
- indirect costs associated with cybercrime, which include such factors as reputational damage to organisations, loss of confidence in cyber transactions by individuals and businesses, reduced public sector revenues and the expansion of the underground economy.

The Detica model uses the above-mentioned definitions in order to investigate the impact of cybercrime on the main affected groups: citizens, labour organisations, and countries. In this context, the economic impact on each group is or should be taken into account. The Ponemon Institute (Ponemon, 2012: 23) carried out similar research and the preparation of a model for calculating operating costs of cyber attacks, which represents the cost model with two separate cost streams (Figure 1) used to measure the total cybercrime cost for an organisation: »These two cost streams pertain to internal security-related activities and the external consequences experienced by organisations after experiencing an attack.«

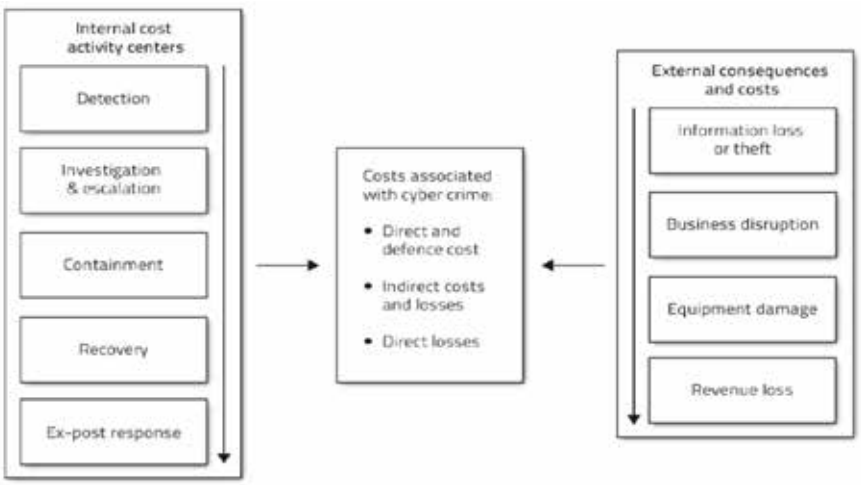

Figure 1: Cost framework for cybercrime (source: Ponemon, 2012: 23)

The study addresses the core process-related activities that drive a range of expenditures associated with a company's cyber attack. The five internal cost activity centres in the framework include (Ponemon, 2012):

- Detection: Activities that enable an organisation to reasonably detect and possibly deter cyber attacks or advanced threats.
- Investigation and escalation: Activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incidents.
- Containment: Activities that focus on stopping or lessening the severity of cyber attacks or advanced persisted threats (APT).
- Recovery: Activities associated with repairing and remediating the organisation's systems and core business processes.
- Ex-post response: Activities to help the organisation to minimise potential future attacks and add new enabling technologies and control systems.

Costs, in addition to internal factors, also result from external factors and costs associated with the consequences of successful attacks on information assets outside the company (Figure 1). The four general cost activities associated with external consequences (Ponemon, 2012) include:

- Cost of information loss or theft - loss or theft of sensitive and confidential information as a result of a cyber attack.
- Cost of business disruption - the economic impact of downtime or unplanned outages that prevent the organisation from meeting its data processing requirements.
- Cost of equipment damage - the cost to remediate equipment and other IT assets as a result of cyber attacks to information resources and critical infrastructure.
- Lost revenue: The loss of customers and other stakeholders because of system delays or shutdowns as a result of a cyber attack.

As the attack techniques are constantly changing, improving, and perfecting, it is necessary, for the actual calculation of costs, to include all known elements, even if some are not included or explicitly mentioned in the presented models. The authors of the »Measuring the Cost of Cybercrime« model decided not to use the aforementioned Detica (2011) and Ponemon (2012) approach, as they believe »that the second heading includes both, direct and indirect costs« (Anderson et al., 2012: 4), and the third heading consists of direct costs in its entirety. In their model, the authors use a more straightforward approach, which splits direct costs from indirect costs and also includes the costs of security and the social and opportunity costs of reduced trust in online transactions. On the basis of the model's development and the simple and clear presentation of costs, the model defines the following categories of costs according to Anderson et al. (2012):

- Criminal revenue is the monetary equivalent of the gross receipts from a crime. Does not include any 'lawful' business expenses of the criminal.
- Direct loss is the monetary equivalent of losses, damage or other suffering felt by the victim as a consequence of a cybercrime.

- Indirect loss is the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out. Indirect costs generally cannot be attributed to individual victims.
- Defence costs are the monetary equivalent of prevention efforts. They include direct defence costs, indirect defence costs, and opportunity costs caused by the prevention measures.
- The cost to society is the sum of direct losses, indirect losses, and defence costs.

Indirect costs in the field of cybercrime are disproportionately high, because the cost of security technologies, such as firewalls, spam filters, and anti-virus programmes, can amount to a few hundred dollars per year. Therefore, those who are assessing the consequences of cybercrime and the authors who are preparing this kind of model are asking themselves (Anderson et al., 2012: 26): »Why does cybercrime carry such high indirect and defence costs? … We are also starting to understand the behavioural aspects: terrorist crimes are salient because the perpetrators go out of their way to be as annoying as possible, while most online crooks go out of their way to be invisible.« This problem is also interesting from the response to cybercrime point of view. Apparently, previous guidelines, instructions, and directives to fight cybercrime have not led to an appropriate situation or a solution in this field. Apart from the aforementioned costs, other »hidden« costs related to the response to and fight against cybercrime have also been appearing recently. According to Forbes[4], a new trend is observed with respect to the provision of cyber attack insurance coverage to enterprises. The costs of insurance in the USA (Hall, 2014), for instance, amounts to »from 2,500 EUR annually for a small business to millions of EUR for larger companies«. On the other hand, the aspiration to »identify what business resources the company has and how they want to protect them« also represents an important trend. These two aspects describe a relatively new way of responding to cybercrime, which shifts from a traditionally technical response to a response based on organisational measures. One of the contemporary measures for defining resources that an organisation wishes to protect is the introduction of Cyber Resilience programmes (SungardAS, 2014), which, among other factors, detail business risks, a security policy and a testing regime.

On the basis of extensive examination and knowledge of issues related to the protection in cyberspace, premises presented in the Detica and Ponemon models, and the »Measuring the Cost of Cybercrime« model (Anderson et al., 2012) depicted in Figure 2, this paper presents an adapted cost model, which may be used by any organisation in order to adopt its own measures and apply both traditional and innovative approaches and/or models to calculate its own costs related to cybercrime. The same may, by adopting a broader view on the model, be achieved by society, while individual users could, by adapting it to their personal situation, also draw from its benefits.

4 *www.forbes.com*

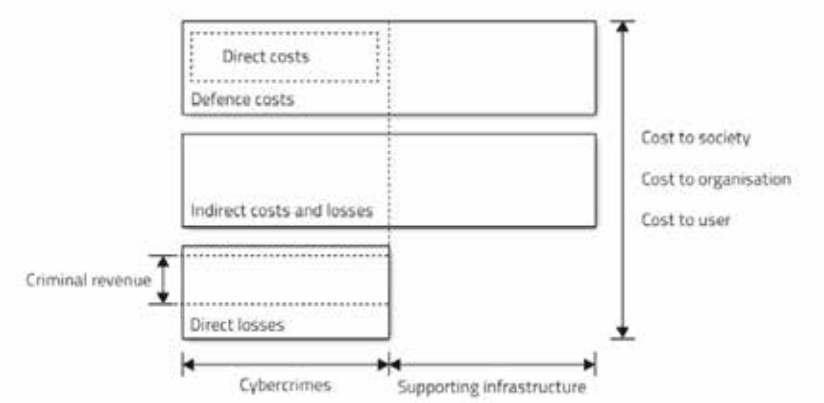

Figure 2: Measuring the cost of cybercrime (modified by: Anderson et al., 2012)

This model presents three principal sources of costs and two main types of monitoring the provision of cyber security, i.e. through the knowledge of cybercrime, as well as through the excellent management of supporting infrastructure. In organisations, direct costs are easily identifiable, as they represent indirect costs of investments into defence. They are, of course, merely a part of comprehensive defence costs, as described above. Indirect costs and losses are incurred due to the impacts of cybercrime and arise from external and internal environments. Direct losses consist of organisations' losses, which represent indirect gross receipts from a crime and losses due to the payment of compensations, court proceedings and defence lawyers' fees that arise as a consequence of data losses.

On the basis of the model and structure of costs and losses, impacts of cybercrime and investments into supporting infrastructure, such costs can actually be evaluated financially. The knowledge of costs enables companies to manage such costs and adopt appropriate measures, which, in the long run, guarantee higher levels of cyber security and better resilience to cybercrime.

4 DISCUSSION AND CONCLUSIONS: DO WE NEED TO THINK ABOUT COSTS?

The models for calculating costs caused by cybercrime, which were presented above, as well as other models, do not show the entire breadth of the problem. The main problem lies in users' dependence on cyber infrastructure and their need for interacting with cyberspace.

In order to guarantee successful performance of an organisation's business operations, it is vital to consider which investments into the protection of cyber infrastructure should be prioritised. Such protection is absolutely necessary and the majority of organisations should also invest much more intensively into organisational approaches aimed at providing protection and security. In addition, a lot of room for improvement is also observed with respect to the raising of organisational culture and awareness of employees regarding

their attitude to and perception of work performed in cyberspace, appropriate identification of threats and a conservative approach towards the level of trust awarded to information exchange. By achieving these objectives, employees could develop personal protection mechanisms, which would have a minimum impact on decreasing the functionality of information and communication systems and significantly contribute to a higher level of security.

Technical protective mechanisms, if these are to be used in a comprehensive and therefore effective way, reduce the functionality and limit normal work. On the basis of the types of costs presented above, the review of research regarding significant losses due to cybercrime, and the realities of modern cybercrime, one cannot but agree with the following statement made by Anderson et al. (2012: 26): »Indeed, the crooks are simply being rational: while terrorists try to be as annoying as possible, fraudsters are quite the opposite and try to minimise the probability that they will be the targets of effective enforcement action.« Do individuals, organisations, and countries cope adequately with the problem of cybercrime and do invested time and money achieve their purpose? It can certainly be established that this is often not the case. In fact, many studies demonstrate (e.g. Ponemon, 2012, 2013; Norton, 2013) that cybercrime costs continue to rise. Therefore, in order to effectively cope with the ever increasing phenomenon of cybercrime and ever more aggressive attacks by modern cybercrime offenders, who mostly work internationally, it is necessary to ensure the quality of international cooperation within institutions and through relevant legal acts, and the implementation of the agreed and applicable international law in order to successfully prosecute crime, take the perpetrators to court and sanction them accordingly. However, this would have to be a topic of further discussions and research, expressions of political motives and the future development of cybercrime.

REFERENCES

Alperovitch, D. (September 1, 2011). *Revealed: Operation shady RAT.* Santa Clara: McAffe. Retrieved from http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

Anderson, R., Bohme, R., Clayton, R., & Moore, T. (January 31, 2008). *Security economics and the internal market*. Retrieved from http://www.enisa.europa.eu/publications/archive/economics-sec/at_download/fullReport

Anderson, R., Barton, C., Boehme, R., Clayton, R., van Eeten, M. J. G., Levi, M., et al. (June 25, 2012). *Measuring the cost of cybercrime.* 11th Annual Workshop on the Economics of Information Security, WEIS 2012. Retrieved from weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Anderson, R., Barton, C., Boehme, R., Clayton, R., van Eeten, M. J. G., Levi, M., et al. (2013). Measuring the cost of cybercrime. In R. Boehme (Ed.), *The economics of information security and privacy* (pp. 265–300). Berlin Heidelberg: Springer.

Ashford, W. (October 8, 2013). Cyber crimes costs UK businesses average of £3m per year. *Computer Weekly.* Retrieved from http://www.computerweekly.com/news/2240206865/UK-average-cyber-crime-cost-up-to-3m-a-year

Bernik, I., & Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.

Bernik, I., & Prislan, K. (2013) Cybercrime in Slovenian enterprises. In G. Meško, A. Sotlar, & J. R. Greene (Eds.), *Criminal justice and security - contemporary criminal justice practice and research: Conference proceedings* (pp. 423–441). Ljubljana: Faculty of Criminal Justice and Security.

Cost per cybercrime victim up 50 per cent: Norton Report [Web log post]. (November 22, 2013). *The Nation.* Retrieved from http://www.nationmultimedia.com/technology/Cost-per-cybercrime-victim-up-50-per-cent-Norton-R-30220318.html

Detica. (February 17, 2011). *Detica and office of cyber security and information assurance: The cost of cyber crime*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

Hall, C. (March 20, 2014). The hidden cost of cyber crime. *Forbes.* Retrieved from http://www.forbes.com/sites/sungardas/2014/03/20/the-hidden-cost-of-cyber-crime/

Krebs, B. (February 10, 2014). *Experts warn of coming wave of cybercrime*. Retrieved from http://www.securitymagazine.com/articles/85220-experts-warn-of-coming-wave-of-cybercrime

McAfee. (July 22, 2013). *The economic impact of cybercrime and cyber espionage*. Retrieved from http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf

The National Bereau of Asian Research. (2013). *The IP commission report: The report of the Commission on the Theft of American Intellectual Property*. Retrieved from http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf

Norton. (October 1, 2013). *2013 Norton report*. Retrieved from http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

Ponemon. (2011). *Second annual cost of cyber crime study: Benchmark study of U.S. companies*. Michigan: Ponemon Institute.

Ponemon. (October 8, 2012). *2012 cost of cyber crime study: United States*. Retrieved from http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

Ponemon. (October 11, 2013). *2013 cost of cyber crime study reports*. Retrieved from http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports

SOCTA. (March 19, 2013). *EU serious and organised crime threat assessment*. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf

SungardAS. (January 15, 2014). Why cyber security is not enough: You need cyber resilience. *Forbes.* Retrieved from http://www.forbes.com/sites/sungardas/2014/01/15/why-cyber-security-is-not-enough-you-need-cyber-resilience/

United Nations Office on Drugs and Crime. (April 8, 2010). *Cybercrime*. Retrieved from http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, *26*(2), 107–124.

About the Author:

Igor Bernik, Ph.D., Assistant Professor of Information Sciences and the head of the Information Security Department at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research fields are information systems, information security, and the growing requirements for information security awareness.