Editorial

Once again, the *Journal of Criminal Justice and Security* is publishing an English language issue, and as Associate Editor for English Issues for the Journal, it is our honour and pleasure to introduce it to you and the rest of the academic and practitioner communities who have interests in the subject dealt with here.

While this issue is not a thematic issue, most of the articles in this edition deal with corporate and information security and cybercrime. The contributions here are of much contemporary interest, as current research points to enormous financial losses suffered by countries, organisations and individuals due to the impact of criminal offences committed in cyberspace. Practitioners in the field of cyberspace security find that increasing awareness is a much more efficient and inexpensive method of protection enabling a higher level of security in cyberspace and in the corporate world. Another of the articles addresses the field of video surveillance and corporate security in companies in Slovenia, and outlines the basic principles, the reasons for their use and the consequences for the companies affected. The remaining articles are very eclectic and timely, and provide excellent examples of the types of current research taking place in the former Yugoslav Republics.

The authors of the respective articles and Journal Editors hope the following contributions are found to be both interesting and educational to you the reader.

Chuck Fields & Gorazd Meško

Associate Editors of English Issues

Uvodnik

Odgovorna urednika angleških številk revije Varstvoslovje z veseljem predstavljava tokratno številko revije akademski in strokovni javnosti.

Kljub temu da številka ni tematska, večina prispevkov obravnava področje korporativne in informacijske varnosti ter kibernetske kriminalitete. Tema je zelo aktualna, saj trenutne raziskave ugotavljajo, da zaradi kaznivih dejanj v kibernetskem prostoru prihaja do ogromne finančne škode za države, organizacije in posameznike. Strokovnjaki s področja informacijske varnosti poudarjajo, da je visoka stopnja osveščenosti uporabnikov najcenejši in najbolj učinkovit način zagotavljanja informacijske in korporativne varnosti. Eden od prispevkov predstavlja osnovna načela in vzroke za uporabo videonadzora v slovenskih podjetjih z vidika korporativne varnosti. Ostali članki v tej številki pa prinašajo odlične primere raziskav s področja bivših jugoslovanskih republik.

Avtorji izbranih člankov in uredniki revije upamo, da bodo pričujoči prispevki zanimivi in poučni za bralce.

Chuck Fields in *Gorazd Meško*

Odgovorna urednika angleških številk revije

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.«

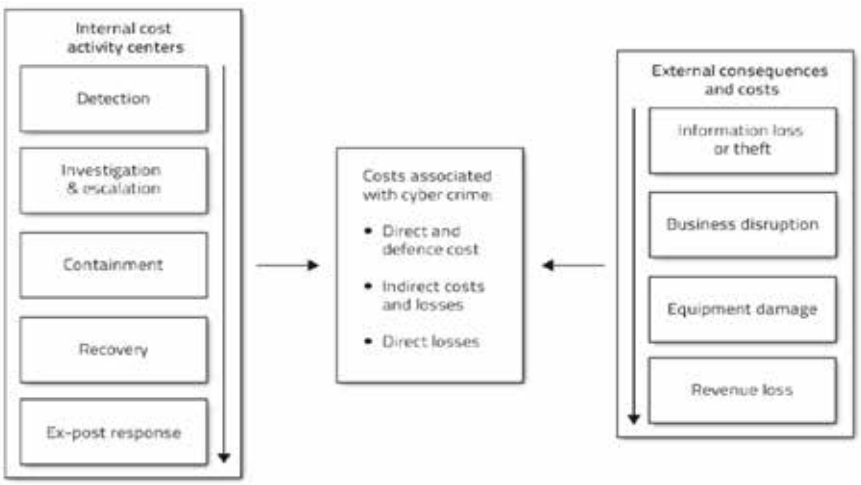


Figure 1: Cost framework for cybercrime (source: Ponemon, 2012: 23)

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*

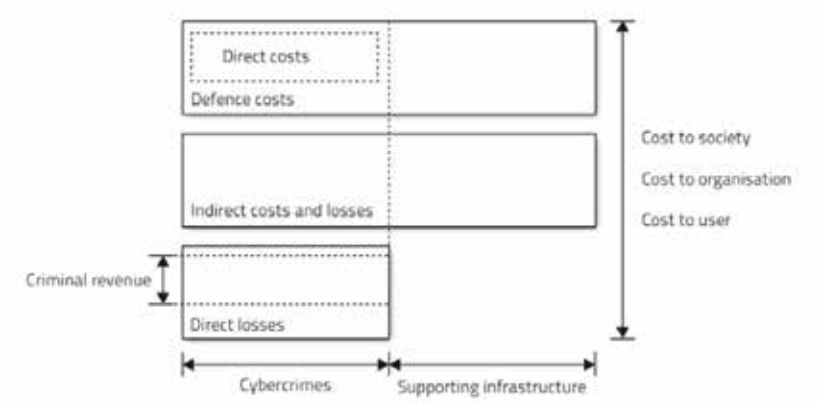


Figure 2: Measuring the cost of cybercrime (modified by: Anderson et al., 2012)

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.

VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 16 no. 2 pp. 117–127

Information Security Related to the Use of Mobile devices in Slovene Enterprises

Blaž Markelj, Igor Bernik

Purpose:

In the business world, mobile devices represent an important tool for carrying out one's work. By providing the possibility to have constant access to different types of data and information, such devices are an important element in the decision-making process. The access to necessary data at any given moment in the decision-making process represents a competitive edge in the business environment. However, despite all of the advantages provided by mobile devices, their users fail to consider the issue of information security, since the access to and transfer of information via mobile devices makes them vulnerable to security risks. The media report on numerous new threats that put mobile devices at risk on a daily basis. The realisation of such threats to information security becomes more likely when users use mobile devices carelessly and simultaneously fail to use adequate security protection. It is therefore important for organisations and experts responsible for the safe use of mobile devices to introduce appropriate technical and organisational solutions and measures for the safe use of such devices.

Design/Methods/Approach:

Conclusions are based on descriptive findings and results of a study conducted among the staff of different Slovene organisations, who are responsible for the safe use of mobile devices by employees.

Findings:

Users of mobile devices in different organisations use their devices both for private as well as for business purposes, and the use of such devices gives them a competitive edge in the business world. Results of a study conducted in 34 Slovene organisations demonstrate that these organisations are currently in the initial stages of introducing both technical and organisational solutions, and measures for the provision of information security related to the use of mobile devices among their employees. According to the findings, the use of regulations and standards, which would define the safe use of mobile devices in relevant organisations, is rare. In mobile devices, the boundary between personal and business data has disappeared completely. The use of mobile devices must, therefore, follow the information security recommendations and provide adequate protection of data accessible to users.

Research Limitations/Implications:

The topic discussed in this paper remains a sensitive issue for different organisations, which is why conducting the study was rather challenging. The number of existing research efforts in this field is limited, and consequently, there are very few grounds that could serve as the basis for the performance of the aforementioned research.

Practical Implications:

Results show the manners in which mobile devices are used and protected against threats. On the basis of these results, organisations could seek ways to improve their methods for the protection of mobile devices and increase the level of protection awarded to their information systems.

Originality/Value:

Work conducted in the field of mobile devices is original and deals with the issues presented hereby in an innovative manner.

UDC: 004.056:[004.382.75+621.395.721.5]

Keywords: mobile devices, threats, security, organisations, Slovenia

Informacijska varnost ob rabi mobilnih naprav v slovenskih podjetjih

Namen prispevka:

Mobilne naprave so v poslovnem svetu pomemben delovni pripomoček. Z možnostjo neprestane povezave do podatkov tovrstne naprave predstavljajo pomemben element v procesu odločanja. Dostop do potrebnih podatkov v trenutku odločanja v poslovnem svetu pomeni konkurenčno prednost. Poleg vseh prednosti, ki jih mobilne naprave ponujajo, pa uporabnik malo razmišlja o informacijski varnosti, saj z dostopanjem in prenosom informacij z mobilnimi napravami le-te izpostavljamo varnostnim tveganjem. V medijih vsakodnevno beremo o številnih novih grožnjah, ki pretijo omenjenim napravam, kar pa ob uporabnikovi nevestni rabi in hkratni neuporabi varnostnih zaščit predstavlja verjetnost za uresničitev groženj informacijski varnosti posameznika in/ali organizacije. Zato je pomembno, da organizacije in strokovnjaki, ki so zadolženi za varno rabo mobilnih naprav, vpeljejo ustrezne tehnične in organizacijske rešitve in ukrepe za varno rabo mobilnih naprav.

Metode:

Ugotovitve temeljijo na deskriptivnih dognanjih in izvedenih raziskavah med strokovnjaki v slovenskih organizacijah, ki so odgovorni za varno rabo mobilnih naprav med zaposlenimi.

Ugotovitve:

Uporabniki mobilnih naprav v različnih organizacijah uporabljajo mobilne naprave tako v zasebne kot v poslovne namene, njihova raba pa predstavlja kokurenčno prednost v poslovnem okolju. Rezultati raziskave, izvedene v 34 slovenskih organizacijah, kažejo, da so organizacije v začetnih fazah

uvajanja tako tehničnih kot organizacijskih rešitev in ukrepov za vzpostavitev informacijske varnosti ob rabi mobilnih naprav med zaposlenimi. Uporaba pravilnikov in standardov, ki bi opredeljevali varno rabo mobilnih naprav v organizacijah je redkost. Pri tem pa je meja med osebnimi in poslovnimi podatki na mobilnih napravah popolnoma izginila, zato je pri njihovi rabi nujno slediti informacijskovarnostnim priporočilom in zagotoviti ustrezno zaščito podatkov, do katerih imamo dostop.

Omejitve/uporabnost raziskave:

Tematika, obravnavana v prispevku, je za organizacije občutljive narave, zato je bila izvedba raziskave zahtevna. Tovrstnih raziskav je malo, zato ni veliko osnov, na katere bi se oprli pri izvedbi predstavljene raziskave.

Praktična uporabnost:

Rezultati raziskave kažejo načine rabe mobilnih naprav in zavarovanja le-teh pred grožnjami. Na podlagi rezultatov organizacije lahko pristopijo k izboljšanju načina varovanja mobilnih naprav in dvigu zaščite informacijskih sistemov.

Izvirnost/pomembnost prispevka:

Predstavljeno delo na področju rabe mobilnih naprav je originalno in na izviren način obravnava predstavljeno problematiko.

UDK: 004.056:[004.382.75+621.395.721.5]

Ključne besede: mobilne naprave, grožnje, varnost, organizacije, Slovenija

1 INTRODUCTION

We all live in a period in which one is assumed and expected to make business decisions at any given moment. In this respect, it is of key importance for one to have constant access to business information. Mobile devices[1] enable users in different organisations to be flexible, efficient and respond rapidly. Various networks (Wi-Fi, UMTS, LTE, etc.) allow users to access information pertaining to their organisations, which are stored in a central information system or in a cloud, from anywhere in the world. Some organisations have developed special applications for mobile devices that provide their employees with easy access to the information they need for the performance of their work. The authors of the *IT Spending Priorities Survey 2012*, which saw the participation of 453 information technology experts, attempted to identify projects into which their companies would invest in the following year. A scale of priority projects was then produced. A project related to investments into mobile applications was put

1 *Mobile devices primarily include devices that use adaptive operating systems, such as iOS, Android, BlackBerry OS or Windows mobile, and are portable (mobile phones, tables, etc.). This category may also contain all devices, which are portable and enable internet access without a physical connection (laptops and other portable computers, game consoles, industrial scanners, etc.), while the group of mobile phones includes both mobile phones intended solely for making phone calls and sending or receiving SMS messages, as well as smart phones, which represent a contemporary communication device, since they not only allow for making phone calls via mobile networks, but also provide a whole range of additional functions similar to those of a PC.*

high on the priority scale (seventh place; 11 percent), while respondents placed a project involving the creation of a central system of control over mobile devices (MDM) on the ninth place (8 percent). The research clearly demonstrated that organisations are extremely interested in investing into mobile devices (Feldman, 2012), which is quite understandable, as trends that have already been observed since 2011 show that the scope of mobile business will increase by 30 percent by 2013 (Mulpuru, Evans, Sehgal, Ask, & Roberge, 2011). This share has been increasing consistently, and in addition, software used in mobile devices has been developing at an extremely rapid pace (Hurlburt, Voas, & Miller, 2011; Oppenheim, 2010), with the purpose to attract the users (Greene, Tamborello, & Micheals, 2013) and increase sales. However, users tend to overlook the dangers they are exposed to in cyberspace when using mobile devices. At the same time, they do not provide for the protection that would enable them to avoid the pitfalls present in cyberspace. This is also supported by the Ponemon Institute's (2012) research dedicated to the identification of risks generated in organisations and posed by mobile devices and information infrastructure used by end users. Seventy percent of respondents stated that mobile devices pose the highest risk for the security of information technology and systems in organisations. The aforementioned research also contains a historical comparison of data, which shows that the same response was provided by a mere 9 percent of respondents in 2010 and 48 percent in 2011. The second most important risk in the 2012 research was attributed to mobile applications of unknown origin (67 percent of respondents), which clearly indicates the continuous increase in the number of those who do not perceive mobile devices merely as a means of but also as a threat (security risk) to information technology.

Mobile devices may become targets of software and applications, which are installed in the device in an uncontrolled manner, such as malware and other threats (e.g. spyware, botnets, Bluetooth connection and contamination originating in online social networks (Leavitt, 2011)). The Juniper Networks Report (2011) shows that 85 percent of users have ineffective mobile phone protection, as (some) manufacturers of software for mobile devices allow for the installation of the so-called »back door«, which enables them to manage software settings on a mobile device without the users' knowledge, obtain data regarding location, which are automatically submitted by the mobile device (e.g. GPS location), or take control over the mobile device, etc. These trends were also confirmed in the 2013 Report (Juniper Networks, 2013), which was compiled on the basis of a one-year continuous monitoring of the development and occurrence of threats to mobile devices and demonstrated that the quantity of malware has increased by 614 percent between March 2012 and March 2013. The lack of knowledge related to the functioning of mobile devices' software and different functionalities that it provides cause users to become targets of cybercrime. The awareness of threats and their implications, which may put the users of mobile devices at risk, is also important in order to become aware of the need to provide sufficient cyber security.

In order to determine the actual state-of-affairs in this field, the authors of this paper conducted a study of Slovene organisations, during which the persons responsible for the safe use of mobile devices among employees were asked

about the manners in which their employees use mobile devices and the methods applied to provide information security. The objective of the research was to obtain information about the possibilities of introducing and using different technical and organisational protective measures related to the use of mobile devices among employees of individual organisations.

2 METHODS

The research was conducted through interviews, with representatives (responsible for the safe use of mobile devices) of 34 organisations completing a questionnaire via e-mail. Twenty-two completed questionnaires were (also via e-mail) sent back to the researchers. When devising open-ended leading questions (19 questions), the researchers followed theoretical premises related to the use of mobile devices, thus stimulating individual respondents to share their experience in and views on the use of mobile devices in their organisations.

Since the research was dedicated to the ways of conducting security-related activities and formal responsibility, the aim of the researchers was to verify *who was in charge of mobile devices in an organisation and was thus formally responsible (for their security, the selection of models, education and training, etc.)*. Responsibilities in the field of mobile devices were most often (40.9%) assumed by ICT departments (information and communication technologies), which is reasonable, as they are familiar with the structure of the IS (information system) and the storage of data, the provision of security and the structure of their organisations. In 31.8 percent of organisations included in the research, several departments within the organisation are in charge of mobile devices (IT department, security department, head of information security and protection, etc.). Organisations are aware of broader issues related to the complexity of the provision of information security for mobile devices and strive to fully meet security criteria in this field, which is why they often involve several departments specialised in different fields of expertise. In 9.1 percent of these organisations, persons in charge of mobile devices work in departments responsible for quality assurance and projects or in general affairs departments. 18.2 percent of organisations leave the responsibility for mobile devices to the employees themselves or do not dedicate any particular attention to this issue. The ways in which organisations provide for the security of devices are presented below.

3 RESEARCH

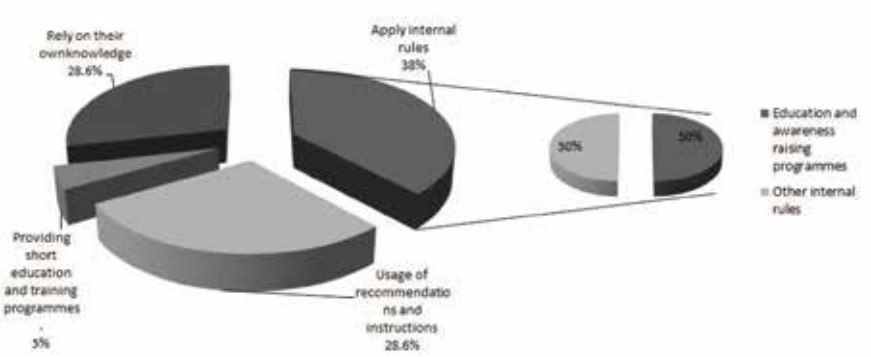
Information regarding the methods used for providing security were obtained by posing the following question: *How does your organisation arrange for the safe use of mobile devices (e.g. regular education and training programmes for users, introduction of standards, etc.)?* Responses were grouped to reflect the following four groups of organisations, which:

- provide for the safe use of devices through security policies and internal rules,
- implement instructions and recommendations to guarantee security,

- raise the security awareness of users by providing education and training, and
- leave security related activities in the hands of individuals without exercising any type of control and are not aware of the threats to information systems and the integrity of data generated by the use of mobile devices.

Researchers also observed the formation of a group of organisations, which do not only use internal rules and regulations but also provide education and awareness raising programmes for users, thus providing adequate measures for the safe use of mobile devices. The above question was answered by 21 organisations (n = 21) as shown on Figure 1.

Figure 1: How does your organisation arrange for the safe use of mobile devices (e.g. regular education and training programmes for users, introduction of standards, etc.)?



This means that 38.6 percent of organisations, i.e. 8 organisations, apply internal rules defining the use of mobile devices. At the same time, 4 (50%) organisations (from 8 organisations) also provide their employees with education and awareness-raising programmes for the safe use of mobile devices in addition to the implementation of internal rules. The group of organisations, which define the use of mobile devices through recommendations and instructions, is composed of 6 organisations. One organisation guarantees the safe use of mobile devices among their employees merely by providing short education and training programmes. Six organisations have not (yet) devised a systematic method for the use of mobile devices, which is why their employees are left to their own devices and have to rely on their knowledge regarding appropriate conduct.

Responses to the next question: *What kinds of procedures does your organisation apply to allow users to use their own mobile devices for work purposes and access to the business environment?* fall within two groups. The first group is composed of 16 organisations (72.8%) that apply a particular procedure defining the use of users' own mobile devices. The second group consists of 6 organisations (27.2%), which do not allow users to use their own mobile devices for work purposes and consequently do not apply any specified procedures to this end. The ways in which an organisation may prescribe the use of users' own devices for access to business systems can be of a technical (a mobile device becomes part of the MDM or MAM tools used in an organisation) (Goldman, 2012) or an organisational nature. MDM tools (Mobile Device Management) focus on exercising control over a mobile

device as a whole (Citrix, 2014; Kwon & Kim, 2013), while MAM tools (Mobile Application Management) control a mobile device on the level of individual applications (Keen, 2013; Murray, 2012). The exercise of control depends on the introduction of organisational measures and adequate rules defining the use of mobile devices in an organisation and prescribing procedures for their use, including or primarily in terms of security solutions.

In order to ascertain whether organisations regulate the use of mobile devices by adopting specific acts, respondents were asked the following question: *Does your organisation have any specific rules concerning the safe use of mobile devices? Which security elements do they contain?* Four (18.2%) organisations adopted rules regulating the safe use of mobile devices, but on the other hand, the fact that 18 (81.8%) organisations do not apply and rules regarding the safe use of mobile devices raises serious concern.

The level of awareness and the implementation of cyber security procedures were ascertained by posing the following question: *How does your organisation raise awareness of users regarding the safe use of mobile devices? Please list the methods and evaluate the time spent for implementing an individual method.* This question was answered by 21 respondents (n = 21). One organisation has never conducted education or training courses for its employees, while 20 organisations responded that they train and raise awareness of their employees regarding the safe use of mobile devices in different ways, e.g. through different memos and information provided via their intranet and internet sites, by organising training programmes for groups of employees or by providing training courses for individuals when these receive a new mobile device, etc. The time organisations dedicate to such education and training activities differs significantly, ranging from 15 minutes per month, three hours per year, one day per year or even two days per month (when this research was conducted, some organisations were in the middle of an intense process for the provision of a higher level of security of their mobile devices). Naturally, the quantity of education and training activities also depends on individual employee's position in the organisation and/or the general provision of cyber security and educational methods (individual or group training, education via the internet, etc.).

When analysing responses to the question regarding procedures applied in case of abuse *(What kind of procedures does your organisation foresee in the event of abuse of information sources via users' mobile devices?)*, the situation varies greatly. Two organisations (9.1%) have not defined any procedures for dealing with abuse, while others (90.9%) would initially consider such abuse as a security incident and then take appropriate steps in line with policies, instructions or guides to good practice adopted by their organisations. They would most often inform the person responsible for security incidents in the organisation, followed by the implementation of a standard procedure foreseen in such cases. None of the organisations concerned has adopted a special procedure to be applied in the event of an abuse of information sources via mobile devices. This means that they use general rules related to security incidents. In the event of abuse, only one organisation would act in line with the legislation and internal rules, and would simultaneously report the incident to the police.

The aim of the following question: *What kinds of responsibilities and powers are attributed to the users of mobile devices?* was to ascertain whether organisations encourage users to use mobile devices in a safe manner, provided they previously attended adequate education and training courses. Some organisations define the responsibility of mobile devices' users in the framework of other rules and regulations (e.g. access to different types of information, password handling and management, handling of computer hardware and software, etc.), while others use general provisions concerning responsibility.

4 DISCUSSION

In organisations, the responsibility for the safe use of mobile devices is mostly attributed to a person who is in charge of information security and, at the same time, possesses appropriate competences and knowledge required to deal with mobile devices. This task combines different aspects that have to be included in order to meet the criteria for the safe use of mobile devices. Those organisations, which provided such a response, are aware of the breadth and complexity of the issue. In some organisations, the safe use of mobile devices is entrusted to those persons or departments that have no background in the field of information security, which is why it is difficult to predict how exactly do they manage to perform their regular daily tasks and simultaneously deal with the rapidly developing/changing and ever more complex field of mobile device security. One may even ask whether they possess adequate knowledge and skills required to do so. With respect to the safe use of mobile devices, the share of organisations (28.6%), in which the manner of using mobile devices and handling data is left to individual users, who may apply completely different practices, which results in an array of methods and ways of using mobile devices within an individual organisation, is alarming. At the same time, one may ask what is the level of knowledge they possess, if any, regarding the safe use of mobile devices. Other groups of organisations are currently developing procedures, which is why it is expected that this field will (mostly) be appropriately regulated in the future.

Procedures allowing the use of one's own mobile device for work or business purposes are defined in an organisations' internal rules, and such procedures are mostly specifically defined. Procedures are initially most often conducted by adopting the view that users may use their own mobile device(s) for work purposes, while the adequate application form is processed by a person responsible for security at a later stage. The responsible person considers the authorisation for and the extent of the use of a device, the implementation of protective measures and security features, and the access to information on the basis of defined methods and criteria that have to be met in order for the user to be able to use a personal mobile device for work or business purposes. Rules that define the safe use of mobile devices mostly contain the following sections:

- steps to be taken in the event of a loss or theft of a mobile device,
- conduct in the event of accessing the internet via public hotspots,
- safe access to the organisation's information system.

None of the organisations involved in the research stated that their internal rules contain a provision which would ban or restrict the use of software that has not been authorised by the organisation concerned. This represents a serious deficiency given the vast amount of different software applications that are accessible via mobile devices and are often the cause of information loss (Josyula, 2013). It is, therefore, vital to take this into account and complement existing internal rules with a section which would contain a detailed breakdown of individual rules and measures, in order to provide for a suitable level of cyber security. With respect to the methods used to raise awareness of users regarding the safe use of mobile devices and cyber security, researchers find that education and training activities are mostly conducted via e-mail memos or information provided via internet sites. Such memos and information are mostly of a general nature, while some organisations occasionally inform their employees about threats when they come across reports about the increased level of threats, and consequently the amount of security incidents, via the internet or in the media. All organisations agree that rules and standards contribute to an increased safety of processes in the organisation, but they add that there is a lot of room for improvement in the field of general awareness raising among users with respect to cyber security, threats and consequences of mobile devices' abuse. In addition, individual elements defined in standards and rules should be more consistently implemented. In case organisations detect the abuse of information sources via a mobile device, they mostly adhere to the prescribed general procedure for security incidents, which is most often conducted through the following steps:

- report of the incident to the responsible person,
- opening of the security incident document,
- identification of the cause and its remedy,
- identification of consequences and their evaluation,
- damage assessment, and
- potential sanctions, provided that these were previously defined and are justified from the point of view of other circumstances affecting the situation.

It is vital to complement the above procedure with actions stemming from internal acts, which are implemented and in line with the legislation, and with the need to report incidents to national authorities, such as the Slovene Computer Emergency Response Team (SI-CERT) and the Police or the national cyber security centre, where such centre exists (a proposal concerning its establishment is currently being discussed in the Republic of Slovenia). Organisations, apart from those that have explicitly defined the provisions related to authorisations and responsibilities, generally do not define any specific provisions, which means that general rules apply for all users of mobile devices.

The responsibility for the safe use of mobile devices and the manner in which these are used are often left in the hands of individual users and their own judgment regarding the sound management of devices and processes. At the same time, organisations presume (often erroneously) that users are aware of security concerns. However, given the trends related to the increasing growth in the number of threats and ever more complex requirements for maintaining a sufficient level

of information security, this is simply unacceptable. Information security of an individual organisation is as strong (protected) as its weakest link, i.e. the user of a mobile device, the device itself, and the access to the comprehensive information system of an organisation. It is, therefore, inappropriate to leave decision-making regarding information security to individual users of mobile devices, who mostly do not possess adequate knowledge and are not willing to encroach upon their own rights for the sake of information security. Decisions regarding information security must be taken by the organisation and persons, who possess adequate knowledge, while the rules regarding the safe use of mobile devices must be introduced into the organisational environment through internal rules and standards.

REFERENCES

Citrix. (2014). *XenMobile*. Retrieved from http://www.zenprise.com/solutions/MDM

Feldman, J. (April 30, 2012). Research: 2012 IT spending priorities survey. *InformationWeek*. Retrieved from http://reports.informationweek.com/abstract/83/8816/it-business-strategy/research-2012-it-spending-priorities-survey.html

Goldman, C. (2012). *What's the difference between MAM and MDM?* [Video]. Retrieved from http://www.apperian.com/mam-mdm/

Greene, K. K., Tamborello, F. P., & Micheals, R. J. (2013). Computational cognitive modeling of touch and gesture on mobile multitouch devices: Applications and challenges for existing theory. In M. Kurosu (Ed.), *Human-computer interaction: Interaction modalities and techniques* (pp. 449–455). Heidelberg: Springer.

Hurlburt, G., Voas, J., & Miller, K. W. (2011). Mobile-app addiction: Threat to security? *IT Professional, 13*(6), 9–11.

Juniper Networks. (2011). *Malicious mobile threats report 2010/2011*. Retrieved from http://www.juniper.net/us/en/dm/interop/go

Juniper Networks. (2013). *Juniper Networks third annual mobile threats report.* Retrieved from http://www.juniper.net/us/en/local/pdf/additional-resources/3rd-jnpr-mobile-threats-report-exec-summary.pdf

Josyula, R. (2013). Application security in mobile devices using unified communications. V N. Meghanathan, D. Nagamalai, & N. Chaki (Eds.), *Advances in computing and information technology* (pp. 135–143). Berlin: Springer.

Keen, M. (January 10, 2013). *Got MAM (mobile application management) in your 2013 mobile menu?* Retrieved from https://www.ibm.com/developerworks/mydeveloperworks/blogs/mobileblog/entry/got_mam_mobile_application_management_in_your_2013_mobile_menu25?lang=en

Kwon, H., & Kim, S. H. (2013). Efficient mobile device management scheme using security events from wireless intrusion prevention system. In Y. H. Han, D. S. Park, W. Jia, & S. S. Yeo (Eds.), *Ubiquitous information technologies and applications* (pp. 815–822). Dordrecht: Springer.

Leavitt, N. (2011). *Mobile security: Finally a serious problem?* Largo: University of Maryland. Retrieved from http://www.computer.org/portal/web/computingnow

Mulpuru, S., Evans, P., Sehgal, V., Ask, J. A., & Roberge, D. (July 17, 2011). *Mobile commerce forecast: 2011 to 2016.* Retrieved from http://www.forrester.com/Mobile+Commerce+Forecast+2011+To+2016/fulltext/-/E-RES58616?objectid=RES58616

Murray, A. (June 5, 2012). *Mobile application management (MAM) has put MDM in its place.* Retrieved from http://www.networkworld.com/news/tech/2012/060512-mam-mdm-259877.html

Oppenheim, R. (2010). *The App in the haystack: Steps to finding useful and usable Apps.* Retrieved from http://www.highbeam.com/doc/1G1-245168524.html

Ponemon Institute. (2012). *2013 state of the endpoint.* Traverse City: Ponemon Institute. Retrieved from http://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf

About the Authors:

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.

Blaž Markelj, Lecturer of Information Science at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research interests include blended threats to mobile devices and information security.

VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 16 no. 2 pp. 128–147

Efficiency of Corporate Security Systems in Managing Information Threats: An Overview of the Current Situation

Kaja Prislan

Purpose:

Information security should be a strategic goal of every responsible and safety-conscious organisation that wants to follow current security and technological trends. The purpose of this paper is to summarize the corporate practices in addressing IT risks, to explain the benefits of a comprehensive approach to information security as a business function, and to improve understanding of the current issues associated with its management.

Design/Methods/Approach:

Topics presented in this paper were analysed using descriptive and qualitative analysis of international reports and surveys. The findings obtained using the comparative method and their synthesis are supported by other research in this area.

Findings:

Due to the large volume of information assets, sophisticated IT threats and the heterogeneous nature of security factors, the efficiency of information security is very difficult to achieve. It has been observed that many organisations are at an early stage in developing a comprehensive approach to information security, since, in practice, they are still dealing with the problems of the past, yet they are very consistent with tracking user trends. This disproportionate situation represents a major security challenge for an organisation's management.

Practical Implications:

The findings of this research are useful for the further analysis and evaluation of information security and victimization of cybercrime, and are also applicable to facilitating strategic planning and decision making.

Originality/Value:

Based on the review of the current corporate state, this paper presents baseline information and security situations in the business environment and evaluates the efficiency of information security as a business tool. Based on the results, contemporary security challenges and organisational guidelines for the future were identified.

UDC: 004.056

Keywords: information security, corporate security, efficiency, management, security challenges

Učinkovitost sistema korporativne varnosti pri upravljanju informacijskih groženj: pregled trenutnega stanja

Namen prispevka:

Informacijska varnost mora biti cilj vsake organizacije, ki želi odgovorno slediti tehnološkim trendom. Namen prispevka je analizirati prakso organizacij pri soočanju z informacijskimi tveganji, pojasniti prednosti celovite ureditve informacijske varnosti kot poslovne funkcije in izboljšati razumevanje aktualnih problemov, povezanih z njenim upravljanjem.

Metode:

Uporabljena je deskriptivna metoda in vsebinska analiza mednarodnih poročil in raziskav, povezanih z informacijsko varnostjo. Ugotovitve pridobljene s komparativno metodo in zaključki so podprti z drugimi strokovnimi viri.

Ugotovitve:

Zaradi velikega obsega informacijskega premoženja, sofisticiranih informacijskih groženj in heterogene narave varnostnih dejavnikov je učinkovitost informacijske varnosti težko uresničljiv cilj. Ugotavljamo, da je veliko organizacij pri celoviti obravnavi informacijske varnosti šele na začetni stopnji, saj se v praksi podjetja še vedno ukvarjajo z zastarelimi problemi, medtem ko je sledenje uporabniškim trendom zelo aktualno. Takšno stanje predstavlja velik izziv za management organizacij.

Praktična uporabnost:

Ugotovitve prispevka so uporabne na znanstveno-raziskovalnem področju oz. ravni analiziranja in ocenjevanja informacijske varnosti, viktimizacije ter upravljavskem nivoju, za lažje strateško načrtovanje in sprejemanje odločitev.

Izvirnost/pomembnost prispevka:

Prispevek s pregledom stanja predstavlja izhodiščno informacijskovarnostno situacijo v poslovnem okolju in podaja oceno razvitosti ter učinkovitosti informacijske varnosti kot poslovne funkcije. Na podlagi analize rezultatov so identificirani tudi sodobni varnostni izzivi in organizacijske smernice za prihodnost.

UDK: 004.056

Ključne besede: informacijska varnost, korporativna varnost, učinkovitost, upravljanje, varnostni izzivi

1 INTRODUCTION

The widespread availability of electronic devices and global connectivity are changing the concepts of social life and business operations. The success of our personal and professional life depends on the information available, on which we base our decisions. However, due to information overload, we are not able to make rational decisions without the use of electronic devices which make it possible to collect and process the information. On the one hand, contemporary information and communication technology [ICT] has made it easier to meet some basic human needs, such as maintaining social life, acquiring knowledge, being informed and productive, etc. On the other hand, it has entirely shaken the foundations of some basic assumptions about security and capability of maintaining social order as well as national security. According to Bernik (2014), military, political and economic powers that create a stairway to success of societies have become dependent on information power and information advantage.

Business entities have also followed the trend of changing power and concepts of success. Consequently, organisations are not able to cope with the rapid business pace and changes without the use of electronic devices and the internet. In order to operate successfully in times of aggressive competition, they must prove flexible, innovative and be able to develop production processes. Therefore, the organisations seek to update existing ICT and extend the amount of information they manage. That improves business operations, though it poses serious information security risks at the same time. Expert discussions and information security studies presented in this paper increasingly emphasize that cybercrime is becoming more organised and focused on the big-data environments.[1] In comparison to the conventional types of deviant behaviour, this kind of crime threatens business security in a different way. Before the exponential development and widespread use of technology, confidential and important business information was relatively less exposed to the risks of unauthorized use. Contemporary threat landscape has become highly uncertain which makes efficient information security an important business advantage. Namely, due to continuous technological changes and innovations, business entities have to constantly be ready to respond properly in case of a confidentiality breach.

1.1 Predictions

Current expert and research reports prove that information security as a business function and an organisational process, is becoming a serious topic of discussion. In addition to the expert reports in this field, much research, market analysis, and reports of international communities deal with this topic as well. The major future predictions for development of information security and threats are highlighted in the following paragraphs:

1 *Companies produce, store and process huge amount of information which is difficult to handle due to the lack of its transparency and extremely large quantities.*

- **Increased number of cybercrime cases**: In terms of information security and cybercrime, the last decade has been marked by exponential development and misuse of ICT. Cybercrime is the major security issue of the 21st century, as it has exceeded conventional crime, meaning it is more common in comparison to conventional violence-related and financial crime (Comprehensive study on cybercrime, 2013).[2, 3]
- **Increased number of state-supported cyber attacks**: At the state level, the number of targeted cyber attacks is expected to increase. Furthermore, the attacks on critical infrastructures are in sight, since it is an important aspect of national sovereignty and functioning of societies. Therefore, the critical infrastructure protection should become a priority in the eyes of states and major operators. Organisations must also be prepared to respond to such attacks, since they can be indirect victims in case of collateral damage (Internet security threat report,[4] 2013).
- **Increased number of threats and risks in cloud computing services**: Cloud computing has become an inevitable part of the internet and corporate infrastructure. Since cyber threats tend to focus on the locations where the big data is stored, cloud computing services are expected to be a future target, as well (ENISA threat landscape 2013 – Overview of current and emerging cyber-threats,[5] 2013; Internet security threat report, 2013).
- **Development of mobile-platform-related threats**: The increased use of mobile devices in the work environment has resulted in evolving new forms of threats and redirecting cybercriminals to the mobile media. Mobile devices are changing the conventional concepts of corporate structure and are causing revolution in the areas of mobile applications in terms of their use and capability. The use of applications has paved the way to easier and faster gathering of the big data; however, this process is more difficult to control. Since mobile platforms will remain the main area of the future innovations, organisations which follow the trend are expected to face a series of challenges (ENISA threat landscape 2013 – Overview of current and emerging cyber-threats, 2013; Internet security threat report, 2013).

2 *For example: e-mail abuse, phishing attacks and identity theft became the most common forms of crime, comparing to those long considered the most widespread problem (e.g. burglary, robbery and car-jacking) (Comprehensive study on cybercrime, 2013).*

3 *Research conducted by UNODC about the state of cybercrime in the 69 Member States of the United Nations. Data was collected in 40 companies, 16 academic institutions and 11 government institutions, while the meta-analysis of 500 publicly available documents was conducted as well. The study highlights the problem of collecting e-evidence, while solution can be seen in the new multilateral legal instruments.*

4 *The report includes an analysis of the IT incidents detected by Symantec's Global Intelligence Network, which records thousands of incidents per second in 157 different countries. In addition to incidents, the research covered 5,291 technological vulnerabilities detected in 2012. The results have shown that perpetrators are using new and innovative techniques, while migrating from classical stationary to mobile, virtual and social platforms.*

5 *Survey performed by ENISA, includes the analysis of 250 public documents and research on the topic of cybercrime. The purpose of the research was the identification of current trends in the field of information security with the aim to predict the future challenges. The results of the analysis showed that the major issue are less common forms of organized and sophisticated attacks that cause serious consequences.*

- **Threat migration to social media**: In recent years, social network sites which enable constant connectivity and knowledge sharing have become social psychological phenomena, and are expected to integrate into individual lives and corporate environments even more in the future. The most problematic is a tendency towards combining social media, mobile platforms and electronic payment system services which the perpetrators are expected to misuse, since they already optimize their operating techniques (Internet security threat report, 2013).
- **Internet of things and interconnection of devices**: Nearly all human needs and the ways of meeting them are somehow technology based. Communication services and electronic devices, which are part of our everyday life, are a great springboard for development of innovations (e.g. e-medical services, smart homes, electronic transportation and electronic cars, industrial control and energetic systems, live stream, etc.). Internet exceeds the limits and capabilities of computers and mobile devices which results in so called micro-digitalisation of organisations (Gartner, 2013).

Considering user trends and development of cybercrime, the future predictions are relatively reasonable. Cybercrime is expected to evolve hand-in-hand with developing science and ICT. If these predictions are right, mobile platforms and applications will continue to be the main source of innovations, whereas internet and information threats will continue to spread to the parts of personal life and business that have not been part of the network so far. According to the UNODC (Comprehensive study on cybercrime, 2013), such information threat development is driven by current socio-economic situation. Namely, people and organisations have gone viral and became connected during strong economic and demographic transformations, growing inequality among social classes, and strong belt tightening in the private sector. Lower financial liquidity of countries and organisations has had major impacts on crime and security situation.

1.2 The Nature of Information Security

In order to explain security trends, it has to be taken into consideration that the security of corporate structures is a very heterogeneous area and information security still plays a supportive role in it, despite its importance. Information security must be flexible and multidisciplinary, since it must ensure business continuity without threatening its functionality. Therefore, the efficiency of information security depends on the level of an organizations management capabilities. According to the Global state of information security survey (Defending yesterday: Key findings from the global state of information security survey, 2014), organisations which seek to be efficient and leaders in the field of information security have to meet three basic conditions:

- **Employing staff in charge of information security**: An organisation has to employ security management staff with adequate management

knowledge, whereas the board of directors must show appropriate support to the management staff regarding their authority and decisions.

- **Adopting detailed information security strategy**: The management staff has to adopt detailed information security strategic plan which must be approved by the board of directors. The strategic plan clearly defines objectives and purposes as well as responsibilities of ensuring information security.
- **Analysing the importance of information resources and assessing the efficiency of security measures:** An organisation has to periodically assess information security risks and evaluate the results of security controls. That makes it clear which parts of the information systems fail to ensure business continuity and which information is important for gaining information advantage. Such analyses also give insights into the efficiency of other conditions listed above.

Inadequate assessments of current situations or the lack of information on this issue can lead to wrong and irrational decisions resulting in inefficient information security. Stewart (2012) describes an optimal security situation in which all organisations first identify their security needs and then allocate the appropriate financial and human resources for managing those needs. Therefore, being acquainted with actual risk situations and information needs is one of the most important conditions for efficient information security. This is extremely difficult due to the specific nature of information security and cybercrime. Despite many available measuring instruments and accessible resources, there are still some methodological questions and practical limitations.

The most difficult task of every researcher is ensuring reliable results in assessing information security. The cybercrime situation is different from the conventional crime issues (e.g. violence-related crime) where more detected criminal offences result in a higher level of crime. Malicious information threats are specific deviances which do not necessarily lead to detection and reporting of incidents. On the one hand, a great number of cybercrime reports may demonstrate a stronger willingness of victims to report detected incidents or higher levels of information security in terms of better detection systems. On the other hand, the low level of reported or detected information incidents does not necessarily reflect high security levels, but incapability of detecting incidents or unwillingness to report them. Since organisations rarely report incidents and police statistics are an unreliable source of information (Comprehensive study on cybercrime, 2013; Goel & Shawky, 2009), business studies can be considered as the satisfying alternative for examining current situation. However, generalizing and explaining the results of such researches require caution due to unrepresentative samples.

2 METHODS

Similar to the general and overall corporate security, ensuring information security is not solely a technical issue, which should be considered while managing information risks. It is a multi-level discipline, which, in addition to the

technical tasks, includes organisational, management, user, strategic, legal and administrative tasks. Information security is a process that needs to live, develop and adapt; however, that requires a systematic and analytical approach.

In order to get an insight into current information security situation and define future challenges in this field, studies assessing the information threat situation in organisations were analysed and compared. The presented studies are international and up-to-date (majority of them published at the latest in 2012), and their findings have been confirmed by other independent professional sources. Detailed analysis of the research results shows that the most common research questions deal with examining the risk level, damages caused by actual incidents, and their impact on performing business operations. Unlike previous research, those which are up-to-date tend to focus on network attacks, social-media-related risks, mobile technology, cloud computing and outsourcing. Other important research topics include: (1) information security organisation, planning and strategy, (2) general management efficiency and feeling of satisfaction with information security (self-perception), (3) board of directors' support and investments, (4) employee information security awareness, (5) compliance with legal regulations, (6) current security controls in use, and (7) business continuity. With regards to these topics, analysis and findings are presented in the following section.

3 INFORMATION SECURITY SITUATION ANALYSIS

Despite the alarming predictions about the future development of information threats, there is one even more alarming finding: The majority of information threats that organisations currently face are occasional and basic in nature. Although this may not seem problematic, considering the fact that the least sophisticated threats can still bypass existing security controls, it actually demonstrates the unpreparedness for the emerging targeted threats. Stagnation of information security is problematic because the simplest forms of incidents are already causing major consequences which will be even greater in future. For example, researchers found that more than one-third of information incidents lead to disclosure of confidential information (Global corporate IT security risks, 2013), which in turn results in the loss of reputation, productivity and business opportunities. Confidentiality breaches, if not managed properly, could also lead to severe financial consequences and business illiquidity. Researchers note that smaller organisations suffer losses of tens of thousands, and perhaps hundreds of thousands of euros due to the event of severe information incidents, while in large corporations financial consequences are incomparably higher (Comprehensive study on cybercrime, 2013; Information security breaches survey, 2013). These and other findings suggest that existing security mechanisms should be immediately upgraded while considering the main corporate risk factors (structure, size, business model, links and partners, amount of technology and information, incident impact, etc.).

The results presented here can raise awareness and knowledge about the consequences of ineffective security systems which makes them important

for different target groups. First and foremost, they should be interesting for smaller organizations, because they are currently the most vulnerable part of the inter-organizational links. Their false sense of security can lead into deeper business insecurity, higher failure rate and greater information risks to connected third parties. Also, companies that are part of the public sector or the development industry, could use the analysis highlights in assessing the contemporary threat landscape. Clear presentation of the results is intended for security professionals, management and leadership, since their awareness is key to long-term effectiveness of corporate information security. Although most results are logical, they clearly show that saving at the expense of information security undermines all other security and business efforts.

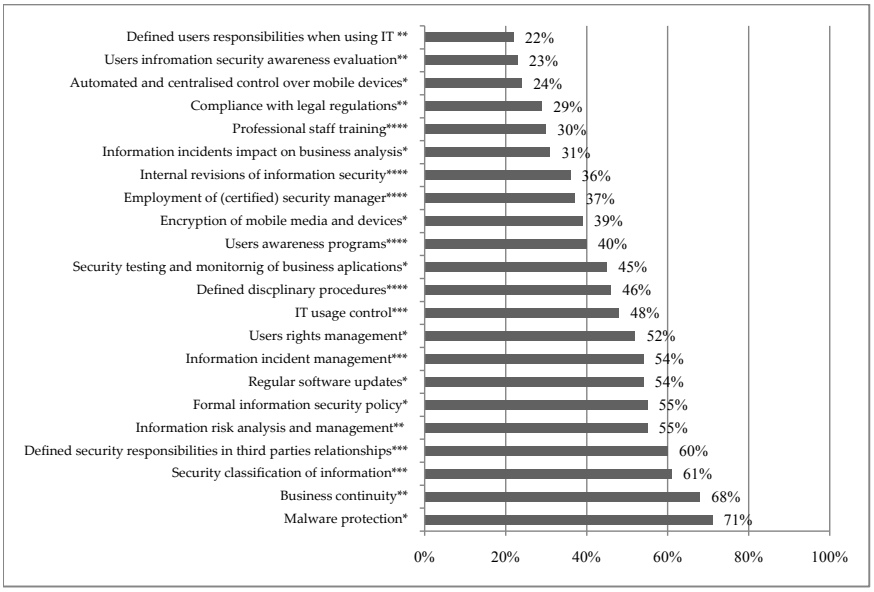
3.1 Current State of Information Security

In The Global state of information security survey (Defending yesterday …, 2014),[6] the opinions of organisations regarding the level of their efficiency in information security were analysed. More than two-thirds of respondents (74 percent) share the opinion that their organisation is efficient, about half of respondents consider themselves as the leading organisations in the field, whereas 11 percent of respondents are reactive rather than proactive in facing cybercrime-related issues. They do not develop a strategy and are inefficient. However, those opinions turned out not to reflect the actual situation. Considering various criteria, only 17 percent of respondents turned out to be leaders in this field. According to other research (Security effectiveness framework study, 2010), small organisations have the least efficient and the riskiest information security, as well as organisations which do not develop security management. In general, approximately 35 percent of organisations are inefficient, whereas the largest barrier to information security efficiency is the lack of awareness of management inefficiency and information vulnerability.

On the other hand, large organisations and the most threatened business activities tend to be more successful in information security planning and achieving its efficiency. There are two reasons why this finding makes sense. Large organisations have more expertise, resources available and experiences with actual incidents, whereas small organisations may have an impression they are less vulnerable due to their size (Comprehensive study on cybercrime, 2013). Figure 1 below shows the results of four studies on the corporate practices in the field of information security. The results indicate that general development of information security is still in relatively initial phases, since the majority of organisations do not adopt some basic security measures.

6 *International research performed by PwC has focused on measuring the state of information security in various business sectors. It was conducted among 9,600 respondents from 115 different countries. The conclusion of the research is that organizations are improving the security situation, but in doing so they are still not effective, nor do they follow the evolution of cyber threats. The results showed that the number of incidents is increasing steadily as well as financial loss caused by those incidents. Generally, organizations still use outdated security measures.*

Figure 1: Information security practices[7]



According to the data presented above, organisations first and foremost focus on regulating software and physical security measures. The results indicate that software protection, which includes antivirus programmes and firewalls, is the most developed security measure, followed by the physical measures for securing corporate capital and ensuring business continuity. Moreover, organisations have grown more aware of the importance of information confidentiality, since a relatively high percentage of organisations manages information resources in terms of resource classification and security during downloading and storing. On the other hand, staff management measures, such as raising employee awareness, staff training and control over ICT use, are less regulated and developed. Compliance with legal regulations is considered an insufficient condition for achieving information security; therefore, it is not a primary concern of organisations anymore (TMT global security study, 2013).[8]

According to the organisations' reports, the major barrier to information security management is the lack of financial means for information infrastructure. Despite growing attention to security, the budget for ensuring information security remains the same or insufficient in average (Defending yesterday …, 2014; TMT Global Security Study, 2013). Due to the lack of resources, many organisations fail to realize their information security plans and policy in practice (Global corporate

7 **Global corporate IT security risks (2013), **Information security breaches survey (2013), ***Defending yesterday … (2014), ****TMT global security study, (2013).*

8 *International research conducted by Deloitte analysed the practice of information security in technology, media and telecommunications sectors. 122 organizations in 37 different countries were included. The main findings highlight the changing motivations of organizations in managing information security. Improving confidence among customers and good security posture in the market are the basic advantages of information security, while compliance is no longer a top priority.*

IT security risks, 2013).[9] Namely, decisions on investments in information security are made by a board of directors; however, the leadership often considers only the financial benefits (Pironti, 2007) and therefore connects the security with costs involved. Concrete benefits of investments into information security are indirect and long term and therefore difficult to measure, and it is hard to assess to what extent an organisation has benefited from preventing attacks by unknown threats. And if a threat is prevented due to security, it might be assumed that the threat did not even exist (Burton & Stewart, 2009). In recent years, organisations allocate more resources to information security management; however, investments are still disproportional with regards to the growing use of ICT and evolution of threats.[10]

3.2 Cybercrime

Research proves that cyber attacks and misuse of information represent a common threat to many organisations, yet they do not address this issue properly. According to various studies (Data breach investigation report, 2013; Defending yesterday …, 2014; ENISA threat landscape …, 2013; Fourth annual cost of cyber crime study, 2013; Global corporate IT security risks, 2013; The impact of cybercrime on business, 2012;[11] Internet security threat report, 2013):

- In the past year, 91 percent of organisations were victims of information breaches;
- Approximately 66 attempts and 1,4 successful cyber attacks happens in a given week;
- The most common form of information threats are network attacks which exploit approximately 20 the most known information vulnerabilities;
- More than 70 percent of information incidents happen to be less or unsophisticated;
- 75 percent of incidents are opportunistic and 25 percent are organised; 66 percent of those incidents are detected several months after an actual attack and nearly 70 percent are detected by third parties; and
- External security incident solving takes approximately 27 days, whereas dealing with the internal incidents takes approximately 53 days.

9 *A survey conducted by Kaspersky Lab on the state of IT security. The sample consisted of 2,895 experts from 24 different countries. The purpose was to analyse their practices in addressing information risks and expectations for the future. The main finding is that cyber threats are a multi-level problem; for that reason, the surface treatment is the wrong approach.*

10 *Studies indicate that companies will have to invest more money in information security; at least a third of finances intended for IT, while in practice they are investing 4–16 percent of IT finances (Information security breaches survey, 2013; Defending yesterday …, 2014).*

11 *International research by Ponemon Institute has analysed the opinions of 2,616 security experts from five different countries on current practices in information security. The survey focused on the qualitative analysis of five different cyber threats: botnets, APTs, DOS attacks, malware and social engineering. The study notes that threats as we knew them no longer exist, because the perpetrators are merging into well-organised criminal groups that follow trends of online communication, mobile technology and cloud.*

According to the findings, organisations mostly deal with less complex information security risks. The majority of risks were opportunistic, meaning they resulted from current circumstances and the lack of basic security measures. This is a troublesome issue, since incapability to ensure protection against basic forms of threats means high vulnerability to more serious threats. Inefficient dealing with basic information security risks raises even more concerns, since 25–35 percent of security incidents cause disclosure or loss of confidential information; more than half of those cases lead to the loss of business reputation and one-third to the loss of important business opportunities and partners (Defending yesterday …, 2014; Global corporate IT security risks, 2013).[12]

According to one of the business research studies, information threats arise mostly from the external corporate environment (Data breach investigation report, 2013). Moreover, the research Internet security threat report (2013) found that the number of network attacks has increased by one-third as compared to the previous year, and that the most common source of cyber attacks are hackers. Other perpetrators might be contractors, suppliers and competitive organisations with financial and espionage motives (Defending yesterday …, 2014). The most common external threat is a malicious code, followed by information system penetration, social engineering, phishing attacks and cases of causing unavailability (e.g. the DOS attacks) (Comprehensive study on cybercrime, 2013; Data breach investigation report, 2013;[13] Global corporate IT security risks, 2013).

In addition to the external threats, information security risks arising from the internal corporate environment should not be neglected. Internal information threats arise from inadequate user behaviour and management decisions, from failure to act or negligence of a specific issue. Therefore, technology performance and information confidentiality depend on the behaviour of employees. The internal threats reflect mostly in the vulnerability of software and applications. That is a consequence of inappropriate maintenance (e.g., security updates) or the lack of understanding of technological innovations which organisations use in order to improve their production processes. Other internal information threats are user threats, which occur in the form of unauthorised data disclosure and negligent use of ICT (Global corporate IT security risks, 2013). A high number of cyber threats is also a consequence of insufficient user knowledge, low employee motivation or dissatisfaction. More than two-thirds of organisations that participated in the TMT global security study (2013) and Data breach investigation report (2013) consider employees as the most important information resource and, consequently, the lack of employee awareness as high information vulnerability. The most common targets of external threats are internal sources;

12 *Analysis highlights the following information as the most important and vulnerable: information about customers, employees, intellectual property, financial statements and financial data, organisational strategy, development and marketing plans, administrator and user rights.*

13 *The research conducted by Verizon, has been carried out in collaboration with 19 organisations (research and scientific institutions, law enforcement agencies, organisations responding to cyber incidents). Information base of 47,000 and 621 incidents of cyber intrusions in 29 different countries was made in the process. The study notes that the new age IT incidents are heterogeneous problem, so one-dimensional characterization, does not capture their complexity. The research concludes that all organizations are potential target of cyber threats, so "Assume you're breached" mentality must prevail.*

beside servers and network, accountants, system administrators, executives and board of directors, marketing and advertising staff are also exploited (Data breach investigation report, 2013; Internet security threat report, 2013).

Generally, all types of organisations deal with external and internal information security threats. However, the comparative graph (Figure 2) below indicates differences in types of threats affecting various types of organisations. Large organisations deal with more incidents on an annual basis (Internet security threat report, 2013) and are mostly exposed to more serious and sophisticated forms of threats (e.g. cyber espionage, DOS attacks, information system penetrations, misuse of confidential information), whereas small organisations are exposed to less serious forms of threats (e.g. viruses, Trojan horses, worms, phishing attacks). Other research also proves that small organisations are the most common target of unsophisticated malicious software or cybercriminals with financial motive (ENISA threat landscape …, 2013).[14]

Although findings indicate that large organisations are more exposed to information risks, small organisations still remain highly threatened. In comparison to small organisations, the larger ones are better protected against cybercrime and employ more experts from this field which results in better knowledge and understanding of information security issues. Therefore, simple threats are not overly troublesome for them, although they more often face organised and dangerous criminals. On the other hand, small organisations are often the target of opportunistic cybercriminals who quickly detect poor and inadequate protection (Internet security threat report, 2013), and spread the word about their findings, which can lead into multiplying threats. The interesting fact is that the targeted attacks equally focus on both small and large organisations (Figure 2) which makes sense. Small and vulnerable organisations represent an entry point to the systems of large organisations in the chain of suppliers/partners and are therefore attractive for wired cybercriminals.

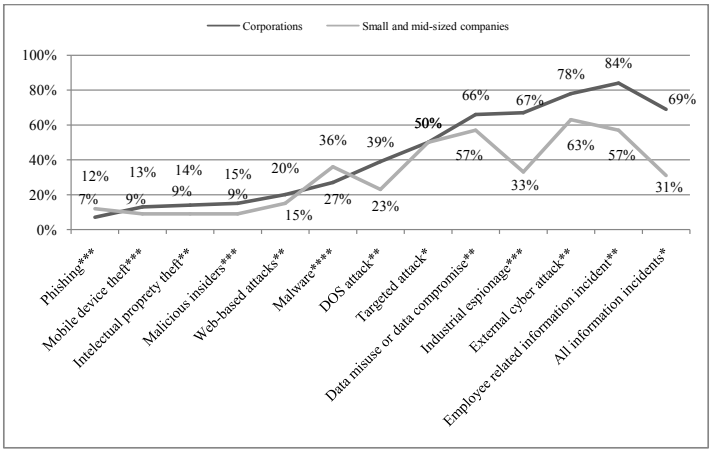


Figure 2: Information threat comparison by organizational size[15]

14 *59 percent of incidents happen in large organisations, 31 percent in the small ones, and the rest percentage in those organisations, which employ 251–1500 people (Internet security threat report, 2013).*

15 **Internet security threat report (2013), **Information security breaches survey (2013), ***The impact of cybercrime on business (2012), ****Comprehensive study on cybercrime (2013).*

In order to determine the most threatened corporate profile, some other factors, besides the size of the organisation, should be taken into consideration, such as the type of business activity and business sector. According to the Data breach investigation report (2013), Fourth annual cost of cyber crime study (2013),[16] The global state of information security survey (Defending yesterday …, 2014), Information security breaches survey (2013),[17] and Internet security threat report (2013), the most exposed to risks are large production facilities and public sector organisations which manage critical services. Those are first and foremost financial institutions (e.g., banks, insurance companies), healthcare services and the pharmaceutical industry, professional services and counselling (e.g. legal, architectural, medical counselling, revisions and system controls) and organisations in the field of ICT development (automobile industry, computer and information science, telecommunications).

Information threat situation analysis in the corporate environment proved that each and every organisation can be the target of a malicious incident. The majority of information threats are not serious, but the incidents are not dealt with within an appropriate response time. Organisations are most commonly challenged by external threats, especially network attacks and malicious software. With regards to internal information risk management, organisations should first and foremost focus on updating software and access control as well as on raising employee awareness. But users and networks are not the only targets of cybercriminals. It is necessary to emphasize that other corporate elements, which are results of micro-digitalisation, enable access from the external to the internal corporate environment.

3.3 Cloud Computing, Outsourcing and Mobile Media

As organisations tend to follow technological trends, they often make false decisions that lead to increased information vulnerability. The question of information security efficiency often coincides with the dilemma of transferring the responsibility for information security to the third professional subjects (so-called outsourcing of security functions), transferring information to the cloud and integrating mobile technology and applications into work processes.

In times of evolving threats and increasing demands for efficient information security, security management departments often decide to outsource. A growing number of organisations use services of cloud computing and exploit

16 *The survey conducted by Ponemon Institute covered 234 companies, 1,935 security professionals and 1,372 security incidents. The results showed that cybercrime is a threat which represents a high financial risk. According to the findings, the annual damage caused by cyber attacks varies between three hundred thousand and tens of millions of dollars per organisation. With that said, the damage depends on the size, business activities and security controls in use.*

17 *A survey conducted by PwC which has analysed the state of information security in British companies. The sample covered 1,402 respondents across different business sectors. The results of analysis showed that cybercrime is an important threat to small businesses which are forced to deal with problems that have long been considered the concern of large corporations. Due to the indifference, many of the small businesses are unprepared to tackle modern information security challenges.*

its advantages, therefore, outsourcing of computer capabilities and security is becoming very common corporate practice (Information security breaches survey, 2013). By outsourcing, some risks are transferred to third parties; however, at the same time, other vulnerabilities arise. Transfer of security functions from the corporate environment to the external one might result in decreasing the number of in-house employees that are responsible for ensuring information security. That makes organisations even more vulnerable, since they have less professional knowledge available and less control over threats. Regarding the transfer of services and computer capabilities, cloud computing appears to be troublesome in terms of its security, since it stores a large number of personal and confidential information.

Current use of cloud computing refers mostly to storing information on the network. Organisations also tend to outsource other services, such as website management, business mail management, payment and accounting services and business applications (Defending yesterday …, 2014; Information security breaches survey, 2013; TMT global security study, 2013). According to the latest McAfee report (McAfee, 2014), cyber attacks are increasingly focusing on business applications used by employees, the majority of which are not checked and approved by a security management department. When an organisation transfers its applications and information to the cloud, it loses security control over their operation and use. The service providers may offer those applications and information on the remote and unknown platforms, which can result in sharing and distributing confidential information in ways organisations are not able to understand and control. Such cases raise a question where information is actually stored and which formal-national regulations apply to information governance (TMT global security study, 2013). Furthermore, service providers often store and manage personal and confidential information of several clients at the same time on the same platform which attracts cybercriminals even more, since they can misuse more information in one place (Internet security threat report, 2013).

In the global online environment, a security incident in one organisation can influence information security in all of its partner organisations. Therefore, information security in the external environment also plays an important role. If organisations decide to cooperate with outsourcing service providers, they need to take care of the control and responsibility aspects of such services. Most importantly, a strict policy should be adopted regulating who is allowed to access the cloud information and under what circumstances, where the information is stored, who is in charge of the information and what is happening with the information during storage.

In addition to cloud computing, the major future security challenge for organisations is mobile technology which is one of the most vulnerable elements of organizational structure (Sjouwerman, 2012). Simple and widespread use gives the impression of a low risk level; therefore, the mobile technology protection has not been sufficiently adapted (Fighting to close the gap, 2012). Recently, the so-called BYOD trend ("Bring your own device") has exponentially increased which made insufficient protections even weaker. The term applies to integrating personal mobile devices, usually used in private life, into the corporate and

work environment for the business purposes. This results in an increase in an organization's vulnerability and, consequently, chances of information misuse. The most complex issues are expected to arise when employees will start to use their personal mobile devices to access business information via cloud computing services. The previous year analysis showed that the evolution of malicious threats and vulnerabilities in mobile media was more intensive and rapid in comparison to the evolution of threats focused on stationary devices. Just in the second half of 2013, the number of malicious threats has increased by one-third (McAfee, 2014).

Considering all those facts, the use of cloud computing services in combination with the use of mobile devices in the work environment, brings new information security challenges and risks which should be of primary concern to management in the near future. Since organisations try to follow security trends and technical innovations, vulnerabilities increase. Therefore, the decisions on changes and integration of new systems into a corporate structure have to be based on justifiable reasons. Negligence of security issues raises even more concerns, regarding the fact that, beside relatively known information threats, there are also well organised cybercriminals that use unpredictable and complex techniques for achieving their objectives.

3.4 Organised Cybercrime

Development of organized and structured cybercrime is the consequence of the increased interconnection of organisations, their mobility, information outsourcing and similar business and user trends which opened new canals for cybercriminals and created vulnerabilities as well as opportunities for attacks (The impact of cybercrime on business, 2012). Sophisticated cyber attacks are usually not carried out by individuals, but are the matter of wide social motivation, such as industrial and state espionage, information warfare, "hacktivism", terrorism and organised criminal underworld activities. Unlike opportunistic cybercriminals, such organised groups are well funded and highly motivated; they carefully set their goals, choose their targets in advance and employ competent hackers. The attacks are well planned and systematic—a great deal of time and means are used for gathering information and victim profiling which increases chances for performing a successful attack. According to the Data breach investigation report (2013) and Internet security threat report (2013), the organised crime groups with financial motive and state-supported espionage activities with military, economic or political motives prevail in this field. Both usually focus on large inter-organisational structures with massive amounts of information.

Cyber attacks caused by such groups are rarely isolated cases, but rather belong to an organised action and consist of various threats. That kind of cyber occurrences are called APTs (advanced persistent threats). And when an attack is focused on a specific target or victim (e.g. a specific organisation), it is called a targeted attack. The research indicate that targeted attacks are skyrocketing, and since they are hybrid threats they are the most sophisticated and troublesome types of cybercrime. Targeted attacks were initially financially motivated and

focused on the private sector, but now they happen to be increasingly politically and socially motivated (McAfee, 2014).

Another important form of organised cybercrime that poses a threat to the confidential information is "hacktivism" which combines social or political activism with hacking. The protesters and activists who used to block access to a certain location, building or physically disable business operation of a certain organisation now use the denial-of-service (DOS) attacks for the same purposes (Data breach investigation report, 2013). Such attacks overload the components of network infrastructures and disable their operation. In 2013, 25–40 percent of organisations were victims of DOS attacks (Information security breaches survey, 2013; TMT global security study, 2013) which resulted in the blockage of websites, postal and communication systems, as well as in general disruption of business operations that usually lasted up to six working days (Information security breaches survey, 2013). In order to redirect a victim's attention, the DOS attacks frequently occur in combination with other cybercrime techniques. The cybercriminals first perform the DOS attack and force an organisation to deal with the incident. During the organisation's focus on incident solving, they try to carry out other system penetrations from the background which the organisation is not able to detect because it still deals with the first incident (Internet security threat report, 2013).

To sum up with regards to the trends described, mobility, information sharing and interconnection of corporate structures cause organised cybercrime to grow. By using reverse engineering, new, less known and resilient cybercrime techniques evolve. Cybercrime tends to develop to such an extent that reactive responding to attacks and trying to mitigate the impact of attacks will not be sufficient for managing information risks anymore. To conclude, the review and analysis of studies reveal that saving money at the cost of security and ignorant behaviour are dangerous and risky approaches that threaten the success, productivity and competitiveness of organisations.

4 CONCLUSION

As organisations decide to regulate or update their information security measures, they need to understand that negligence of information security may cause higher costs than its maintenance. While it is true that initial planning and establishing information security is more difficult in comparison to its maintenance, it should be kept in mind that the impacts of efficient security pay off in the long term. On the basis of the prior research and expertise in the security field, a wide range of measures that appear to be the most efficient in practice is offered in the following list:

- Automated intelligent systems for threat detection and prevention (IDS, IPS);
- Mobile devices management, user policy and encryption;
- Advanced network and access control (UTM, NGFW);
- Risk management: assessment of information capital, vulnerability and threats;

- Processes and systems for preventing information loss and information recovery;
- Cryptography of mobile devices and information during communication or transferring;
- User rights management and system access control;
- Automated updating and security testing of applications and software;
- Efficient firewalls and prompt antivirus programs at all entry points,
- The list of authorised and unauthorised software and electronic devices;
- Professional staff training and competencies assessment;
- Separation of system and security roles and responsibilities, the control over the use of administrator rights;
- The control over users' insight with the need-to-know policy;
- Ensuring trailing and audit trail maintenance;
- Crisis management: response plans for the most important risks;
- Penetration tests: assessment of organisation's defence capabilities.

Currently, those measures listed are the most recommended and efficient security controls, and include not only technical security demands, but also other aspects of security management. However, it has to be taken into consideration that each individual measure does not ensure efficient information security. In order to be able to manage threats proactively, combining measures and multi-level protection are needed.

After planning and adopting changes, users have the greatest impact on information security efficiency; therefore, user management is the field that needs to be given more attention in practice. It depends on the security-aware and motivated users whether the plan and the rules adopted will indeed be considered in practice. Here are some recommendations for directing organisational behaviour and establishing strong security culture among employees:

- **Raising user awareness**: Regular seminars need to be organised for people who use ICT or manage confidential information at work. The seminars must be adjusted to user knowledge and situations (threats, vulnerabilities, rules) that are typical for a specific organisation. Moreover, the users must be acquainted with reasons for adopting rules and dangers that might occur if they do not act according to the rules.
- **Professional training of expert staff**: Since ICT and threats constantly change and develop, professional training of employees must be provided as well. Useless management and old-fashioned management techniques can be a huge barrier to the efficiency of information security and technology. A good way to follow security trends is by attending professional conferences and informal trainings.
- **Confidentiality statements and agreements**: User obligations and responsibilities need to be well defined and formal regulations for dealing with confidentiality breaches specifically outlined. By signing a confidentiality agreement, employees accept the risks and assure they understand what their responsibilities are as well as bind to protection of confidentiality. On the other hand, organisations need to clearly define what kind of behaviour is forbidden.

- **Motivating employees**: Any change adopted may bring disapproval and rejection among employees, especially if current processes are in use for a long period of time. Resistance to change is very common in technology fields and when restrictive rules are adopted. In order to integrate information security into the organisational culture and employee ethics, the needs of employees and their feedbacks on control functionality must be taken into consideration. Furthermore, while implementing restrictive rules, organisations need to respect the right to privacy and integrity.
- **Regular security meetings**: Information security must be discussed within the entire hierarchical pyramid. Management in the organisation should regularly report on innovations and current issues, help users to manage everyday dilemmas and encourage them to behave in accordance with the policies. Management should also inform board of directors about security needs and lobby for attention and financial means.

According to the given recommendations for regulating information security, it is clear that information security is very heterogeneous field which covers the variety of processes. Since technology changes on a daily basis, it is of great importance for organisations to choose services and devices rationally and carefully. Every change adopted by organisations also brings some negative impacts and vulnerabilities, therefore, they should adopt only such measures and follow only such trends they really need. Organisations must justify their decisions with concrete information and bear in mind their actual security needs.

The wide and macro aspect of information security issues need to be emphasized as well. In order to properly govern cybercrime, organisations need to design strong security architecture that goes beyond organisational boundaries. Most importantly, new and better cooperation methods between private and public sector must be adopted. Such cooperation must be based on mutual trust and sharing of responsibility. Organisations and both sectors must establish long-term partnerships that are beneficial in terms of helping in case of actual incidents and exchanging of information on threats, risks, trends, development, good practices and experiences regarding preventing measures. Such strategic partnerships and coordinated cooperation involving organisations that encourage each other rather than compete, would strongly contribute to better information security situation, improve understanding of the nature of cyber threats as well as raise general awareness.

REFERENCES

Bernik, I. (2014). *Cybercrime and cyber warfare*. London: Wiley.

Burton, S., & Stewart, S. (2009). *Security implications of the global financial crisis*. Austin: Stratfor Global Intelligence. Retrieved from http://www.stratfor.com/weekly/20090304_security_implications_global_financial_crisis

Comprehensive study on cybercrime. (2013). New York: United Nations Office on Drugs and Crime. Retrieved from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Data breach investigation report. (2013). New York: Verizon. Retrieved from http://www.verizonenterprise.com/DBIR/2013/

Defending yesterday: Key findings from the global state of information security survey 2014. (2014). London: Price Waterhouse Coopers. Retrieved from http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

ENISA *threat landscape 2013 – Overview of current and emerging cyber-threats*. (2013). Heraklion: European Union Agency for Network and Information Security. Retrieved from http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

Fighting to close the gap. (2012). London: Ernst & Young. Retrieved from http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf

Fourth annual cost of cyber crime study: Global. (2013). Traverse City: Ponemon Institute. Retrieved from http://www.hpenterprisesecurity.com/register/2013-fourth-annual-cost-of-cyber-crime-study-global

Gartner. (2013). *Gartner identifies the top 10 strategic technology trends for 2014*. Retrieved from http://www.gartner.com/newsroom/id/2603623

Global corporate IT security risks: 2013. (2013). Moscow: Kaspersky Lab. Retrieved from http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

Goel, S., & Shawky, H. A. (2009). Estimating market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404–410.

The impact of cybercrime on business. (2012). Traverse City: Ponemon Institute. Retrieved from http://www.checkpoint.com/products/downloads/whitepapers/ponemon-cybercrime-2012.pdf

Information security breaches survey. (2013). London: UK Department for Business Innovation & Skills. Retrieved from http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf

Internet security threat report. (2013). Mountain View: Symantec Corporation. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

McAfee. (2014). *McAfee Labs 2014 threats predictions*. Retrieved from http://www.mcafee.com/uk/resources/reports/rp-threats-predictions-2014.pdf

Pironti, J. P. (2007). Developing metrics for effective information security governance. *ISACA Journal*, 7(2), 1–5.

Security effectiveness framework study. (2010). Traverse City: Ponemon Institute. Retrieved from http://h71028.www7.hp.com/enterprise/downloads/software/Security%20Effectiveness%20Framework%20Study.pdf

Sjouwerman, S. (December 10, 2012). 2013 security prediction. *Cyberheist News*, 2(54). Retrieved from http://blog.knowbe4.com/cyberheistnews-vol2-53/

Stewart, A. (2012). Can spending on information security be justified? *Information Management & Computer Security, 20*(4), 312–326.

TMT global security study. (2013). New York: Deloitte. Retrieved from https://www2.deloitte.com/content/www/global/en/pages/technology-media-and-telecommunications/articles/2013-tmt-global-securitystudy.html

About the Author:

Kaja Prislan, MA in Criminal Justice and Ph.D. student at Faculty of Criminal Justice and Security, University of Maribor.

VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 16 no. 2 pp. 148–163

Video Surveillance and Corporate Security

Marko Potokar, Sanja Androić

Purpose:

This article addresses the field of video surveillance and corporate security in companies in Slovenia, and attempts to show the basics of corporate security and the use of video surveillance, the reasons for their use and the consequences for the companies.

Design/Methods/Approach:

This research into the fields of corporate security and video surveillance used the description method, which provides basic definitions of terms, individual expert theories, and the survey technique that was used for the questionnaire in the empirical part of the research. The questionnaire was designed using the web program EnKlikAnketa (www.1ka.si), and the information gathered was processed using descriptive statistics in the program tool Microsoft Office Excel.

Findings:

The findings show that the field of corporate security in Slovenia is becoming increasingly important and companies in Slovenia use video surveillance exclusively for protection, but there are already signs of the need in other fields as well. We find that companies in Slovenia are already aware of the need for changes in the fields under research, and there are also indications of changes in linking systems of protection.

Research Limitations/Implications:

Conducting research in the fields of corporate security and video surveillance is difficult due to the delicate nature of the subject and also partly due to the lack of knowledge in these areas on the part of the employees in Slovenian companies.

Practical Implications:

The results gained and their interpretation can be the starting point for further in depth research in the fields of video surveillance and corporate security.

Originality/Value:

The research can provide the professional public with answers from the fields of video surveillance and corporate security that are as yet not adequately investigated.

UDC: 005.934

Keywords: video surveillance, corporate security, companies, protection, Slovenia

Video nadzor in korporativna varnost

Namen prispevka:

Prispevek obsega področje video nadzora in korporativne varnosti v podjetjih v Sloveniji. Prikazati želimo osnove korporativne varnosti ter uporabo video nadzora, razloge za uporabo le tega in učinke za podjetja.

Metode:

Raziskava o področju korporativne varnosti in področju video nadzora je bila opravljena s pomočjo deskriptivne metode, ki smo jo uporabili za podajo osnovnih definicij pojmov in posameznih strokovnih teorij, ter metode anketne tehnike, ki smo jo uporabili za vprašalnik v empiričnem delu raziskovanja. Vprašalnik smo pripravili v spletnem programu EnKlikAnketa (www.1ka.si), pridobljene odgovore pa smo obdelali z deskriptivno statistiko v programskem orodju Microsoft Office Excel in jih ustrezno interpretirali.

Ugotovitve:

Izsledki raziskave kažejo, da postaja področje korporativne varnosti v Sloveniji vse bolj pomembno in da podjetja v Sloveniji uporabljajo video nadzor večinoma zgolj za varovanje, a se že kaže zavedanje o potrebah tudi na drugih področjih. Ugotavljamo, da se podjetja v Sloveniji že zavedajo potrebnosti sprememb na raziskovanih področjih. Nakazujejo se tudi spremembe v povezovanju sistemov za varovanje.

Omejitve/uporabnost raziskave:

Opravljanje raziskav na področju korporativne varnosti in video nadzora je oteženo zaradi občutljivosti tematike in delno tudi zaradi premajhnega poznavanja teh področij s strani zaposlenih v slovenskih podjetjih.

Praktična uporabnost:

Pridobljeni rezultati in njihova interpretacija bodo lahko iztočnica za nadaljnje poglobljene raziskave na področju video nadzora in korporativne varnosti.

Izvirnost/pomembnost prispevka:

Z raziskavo bo lahko strokovna javnost pridobila odgovore na sedaj še premalo raziskanem področju video nadzora in korporativne varnosti.

UDK: 005.934

Ključne besede: video nadzor, korporativna varnost, podjetja, varovanje, Slovenija

1 INTRODUCTION

Video surveillance systems are one of the most frequently used surveillance technologies today, and represent one of the non-invasive surveillance technologies, since their use often remains unnoticed by inattentive individuals. And herein lies the hidden danger of (ab)use, since individuals are often not even aware of the existence of video surveillance in a certain area or gradually get so used to it they forget about it. The use of video surveillance has origins in Great Britain, where video surveillance systems were first installed in London

underground in 1961 (McCahill & Norris, 2002). Video surveillance gradually expanded to the trade sector, where it came to full swing in the 1990s (Beck & Willis, 2011). The use of video surveillance technologies has divided the society into two polar opposite views. Some agree with the opinion that video surveillance is efficient (from the point of view of protection), while the civil society however focuses on dangers deriving from control (Groombridge, 2002). On the one hand, the installation and use of video surveillance causes concerns because of invasion of privacy and fear from the authorities' control of the citizens, and on the other, it is welcome, because it raises the level of security and reduces socially unacceptable behaviour (Davies & Velastin, 2005). The fact is that video surveillance is also used in corporate environments as one of the methods of technical protection.

2 VIDEO SURVEILLANCE AND CORPORATE SECURITY

Despite the fact that video surveillance is widespread and has been used for many years, there are only descriptive definitions of the term video surveillance system or system of video surveillance. One of them defines the video surveillance system as functionally linked special technical means that by receiving, transmitting, processing, storing records and presenting received images enable visual observing and surveillance, and later analyses of activities in protected premises (Golob, 1997).

The original video surveillance system consisted of a camera directly linked with a screen on which a person (operator) observed activities recorded by the camera (Davies & Velastin, 2005). It was the so called first generation of video surveillance systems with a »dumb« camera that needed the presence of a person to analyse the images. The first generation of video surveillance systems, which were analogue, was followed by the second generation, where the camera was connected to a computer that »evaluated« the gathered images itself (Surette, 2006). The systems of the second generation are, among other things, capable of automatic processing and storing of captured images, recognizing buildings and analysing the surroundings before presenting the captured data to the observer (Davies & Velastin, 2005). Video surveillance systems of the second generation are characterized by digitalization and digital data processing. Currently and already in use are video surveillance systems of the so called third generation, characterized by the use of IP protocol and connections to the internet.

Besides »classic« video surveillance systems for identifying faces, movement and position, which operate in the visible field of the electromagnetic spectrum, there are also video systems for thermo-vision, based on perceiving thermal radiation, being used successfully (Golob, 1997). Besides technical limitations, in practice there also occurs numerous questions about the meaning and efficiency of using video surveillance systems. The number of cameras is often inadequate to guarantee effective supervision, their installation is faulty, and the quality of the picture is low due to incorrect choice of objectives (Ivanovič & Habbe, 1998).

With digitalization and the introduction of computer technology, video surveillance became of interest for commercial purposes as well. So for example

during elections in Mexico in 2000 and 2006, a system for recognizing faces was used, by which the government prevented voters from multiple voting (Vacca, 2007). The basic use of video surveillance in city centres is to detect criminal acts and misdemeanours as soon as they happen. Based on the recordings of video surveillance system, the police gather evidence which can direct crime investigation to quickly find the perpetrator. There is a lot of evidence that video surveillance is often used in dealing with socially unacceptable and criminal behaviour (Mencinger & Meško, 2004). In addition, performing video surveillance also serves as a measure in preventing criminality. Installing technical means for controlling public places such as shopping centres, banks and parking lots with the purpose of reducing possibilities of theft and other criminal acts, belongs to the so called situational strategy of criminality prevention (Meško, 2000).

In the corporate environment, physical protection complements technical protection with various technical means of protection. Ramšak (2010: 33) differentiates the following forms:

- Electro-mechanical protection, which is a kind of improvement of mechanical protection. Here belong devices that automatically report fire, unauthorized entry to the protected area, or excessive concentrations of dangerous substances.
- Video surveillance, which enables companies to exercise direct control by means of cameras and later analyse occurrences in business buildings and their surroundings.
- Access control, which identifies the access of employees or guests to the secured area or merely to the company itself. There are various ways of identification.
- Security lighting that illuminates the secured area.

Video surveillance systems are thus an important component of security systems that guarantee appropriate levels of corporate security. Čaleta (2011: 40–41) believes that in its broadest meaning, corporate security is an activity that identifies and performs all necessary measures for controlling security risks in an individual company. Therefore, it is one of the basic functions for operation of the company and must be performed in close cooperation with all other key functions within the company. Its primary purpose is to improve productivity and the competitive position of a company by decreasing security risks in operation to a minimum. A lowered internal level of a companies' protection can be particularly seen by increased sensitivity to internal and external security threats and various harmful influences connected with different forms of corruption and crime. For these reasons, it is important that companies even in the time of economic crisis, use a portion of their profit to improve corporate security of the company. This guarantees a firm support to the efficiency of the company and is of vital importance in safeguarding critical infrastructure (Trivan, 2013: 61–62).

Vršec (1993: 109–111) estimates that key security activities in protecting the company's property is protection of buildings, (pieces of) land, equipment, machines, tools, vehicles, raw materials, material, stock, money, claims, loans, etc. In most companies, protection of property is limited only to physical and technical

protection, which mostly means protection against burglary and fire. The greatest damage to companies is by different forms of economic crime, which causes extensive damage and losses of the company. Adding petty thefts of material, tools and other things, the total damage to the company can be so great that it disturbs even those regarding damage most uninterested owners and managers of the companies (Vršec, 1993: 112–116).

We can conclude that due to inappropriate level of security, companies simply do not understand the gravity and danger of modern threats or even have erroneous notions about them. It would be much better if companies spent the money they currently use for repairing damage, to introduce better security systems. Companies often do not want to admit the frequency of attacks and size of damage publicly, since they do not want to admit they underestimated potential dangers and most often ignored danger of human factor (Bernik & Prislan, 2013: 220).

3 METHOD

The theoretical or qualitative portion of the research, into the fields of corporate security and video surveillance, was conducted by means of description method, which was used to present basic definitions of terms and individual expert theories. In the empirical or quantitative part of the research, we used the survey technique, whereby a questionnaire to acquire the opinion and evaluation of the asked employees in Slovenian companies was utilized. The questionnaire was designed in the web program 1nka, the answers received were processed by means of descriptive statistics in the program tool Microsoft Office Excel, and adequately interpreted. Employees in Slovenian companies were asked to participate in the research by e-mail. The questionnaire consists of closed-type multiple choice questions, and some questions have an »other« category, where the respondent could write their opinion that was not offered among given choices. The results are presented in the following graphs and tables.

The sample was comprised of about 400 persons employed in Slovenian companies, and who were sent invitations to fill in the web questionnaire by e-mail. We received 112 completed or finished questionnaires. Interesting is the analysis of EnKlikAnketa web survey program (www.1ka.si), in which the web survey was performed, showing that as many as 312 persons clicked the address of the survey, 227 persons clicked the survey itself, and 132 persons started and partially completed the questionnaire. Partially completed surveys were removed from the analysis, since most of them finished the first few questions of the questionnaire. We think that such responses indicate their lack of time or lack of interest to participate in research.

Figure 1 shows that the majority or 63% of the respondents are employed in middle sized companies or organizations, followed by 23% of those employed in small organizations. The fewest or 14% are employed in large organizations.

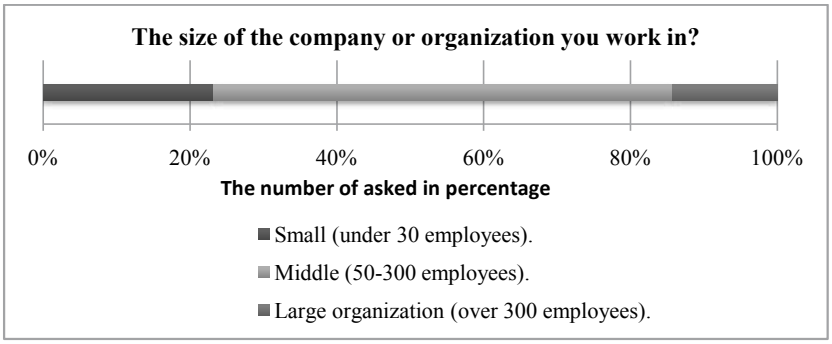


Figure 1: The size of the company or organization where the asked are employed

4 RESEARCH RESULTS

Figure 2 shows evaluations of the employees responding in Slovenian companies regarding the importance of corporate security field. As many as 140 (85%) of the see this field as very important or important, 25 (15%) were undecided, one (1%) considers this field almost unimportant. We can conclude that the respondents perceive the field of corporate security in the company as important. (Androić, 2013: 54).

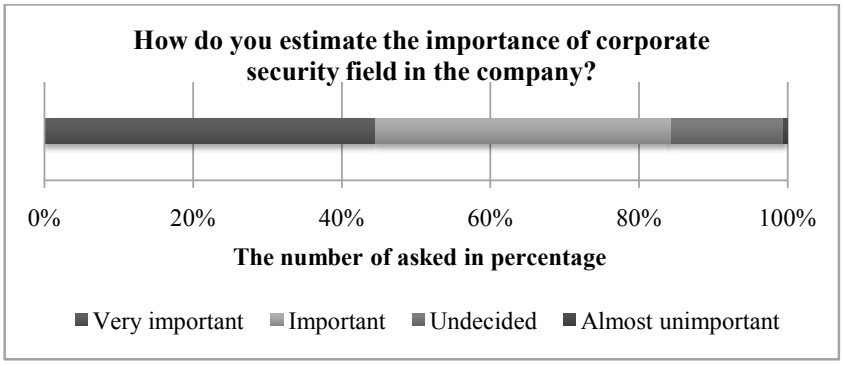


Figure 2: Estimation of the importance of corporate security field (Androić, 2013: 54)

Figure 3 shows the answers of the asked to the question »Is there a person employed in your company whose working task is merely care for corporate security?« The majority, 61% of the respondents answered there was no one employed in their company whose primary work task was corporate security. 20% of the employees in Slovenian companies do not know if such a person is employed in their company. Only 19% answered there was a person employed in their company who is responsible merely for the field of corporate security. The answers show that companies do not emphasize the field of corporate security, or incorporate it in other business functions of the company (Androić, 2013: 54).

Figure 3: Employment of a person whose work task is merely care for corporate security (Androić, 2013: 54)

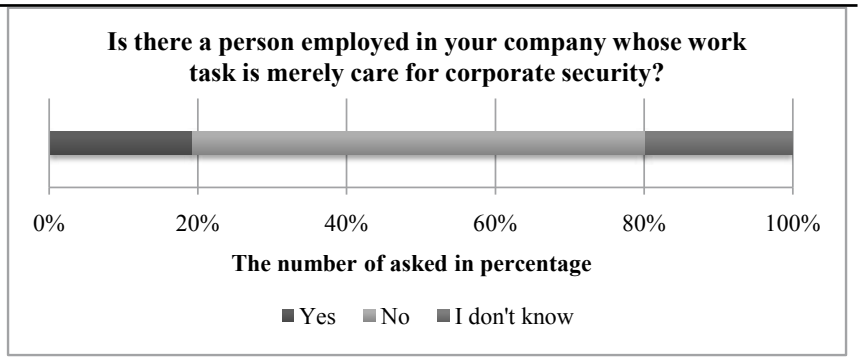


Figure 4 below shows that the majority of Slovenian companies take care of technical protection of the building by outsourcing for the whole field. This answer was chosen by 37%. They are followed by companies that provide technical protection of the building with their own personnel and equipment. This answer was chosen by 30% of the respondents, while 27% answered that their company takes care of technical protection of the building with outsourced personnel and their own equipment. Only 5% of the answered that their company takes care of technical protection of the building with their own personnel and hired equipment. We can conclude that the majority of companies in Slovenia hand over the entire or at least partial care for technical protection to outsourced personnel, since only less than a third of Slovenian companies take care of this field with their own personnel and their own equipment.

Figure 4: The care of Slovenian companies for technical protection of the building

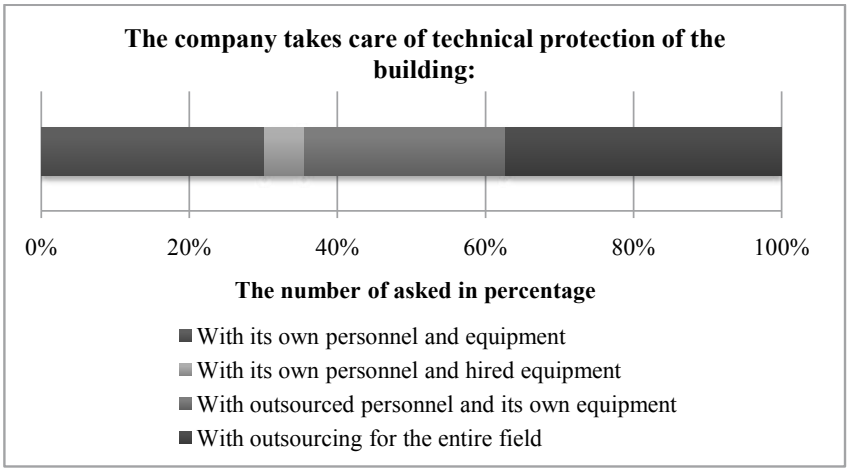


Table 1 shows the distribution of answers regarding the frequency of use of individual types of security surveillance, about which we inquired by means of question Q31. Video surveillance and alarm devices are used the most frequently, each occupying a 17% share among enumerated types of security surveillance. With smaller shares, together occupying a 65% share among all enumerated types of video surveillance, they are followed by cards for keeping records of coming to and leaving work, devices for detecting and preventing fire, entering cards for entering the premises, security guards, devices for detecting and preventing

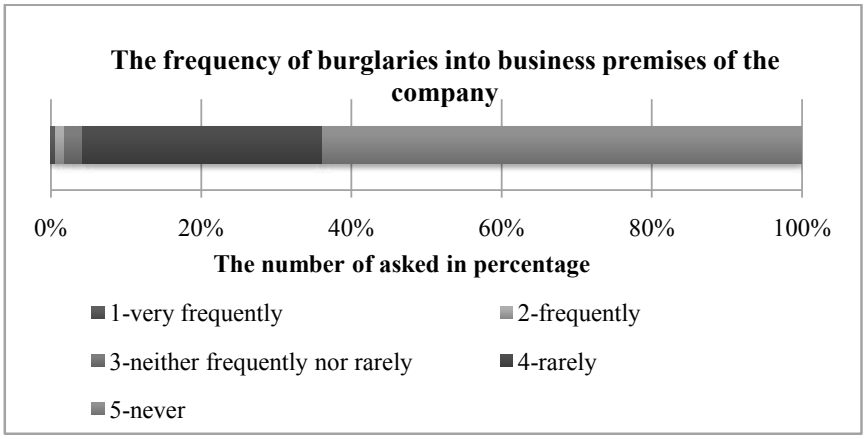
burglary (e.g. smoke screen), electronic key holes and recording telephone calls. Only a 1% share is occupied by biometry. Specifics of individual shares of answers are seen in the table below. Based on the answers received, we can infer that companies take good care of property protection, and indirectly also of the field of employees protection and the field of processes, data, information and documentation protection (Androić, 2013: 56–57).

Q31	**For security surveillance in the company the company uses:**					
	Sub questions	**Answers**		**Num. of units**	**Statements**	
		Frequencies	%		Frequencies	%
Q31a	Video surveillance	130	78%	166	130	17%
Q31b	Entering cards for entering premises	67	40%	166	67	9%
Q31c	Cards for keeping records of coming to and leaving work	115	69%	166	115	15%
Q31d	Electronic key hole	42	25%	166	42	6%
Q31e	Biometry	11	7%	166	11	1%
Q31f	Security guard	86	52%	166	86	11%
Q31g	Alarm devices	126	76%	166	126	17%
Q31h	Devices for detecting and preventing fire	100	60%	166	100	13%
Q31i	Devices for detecting and preventing burglary (e.g. smoke screen)	45	27%	166	45	6%
Q31j	Recording telephone calls	35	21%	166	35	5%
	TOTAL			166	757	100%

Table 1: Types of security surveillance (Androić, 2013: 57)

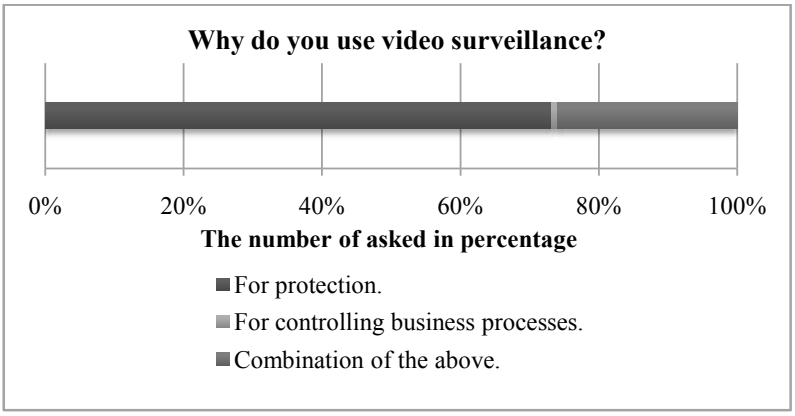
By using a 5-point Likert scale (1-very frequently, 2-frequently, 3-neither frequently nor rarely, 4-rarely, 5-never) respondents were asked to estimate the frequency of burglaries of the business premises of the company. Figure 5 shows that the most (64%) estimated that burglary never happens, while 32% estimated that burglaries are rare. 2% answered »neither frequently nor rarely«. Only 1% of the respondents estimated that burglaries of the business premises of the company are frequent or very frequent. The representative pattern shows that burglaries into business premises of Slovenian companies are as yet rare.

Figure 5: The frequency of burglaries into business premises of the company



In the research, we asked the question »Why do you use video surveillance?« The answers are summarized in Figure 6 below. The majority (69%) uses video surveillance for protection. They are followed by those who use video surveillance as a combination of protection, increasing the efficiency of operation and control of business processes. This combination was chosen by 26% of the respondents. Only 1% use video surveillance for controlling business processes. The answers of the representative pattern show that the majority of Slovenian companies use video surveillance only for protection purposes.

Figure 6: The purpose of using video surveillance



Question Q2 asked the respondents their opinion on the statements shown in Figure 7. The answers available were Yes and No. Figure 7 includes only »yes« answers, so the distribution of their answers can be seen more clearly. The most, as many as 97%, agreed with the given statement that the use of video surveillance deters potential offenders from forbidden actions (preventive function of video surveillance). 67% agreed with the statement that the use of video surveillance increases the sense of security of employees and customers. 58% agreed with the statement that due to the introduction of video surveillance, the employees behave »more carefully«, as they consider it as increase in security of the employees and visitors of the company. We can also conclude that the use of video surveillance

discourages potential offenders from forbidden actions and also increases the number of solved security incidents.

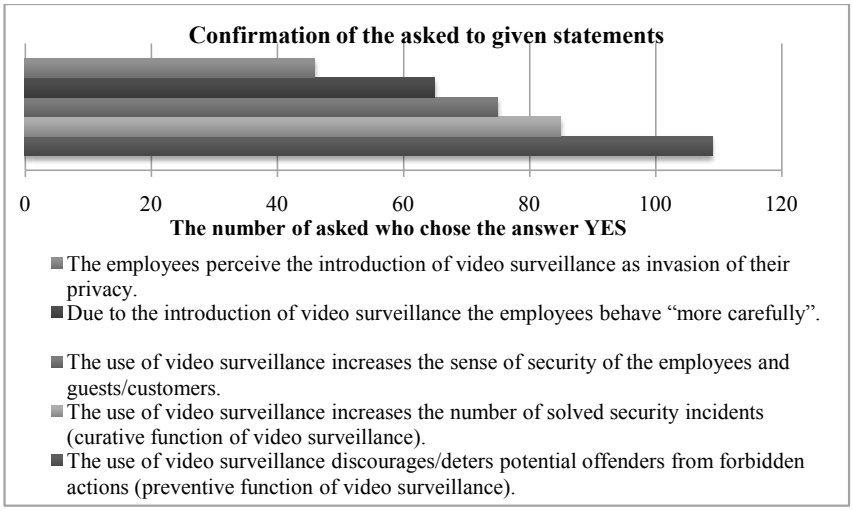


Figure 7: Confirmation of the asked to given statements referring to the use of video surveillance

The answer to the question »Do you have regulated security policy or directions of use and management of video surveillance?« was »Yes« by the majority (57%) of respondents. 20% answered »No«. It is interesting that as many as 23% answered »I don't know«. The distribution of answers is summarized in Figure 8. The representative pattern shows that an odd majority of Slovenian companies have regulated security policy or directions of use and management of video surveillance. Slightly alarming is the large percentage answering »I don't know«, which according to our estimation, shows that the employees are not sufficiently informed of internal acts of the company or security policies of the company.

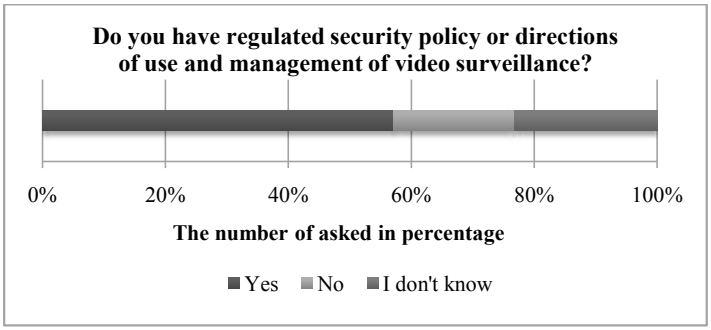


Figure 8: Security policy or directions of use and management of video surveillance

Figure 9 below summarizes answers to the question »Do you have a designated caretaker of video surveillance?« 44% responded that the company had outsourced security service as caretaker of video surveillance, while 35% answered that in their company, the caretaker of video surveillance was the person responsible for security or the company's security service. 11% chose the

answers »No« and »I don't know«. Based on the representative pattern, it can be concluded that the majority of Slovenian companies outsource security services as caretakers of video surveillance or use the company's security service. We believe the share of answers »No« and »I don't know« is too high, since security and video surveillance of the company belong to important business functions and processes of the company.

Figure 9: Designation of video surveillance caretaker

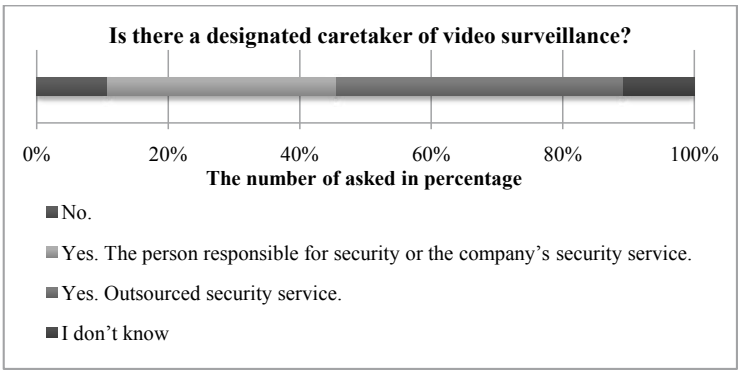
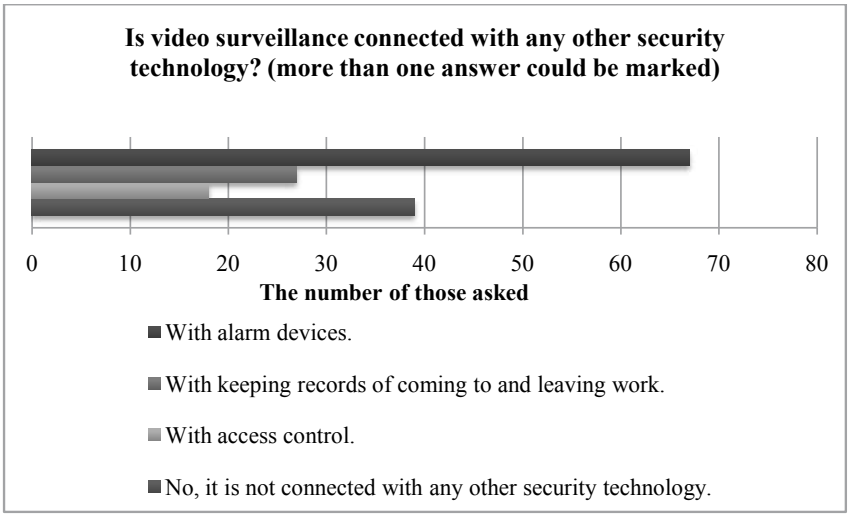


Figure 10 shows answers to the question »Is video surveillance connected with any other security technology? (more than one answer can be selected)«. We can see that most of the respondents, as many as 60%, think that video surveillance in the company is connected with alarm devices. This answer includes a 44% share of all answers among given choices. Then follows the answer that includes a 26% share of all given choices and was opted for by 35% of the respondents thinking that video surveillance in the company is not connected with any other security technology. The answer that video surveillance in the company is connected with keeping records of coming to and leaving work was chosen by 24%, and includes an 18% share of all answers among given choices. The fewest (26%) think that video surveillance in the company is connected with access control.

Figure 10: Connection of video surveillance with any other security technology



This answer includes a 16% share of all answers to a given choice. We think that the representative pattern shows the connection of video surveillance with other security technologies, which can however still be increased and expanded to connection with other security technologies that are constantly developing in today's technologically advanced world.

Table 2 shows the shares of answers to given statements. 39% of the respondents think that before the introduction of video surveillance, the company made risk analysis and evaluated the efficiency of existent security measures and consulted about legal requirements, 27% answered »No«, and 37% answered »I don't know«. 21% think that the organization follows or measures the efficiency of the CURATIVE function of video surveillance (comparison of the number of successfully SOLVED security incidents before and after the introduction of video surveillance, damage assessment before and after the introduction, etc.), 50 % answered »No«, and 29% »I don't know«. Only 19% of those responding think that the organization follows or measures the efficiency of PREVENTIVE function of video surveillance (comparison of the number of DISCOVERED security events before and after the introduction of video surveillance, damage assessment before and after the introduction, etc.), 51% answered »No«, and 30% answered »I don't know«. Based on the representative pattern, we believe this is alarming.

Q6	**Answer the following statements with yes or no:**					
	Sub questions	**Answers**				**Standard deviation**
		Yes.	No.	I don't know.	Total	
Q6a	Before the introduction of video surveillance you made risk analysis and efficiency assessment of existent security measures and consulted about legal requirements.	44 (39%)	27 (24%)	41 (37%)	112 (100%)	0.9
Q6b	The organization follows or measures PREVENTIVE function of video surveillance (comparison of the number of successfully SOLVED security events/incidents before and after the introduction of video surveillance, damage assessment before and after the introduction, etc.).	21 (19%)	57 (51%)	34 (30%)	112 (100%)	0.7
Q6c	The organization follows or measures the efficiency of CURATIVE function of video surveillance (comparison of the number of successfully SOLVED security events/incidents before and after the introduction of video surveillance, damage assessment before and after the introduction, etc.).	23 (21%)	56 (50%)	33 (29%)	112 (100%)	0.7

Table 2: Making the risk analysis before the introduction of video surveillance and measuring efficiency of preventive and curative functions of video surveillance

5 DISCUSSION

There is no doubt we live in a technological world. In the last few decades, information technologies have penetrated all aspects of our lives and organizations, and people are tightly coupled with information technology. Many vital processes and infrastructures are dependent on information systems that are based on sophisticated technologies (Potokar & Bernik, 2013). The results of our research show that the field of corporate security in Slovenia is becoming increasingly important and the companies in Slovenia mostly use video surveillance exclusively for protection, but there are already signs of awareness of the need in other fields as well. We find that companies in Slovenia are already aware of the need of changes in fields under research. There are also indications of changes in linking systems of protection.

From the results of the research, we can conclude that the field of corporate security in a company is important. On the other hand, companies do not seem to emphasize corporate security, or incorporate it in other business functions of the company. That may be because, as shown in Figure 5, the frequency of burglaries of business premises of the companies are as yet rare, as most of the respondents (64%) estimated that burglary never happens and 32% estimated that burglaries are rare. The reason for such an estimation can be in performing video surveillance which also serves as a preventive measure in preventing criminality. The most, as many as 97% of those responding, agreed with the given statement that the use of video surveillance deters potential offenders from forbidden actions (Question Q2 – preventive function of video surveillance). It is known that installing technical means for controlling public places such as shopping centres, banks and parking lots, for the purpose of reducing possibilities of theft and other criminal acts, belongs to the so called situational strategy of criminality prevention (Meško, 2000).

We can conclude that the majority of companies in Slovenia hand over the entire or at least partial care for technical protection to outsourced personnel, since less than a third of Slovenian companies take care of this field with their own personnel and their own equipment. Regarding the use of the individual types of security surveillance, video surveillance and alarm devices are used the most frequently, each occupying a 17% share among enumerated types of security surveillance.

The research (Table 2) revealed that only a small share of Slovenian companies conduct risk analysis and efficiency assessments of existent security measures and consult about legal requirements before the introduction of video surveillance. Alarming is also a small share of Slovenian companies that follow or measure the efficiency of preventive and curative functions of video surveillance. We think that many Slovenian companies were unprepared when they introduced video surveillance and they somehow do not know how to use its abilities and advantages entirely, since they mostly cannot measure the efficiency of video surveillance.

The majority of Slovenian companies (69%) use video surveillance only for protection purposes, which can be due to the legal regulations in Slovenia. Video surveillance is regulated in Articles 74 to 77 of chapter 2 of the Personal Data Protection Act (Zakon o varstvu osebnih podatkov, 2007). General provisions define the implementation of video surveillance and state that the public and private sectors may implement video surveillance of access to their official office premises or business premises if necessary for the security of persons or property, for ensuring supervision of entering to or exiting from their official or business premises, or where the nature of the work presents a potential threat to employees (ZVOP-1, 2005). If we compare the results from the research about video surveillance use in the Republic of Slovenia that was conducted, with the analysis of the results of personal data inspections and reports of Information Commissioner of the Republic of Slovenia, we can state that the results of the research show that video surveillance is rapidly growing and that the main irregularity stays the same. In the last period, it is perceived that video surveillance also appears in the fields where it is forbidden by the law (Potokar & Bernik, 2014). This statement is supported by the representative pattern in Figure 10 which shows the connection of video surveillance with other security technologies, which can however still be increased and expanded to connection with other security technologies that are constantly developing in today's technologically advanced world. We can conclude the use of video surveillance systems and its problems are manifold. The use of video surveillance has positive effects on the level of security in the environment where it is used, and it helps in investigation of criminal offences, but the danger is in the use of these systems merely for surveillance and control of people. The risk of abuse can increase if several technologies are combined.

In Europe there is quite a lot of literature and research in the field of video surveillance systems and privacy (see, e.g. Armitage, 2002; Armitage, Smyth, & Pease, 1999; Beck & Willis, 2011; Brown, 1995; Capers, 2008; Cerezo, 2013; Davies & Velastin, 2005; Groombridge, 2002; McCahill & Norris, 2002; Surette, 2006). But in the region of Slovenia, there are only few research projects and papers regarding video surveillance in view of information security and privacy. Results outlined in this paper and their interpretation will be the impetus for further research regarding video and other surveillance systems and systematic approach of their regulation in Slovenia.

REFERENCES

Armitage, R. (2002). *To CCTV or not to CCTV.* London: Nacro Crime and Social Policy Section.

Armitage, R., Smyth, G., & Pease, K. (1999). Burnley CCTV evaluation. *Crime Prevention Studies, 10*, 225–249. Retrieved from http://www.popcenter.org/library/crimeprevention/volume_10/09-Armitage.pdf

Androić, S. (2013). *Upravljanje s poslovno dokumentacijo in korporativna varnost* (Master thesis). Celje: Mednarodna fakulteta za družbene in poslovne študije.

Beck, A., & Willis, A. (2011). *Context-specific measures of CCTV effectiveness in the retail sector.* Retrieved from http://www.urbaneye.net/results/ue_wp6.pdf

Bernik, I., & Prislan, K. (2013). Information security in risk management systems: Slovenian perspective. *Varstvoslovje, 13*(2), 208–221.

Brown, B. (1995). *CCTV in town centres: Three case studies.* Police Research Group Crime Detection and Prevention, Series Paper 68. London: HMSO.

Capers, C. T. (2008). *Effectiveness of situational prevention strategies to deter organized retail theft* (Doctoral thesis). Phoenix: University of Phoenix.

Cerezo, A. (2013). CCTV and crime displacement: A quasi-experimental evaluation. *European Journal of Criminology, 10*(2), 222–236.

Čaleta, D. (2011). Varnost mojega podjetja. *Podjetnik, 11*(10), 40–41.

Davies, A. C., & Velastin, S. A. (2005). *A progress review of intelligent CCTV surveillance systems.* Paper presented at IDAACS'05 Workshop, Sofia, September 2005. Retrieved from http://www.async.org.uk/Tony.Davies/pubs/CCTV_ACDavies_for_IDAACS.pdf

Golob, R. (1997). *Sistemi zaščite in varovanja oseb in premoženja.* Ljubljana: R. Golob.

Groombridge, N. (2002). Crime control or crime culture TV. *Surveillance & Society, 1*(1), 30–46.

Ivanovič, Ž., & Habbe, J. (1998). *Kako preprečiti tatvine v prodajalnah*. Ljubljana: Lisac & Lisac.

McCahill, M., & Norris, C. (2002*). CCTV in London*. Retrieved from http://www.urbaneye.net/results/ue_wp6.pdf

Mencinger, J., & Meško, G. (2004). Veliki brat in učinkovitost video nadzorovanja v Angliji. In T. Pavšič Mrevlje (Ed.), *Zbornik prispevkov 5. slovenski dnevi varstvoslovja* (pp. 862–872). Ljubljana: Fakulteta za varnostne vede.

Meško, G. (2000). Pogledi na preprečevanje kriminalitete v pozno modernih družbah. *Teorija in praksa*, *37*(4), 716–727.

Potokar, M., & Bernik, I. (2013). The phenomenon of information social networks and security challenges. In D. Čaleta & M. Vršec (Eds.), *Management of corporate security: New approaches and future challenges* (pp. 201–207). Ljubljana: Institute for Corporative Security Studies.

Potokar, M., & Bernik, I. (2014). Video surveillance from the personal data protection point of view. In D. Čaleta, M. Vršec, & B. Ivanc (Eds.), *Corporate security – open dilemmas in the modern information society* (pp. 131–138). Ljubljana: Institute for Corporative Security Studies.

Ramšak, R. (2010). *Priprava ter izdelava in uporaba načrta varovanja oseb in premoženja v gospodarski družbi Premogovnik Velenje d.d.* (Diploma thesis). Velenje: Fakulteta za varnostne vede.

Surette, R. (2006). The thinking eye: Pros and cons of second generation CCTV surveillance systems. *Policing: An International Journal of Police Strategies & Management*, *28*(1), 152–173.

Trivan, D. (2013). Corporate security in the Southeast European countries under conditions of global economic crisis. In D. Čaleta & M. Vršec (Eds.), *Management of corporate security – new approaches and future challenges* (pp. 51–62). Ljubljana: Institute for Corporative Security Studies.

Vacca, J. R. (2007). *Biometric technologies and verification systems*. Burlington: Elsevier.

Vršec, M. (1993). *Varnost podjetja – tokrat drugače.* Ljubljana: Viharnik.

Vršec, M. (2013). Varovanje poslovnega informacijskega sistema na osnovi politike informacij. *Korporativna varnost,* (3), 9–11.

Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1) [Personal Data Protection Act]. (2007). *Uradni list RS*, 94/2007.

About the Authors:

Marko Potokar, M.Sc., State Supervisor for Personal Data Protection at Information Commisioner of the Republic of Slovenia and an invited lecturer on faculties and colleges. His research fields are information technologies and there influence on security and privacy.

Sanja Androić, Master of management, Head of reception office, Public Water Supply Company Maribor (Mariborski vodovod d.d.), Slovenia. Her research fields are management with business documentation, knowledge management, and corporate security.

VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 16 no. 2 pp. 164–177

»Persona Sine Anima« – Towards an Innovative Classification of Legal Persons

Bojan Tičar

Purpose:

In this article, the author defines legal entities (in title as *»personas without soul«* according to pope Innocent IV.) and classifies them by applying interest theory and an adapted method of system analysis, also taking into account the legal personality of legal entities. An innovative classification that is applicable not only for *ad hoc* legal-economic analyses but also for a practical classification of legal entities when establishing their personality, concerning both private and public law, is demonstrated in an original manner.

Design/Methods/Approach:

The research approach of this article is theoretical and uses comparative analysis. The author's goal was to prove that legal entities can be classified in a legally-correct and economically-applicable manner, according to the interest and classical theories of systems, and not only through the forms of legal entities recognised in law. The classification originates in the ancient Roman classification of legal entities as corporations and foundations *(universitas personarum, universitas bonorum)* and classifies them according to the criteria of authoritativeness, functionality, and voluntary association. The approaches are compatible and can easily be arranged in a schematic form.

Findings:

The *thema probandi* of this article is to prove that legal entities can be classified in a legally-correct and economically-applicable manner also according to the interest and classical theories of systems and not only through the forms of legal entities recognised in law. The approaches are compatible and can easily be arranged in a schematic form. Such classification of legal persons is appropriate for security studies, as well as for broader economic and legal research.

Originality/Value:

The value of this article is that it proposes a new and original classification of legal entities. This is applicable, in a practical sense, universally and globally. In Slovenia it is applicable in its entirety, and can be partly applicable, however, in cases in which the legal order of a state determines the personality of legal entities, differently than is the case in Slovenia. In such an instance, the table can be easily and quickly adapted, as the criteria for the classification of legal entities into authoritative, functional, and associative, are, in the opinion of the author, universal.

UDC: 347.191

Keywords: legal entity, personality of a legal entity, systemic theory, interest theory, profitability, unprofitability

»Oseba brez duše« – nasproti inovativni klasifikaciji pravnih oseb

Namen prispevka:

Avtor je v pričujočem prispevku pravne osebe klasificiral z vidika uporabnosti nove in inovativne tabele za raziskovalne in praktične namene. Pravne osebe (ki jih avtor naslovno imenuje *»osebe brez duše«* tako kot papež Innocent IV.) je avtor razvrstil po interesni teoriji in preneseni metodi klasifikacije upravnih sistemov, upoštevaje njihovo pravno subjektiviteto. Originalno je prikazana inovativna klasifikacija, ki je uporabna tako za *ad hoc* pravno-ekonomske analize kot tudi za praktično razvrščanje pravnih oseb pri potrebah za ugotavljanje njihove subjektivitete, pa naj gre za ekonomsko analizo prava, vprašanja zasebnega ali javnega prava ali praktične pravne postopke.

Metode:

Raziskovalni pristop oziroma metode v članku so kombinacija klasičnih pravnih metod teleološke razlage ureditve v kombinaciji s historično in delno komparativno analizo. Klasifikacija pravnih oseb zgodovinsko izhaja iz antične rimske in nato nemške razvrstitve pravnih oseb na korporacije in ustanove *(universitas personarum, universitas bonorum)* in jih sodobno umešča po merilih oblastnosti, funkcionalnosti in nepridobitnosti (oz. dobrodelnosti).

Ugotovitve:

Thema probandi raziskave, predstavljene v članku, je dokazati, da lahko pravne osebe pravno-pravilno in ekonomsko-uporabno klasificiramo tudi interesno in po klasični teoriji sistemov, ne samo skozi statusno-pravno obliko. Pristopi so med seboj združljivi in se jih da enotno tabelarično prikazati. Takšna klasifikacija je uporabna tako za varnostne študije kot tudi za ekonomske in pravne analize, ko je treba opredeliti subjektiviteto organizacij.

Izvirnost/pomembnost prispevka:

Izvirnost članka je v oblikovanju nove sodobne klasifikacijske tabele pravnih oseb, ki je uporabna tako za raziskovalne kot za praktične namene. Uporabnost navedene tabele je v njeni hitri uporabi, saj je iz nje *prima vista* razvidno, katere pravne osebe sodijo v javni sektor in katere v zasebnega. Nadalje je iz tabele razviden tudi interes, zaradi katerega so ustanovljene, ki je lahko javni/oblastni ali javni/neoblastni ter zasebni/profitni ali zasebni/neprofitni. Tabela omogoča nazorni pregled nad pravno subjektiviteto organizacij in ločevanje le-teh od organizacij, ki pravne subjektivitete nimajo. To je pomembno tako za delovanje pravnega sistema, pravno-ekonomske raziskave kot tudi za praktične pravne postopke.

UDK: 347.191

Ključne besede: pravna oseba, subjektiviteta pravne osebe, sistemska teorija, interesna teorija, profitnost, neprofitnost

1 INTRODUCTION

This article is based on the theoretical assumption that a legal entity is a social organisation, i.e., a special form of a social system. From a systemic-theoretical point of view, we proceed from the assumptions that were formulated and developed by Harvard sociologist *T. Parsons* in the 1950s (Parsons, 1951; Turner, 1991). From a legal point of view, we applied these assumptions using a prism of interest-legal theory (Kelsen, 1992; Pavčnik, 2001) and a contemporary American view of the economic interest of an organisation (Hazlitt, 1962). Furthermore, from a legal point of view, we proceed from an ancient Roman understanding of a legal entity as a corporation or foundation (Bohinc, 2005; Grafenauer & Brezovnik, 2006; Trstenjak, 2003) and from an understanding of the corporate personality, as was developed by *A.W. Machen* in the 1910s (Machen, 1910). By combining these assumptions, we created a new model of a *sectoral and interest-systemic classification of legal entities.*

The *thema probandi* of this article is to prove that legal entities can be classified in a legally-correct and economically-applicable manner according to the interest and classical theories of systems, and not only through the forms of legal entities recognised in law. The approaches are compatible and can easily be arranged in a schematic form. We prove this using an applicative table elaborated in the third section of this article.

In our opinion, such an approach is a theoretical addition to a *Pareto-Parsons* (U. S. Department of Labor, Bureau of Labor Statistics, 2006) conception of social systems, as the classic systemic theory does not take into account that a social system can also have a legal personality. Furthermore, our approach is a new perspective of Machen's model of a corporation as exclusively a public limited company, that in our opinion, corporations can also be authoritative and associative organisations.

The objective of this article is to create a new, relatively simple tool for correctly, quickly, and efficiently classifying legal entities in the public and private sectors, and for distinguishing legal entities regarding their substantive essence (e.g. their profitability, unprofitability, authoritative, and associative natures).

All of the above mentioned is important for a legal-economic analysis of the operation of legal entities, particularly for an economic analysis of law (Zajc, 2009). In the private sector, it is practically applicable for management in business decision-making and management accounting, whereas in the public sector it is applicable in the identification of the functionality of the public interest and the level of authoritativeness of legal entities.

We are aware of the fact that by a sectoral classification of legal entities based on interest and systemic theories, we might be leaving out certain classification elements according to the criteria of other theories. Perhaps we have not included certain *sui generis* forms of legal entities. However, we are of the opinion that the majority of the forms of legal entities are included and that our classification retains essential substantive classification elements and consequently allows for effective *ad hoc* analysis, which is intended for university-level education and quick application in practice.

In the second section of the article, we outline what a legal entity represents from a legal-theoretical point of view and delimited it from other subjects under law, i.e., natural persons. A legal entity is *per definitionem* an artificial legal structure that comprises assets intended for a certain purpose *(universitas bonorum; i.e. foundations)* or a group of individuals *(universitas personarum, i.e. corporations)*, whereas a given legal order recognises legal entities the position of subjects under law (Aubelj, 2003; Bohinc & Tičar, 2006; Trstenjak, 2003). The bodies of the legal entity act in its name in legal transactions. Different from natural persons, legal entities, as a general rule, gain legal capacity upon registration in an appropriate register or by means of some other legal act. A legal entity has narrower legal capacity than a natural person, and its contractual capacity is limited by its legal capacity.

In the third section of the article, we classify legal entities by applying an adapted method of system analysis, also taking into account the legal personality of legal entities. In our opinion, such a classification is applicable for study purposes, and is practical, universal, and global. In Slovenia, it is applicable in its entirety, for it is based on the Slovenian legal regulation of the forms of legal entities. The table can be partly applicable, however, in cases in which the legal order of another country determines the personality of legal entities differently than is the case in Slovenia. In such an instance, the table can be easily and quickly adapted, as the criteria for the classification of legal entities are, in our opinion, universal. The classification, as mentioned above, originates in the classification of legal entities into corporations and foundations (Trstenjak, 2003) and classifies them according to the criteria of authoritativeness, functionality, and association.

2 DEFINITION OF LEGAL ENTITY

In the legal orders of various countries, two types of subjects are, as a general rule, holders of individual property rights, i.e., natural persons and legal entities.

Natural persons are humans and in law, they are also known as individuals. Legal entities are not humans, but organisations that are artificial legal subjects established by legal acts. Legal entities are artificial social structures that are granted legal personality by law (Tičar, 2012).

A legal entity is an artificial social structure whose legal personality is based on a legal fiction (Aubelj, 2003) and is a special institution under law - *persona ficta* (Dewey, 1926). The legal personality of a legal entity entails that legal entities, in addition to natural persons, are the subjects (Bradač, 1990) that can hold the majority of property rights and obligations or duties that are recognised to them by the legal order (Trstenjak, 2003).

A legal entity is an organisation and a social system that has legal and contractual capacities and acts as an independent subject in legal transactions. A legal entity does not begin naturally by birth, as a natural person, but legally by its articles of association, which are always a legal act.

The legal order recognises a legal entity the status of a subject under law and legal capacity due to its particular characteristics. The legislation prescribes the

conditions for the establishment and existence of legal entities, such as the purpose of the establishment of the legal entity, its bodies, organisation, and assets.

2.1 Corporations and Foundations as Legal Entities

As mentioned above, from a legal point of view there are two forms of legal entities:

1. as a result of an association of other persons – *a corporation*, and
2. as assets intended for a special purpose – *a foundation*.

A corporation *(universitas personarum)* is a membership organisation intended for the purposes of its members. The essential elements of a foundation are assets *(universitas rerum, universitas bonorum)* which the founder(s) intend(s) for a special purpose. A foundation does not have members, but only assets intended for a certain purpose.

A corporation is a different type of a legal entity. A defining element of a corporation is that it unites several entities in a manner such that a new entity is established. From a legal point of view, a new entity is different from those united in a corporation. The individuals or entities that establish a corporation are its founding members. They can be legal entities or natural persons (in certain cases, one founder suffices to establish a corporation; e.g. under Slovenian law one founder suffices to establish a limited liability company). However, from a legal point of view, the essence of a corporation is that it remains an entity, regardless of the fact that its members change (Trstenjak, 2003).

The members of a corporation form and express the will of the corporation by appointing its management (e.g., the president of a society, the director of a limited liability company, the management or management board of a public limited company, etc.).

The legal sphere of the property rights of the corporation is separated from the legal sphere of the property rights of its members (i.e. shareholders). If a corporation is a company with shared capital, the legal order prescribes minimal founding capital for the protection of the creditors of the corporation. The members do not have any rights regarding the assets of the legal entity, as it is itself the holder of its rights. Members have membership or corporate rights in relation to the corporation. In cases of companies with share capital, they may appoint management, participate in the annual profit distributions (i.e. dividends) in proportion to their share, and participate in the liquidation of the estate in the case of the termination of the corporation by liquidation.

The bodies of the corporation (i.e. the president, director, management, and management board, depending on the form of the corporation) act in its name in legal transactions. Members of the corporation influence the management and business operations of the corporation by appointing or electing the bodies and by giving them instructions regarding the relevant circumstances.

The two main types of public sector corporations are the state and municipalities. The members of the state are the citizens and legal entities that

have their head office in the territory of the state. Municipalities, and in certain instances localities, if they have their own legal personality in accordance with the municipal charter, are also corporations.

In the private sector, corporations are commercial or associative. Commercial corporations include most of all companies with shared capital. Partnerships are not classified among corporations, as in the legal order they usually do not have legal personality. Associative private corporations include societies with their members, religious communities with their members; believers, political parties with party members, and trade unions with trade union members.

A foundation, on the other hand, is a legal entity whose basis are assets. The foundation's assets are managed by the management for a certain purpose. Foundations do not have members or shareholders, but only management and possibly other bodies as determined by law. A surplus of income over expenditures from business activities and financing is directed towards the purpose for which the foundation was established and may not be distributed as profit to its founders. In the private sector, foundations are private foundations, whereas in the public sector they are public funds.

2.2 The Legal Personality of a Legal Entity

Legal personality is a legal characteristic of subjects so that they can be holders of legal rights and obligations (Martin, 2003). For a definition of the legal personality of a legal entity, it is essential that it can be a holder of property rights and obligations in legal transactions. The state, through its legal order, recognises legal personality to a legal entity so that it defines it by law as a special subject under law.

As a general rule, it applies that there is a limited number of legally recognised forms of legal entities. This is the principle of a closed number or the *numerus clausus* principle. This principle fully applies to the private sector, whereas in the public sector it applies only partly, as the legislature can always introduce a new form of legal entity by a new *lex specialis* (Pirnat, 1995).

The state is also a legal entity, whose legal personality is recognised by other states and consequently by the international legal orders (Shaw, 2003).

A legal entity is thus an organisation having legal capacity and an independent subject in legal transactions. In order for a certain organisation in a certain legal order to acquire the status of legal entity (i.e. legal personality), basic conditions must be fulfilled, including:

1. there must be a certain purpose for establishing the legal entity;
2. there must be means to achieve such purpose of the legal entity;
3. there must be management (and other bodies) necessary to achieve the purpose of the legal entity; and
4. it must have a legally admissible organisational form of a legal entity (Trstenjak, 2003).

The legal personality of a legal entity furthermore entails that:

1. it can own movable property and real estate;
2. it can acquire property rights and assume obligations;
3. it can sue and be sued; and
4. it is responsible for its obligations with all its assets (Bohinc & Tičar, 2006).

The legal order recognises a legal entity having the status of a subject under law and legal capacity due to its particular characteristics. In order to define a legal entity from the legal point of view, the basic defining elements of its status as a legal subject must be identified. These are:

1. its form as a legal personality;
2. the designation of its name in legal transactions (i.e. the name of the company);
3. its head office, i.e. the place where the legal entity is based;
4. its activity – production or services; and
5. the means necessary for its operations (e.g. minimal founding capital in the case of companies with share capital).

From the perspective of legal transactions, it is most important that the legal entity has legal capacity and contractual capacity. The legal capacity of a legal entity entails that it is capable of being a holder of rights and obligations. This is passive capacity. Legal capacity is a characteristic of a legal entity, and is not a special right, but the foundation of all rights and obligations. The abstract nature of legal capacity entails that a legal entity is capable of accepting certain rights and obligations in legal relations, if the conditions that are prescribed particularly for such are fulfilled. Furthermore, the general nature of legal capacity entails that it refers to all property rights (except for those property rights granted only to individuals) and legal relations, and that there are no reservations for the acquisition of any of the specific rights and legal positions if the conditions for such are fulfilled.

In addition to legal capacity, legal entities must also have contractual capacity in order to enter into legal transactions. This is active capacity. Contractual capacity is the capacity to perform legally binding actions, which is, as a general rule, expressed by the management of the legal entity in its name. Legal entities gain both capacities simultaneously, i.e. when management is appointed and a decision on their registration in an appropriate register becomes final.

The capacity to act is the capacity to form the legal entity's will regarding its business operations. Management, as the legal representative of a legal entity, has such capacity and it entails the capacity to decide on facts that cause legal consequences. Contractual capacity is also the capacity to form a will regarding business operations and express decisions in a manner such that a legal entity enters into legal relations. It thus concerns the capacity to express the will of the legal entity regarding business operations in a legally effective manner. The contractual capacity of a legal entity is the capacity of its management to form and express the legal entities will regard business operations in its name and on its account.

2.3 The Economic Reasons for the Legal Regulation of a Legal Entity as a Special Subject under Law

Why is the regulation of a legal entity as a special subject under law at all necessary?

The answer can be found in substantive logic, which in law is economic in nature, as a general rule.

Historically, the concept of the personality of a legal entity arose in medieval, Catholic ecclesiastical law. According to the American legal historian John Dewey, the author of the idea was Pope Innocent IV (1195–1254), who gave legal personality to monasteries in order to separate their assets from the assets of monks. Such a monastery with legal personality was named a *persona ficta*. The reason for the introduction of the concept of the *persona ficta* was originally economic, as a *persona ficta* did not have a soul and thus could not be guilty of property offences (Dewey, 1926).

Similarly, a legal entity is also today an artificially created entity for economic reasons. From a legal point of view, the reason for such is so that it can be a holder of property rights and obligations equal to a natural person. Property rights are in general economic rights.

A property right in the context of contemporary understanding of the personality of legal entities represents a protected individual and concrete entitlement of subjects under law (Pavčnik, 2001; Perenič, 2005). Legal entities and natural persons are equal holders of property rights, unless the legal order explicitly reserves such only for natural persons (e.g., personal easements).

From a theoretical point of view, a property right entails a legally protected proerty entitlement *(facultas agendi)*, and on the basis of a property right, a subject has a legal entitlement to act in a certain manner. In cases of property-related legal rights, by means of its coercive apparatus, the state protects the private interests of the subject (e.g. property) that are in actual or potential conflict with the interests of other subjects. The interests of a subject may also be in conflict with the interests of the state; however, a state governed by the rule of law must protect the subject's interests to the subject's benefit, not its own. Therefore, only law, as a special and unique normative system, in fact restricts the arbitrary or discretionary use of the monopolistic power of the state (Pavčnik, 2001).

The property right of a subject under law always entails the property obligation of other subjects to act in a certain manner or to refrain from certain conduct to the benefit of the subject who has the property right.

A legal right is a double and ambiguous term. In its substance, every property right is comprised of the legally protected property interest of one legal subject and the legally determined property duty of other legal subjects. On the whole and from the viewpoint of both, a right is in fact a claim right, as upon its legal implementation an exchange of legally protected interests between both subjects occurs.

A property right is comprised of two entitlements: a basic property entitlement and a property claim. A basic entitlement allows subjects to exercise their own interests if they are in accordance with the legal purpose of the entitlement. A legal claim contains the possibility that the state will, in the interest of the subject,

impose a coercive sanction if a subject who has an obligation arising from the right does not act in accordance with their obligation.

A property right, on the one hand, thus contains a property entitlement of one subject, and a duty or obligation of other subjects, on the other. Therefore, broadly speaking (e.g. in accordance with the will theory and the interest theory), a property right is always a claim right of the subject (Aubelj, 2003).

A property right is absolute if it applies to everyone (i.e. with *erga omnes* effect; e.g. an ownership right, an easement, a lien, a land debt). However, a property right is relative if it applies only between given subjects (Pavčnik, 2001).

The essence of the existence of a legal entity is that the legal order recognises it to be a holder of rights and obligations equal to a natural person, unless such rights are reserved exclusively for individuals (e.g. moral copyright is reserved only for a person and not for a legal entity).

3 NEW CLASSIFICATION OF LEGAL ENTITIES

As mentioned above, legal entities are social organisations that are holders of property rights and represent a group of membership, or property-oriented entities that mutually cooperate in order to achieve a common, specific, and legally admissible objective. In general, organisations are established, founded, and created to achieve certain objectives.

Subjects establish organisations or are included therein in order to achieve one of the set objectives. Such objectives are thus a primary element of an organisation. Objectives entail what the organisation wants to achieve, and therefore are the basic starting points for the decision-making and operations of the organisation.

The general elements of an organisation are the following: (1) the objectives of the organisation; (2) the personal substrate (the people in the organisation); (3) the material substrate (the means of the organisation); (4) the independence of the organisation; and (5) its internal organisational structure (Grafenauer & Brezovnik, 2006).

The elements of the organisation as a legal entity are the same as in all other organisations. However, the elements of organisations, i.e. legal entities, also have distinctive characteristics. The latter are the only organisations having a legal personality (Pusić, 2002).

As organisations, and with regard to their objectives and manner of operation, legal entities are divided into: (1) territorial legal entities in the public sector; (2) functional legal entities in the public and private sectors; and (3) associative-voluntary legal entities in the private sector which operate in the public or private interests (Grafenauer & Brezovnik, 2006). The structure of legal entities as organisations is shown in the Table 1.

Table 1: Sectorial (interest-systemic, legal) classification of legal entities

PUBLIC SECTOR – PUBLIC (INCLUSIVE) INTEREST		PRIVATE SECTOR – PRIVATE (EXCLUSIVE) INTEREST			
1. SYSTEMIC CLASSIFICATION ACCORDING TO THE TYPE OF A LEGAL ENTITY AS A SOCIAL SYSTEM					
TERRITORIAL AND AUTHORITATIVE LEGAL ENTITIES (CORPORATIONS)		FUNCTIONAL LEGAL ENTITIES (FOUNDATIONS AND CORPORATIONS)			CHARITABLE-VOLUNTARY LEGAL ENTITIES (CORPORATIONS)
2. INTEREST CLASSIFICATION ACCORDING TO THE TYPE OF INTERESTS NECESSARY FOR THE ESTABLISHMENT OF THE LEGAL ENTITY					
PUBLIC AUTHORITATIVE INTEREST	PUBLIC NON-ECONOMIC INTEREST	PRIVATE NON-ECONOMIC INTEREST	PRIVATE ECONOMIC INTEREST		PRIVATE NOT-FOR-PROFIT INTEREST table
3. LEGAL CLASSIFICATION ACCORDING TO THE CLASSIC TYPES OF LEGAL FORMS OF LEGAL ENTITIES					
PUBLIC NOT-FOR-PROFIT CORPORATIONS	**PUBLIC PARTLY FOR-PROFIT FOUNDATIONS**	**PRIVATE PARTLY FOR-PROFIT FOUNDATIONS**	**PRIVATE FOR-PROFIT CORPORATIONS**		**PRIVATE NOT-FOR-PROFIT CORPORATIONS**
STATE	PUBLIC INSTITUTIONS (NOT-FOR-PROFIT)	PRIVATE INSTITUTIONS (NOT-FOR-PROFIT)	COOPERATIVES (BUSINESS COOPERATION BETWEEN MEMBERS, RISTORNO) COMMERCIAL ASSOCIATIONS (BUSINESS COOPERATION BETWEEN MEMBERS)		SOCIETIES
	PUBLIC AGENCIES	PRIVATE INSTITUTIONS WITH CONCESSION	COMMERCIAL COMPANIES – ABSOLUTELY PROFIT-ORIENTED LEGAL ENTITIES (FOR-PROFIT)		FEDERATIONS OF SOCIETIES
MUNICIPALITIES (LOCALITIES IF THEY ARE LEGAL ENTITIES)	PUBLIC FUNDS	FOUNDATIONS	COMPANIES WITH SHARE CAPITAL	PARTNERSHIPS	RELIGIOUS COMMUNITIES
	PUBLIC COMMERCIAL INSTITUTIONS		PUBLIC LIMITED COMPANIES (LIMITED PARTNERSHIPS WITH SHARE CAPITAL)	UNILIMITED COMPANIES	POLITICAL PARTIES
	SUI GENERIS CORPORATIONS (PUBLIC AND PRIVATE), e.g. SLOVENIAN ACADEMY OF SCIENCES AND ARTS, PUBLIC CHAMBERS, PRIVATE CHAMBERS		LIMITED LIABILITY COMPANIES	LIMITED PARTNERSHIPS	TRADE UNIONS

In Table 1, legal entities are classified into the public or private sector regarding sectoral, systemic, interest, and legal-organisational criteria. The table is based on the following theoretical assumptions:

1. sectoral division into public and private sectors;
2. the interest theory of the general theory of law *(Kelsen's model)*;
3. the systemic theory *(Parsons' model)* of an organisation as a social system; and
4. the general *(ancient Roman model)* theory of legal entities.

The table can be read vertically and/or horizontally. If read vertically, a line between the public and private sectors that divides legal entities into legal entities under public law and legal entities under private law can be seen. Horizontally, interests and the types of legal-organisational forms are shown. The primary characteristic of the public sector is that it serves the pubic interest, and of the private sector that it serves the private interest. The public interest is authoritative and is served by the state and municipalities, i.e. it is »functional and non-economic«, which is demonstrated mostly through the provision of public

services. The latter is ensured by specialised entities under public law that are not a part of the state or municipal administrations. A private interest is functional and associative-voluntary.

The first is either non-economic and served primarily by private institutions, or economic, which entails an interest in profit. It is served by companies with share capital and partnerships. However, this may also entail an interest in business cooperation between members and not primarily in profit. It is a foundation for the establishment of cooperatives and commercial associations. Special legal entities, such as societies, religious communities, and trade unions carrying out voluntary activities serve private interests.

In Table 1 the public sector comprises, *de lege* lata, in addition to the state and municipalities, non-economic activities of public importance that are, in accordance with the law, organised directly by the state or local administration, with the assistance of entities under public law (e.g. public institutions, public agencies, public funds) and which are not an integral part of the authoritative (territorial) public administration. The mere fact that the state or a local community has a capital investment in a given subject under law does not entail that it is a subject of the public sector. Regardless of the fact that the legal character of such investment is public (i.e. state, local) ownership, the legal regime over its management from the viewpoint of the status of employees and of the market is predominantly that of private law (apart from exceptional cases in the field of public procurement and public-finance reporting, in which also such legal entities are obliged to carry out public procurement procedures and public-finance reporting). If, for example, the case concerns a company owned by the state (e.g. The Postal Service of Slovenia, Slovenian Railways, The Port of Koper), the applicable legal regime is that of private law and the regulatory function of the state may not influence its capital entitlements.

4 DISCUSSION

One practical value of this table is its quick application. It is *prima vista* evident from the table which legal entities are a part of the public sector (i.e. the state, municipalities, and functional legal entities under public law) and which fall under the private sector (i.e. commercial companies, cooperatives, commercial association, societies, and other subjects under civil law). Furthermore, the interests due to whom legal entities are established are clearly evident from the table, and such interests can be public/authoritative or public/non-authoritative (Vodovnik, 2013), or private/profit or private/not-for-profit.

Thus, in the Republic of Slovenia, the state and all territorial communities having legal personality (i.e. municipalities and localities if they have legal personality in accordance with the municipal charter) are included within the scope of authoritative legal entities. Territorial legal entities are legal entities whose activities are directed at a certain territory and at dealing with problems concerning the life and public interests of such territory. A key characteristic of territorial legal entities is authority. An authority (sociologically defined as power)

entails that one subject can impose their will on another. Territorial legal entities are the only type of legal entity that can subordinately impose the will of the public interest on other subjects, regardless of the fact whether such other subjects want or accept it. The fundamental functions of territorial legal entities include carrying out so-called regulative functions as well as ensuring and creating general possibilities for the life and work of the people, and the functioning of commercial and other legal entities in the given territory. They provide for carrying out activities in numerous areas; for example, the security of people and property, the functioning of political and economic systems, and the functioning of all necessary economic and other activities. A characteristic of territorial legal entities is that they have political authority that they can use within the framework of constitutional and statutory provisions when performing their tasks. Such authority entails the ability to implement decisions even if »addressees« resist.

Non-authoritative functional organisations include specialised legal entities under public law (e.g. public institutions) and specialised legal entities under private law (e.g. private institutions in the field of social activities and commercial companies). In the case of functional legal entities, neither authority nor territory plays a decisive role. These are primarily organisations that function in accordance with market principles.

Public functional legal entities (e.g. public institutions) carry out service activities (e.g. public services of general interest) in the public interest, and it can be established from the interest part of the table that these legal entities are *not-for-profit* oriented. They are not pure non-profit organisations, as they are allowed by law to make a profit from accessory activities. Most of all, these organisations carry out social activities (e.g. services in the fields of health care, education, culture, sport, child care, care for the elderly). In as much as such services are provided by entities under public law, they are public services of general interest. The *not-for-profit* orientation entails that such legal entities may not primarily make a profit, they may, however, make such by accessory (market) activities. That is to say, making a profit is not prohibited by law; it is, however, of secondary importance. Social activities have priority. Inasmuch as they make a profit, such may not be distributed to the founders, but must be invested back into the activity.

The situation is different in the case of commercial companies, which are functional legal entities whose purpose is to make an economic profit. They are (apart from rare exceptions) exclusively *for-profit* oriented and established so that they provide new value (i.e. capital profit and dividends) to their members or shareholders.

However, in the Slovenian tax system, all functional organisations are taxed in the same manner, as are those that carry out public services who must pay the income tax imposed on legal entities (i.e. the corporate tax) on all income made on the market in a business year outside the scope of the public service.

Associative and voluntary legal entities are legal entities that individuals join voluntarily in order to fulfil their personal and non-profit interests. These are pure *not-for-profit* organisations. Some of them are prohibited by law from making a profit (e.g. political parties, religious communities, trade unions), and

are established within the framework of voluntary activities, e.g. clubs, churches, trade unions, political parties.

Such organisations also include societies that may carry out authoritative tasks in the public interest on the basis of public authority (e.g. vehicle registration, issuing vehicle registration certificates). However, they may also include religious communities and political parties, which are prohibited by law from bearing public authority.

In short, the present *sectoral classification of legal entities* enables readers and users to correctly and quickly classify individual subjects under law in the public or private sectors and simultaneously offers the possibility to separate individual bodies of legal entities (e.g. state authorities, such as courts, the national legislature, the government, or municipal bodies such as municipal administrations, municipal councils) from legal entities as such.

Thus, the table demonstrates that the owner of a police vehicle is not the police, but the Republic of Slovenia as the state. It is also not possible to sue a court, but the Republic of Slovenia as the state.

An entity and not a body of the entity can be a holder of property rights; therefore the legal personality of a legal entity is particularly relevant for a clear understanding of the functioning of the legal system.

REFERENCES

Aubelj, B. (Ed.). (2003). *Pravo: leksikon*. Ljubljana: Cankarjeva založba.

Bohinc, R. (2005). *Pravne osebe javnega prava*. Ljubljana: GV Založba.

Bohinc, R., & Tičar, B. (2006). *Upravno pravo – splošni del*. Ljubljana: Fakulteta za varnostne vede.

Bradač, F. (1990). *Latinsko-slovenski slovar*. Ljubljana: Državna založba Slovenije.

Dewey, J. (1926). The historic background of corporate legal personality. *Yale Law Journal, 35*(6), 655–673.

Grafenauer, B., & Brezovnik, B. (2006). *Javna uprava.* Maribor: Pravna fakulteta.

Hazlitt, H. (1962). *Economics in one lesson: The shortest and surest way to understand basic economics*. New York: Three Rivers Press.

Kelsen, H. (1992). *Reine Rechtslehre von Hans Kelsen*. Wien: Österreichische Staatsdruckerei.

Machen, A. W. (1910). Corporate personality. *Harvard Law Review, 24*(4), 253–267.

Martin, E. A. (2003). *Oxford dictionary of law* (7th ed.). Oxford: Oxford University Press.

Parsons, T. (1951). *The social system*. Glencoe: The Free Press.

Pavčnik, M. (2001). *Teorija prava: prispevek k razumevanju prava*. Ljubljana: Cankarjeva založba.

Perenič, A. (2005). *Uvod v razumevanje države in prava*. Ljubljana: Fakulteta za policijsko-varnostne vede.

Pirnat, R. (1995). Osebe javnega prava: prispevek k reinstituciji pojma v slovenskem pravu. *Javna uprava, 31*(4), 477–492.

Pusić, E. (2002). *Nauka o upravi*. Zagreb: Školska knjiga.

Shaw, M. N. (2003). *International law*. Cambridge: Cambridge University Press.

Tičar, B. (2012). *Understanding state and the law*. Maribor: Inštitut za lokalno samoupravo in javna naročila.

Trstenjak, V. (2003). *Pravne osebe*. Ljubljana: GV založba.
Turner, B. S. (1991). *The social system/Talcott Parsons*. London: Routledge.
U. S. Department of Labor, Bureau of Labor Statistics. (2006). *Occupational outlook handbook* (2006-07 ed.). Washington: U. S. Bureau of Labor Statistics, Office of Occupational Statistics and Employment Projections.
Vodovnik, Z. (2013). Employment relationships in the public sector: A balance between the state, local and autonomous regulations. *Lex localis, 11*(3), 497–512.
Zajc, K. (2009). *Ekonomska analiza prava*. Ljubljana: Uradni list Republike Slovenije.

About the Author:

Bojan Tičar, Ph.D., professor and doctor of legal sciences. He works at the University of Maribor, Faculty of Criminal Justice and Security (FVV UM – as vice dean and professor), at University of Primorska, Faculty of Management (FM UP – as professor and senior researcher) and at College for Accountancy Ljubljana (VŠR – as professor). At these institutions he researches and teaches Law, Public Law, Public Administration and Legal Regulation of the Management.

VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 16 no. 2 pp. 178–200

Social Strain: An Empirical Study of Contextual Effects and Homicide Rates in Europe

Luis David Ramírez-de Garay

Purpose:

The objective of this work is to propose alternative strategies to assess the link between social context and violent crime through the use of quantitative analysis. For this purpose, I use Social Strain, a newly developed concept for the empirical assessment of contextual effects on violent crime.

Design/Methods/Approach:

Social Strain has three components: Ascribed Economic Conditions, Opportunities Structure, and Institutional Support. Each component was identified with a Confirmatory Factor Analysis. Afterwards, the resulting components were tested using an exploratory application of Structural Equation Modelling to detect different articulations between the components and homicide rates. This work used the Eurostat database to measure the death rate in 193 European regions from 13 EU countries (2001–2006), and socio-economic statistics from different sources for the elaboration of the components.

Findings:

The results of this work showed the relevance of the regional institutional structure for the variation of homicide rates at the cross-national level. Social strain turned out to be a useful instrument to detect the basic components linked with criminogenic contexts and, even more appealing, the differential articulations between the same components.

Research Limitations/Implications:

The results of this research showed that more detailed data are needed in order to take full advantage of the techniques utilized here. However, the application of SEM modelling proved to be a promising route in empirically-based crime research.

Originality/Value:

In comparison with other studies of violent crime in Western Europe, the present work is the first to incorporate a cross-national and longitudinal analysis of homicide rates to address particular theoretical questions at the meso-level. It is also the first attempt to use the Eurostat regional database as its empirical source.

UDC: 343.3/.7(4)

Keywords: homicide, social strain, contextual effects, quantitative, Europe

Družbeni pritisk: empirična raziskava vsebinskih učinkov in števila umorov v Evropi

Namen prispevka:

Namen prispevka je s pomočjo kvantitativnih metod določiti alternativne strategije ovrednotenja povezave med družbenim kontekstom in nasilnimi kaznivimi dejanji. V ta namen je uporabljen koncept »družbenega pritiska« kot novo razvitega koncepta za empirično ovrednotenje vsebinskih učinkov na nasilno kriminaliteto.

Metode:

Družbeni pritisk vsebuje tri komponente: pripadajoče ekonomske pogoje, strukturne priložnosti in institucionalno podporo. S potrjevalno faktorsko analizo (CFA) dobljene komponente so bile v nadaljevanju preverjene še s pojasnjevalno aplikacijo modelov strukturnih enačb (SEM) za razpoznavo različnih povezav med komponentami in številom umorov. Podatki o številu umorov za 193 evropskih regij iz 13 držav Evropske unije v letih 2001–2006 so iz baze Eurostat, socio-ekonomske statistike (za komponente) pa iz različnih drugih virov.

Ugotovitve:

Rezultati pokažejo, da ima regionalna institucionalna struktura vpliv na variiranje števila umorov na mednarodni ravni. Družbeno breme se pokaže kot učinkovit instrument za razpoznavo osnovnih komponent, povezanih s kriminogenimi konteksti oziroma, kar je še pomembneje, z različnimi povezavami med istimi komponentami.

Omejitve/uporabnost raziskave:

Rezultati pokažejo, da so za popolni izkoristek uporabljenih metod potrebni še natančnejši podatki. Kljub vsemu se SEM izkaže za obetajočo pot pri empiričnem preiskovanju kriminalitete.

Izvirnost/pomembnost prispevka:

V primerjavi z drugimi študijami nasilne kriminalitete v Zahodni Evropi je ta prispevek prvi, ki vključuje mednarodno in longitudinalno analizo števila umorov za odgovore na določena vprašanja na mezoravni. Je tudi prvi poskus uporabe regionalne baze Eurostat kot empiričnega vira.

UDK: 343.3/.7(4)

Ključne besede: umor, družbeni pritisk, vsebinski učinek, kvantitativno, Evropa

1 SOCIAL STRAIN

Social strain is a working concept for the explanation of violent crime at the aggregate level. It is the contextual configuration emerging from the operation of social mechanisms at the meso-level of observation and a connecting factor between macro and micro explanations. Social strain is based on the identification of its generating social mechanisms in a particular time and geographical area. I have identified three basic mechanisms needed for the emergence of social strain:

the consolidation of Ascribed Economic Condition (AEC), the expansion and contraction of the Opportunities Structure (OS), and alterations in the framework of Institutional Support (INST). These mechanisms also entail a qualitative differentiation namely, that the effects of the AEC are regarded as the main effects while the opportunity and institutional mechanisms mediate the AEC.

The Ascribed Economic Condition (AEC) relies on the idea that economic variables are not a sufficient explanation for the formation of criminogenic contexts if the corresponding factors of ascription are not taken into account (Blau, 1977; Blau & Blau, 1982). These factors entail some characteristics of the stratification structure that, when combined with an economic aspect like income,acquire its criminogenic characteristics. A classic example is the combination of low income and ethnic-group membership. In a particular urban context, this combination results in a higher probability of crime because the AEC is directly connected with other social processes behind the emergence of criminogenic contexts (South & Messner, 2000).

One advantage of the AEC concept is that the connection between economic aspects and stratification is historically conditioned, meaning that one combination cannot be arbitrarily applied to social contexts where the processes of stratification have followed different historical paths. For example, in the United States, economic inequality and poverty have been largely linked with historical patterns of ethnic discrimination, resulting in a particular configuration of AEC connected with criminogenic contexts. However, countries with different historical paths of stratification will also have distinct pairs of AEC. In the European context, and specifically the countries included in my research, the AEC cannot be the same as in the USA because of differential historical patterns (Blau, 1986). To find the correct factor for the European countries, we need to look into other characteristics, such as: urbanization settings, migration trends, educational past, and welfare between others. An empirical study with the component AEC needs to include both economic elements and social stratification elements. For the identification of AEC, we need to find a group of at least two indicators grouped into two correlated factors: A Stratification Factor (SF) and an Economic Factor (EF). If two factors are identified but without a connection between them, then the indicators used are not appropriate for the concept of AEC.

The second component of social strain is the Opportunities Structure (OS) and is the first mediation component of social strain. OS comes from the latter reformulations of Merton to his anomie-strain theory of deviant behaviour (Merton, 1995, 1997). As a component of social strain, the OS reflects the distribution and availability of chances of economic success for the inhabitants of a particular area. Merton's original concept of opportunities structure is based on the existence of contextual characteristics as factors determining the probability of achieving economic stability. In Merton's formulation, the two most relevant aspects are related to employment conditions and educational chances. In the framework of social strain, the OS is a mediator of the effects coming from the AEC. The basic idea is that the probability of a criminogenic context is not exclusively limited to the conditions that emerge from the AEC. Similar to the AEC, the OS is a component is made up of two factors: Labour Conditions (LABC)

and Education (EDU). Each of these needs to be significantly associated with the proper indicators and there should be a connection between the factors.

The second mediation component of social strain is Institutional Support (INST). In general, this is conceived as the institutional framework of a region whose work helps to reduce the pervasive influence of the AEC in the formation of crime-prone contexts. Its theoretical basis is Institutional-Anomie theory (IAT) (Messner, 2003; Messner & Rosenfeld, 1997, 2009; Messner, Thome, & Rosenfeld, 2008), and focuses on the role of pro-social institutions to thwart the effects of adverse economic conditions in the formation of crime-prone contexts. Institutional-Anomie theory describes the institutional structure of Western-industrialized societies as a field where economic institutions and political institutions are in constant competition to impose their commanding values and orientations. A state of Institutional-Anomie will come forward when the actual configuration,or in IAT terminology: institutional balance of power, is dominated by economic institutions. Such misbalance is a proper condition for criminogenic contexts, because the social-institutions cannot lessen the effects of economic hardship through the institutional framework. There are various forms in which social-supportive institutions can be present in a social context. To identify the presence of supportive institutions, the proponents of the IAT have focused their attentions on welfare, political participation, and civic engagement, among others.

1.1 The Structural Model

As already mentioned, the social strain model includes not only three components but also the relationship between them. The structural part of the model explains the connections between the input component, or exogenous independent variable (AEC), and the mediator components or endogenous independent variables (OS and INST). The underlying idea is that in a contextual configuration where the three components are present, there is substantive difference in the position each component occupies. The original formulation of social strain places the input sources on the side the AEC, while the mediators are represented by the corresponding factors of OS and INST (the complete model is depicted in Figure 1).

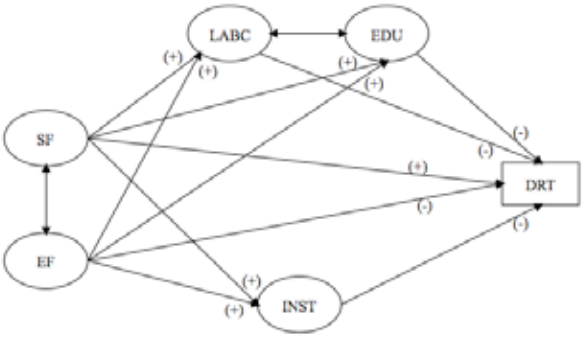
The first relationships to be acknowledged are the direct paths from the AEC to the dependent variable (homicide rates). For these relationships, we can derive two initial hypotheses:

- The SF factor is positively associated with death rates, meaning that intense conditions of social segregation are conducive to higher death rates.
- The EF factor is negatively related with death rates, where higher scores of income and wealth are linked with lower death rates.

A second group of paths is needed to include the mediators and their effects on the dependent variable. The effects of AEC on the mediators and their corresponding effects on the dependent variable are represented in the following hypotheses:

- The factor SF is positively associated with LABC and EDU.
- The factor EF is positively associated with LABC and EDU.
- The factors SF and EF are positively associated with the factor INST.
- The factors LABC and EDU are negatively associated with the variation of death rates.
- The factor INST is negatively associated with the variation of death rates.

Figure 1: The structural model of social strain



2 DATA AND METHODS

To make a comparative study of crime rates in Europe possible, one difficulty to overcome is the available data.[1] For Europe, the availability of highly aggregated data is well extended and the information is easily accessible in the corresponding national statistics offices. On the contrary, access to disaggregated data beyond the national level is more difficult. According to my own review of available sources, there are only two sources of disaggregated data: Urban Audit and Eurostat Regional Statistics (ERS).

The Urban Audit is a project to collect, organize and maintain data on the quality of life in European cities. The database contains a wide array of information about the socio-economic aspects of urban life. However, although the data covers a period of time from 1989 to 2006, divided into four reference periods (89–93; 94–98; 99–02; 03–06), the available data for core cities is available only for the 99–02 and 03–06 periods.

The ERS (Eurostat, 2009) contains information on causes of death by homicide. The principal advantage of Eurostat is its wider time period (1994–2004) and geographic coverage (15 EU states at NUTS-2). The principal problem with Eurostat is that the data on Causes of Death (COD) are based on the International Statistical Classification of Diseases and Related Health Problems (IDC-10) of the World Health Organization (WHO). In the IDC-10, the categories of death by homicide and assault are merged into one category, making it impossible to create

1 *Generally, institutions and services in charge of official crime statistics in the EU member states do publish their data exclusively on highly aggregated spatial levels. Crime data of higher spatial detail, in contrast, is normally only available on request and may require non-routine (mainframe) evaluations on the part of the relevant agencies.*

a differentiated indicator of homicide. However, this is a minor problem that did not diminish the possibilities of the database.

The ERS contains aggregated data at three different regional levels. Eurostat used a regional breakdown based on the existence of administrative boundaries and structures. In other words, the different regional levels reflect real and effective administrative divisions between regions (or regions as an administrative concept). The ERS data uses the 1970 classification Nomenclature of Statistical Territorial Units (NUTS, for the French *nomenclature d'unités territoriales statistiques*) as a single, coherent system for dividing up the European Union's territory (refer to tables 1 to 3 for some characteristics of the NUTS regions).

Table 1: Average size of regions NUTS 1-3

Average size of NUTS regions (in 1000 population) 2005			
	Level 1	*Level 2*	*Level 3*
Austria	2,755	918	236
Belgium	3,504	956	239
Finland	2,628	1,051	263
France	6,987	2,419	629
Germany	5,152	2,114	192
Greece	2,781	856	218
Ireland	4,159	2,105	526
Italy	11,750	2,798	549
Netherlands	4,084	1,361	408
Portugal	3,523	1,510	352
Spain	6,251	2,303	742
Sweden	3,016	1,131	431
United Kingdom	5,033	1,632	454

Table 2: Average size regions NUTS-2

	Pop 99	Area km2	NUTS2	NUTS2 (study)	Pop/#NUTS2	Area/#NUTS2
Austria	8,177,000	82,444	9	9	908,556	9,160
Belgium	10,152,000	30,278	11	11	922,909	2,753
Finland	5,165,474	304,473	6	5	860,912	50,746
France	59,099,433	640,053	26	22	2,273,055	24,617
Germany	82,087,000	349,223	40	34	2,052,175	8,731
Greece	10,626,000	130,800	13	13	817,385	10,062
Ireland	3,744,700	68,890	2	2	1,872,350	34,445
Italy	57,343,000	294,020	20	20	2,867,150	14,701
Netherlands	15,810,000	33,883	12	12	1,317,500	2,824
Portugal	9,988,520	91,951	7	7	1,426,931	13,136
Spain	39,418,017	499,452	18	18	2,189,890	27,747
Sweden, United Kingdom	8,857,361	410,934	8	8	1,107,170	51,367
	58,744,000	241,590	36	32	1,631,778	6,711

Table 3: NUTS population thresholds

	Population	
	Minimum	*Maximum*
NUTS-1	3 million	7 million
NUTS-2	800,000	3 million
NUTS-3	150,000	800,000

Table 4: List of Indicators

Indicators		
Variable	*Name*	*Description*
DEN	Population density	Inhabitants per km^2.
HURB1	Households in densely populated areas	Number of households in an area with at least 500 inhabitants/km^2.
GDP	Regional Gross Domestic Product	The GDP is measured in (PPS). In order to obtain figures per inhabitant, the figures are divided by the regional average population figures for the same year. Based on the European System of Accounts 1995 (ESA95).
INCD	Households disposable Income	Households balance of primary income in PPS per habitant.
EMPRA	Employment rate 15–24	Employed persons as a percentage of the population living in private households by age 15–24 (Labour Force Survey).
EMPRB	Employment rate 25–34	Employed persons as a percentage of the population living in private households by age 25–34 (Labour Force Survey).
EMPRC	Employment rate 35–44	Employed persons as a percentage of the population living in private households by age 35–44 (Labour Force Survey).
EMPRD	Employment rate 45–54	Employed persons as a percentage of the population living in private households by age 45–54 (Labour Force Survey).
UEMPC	Unemployment	Persons aged 25 to max who were without work during the reference week, were currently available for work and were either actively seeking work in the past four weeks or had already found a job to start within the next three months.
POPEA	Pre-primary, primary and lower secondary education	Population aged 15 to max by the highest level of education attained per 1000 persons. The education level is classified according to the International Standard Classification of Education (1997).
POPEB	Upper secondary and post-secondary non-tertiary education	Population aged 15 to max by the highest level of education attained per 1000 persons. The education level is classified according to the International Standard Classification of Education (1997).
POPEC	Tertiary education	Population aged 15 to max by the highest level of education attained per 1000 persons. The education level is classified according to the International Standard Classification of Education (1997).
LLL	Life-long learning	The participation of adults (per 1000) aged 25–64 in education and training.
SECB	Regional social benefits other than social benefits in kind	Includes social security benefits in cash, private funded social insurance benefits, unfounded employee social insurance benefits and social assistance benefits in cash received by households resident in a specific region (ESA95).
SECS	Secondary distribution social contributions	Social contributions and imputed social contributions in a specific region (ESA95).
SECT	Second income distribution current taxes on income	All compulsory, unrequited payments in cash or in kind, levied periodically by general government and by the rest of the world on the income and wealth of institutional units, and some periodic taxes which are assessed neither on the income nor on the wealth in a specific region (ESA95).
DRT	Rate of deaths by homicide and assault (per 100,000 inhabitants)	Based on the International Statistical Classification of Diseases and Related Health Problems (ICD). Homicide and Assault (X85-Y09) which includes the deaths by homicide and injuries inflicted by another person with intent to injure or kill, by any means.

The ERS presents a good opportunity for the comparative study of crime at a regional level. To my knowledge, there has not been a similar data collection as extensive and of the quality of the ERS. However, the most important limitation of the ERS is the extended presence of missing values for a large number of regions and indicators. To obtain a sample of data with the fewest missing values possible,

I have applied some criteria to concentrate the size and the scope of the sample in the countries with better scores of complete data, and with relevant indicators for the theory.

First, I selected indicators that, according to the theoretical base of my hypotheses, could work as viable observable measures for the latent factors. The result was an initial selection of more than 200 indicators on demographic statistics, economic accounts, education, labour market, employment, unemployment, socio-demographic labour force, labour market disparities, migration, structural business and health.

During the first screenings of the data, it became evident that the missing cases were mainly clustered in the most recent Member States and in the older entries. There was also a disparity in the years in which the first entries were collected. For example, all the economic data from The European System of Accounts (ESA95) started in 1999, while the health statistics are available from 1994. In view of the missing values' distribution, a second selection was made between the Member States with the highest rate of complete entries. From the initial 27 Member States, I reduced the sample to the 15 Member States of the EU's fourth expansion. After this selection, I conducted more diagnostics of the distribution of missing cases and, although their number reduced, there were still cases and variables with more than 30 percent missing values.

For the next selection of data, I kept the years with the most complete entries. As a result, I initially chose the data from 1999 to 2006. The missing values decreased, but their total number was still too high for a reliable multivariate statistical analysis. Looking at the distribution of missing values, it became evident that a large percentage was concentrated in two years (1999 and 2000) and in some specific regions. Based on this, I made a third and final selection and the final sample was reduced to thirteen countries for the period 2001–2006.

After cleaning the data, the indicators from the original list still had a considerable number of incomplete data, and I finally deleted the indicators with more than 20 percent total missing values. The final number of indicators was reduced to 58, which ultimately constituted the independent variables plus the dependent variable.

To reduce the missing values to a minimum, I completed the missing entries with data from other sources. Of particular priority was the dependent variable, which still had various regions with missing cases. Table 5 illustrates the sources, the data, and the regions (countries) that were completed without Eurostat data.[2] The most similar, accessible and reliable options for some regions were the regional database of the Organisation for Economic Co-operation and Development (OECD, 2009) and some national government agencies.[3] Finally, the sample included 13 Member States for a total of 193 regions from 2001 to 2006.

2 *The use of data from other sources carries with it the problem of different definitions of the dependent variable. This is the case of the data from the OECD, Home Office and the Belgian Federal Police where their definition of homicide is not based on the ICD-10. It is based on murders reported by the police. The police data utilized did not include assault but only murder, and it may under-represent the real variation of violent crime in those areas.*

3 *The homicide rate for UK is self-calculated based on Home Office data.*

Only nine nations kept their complete number of regions, and for France, the United Kingdom, Finland and Germany, some regions with a higher percentage of missing values were deleted from the database.

Table 5: No-ESR Data

	Alternative Sources		
	Regions/years	*ICD-10*	*Police Data*
OECD	AT21/01-06 IT (all)/05		*
Home Office	UK(all)/02-06		*
Belgian Federal Police	BE (all)		*
Austria National Statistics	AT06/01-06	*	
French National Institute for Statistics and Economic Studies	FR (all)/06	*	

2.1 Describing the Data

Basically, the final sample has a high percentage of variables with complete information,[4] and contains indicators on the following aspects: urban composition, income, wealth, tax income, public social benefits, various indicators of employment, and educational attainment (Table 4).

To identify the presence of multivariate outliers, I conducted a Hadi test.[5] The presence of multivariate outliers is a good sign of a non-normal distribution, however, I have also conducted the Jarque-Bera tests for skewness and kurtosis for each variable. The results show that almost one-half of the indicators of the independent variables are non-normally distributed with variant scores of skewness and kurtosis. The other half of the indicators was at least moderately skewed (particularly the indicators of income and taxes).

The distribution of the dependent variable has high skewness and kurtosis scores for all years. This is a common characteristic of crime data (particularly homicide data) for two reasons: homicide is a very improbable event with a low frequency, and the distribution of high rates of homicide tends to be concentrated in a reduced number of cases who attract the whole variance of the variable. To improve the distribution of the data, I used a natural log transformation for all the remaining variables.[6]

4 *There were only two exceptions: the independent variable households in densely populated areas (HURB1) with a missing value around 10 and 13 percent, and the dependent variable for Italy in 2004 with 10 percent.*

5 *The Hadi test consists in the usage of a measure of distance from an observation to a cluster of points. A base cluster of r points is selected and then the cluster is continually redefined by taking the r+1 points closest as a new cluster. The procedure continues until some stopping rule is encountered. (In Appendix table for the list of regions for every year – available upon request at the author or editors).*

6 *I used the transformation ln(x+100) because there were some variables with zeros as values.*

2.2 The Regional Death Rate

The dependent variable (homicides per 100,000 inhabitants) has a mean of 0.93 for the reference period. The year 2003 had the lower mean (0.85) while 2004 showed the highest score with a mean value of 1.06. For my group of 193 regions, 75% have a death rate value ranging under 1.1 to 1.3. The four regions with the lowest mean death rate in the six years are: Prov. Brabant Wallon (0.2) in Belgium; the Gloucestershire, Wiltshire and Bristol/Bath and the Herefordshire, Worcestershire and Warwick region (0.3) in United Kingdom; and The Border, Midland and Western region (0.3) of Ireland.

The distribution of death rates reflects the typical distribution of these kinds of variables. Because death by homicide and assault is an inherently improbable phenomenon, their distribution tends to be accumulated in the lower scores. In my sample, the distribution is positively skewed and with high kurtosis levels (particularly the year 2001), which means that the vast majority of cases are distributed around the lower death rates.

Other interesting characteristic is the concentration of higher values in a compact group of regions. Calculating the Interquartile Ranges of the dependent variable, the following regions qualified as severe outliers for different years: Corsica (France), Ceuta, Melilla (Spain), Pohjois-Suomi, Itä-Suomi (Finland), Algarve, Madeira (Portugal), and Calabria, (Italy).[7] Of particular interest are the cases of Corsica in 2001, with an extraordinary rate of 9.9, and Ceuta in 2005, with a rate of 6.0. In the case of Finland, the two regions have also a lower population density: Itä-Suomi had the fourth lowest (9.5) and Pohjois-Suomi the sixth lowest (22.9).

Alone, these eight regions had a mean of 3.01 from 2001 to 2006, while the entire sample's mean (without outliers) is 0.83 for the same years. In comparison with the sample average, these eight cases are more densely populated and have a lower GDP and income level than the sample, but they are not close to the mean of the poorer regions. Their employment and unemployment rates are very close to the ones of the sample. Concerning educational level, there is a relatively large difference between the sample and the outliers but they are still distant from the regions with the lowest scores. Finally, the level of levied taxes and received public monetary benefits are smaller in comparison with the sample, but not close to the regions with lower indicators.[8]

The descriptive statistics of the group of eight outliers have an interesting characteristic; namely, they do not comply with the expected or common characteristics of these types of outliers. It has been widely discussed in the empirical literature that units with unexpected rates of violent crime, are also among other low performers on economic development and education. However, in this case the eight regions have lower scores than the rest of the sample, but their socio-economic indicators are not those of the regions with the worst

7 *The test also detected the region of Madrid (4.0) in 2004 and Inner London (3.1) in 2006, however these rates are counting the terrorist attacks of 2004 and 2006 and do not reflect the »normal« rate of those cities.*

8 *More descriptive data in Appendix (available upon request at the author or editors).*

socio-economic conditions. Considering these reasons, I have decided to leave the eight regions with particular high rates of death in the sample, because their high scores are not related with extreme values on the independent variables.

3 FACTOR ANALYSIS AND STRUCTURAL EQUATION MODELLING

For the analysis of the proposed model, I have applied Structural Equation Modelling (SEM) techniques to test the empirical viability in a sample of European regions. The first part of the analysis determines the factors for the components of social strain. Having found the corresponding factors, I have used SEM[9] to test the identified structural relations between the components. I first ran a confirmatory application of SEM to the original model of social strain, and then performed an exploratory usage of SEM modelling to find alternative structures for the regions under study. For both the factor analysis and structural equation modelling, I used the full information maximum likelihood estimation method to deal with the still present missing values in the sample.

3.1 Confirmatory Factor Analysis

The first part of the empirical study is based on the application of Confirmatory Factor Analysis (CFA) to find the best group of indicators for each component of social strain in all the regions from 2001 to 2006. From all the available variables in the final sample, the construction of the factors was first conducted by a pre-selection of the indicators according to their theoretical relevance or closeness to the components of social strain. This first classification was the starting point for the CFA. The general procedure was first to find a good fitting model for the year 2006 and if the model worked to test it on the remaining years. The final factors are the ones that showed good measures of fit for all the years. In other words, all the factors are empirically valid for the period 2001–2006. These are the results of the CFA and the best factors whose structure gave a better representation of the concepts postulated in the theory.[10, 11]

3.2 Factor AEC

The original formulation of AEC would have needed a second-order factor to capture the complete dimension of the concept. However, second-order factors need three first-order factors with at least four indicators. With the available data, it was impossible to find the required number of indicators, so I have stayed with a simpler first-order factor for the AEC.

9 *I used the program Amos v.17 for the factor analysis and the structural equation modelling.*

10 *The tables with the factor loadings are in the Appendix (available upon request at the author or editors).*

11 *To achieve a better goodness of fit, I have equalled some parameters according with an analysis of the critical ratios for differences between parameters.*

The final configuration of AEC included two factors: the Stratification Factor represented by Urbanism (URB) and the Economic Factor represented by Economic Wealth (EW) (see Table 6). According to the indicators qualified for the factor URB, the element of social stratification is the degree of urbanization, where highly urbanized regions are depicted through high levels of population density and of households in urbanized areas. The other factor is capturing the variation of two measures of regional economic wealth. The resulting AEC factor measures the regions ranging from highly urbanized and economically wealthy regions, to low urbanized regions with a lower economic performance.

Table 6: Factor AEC

Standardized Regression Weights

			2006	*2005*	*2004*	*2003*	*2002*	*2001*
DEN	<---	urb	0.761	0.762	0.760	0.761	0.761	0.760
HURB1	<---	urb	0.709	0.699	0.701	0.706	0.710	0.712
GDP	<---	ew	0.879	0.881	0.882	0.881	0.885	0.889
INCD	<---	ew	0.809	0.812	0.824	0.801	0.794	0.809
all sig	$p < .001$							

Correlations

			2006	*2005*	*2004*	*2003*	*2002*	*2001*
ew	<-->	urb	0.644	0.657	0.653	0.652	0.643	0.638
all sig	$p < .001$							

Model Fit Summary

χ^2	df	*p*	RMSEA	CFI	ECVI
27.631	28	0.484	0	1	0.121

3.3 Factor LABC and EDU

For the component OS, the ideal constitution of factors would have also been of the second order, however, again data insufficiency made this impossible. Nevertheless, I have managed to identify a structure with two factors for the OS component: Labour Conditions and Education. The factor Labour Conditions (LABC) was finally constructed with three measures of employment rate by age and one indicator of unemployment (see Table 7). The second factor, Education (EDU) had two indicators: achieved educational level and long-life learning (see Table 8). For the two factors of the OS component, no connection or link (correlation) could be identified. As a result, the presumed theoretical connection between the factors of the component Opportunities Structure does not have empirical support of the data. The OS component is represented with two non-correlated factors.

This empirical depiction of the component OS is based on the idea that regions with a good opportunities structure should also have high scores of employment

and lower levels of unemployment, as well as high levels of educational attainment in the three educational sectors and for long-life learning.

Table 7: Factor LABC

Standardized Regression Weights

			2006	*2005*	*2004*	*2003*	*2002*	*2001*
EMPRD	<---	labc	0.814	0.811	0.819	0.836	0.840	0.844
EMPRB	<---	labc	0.852	0.859	0.852	0.873	0.887	0.895
EMPRA	<---	labc	0.708	0.740	0.730	0.756	0.777	0.778
UEMPC	<---	labc	-0.736	-0.749	-0.800	-0.788	-0.801	-0.794

all sig $p < .001$

Model Fit Summary

χ^2	df	*p*	RMSEA	CFI	ECVI
70	23	0	0.42	0.981	0.167

Table 8: Factor EDU

Standardized Regression Weights

			2006	*2005*	*2004*	*2003*	*2002*	*2001*
POPEC	<---	edu	0.919	0.919	0.916	0.914	0.911	0.911
POPEB	<---	edu	0.942	0.942	0.941	0.941	0.941	0.941
POPEA	<---	edu	0.789	0.788	0.766	0.756	0.751	0.752
LLL	<---	edu	0.786	0.761	0.829	0.708	0.580	0.544

all sig $p < .001$

Correlations

			2006	*2005*	*2004*	*2003*	*2002*	*2001*
e8	<-->	e9	-0.181	-0.181	-0.341*	-0.314*	-0.219	-0.127
e6	<-->	e9	0.618*	0.609*	0.308*	0.466*	0.483*	0.538*

*sig $p < .001$

Model Fit Summary

χ^2	df	*p*	RMSEA	CFI	ECVI
20.33	11	0.983	0.027	0.997	0.144

3.4 Factor INST

For the component Institutional Support, there was only sufficient data to create a single factor (INST) with three indicators (see Table 9). These measures represent the presence of institutional support to the extent that public institutions act as economic regulatory agents in the studied regions. The measures included two underlying characteristics: two indicators of the amount of money paid by households to the state in the form of taxes and social contributions, and an indicator of the quantity of monetary resources returned to households from the

state in the form of social benefits. This factor accurately captures the regions with high scores of institutional intervention in the form of levied taxes and monetary returns from the state.

Table 9: Factor INST

Standardized Regression Weights

			2006	*2005*	*2004*	*2003*	*2002*	*2001*
SECB	<---	Inst	0.985	0.985	0.985	0.985	0.985	0.985
SECS	<---	Inst	0.985	0.985	0.985	0.985	0.985	0.986
SECT	<---	Inst	0.952	0.959	0.960	0.957	0.959	0.956
all sig	$p < .001$							

Correlations

			2006	*2005*	*2004*	*2003*	*2002*	*2001*
e2	<-->	e3	0.081	-0.153	-0.325	-0.39	-0.386	-0.368

Model Fit Summary

χ^2	df	*p*	RMSEA	CFI	ECVI
13.662	5	0.018	0.039	0.999	0.097

After the identification of the factors for the three social strain components, there are a total of +four factors to construct and test the structural model. As already mentioned, the results of the CFA are not the expected reflection of the theoretical construct. One concern is that for the components AEC and OS, it was not possible to create a second order factor. Another important shortcoming is that the four factors had a relatively small number of indicators, ranging from 2 to 5 observed variables. According to the statistical literature (Blunch, 2008; Bollen, 1989; Kaplan, 2004), the latent variables in CFA and SEM modelling should have the most indicators possible to assure an increased variance for the latent variables. Unfortunately in this case, the final factors have a small number of indicators. Nevertheless, with this limitation, the resulting factors showed very acceptable goodness of fit scores and they can be considered as reliable and suitable factors to test the structural model. Also problematic is that in the original formulation of social strain, the factors of the component OS, do not have the expected correlation. Finally, taking into account a two-step approach to model identification, I made a CFA with the five factors to assess probable identification problems of the measurement model. The CFA is identified with 571 degrees of freedom.

3.5 SEM Confirmatory

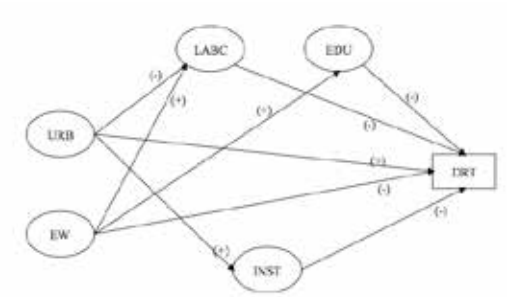
The second step of the study is to test the complete model of social strain. To do this, I have implemented Structural Equation Modelling (SEM) techniques in order to find the presence of social strain in the regions under study. I have used the resulting factors as measurement models of the complete model. According to

the theory, the next diagram (Figure 2) is an illustration of the structural model that accounts for the hypotheses of social strain. I tried to test the complete structural model of social strain, however, the model as stipulated by the theory had several problems when it was transferred to structural equations, and it could not be minimized because of identification problems.

Other problems in the minimization of the original model came from a negative variance for the residuals of the factor EDU. Negative error variance is a problem for various reasons, but in general can be assumed as a fit problem. One reason for serious fit problems is an underlying correlation in the data that had not been adequately incorporated in the model. In this case, I tested for the existence of significant correlations between the factors. One interesting result is the presence of a quite strong correlation between the factors EDU and INST, and lower but still significant correlations between EDU, and the URB and EW factors. These correlations, and particularly the EDU-INST, could be the reason behind the negative variances, and a sign of the existence of a different structure in the articulation of the components.

To deal with these problems, I progressively introduced the paths of the structural model. The objective was a step-by-step incorporation of regression weights in order to maintain identification and to get as close as possible to the original model with a structure that could be adjusted to the data. With this strategy, the first adjusted model without errors in the procedure is presented in Figure 2.

Figure 2: Model No. 1



The results produced by this first model of social strain were not as expected (see Table 10). The principal problem is the unstable significance of the paths across the six years.[12] Concerning the relations between the independent variables, all the paths were significant for the six years, while the paths to the dependent variable were very irregular. The stronger relationship found was the effect of the latent factor EDU on DRT, followed by the effect of INST and URB. However, the first was significant in five years only while the other two relationships were significant in three years only. There are also problems with the signs in various paths; of particular concern is the change of the path SS-LABC from positive to negative. At the same time, the fit values of the whole model for the complete period were not satisfactory.

12 *It was not possible to include the correlations between the factors SS-ES because of errors in the minimization process.*

Table 10: Model No. 1

Model No. 1

			2006		2005		2004		2003		2002		2001	
			r	*p*	*r*	*p*	*r*	*p*	*r*	*p*	*r*	*p*	*r*	*p*
labc	<---	urb	-0.360	***	-0.338	***	-0.337	***	-0.345	***	-0.288	***	-0.280	***
labc	<---	ew	0.686	***	0.677	***	0.677	***	0.681	***	0.679	***	0.680	***
edu	<---	ew	0.432	***	0.440	***	0.465	***	0.442	***	0.437	***	0.441	***
Inst	<---	urb	0.707	***	0.730	***	0.744	***	0.738	***	0.746	***	0.745	***
DRT	<---	urb	0.547	***	0.962	***	0.810	***	0.037	0.734	-0.294	0.033	0.065	0.649
DRT	<---	ew	-0.290	0.004	-0.319	0.005	-0.305	0.015	0.003	0.974	0.121	0.275	0.142	0.226
DRT	<---	labc	0.076	0.461	0.065	0.570	0.229	0.070	-0.210	0.021	-0.287	0.007	-0.381	***
DRT	<---	edu	-0.412	***	-0.273	***	-0.340	***	0.489	***	0.376	***	0.244	0.002
DRT	<---	Inst	0.080	0.370	-0.549	***	-0.328	0.015	-0.701	***	-0.299	0.008	-0.536	***

$p < .001$

Model Fit Summary

χ^2	df	*p*	RMSEA	CFI	ECVI
10366.21	625	0	0.116	0.594	9.497

Taking this model as a starting point, I have made some *ad hoc* procedures in order improve it. The result was a trimmed model where the factors LABC and INST did not hold any strong relationship with the dependent variable and were taken out of the model. The remaining model has two exogenous latent variables and one endogenous variable (see Table 11). And together with the irregular significance of the regression paths and the marginal improvement in goodness of fit, the resulting model has nothing to do with the original formulation of social strain.

Table 11: Model No. 2

Model No. 2

			2006		2005		2004		2003		2002		2001	
			r	*p*	*r*	*p*	*r*	*p*	*r*	*p*	*r*	*p*	*r*	*p*
edu	<---	ew	0.424	***	0.440	***	0.462	***	0.439	***	0.437	***	0.444	***
DRT	<---	urb	0.471	***	0.613	***	0.477	***	0.220	0.006	-0.053	0.537	0.177	0.036
DRT	<---	ew	-0.261	***	-0.289	***	-0.168	0.034	-0.319	***	-0.192	0.032	-0.222	0.010
DRT	<---	edu	-0.197	0.006	-0.372	***	-0.330	***	-0.198	0.011	-0.012	0.884	-0.175	0.038

$p < .001$

Model Fit Summary

χ^2	df	*p*	RMSEA	CFI	ECVI
3110.949	171	0	0.122	0.633	2.966

Despite the progressive incorporation of paths and the ad hoc procedures, the failure of the model is reason enough to consider the creation of an alternative configuration. I have mentioned that the most probable reason behind the negative variance is the existence of a strong correlation between the factors EDU and INST. This correlation can be interpreted as a direct consequence of the way in which the European educational systems are structured. There are two points to consider. First, in terms of the ideas of the Institutional-Anomie Theory, it could be possible that both the educational and the institutional structures are closer than in other

countries,[13] and consequentially are a more decisive factor on the availability of opportunities than the employment dimension. Second, because of the size of the units of analysis, it could also be possible that the link between education and institutional support is stronger at the meso-level because of the prevalence of decentralized structures in most of the countries represented in the data. A third probable reason points to the nature of the indicators of the latent factor INST. The measures used for this variable are general measures of the amount of taxes levied by the state and state financial support. In this case, it would not be strange to find that in the regions where the levying of taxes is high, the local educational level is consequentially elevated.

In view of these results, I decided to leave the confirmatory approach and go further with an exploratory analysis of social strain with some alternative configurations. My objective is to find, perhaps with other combinations between the latent factors, a stable model that could give empirical support to social strain.

3.6 SEM Exploratory

As a starting point for the exploratory application of SEM, I have taken into consideration the problems of the original model. From the start, there are two problematic correlations: a weak link between EW and EDU, and a stronger one between EDU and INST. To see if these correlations correspond to an empirical structure in the regions, I tried two new factors.

The first factor was a reformulation of the exogenous variable of social strain. I incorporated the factor INST to the factors URB and EW, as three latent variables with the corresponding correlations. The factor INST-URB-EW did not work and could not be minimized. In a second attempt, I created the factor EDU-INST to capture the correlation between the two latent variables. The new latent factor was stable and significant in the six years (see Table 12).

Table 12: Factor INST-EDU

Standardized Regression Weights

			2006	*2005*	*2004*	*2003*	*2002*	*2001*
POPEC	<---	edu	0.927	0.927	0.925	0.923	0.92	0.921
POPEB	<---	edu	0.950	0.950	0.949	0.949	0.949	0.949
POPEA	<---	edu	0.749	0.752	0.730	0.721	0.715	0.717
LLL	<---	edu	0.817	0.790	0.832	0.743	0.650	0.632
SECS	<---	Inst	0.986	0.986	0.986	0.986	0.986	0.986
SECT	<---	Inst	0.949	0.949	0.946	0.941	0.943	0.941
SECB	<---	Inst	0.986	0.986	0.986	0.986	0.986	0.986
all sig	$p < .001$							

Correlations

			2006	*2005*	*2004*	*2003*	*2002*	*2001*
Inst	<-->	edu	0.991	0.991	0.993	0.999	0.994	0.987
e1	<-->	e4	0.544	0.523	0.272	0.385	0.351	0.392
e4	<-->	e7	0.501	0.551	0.525	0.498	0.515	0.527
e1	<-->	e5	-0.486	-0.412	-0.486	-0.472	-0.462	-0.459
all sig	$p < .001$							

Model Fit Summary

χ^2	df	*p*	RMSEA	CFI	ECVI
530.927	82	0	0.069	0.966	0.683

13 *Apparently for the case of Europe it is not possible to find an opportunity structure like in the USA where education and labour opportunities are conceptually closer.*

I have incorporated this new factor in a CFA with all the latent variables to see if the measurement model can be identified. The measurement model is identified with 565 degrees of freedom.

With these latent variables, I propose an alternative model of social strain with one exogenous independent variable (URB-EW) and two endogenous independent variables or mediators (LABC and EDU-INST) (see Table 13). It was not possible to maintain the correlation linking the latent variables EDU and INST because of its function as an endogenous variable. However, I expect that the existent correlation can be assessed through the three covariances of the residuals. The following diagram (Figure 3) shows the resulting structural model followed by its corresponding tables.

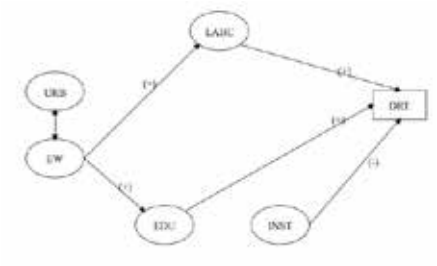


Figure 3: Model No. 3

Table 13: Model No. 3

Model No. 3													
			2006		*2005*		*2004*		*2003*		*2002*		*2001*	
			r	*p*	*r*	*p*	*r*	*p*	*r*	*p*	*r*	*p*	*r*	*p*
labc	<---	ew	0.507	***	0.501	***	0.510	***	0.505	***	0.534	***	0.538	***
edu	<---	ew	0.442	***	0.464	***	0.465	***	0.455	***	0.455	***	0.464	***
DRT	<---	labc	-0.212	0.006	-0.152	0.013	0.014	0.823	-0.181	***	-0.199	0.005	-0.284	***
DRT	<---	Inst	0.125	0.069	-0.554	***	-0.524	***	-0.652	***	-0.360	***	-0.408	***
DRT	<---	edu	-0.160	0.029	0.362	***	0.385	***	0.483	***	0.249	***	0.233	***

$p < .001$

Model Fit Summary					
χ^2	df	*p*	RMSEA	CFI	ECVI
10271.749	631	0	0.115	0.598	9.404

Table 14: Models Comparison

Model Fit Summary						
	χ^2	df	*p*	RMSEA	CFI	ECVI
Model No. 1	10366.205	625	0	0.116	0.594	9.497
Model No. 2	3110.949	171	0	0.122	0.633	2.966
Model No. 3	10271.749	631	0	0.115	0.598	9.404

As indicated in the model and in the corresponding tables, there are no direct links connecting the exogenous variable to the dependent variable. According to the model, all the probable effects of the latent factors representing the AEC go through the endogenous factors. The paths between exogenous variables and endogenous variables were significant for the six years and have a positive sign.

Concerning the endogenous variables and the dependent variable, the factor LABC has a small negative effect on death rates and is only significant for 2001 and 2003.[14] For the factor INST, there are relatively strong significant negative effects for the five year-period, 2001–2005. In the case of EDU, there are modest positive and significant effects for the same years. Finally, goodness of fit scores represent a very marginal improvement in comparison with the original model of social strain (see Table 14).

4 DISCUSSION

The first interesting result is related to the factors identified in the CFA or the measurement model. The identification of five stable factors representing the core components of social strain is a good indicator of the existence of such concepts as empirical structures in the regions under study.

Although the original formulation of social strain did not work with SEM modelling, two important ideas can be derived from the study. First, the fact that the original configuration of social strain did not find support in the studied regions is an indicator of the existence of differential institutional and structural arrangements related with the appearance of criminological contexts. Second, the modest but still significant results of the last model throw light on the presence of those different structures. Especially relevant is the reformulation of the factors for the component Institutional Support through the incorporation of EDU.

Together with the concept of social strain, another important objective of the study was the finding of mediators regulating the effects of the exogenous independent variables. Looking at the two complete models (No. 1 and No. 3), the direct effects of the factors from the component AEC were not supported in almost any regression path of the structural parts of the models. On the contrary, in the two models there were several significant regression paths from the mediators through the dependent variable. For the case of the last model (No. 3), the direct effects where not at all present in the final configuration, while the stronger effects on the dependent variable came from one mediator: the factor EDU-INST. A different case is the component OS and its latent factor LABC. In the two models and even after ad hoc procedures, LABC as a mediator has not had an effect on the dependent variable.

Finally, the most important finding of the application of CFA and SEM modelling to the studied regions is contained in the last model. The fact that the paths coming from the AEC factors are mediated through Institutional Support and have some influence on the variance of death rates is an appealing evidence for the role of institutional frameworks on the formation of criminogenic contexts.

One important problem of my empirical research is the absence of stronger scores for the goodness of fit measures in all the tested models. One probable reason for this could be a poorly specified model without equivalence in the data. However, before the pertinence of the theoretical model is rejected, there are also

14 *There is also a change of sign of the effects in 2004 but it is very small and not significant.*

some important limitations related with the data that need to be appraised. The final size of the sample, although within the limits, is still far from the ideal size that a sample must have for a completely satisfactory use of the SEM models. At the same time, the absence of more indicators of violent crime also represents a considerable reduction of the explicable variance of the dependent variable. Finally, the impossibility of gathering more indicators for the latent variables could also have hindered the results of the model.

In comparison with other studies of violent crime in Western Europe, the present work is, to my knowledge, the first to incorporate a cross-national and longitudinal analysis of homicide rates to find an answer to particular theoretical questions at the meso-level. It is also the first attempt to use the Eurostat regional database (with disaggregation level NUTS-2) as its empirical source.[15]

This work is also the first attempt to find support for two appealing ideas: the existence of different contextual configurations related to criminogenic contexts; and the relevance of the institutional framework as a way of containing the pervasive effects of social stratification and economic hardship. The latter finding in particular has captured the attention of scholars in Europe (Aebi, 2004) and in the western world (LaFree, 1999; Pratt & Cullen, 2005).

A particularly appealing result not previously found in the literature, is related to the contra-intuitive effect found in the last model for the factor EDU-INST. According to the theory, EDU as a factor of the component OS has a negative influence on the variation of death rates, where better scores of educational attainment are related with smaller death rates. On the contrary, for the factor EDU-INST the direction of the relation has changed. The change of the sign implies higher death rates when the conditions of institutional support are lower and educational attainment is higher.

This effort to make an empirical evaluation of social strain with available regional socio-economic data from Western Europe has signalled interesting ways that need to be further developed, both theoretically and empirically.

Concerning the empirical work, the original formulation of social strain needs more specific data to adequately include the particularities behind each concept. An example is the contrast between the original theoretical formulation of Ascribed Economic Conditions and the factors (URB and EW) used in the models. As a concept largely based on the work of Blau and Blau (1982), the AEC tries to illustrate the conjunction between economic inequality (as lack of economic resources) and the position in the social structure (system of stratification). In the original formulation of Blau and Blau (1982), the concept was connected to the membership in ethnically differentiated groups in the United States. The application of this concept in Europe requires a different operationalization to give account of the particular historical patterns of the European context. However, there are not sufficient data to make cross-national and longitudinal comparisons. For this reason, the indicators used to measure the latent variables of the AEC need to be improved in future research.

15 *A previous cross-national study of city-level homicide rates had been made by (McCall & Nieuwbeerta, 2007) using the Urban Audit database of Eurostat.*

With reference to the theory, the resulting effects of Institutional Support as a mediator, point to an already present issue in the literature. Many studies affirm the negative effects of welfare structures and their provisions on the variation of crime rates (Albrecht, 2001; Oberwittler, 2007; Savage, Bennett, & Danner, 2008). There is also interesting evidence on differentiated effects of welfare on different types of crime (Chamlin, Cochran, & Lowenkamp, 2002), as well as recent theory that has incorporated these ideas into a more systematized conceptual framework (Chamlin & Cochran, 2007; Messner & Rosenfeld, 2009).

The results also have connections with a well-presented argument by Killias about the limits of USA-based theories, and the different conditions in which criminogenic contexts can appear (Killias & Aebi, 2000). In the last model, the observed variation of the components and their articulation could be generated by a particular institutional structure of the 13 European nations under study. For example, the high correlation between the factors INST and EDU (and the resulting factor) can be observed as a probable indicator of a differential institutional arrangement in some European regions. For some societies, education is closer to and more dependent on the institutional framework than on the opportunities structure. This may be possible because the concepts of AEC and Institutional Support strongly rely on the development of historical patterns.[16] These differential trajectories could be the reason behind the last model. However, this possibility should be further tested with better data and in other contexts.

Finally, the general focus of this study could be of interest for other theories and research questions, particularly regarding the heuristic possibilities of cross-national and longitudinal studies at the meso-level. If the findings here can be supported with different data, then it would be appealing for future research to go further on the exploration of theories and methods based on the existence of mechanisms, structures or relations particular of the meso-level. These studies could provide opportunities to confront different theories, resolve theoretical or empirical problems, find an increased differentiation according to contexts, and improve the dialogue between theory and empirical work.

REFERENCES

Aebi, F. M. (2004). Crime trends in Western Europe from 1990 to 2000. *European Journal on Criminal Policy and Research, 10*(2–3), 163–186.

Albrecht, G. (2001). Soziale Ungleichheit, Deprivation und Gewaltkriminalität. In G. Albrecht, O. Backes, & W. Kühnel (Eds.), *Gewaltkriminalität zwischen Mythos und Realität* (pp. 195–235). Frankfurt am Main: Suhrkamp.

Blau, P. M. (1977). *Inequality and heterogeneity*. New York: Free Press.

Blau, P. M. (1986). Metropolitan structure and criminal violence. *Sociological Quarterly, 27*(1), 15–26.

Blau, J. R., & Blau, P. M. (1982). The cost of inequality: Metropolitan structure and violent crime. *American Sociological Review, 47*(1), 114–129.

16 *For example: the historical patterns of ethnical discrimination and inequality; the boundaries of the political institutions; and the connections between market and polity.*

Blunch, J. N. (2008). *Introduction to structural equation modelling using SPSS and AMOS*. London: Sage.

Bollen, K. A. (1989). *Structural equations with latent variables*. New York: Wiley.

Chamlin, B. M., & Cochran, J. K. (2007). An evaluation of the assumptions that underlie institutional anomie theory. *Theoretical Criminology, 11*(1), 39–61.

Chamlin, M. B., Cochran, J. K., & Lowenkamp, C. T. (2002). A longitudinal analysis of the welfare-homicide relationship: Testing two (nonreductionist) macro-level theories. *Homicide Studies, 6*(1), 39–60.

Eurostat. (2009). *European regional and urban statistics reference guide*. Luxembourg: Office for Official Publications of the European Communities.

Kaplan, D. (2004). *Structural equation modeling: Foundations and extensions*. New York: Sage.

Killias, M., & Aebi, F. M. (2000). Crime trends in Europe from 1990 to 1996: How Europe illustrates the limits of the American experience. *European Journal on Criminal Policy and Research, 8*(1), 43–63.

LaFree, G. (1999). A summary and review of cross-national comparative studies of homicide. In M. D. Smith, & A. M. Zahn (Eds.), *Homicide: A sourcebook of social research* (pp. 124–148). Thousand Oaks: Sage.

McCall, P. L., & Nieuwbeerta, P. (2007). Structural covariates of homicide rates: A European city cross-national comparative analysis. *Homicide Studies, 11*(3), 167–188.

Merton, R. K. (1995). Opportunity structure: The emergence, diffusion, and differentiation of a sociological concept 1930–1950. In F. Adler, & W. S. Laufer (Eds.), *The legacy of anomie theory* (pp. 3–78). New Brunswick: Transaction Publishers.

Merton, R. K. (1997). On the evolving synthesis of differential association and anomie theory: A perspective from the sociology of science. *Criminology, 35*(3), 517–525.

Messner, S. F. (2003). An institutional-anomie theory of crime: Continuities and elaborations in the study of social structure an anomie. *Kölner Zeitschrift für Soziologie und Sozialpsychologie, 43*, 93–109.

Messner, S. F., & Rosenfeld, R. (1997). *Crime and the American dream* (2nd ed.). Belmont: Wadsworth.

Messner, S. F., & Rosenfeld, R. (2009). The present and future of institutional-anomie theory. In F. T. Cullen (Ed.), *Taking stock: The status of criminological theory* (pp. 127–148). New Brunswick: Transaction.

Messner, S. F., Thome, H., & Rosenfeld, R. (2008). Institutions, anomie, and violent crime: Clarifying and elaborating institutional-anomie theory. *International Journal of Conflict and Violence, 2*(2), 163–181.

Oberwittler, D. (2007). *The effects of ethnic and social segregation on children and adolescents: Recent research and results from a German multilevel study*. Berlin: Social Science Research Centre.

Organisation for Economic Co-operation and Development [OECD]. (2009). *Regional statistics and indicators*. Retrieved from http://www.oecd.org/gov/regional-policy/regionalstatisticsandindicators.htm

Pratt, T. C., & Cullen, F. T. (2005). Assessing macro-level predictors and theories of crime: A meta-analysis. In M. Tonry (Ed.), *Crime and justice: A review of research* (pp. 373–450). Chicago: University of Chicago Press.

Savage, J., Bennett, R. R., & Danner, M. (2008). Economic assistance and crime: A cross-national investigation. *European Journal of Criminology, 5*(2), 217–238.
South, S. J., & Messner, S. F. (2000). Crime and demography: Multiple linkages, reciprocal relations. *Annual Review of Sociology, 26*(1), 83–106.

About the Author:

Luis David Ramírez-de Garay, Ph.D., Professor of Sociology of Crime at The College of México, Centre for Sociological Studies, México. Email: ldramirez@colmex.mx

VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 16 no. 2 pp. 201–211

Differences in Attitude towards Sports by Intervention Police and Regular Police

Damir Lauš, Goran Ribičić, Tatjana Badrov

Purpose:

The aim of this paper is to determine the differences in attitude towards sports, level of dedication to sports, level of achievements in sports, sports preferences and general satisfaction with life, in police officers in intervention and regular police forces.

Design/Methods/Approach:

The subjects of this research were police officers in the Ministry of Internal Affairs of the Republic of Croatia. Subjects completed questionnaires independently upon receiving instructions by the main researcher, and the following questionnaires were used: Attitude towards Sports (K1), Level of Dedication to Sports (K2), Level of Achievement in Sports (POSTS) Sports Preferences (PREFS) and Satisfaction with Life (SWLS).

Findings:

The three groups of subjects, intervention police officers, junior police officers and senior police officers, differ significantly in their attitudes towards sports, level of dedication to sports, sports achievements, sports preferences and the level of satisfaction with life. For all variables examined, the best results were observed in the intervention police group.

Research Limitations/Implications:

Future research should focus on combat sports.

Practical Implications:

Results of the paper should be the development of a new approach toward different models of lifelong learning and skills training of police officers according to their professional position.

Originality/Value:

Originality of the paper are determined differences in attitude towards sports, level of dedication to sports, level of achievements in sports, sports preferences and general satisfaction with life in police officers in intervention and regular police forces. Results could be helpful for the implementation of changes into the education of police officer.

UDC: 796:351.74/.76

Keywords: sports, police, attitude towards sports, sports preferences, sports achievement

Razlike v odnosu do športa med policisti posebne policijske enote in policijskimi uradniki

Namen prispevka:

Namen prispevka je ugotoviti razlike v odnosu do športa, stopnjah predanosti športu, stopnjah športnih dosežkov, športnih preferencah in splošnega zadovoljstva v življenju med policisti posebne policijske enote in policijskimi uradniki.

Metode:

Populacijo so predstavljali policisti Ministrstva za notranje zadeve Republike Hrvaške, ki so na osnovi navodil raziskovalcev neodvisno izpolnili vprašalnike. Uporabili smo naslednje vprašalnike: Odnos do športa (K1), Stopnja predanosti športu (K2), Stopnja športnih dosežkov (POSTS), Športne preference (PREFS) in Zadovoljstvo z življenjem (SWLS).

Ugotovitve:

Vse tri skupine policistov, policisti posebne policijske enote ter nižji in višji policijski uradniki, se med seboj razlikujejo v odnosu do športa, stopnji predanosti športu, športnih dosežkih, športnih preferencah in stopnji zadovoljstva v življenju. Najboljše rezultate pri vseh spremenljivkah dosegajo policisti posebne policijske enote.

Omejitve/uporabnost raziskave:

Prihodnje raziskave naj bi se osredotočile na borilne športe.

Praktična uporabnost:

Rezultati naj bi služili kot nov pristop k različnim modelom vseživljenjskega učenja in usposabljanja policistov skladno z njihovo poklicno usmerjenostjo.

Izvirnost/pomembnost prispevka:

Izvirnost prispevka je v ugotovljenih razlikah v odnosu do športa, stopnji predanosti športu, športnih dosežkih, športnih preferencah in stopnji splošnega zadovoljstva z življenjem med policisti posebne policijske enote in policijskimi uradniki. Rezultati so lahko v pomoč pri uvajanju sprememb izobraževanja policistov.

UDK: 796:351.74/.76

Ključne besede: šport, policisti, odnos do športa, športne preference, športni dosežki

1 INTRODUCTION

Physical ability (motor and functional abilities and fitness disposition) of police officers is the foundation upgraded by specific police knowledge and specific police skills for the purpose of creating a quality individual. The importance of

assessing the current state has been recognized for a long time in military systems worldwide and in our country as well (Jukić et al., 2008). Examining the attitude of individuals towards sports involves examining attitudes and behaviour related to sports generally. Behaviour may be observed from two standpoints, i.e. how much time and effort a person invests in a sports activity, and how successful they are in it (Bosnar & Prot, 1995). Attitudes of adults are difficult to change, and it is much more efficient to develop preferable attitudes in childhood and adolescence. This very population should be paid special attention when it comes to attitudes towards certain sports or exercising in general (Prot, Bosnar, & Sertić, 1999).

Picarielo (2000) points out that conditioning is based on programs aimed at developing endurance, power and speed, as well as the development of mental skills, group cohesion and factors related to conditions in real situations. Even without additional environment factors, many police officers face considerable problems related to their own bodies, which are more problematic than the level of difficulty of tasks that they are to carry out (obesity and obesity-related problems, locomotor system problems, every-day exposure to stressful situations). Mišigoj-Duraković (2003) states that physical activity leads to a wide range of physical and biochemical changes in the organism, as well as to changes in the way people think and perceive themselves and their environment. The fundamental condition for achieving such a state is creating an exercising routine.

The notion of subjective welfare may generally be defined as the assessment of welfare, satisfaction and happiness. Satisfaction with life represents the basic element of subjective welfare, accompanied by positive and negative effects and, according to Diener (2000), the notion of subjective welfare includes optimism and the feeling of fulfilment. Several researchers (Diener & Biswas-Diener, 2000; Diener, Suh, & Oishi, 1997; Myers & Diener, 1995) have determined that people are generally satisfied with their lives. The first feature relates to satisfaction as being personal and subject to one's own perception. Definitions of subjective satisfaction do not list objective conditions, such as health, financial situation, comfort, which may affect subjective satisfaction, but are not directly connected to it. The second feature relates to subjective satisfaction as containing positive criteria. Therefore, determining satisfaction does not only refer to the lack of negative factors, but also to the presence of positive factors. The third feature of subjective satisfaction contains global assessments of all life aspects of an individual. Even though a person may achieve satisfaction in only one area of life, subjective satisfaction is an integrated assessment of a person's life.

The objective of this research was to determine differences in the attitude towards sports, the level of dedication to sports, the level of achievement in sports, sports preferences and general satisfaction with life in intervention and regular police officers. According to this objective, a hypothesis was developed that presupposes the existence of differences in the aforementioned features between intervention and regular police officers.

2 METHODS

2.1 Subjects

The sample included 318 police officers of the Ministry of Internal Affairs of the Republic of Croatia (82 intervention police officers, 93 senior police officers and 143 junior police officers). Subjects participated in the research voluntarily, and the results were collected anonymously. The fundamental condition for forming the sample was that all subjects were police officers. The largest number of subjects (39.9%) belong to the age group 41 to 45 (Table 1), and most of them (59.3%) finished a four-year high school (Table 2).

Table 1: Age of subjects

Age	percentage
Up to 25	7.8
26 to 30	8.9
31 to 35	15.5
36 to 40	29.5
41 to 45	39.9
46 to 50	16.7
51 to 55	4.7
Older than 55	0.4

Table 2: Level of education of subjects

Level of education	percentage
high school (level 4)	59.3
university degree (bachelor) (level 6)	18.2
professional specialist and university degree (master) (level 7)	22.5

2.2 Variables

Attitude towards Sports (K1), (Bosnar & Prot, 1993, 1995; Mraković, 1970). The K1 scale of general attitude towards physical exercise and sports contains 30 items. The reliability of the overall scale result of standardized items presented by the Cronbach's alpha was 0.94 in this research.

Dedication to Sports (K2), (Bosnar & Prot, 1995; Mraković, 1970; Prot & Mraković, 1988). The level of dedication to sports was measured by the Mraković's K2 scale in the version with four items of the Thurstone type. In each item there are eleven sub-items constructed by the ascending intensity sequence. The Cronbach's alpha in this research was 0.86.

Sports Preferences (PREFS), (Prot & Bosnar, 2000). This is a five-degree scale of behavioural intentions containing 52 sports. Subjects were asked to determine to which extent they would go in for each sport. The sum of the results was taken as the final result.

Level of achievement in sports (POSTS), (Bosnar & Prot, 1995). The level of achievement in sports was assessed using a six-degree scale.

The result is the scale value of the highest item circled by subjects, and the sum of the results was taken as the final result.

Satisfaction with Life Scale (SWLS), (Diener, Emmons, Larsen, & Griffi, 1985). Among various elements of the subjective feeling of welfare, this scale is narrowly aimed at measuring general satisfaction with life and is related to similar constructions, such as positivity, love and loneliness, and represents cognitive aspects of satisfaction with life. The results on the scale may be marked as a global assessment of life quality according to personal criteria. The scale includes five items, related to which subjects should mark an answer ranging from 1 (completely false) to 7 (completely correct) (Masten, Dimec, Ivanovski Donko, & Tušak, 2010). The overall sum result was taken as the final result, with a Cronbach's alpha of 0.85.

2.3 Procedure

Data were collected during June, July and August of 2012 in various police units. Subjects completed the questionnaires independently upon receiving instructions by the primary researcher. Data were analyzed using the SPSS statistical program package (Discriminant Analysis and One way analysis of variance).

3 RESULTS

The descriptive statistics of the overall results shows that sports achievements are average (*AM* = 3.01; *SD* = 1.21), while the attitude towards sports is above average (*AM* = 90.97; *SD* = 21.15). The level of dedication to sports is average (*AM* = 22.19; *SD* = 7.55). Sports preference is a bit above average (*AM* = 136.43; *SD* = 39.32), while the satisfaction with life is above average (*AM* = 22.31; *SD* = 5.51).

Table 3 shows the differences between subject groups in observed variables. It is visible that differences are significant in all five variables.

Variable	Intervention police officers		Junior police officers		Senior police officers			
	n = 82		*n* = 143		*n* = 93			
	AM	*SD*	*AM*	*SD*	*AM*	*SD*	*F*	*p*
POSTS	3.35	1.39	2.80	1.10	3.03	1.15	5.69	.004
K1	99.79	22.33	89.02	20.56	86.17	18.73	10.76	.000
K2	26.30	8.37	20.41	6.85	21.31	6.47	18.61	.000
PREFS	151.71	39.39	131.82	41.47	130.05	32.01	8.81	.000
SWLS	23.72	5.13	21.13	5.87	22.88	4.91	6.67	.001

AM – arithmetic mean, SD – standard deviation, F – F test, p – F test significance

Table 3: Differences between intervention police officers, junior police officers and senior police officers*

**Differences between intervention police officers, junior police officers and senior police officers in the level of achievement in sports (POSTS), attitude towards sports (K1), level of dedication to sports (K2), sports preferences (PREFS) and satisfaction with life (SWLS).*

The results of discriminant analysis show a statistically significant ($p < 0.05$) difference between the three groups of subjects on each observed

variable. It is assumed that these differences are due to level of education, which affects professional aptitude. Furthermore, it may be concluded that differences also arise from the difference in the scope of work activities of the observed groups. Intervention police officers perform activities that require a higher level of physical aptitude, while in regular police officers prevail abilities related to legal and criminalist regulations.

Table 4 shows between which groups of subjects and in which variables there are statistically significant differences. The results show that intervention police officers positively differ the most from junior police officers, on all measures, while they do not differ significantly from senior police officers only in variables related to sports achievements and satisfaction with life.

Table 4: Significance of differences in variables between subject groups

variable	group	Intervention police officers		Junior police officers	
		F	*p*	*F*	*p*
POSTS	Junior police officers	10.98	**.001**		
	Senior police officers	2.81	.096	2.50	.116
K1	Junior police officers	13.43	**.000**		
	Senior police officers	19.24	**.000**	1.16	.283
K2	Junior police officers	32.74	**.000**		
	Senior police officers	19.72	**.000**	1.01	.315
PREFS	Junior police officers	12.43	**.001**		
	Senior police officers	16.08	**.000**	.12	.723
SWLS	Junior police officers	11.01	**.001**		
	Senior police officers	1.28	.271	5.67	**.018**

POSTS – *level of achievement in sports*, K1 – *attitude towards sports*, K2 – *level of dedication to sports*, PREFS – *sports preferences*, SWLS – *satisfaction with life*, *F – F test*, *p –F test significance*

The reasons for observed differences in all three groups are evident during the selection of staff for various police services. Based on the results obtained, it may be concluded that groups of subjects were not selected by chance for performing official tasks characteristic for the group they are in, which means that they were purposefully selected for jobs they hold in their departments.

Table 5 contains correlations between variables, and the results indicate that scale K1 is more connected with the level of dedication to sports than K2 with achievement in sports (Bosnar & Prot, 1995). The correlation between the level of sports achievement and dedication to sports is high, as was expected (r = 0.68), so based on this it may be concluded that a higher level of dedication to sports conditions better sports achievements, i.e. better results in sports.

Table 5: Correlations*

	POSTS	K1	K2	PREFS	SWLS
POSTS	1.000				
K1	**.490**	1.000			
K2	**.677**	**.594**	1.000		
PREFS	.099	.394	.178	1.000	
SWLS	.129	.185	.126	.154	1.000

**Correlations between variables, POSTS level of achievement in sports, K1 attitude towards sports, K2 level of dedication to sports, PREFS sports preferences and SWLS satisfaction with life.*

By analogy of achieving sports mastery, for which one requires between 15 and 30 years of sports training, more dedication to sports in police officers resulted in a higher level of sports achievement.

By means of discriminant analysis, two functions were obtained, which statistically significantly discriminate between the three groups (intervention police officers, junior police officers and senior police officers) (Table 6). The first discriminant function contains 80.5% and the second one the remaining 19.5% of the common variance.

Table 6: Canonical discriminant function

Functions	Inherent value	% variance	Cumulative variance %	Canonical correlation	Wilk's lambda	Chi-squared	df	Sig.
1	.165	80.5	80.5	.376	.826	59.964	10	.000
2	.040	19.5	100.0	.196	.962	12.243	4	.016

df – degrees of freedom, Sig. – level of significance of the canonical discriminant function

The largest impact on the formation of the first discriminant function was made by the K2 variable – level of dedication to sports. It is followed by K1 – attitude towards sports, PREFS – sports preferences and POSTS – level of achievement in sports. The second significant canonical discriminant function was determined by the SWLS variable – satisfaction with life.

Table 7: Coefficients of standardized canonical discriminant function and structure matrix coefficients

	Standardized coefficients of discr. function Function **1**	Standardized coefficients of discr. function Function **2**	Structure matrix Function **1**	Structure matrix Function **2**
POSTS	-.229	.610	**.448***	.275
K1	-.052	-.905	**.596***	-.494
K2	.925	.051	**.847***	-.009
PREFS	.400	-.097	**.566***	-.284
SWLS	.289	.649	.428	**.552***

**High absolute correlations between variable and discriminant function*

The largest differences between the groups (intervention police officers, junior police officers, and senior police officers) appeared in the area that is related to physical exercise and sports, level of dedication to sports, attitude towards sports, sports preferences and level of achievement in sports, and then also in the area related to satisfaction with life (Table 7).

Centroids of groups refer to the arithmetic mean values of analyzed groups of subjects in the coordinate system of discriminant functions and show to which extent the groups differ according to each discriminant function. Table 8 shows the centroids of the three groups in the coordinate system of two discriminant functions. The intervention police group differs significantly from the groups of junior and senior police officers according to the first discriminant function. Observing the second discriminant function, there is a significant difference between the group of junior police officers and the other two groups, intervention police officers and senior police officers, which are, according to the second discriminant function, very similar.

Table 8: Centroids of groups in the discriminant function

	Function 1	Function 2
Intervention police officers	.676	-.054
Junior police officers	-.295	-.165
Senior police officers	-.142	.301

4 DISCUSSION

Groups of subjects in this research significantly differ in ***the level of achievement in sports***. On average, all groups had achieved »the level of active training and competition in school sports«. However, a somewhat larger number of subjects in the group of intervention police, who had achieved the level of »doing sports and achieving the results at the state or international level«, increased the average of this group. The level of physical activity and achievements in sports at the beginning of a career in police has a significantly high correlation with the level of being fit, as well as a higher correlation with the level of being fit fifteen years later than it is the case with the level of physical activity at the same time (Smolander, Louhevaara, & Oja, 1984; Sorensen, Smolander, Louhevaara, Korhonen, & Oja, 2000).

All three groups of subjects have a positive ***attitude towards sports***. By far the best attitude towards sports has the group of intervention police and they statistically significantly differ from other groups on the level of $p < .000$. In groups of junior and senior police officers there is no significant difference in the attitude towards sports. Subjects mostly engage in sports in order to develop and maintain their physical abilities, to stay healthy and in good shape. In this research, attitudes towards sports share a larger proportion of variance with the level of dedication than with the level of achievement in sports (Bosnar & Prot, 1995).

The largest difference between the observed groups of subjects was found in the ***level of dedication to sports***. It determines the significant 72% of variance of the first canonical discriminant function. The group of intervention police officers has the highest level of doing physical exercise and dedication to sports. It is assumed that the positive selection of police officers for the intervention unit contributed to such results. The relation between the level of dedication to sports and the attitude towards sports is visible (35.3% common variance).

The most marked ***sports preferences*** are presented by the group of intervention police officers. All groups prefer the following sports the most: swimming, soccer,

and shooting, while the group of intervention police officers, on the same level, additionally prefers diving, alpinism and archery. All combat sports that were offered in the sports preference scale were marked with the middle grade (3) or »sport I would do occasionally or in convenient conditions«. This research also included the scale of attitudes towards combat sports SBS96 (Bosnar, Sertić, & Prot, 1999), but the scale reliability was too low due to the characteristics of the sample (Cronbach's alpha .407).

The research showed levels of ***satisfaction with life*** above average. The satisfaction with life variable is the one with the largest impact on generating the second significant canonical discriminant function, which, due to this, may be named satisfaction with life. It explains 19.5% of the total variance. At the level above average satisfaction with life, there are significant differences between the groups of intervention police officers and junior police officers, as well as between senior and junior police officers. However, between the groups of intervention police officers and senior police officers there is no statistically significant difference regarding satisfaction with life.

5 CONCLUSION

Generally speaking, a statistically significant difference between all three groups of subjects (intervention police officers, junior police officers and senior police officers) was found in variables by means of which their sports achievements, attitude towards sports, the level of dedication to sports, sports preferences and satisfaction with life were diagnosed. Based on this the hypothesis was confirmed as well.

The three groups of subjects, intervention police officers, junior police officers and senior police officers, significantly differ in their attitudes towards sports, level of dedication to sports, sports achievements, sports preferences and the level of satisfaction with life. In all scales that were used for assessing the subjects, the best results were achieved by the group of intervention police officers, followed by the group of senior police officers, and finally the group of junior police officers. It is assumed that positive selection with respect to sports achievements and the level of dedication to sports had contributed to such results. Future research should focus on combat sports.

REFERENCES

Bosnar, K., & Prot, F. (1993). Prilagodbe skale K1 stava prema športu populaciji studenata kineziloških fakulteta. In V. Findak (Ed.), *Zbornik radova 2. ljetne škole pedagoga fizičke kulture Republike Hrvatske* (pp. 64–68). Zagreb: Fakultet za fizičku kulturu.

Bosnar, K., & Prot, F. (1995). Konkurentna validacija mjera stava i angažmana sportskim aktivnostima. In V. Findak (Ed.), *Zbornik radova 4. ljetne škole pedagoga fizičke kulture Republike Hrvatske* (pp. 139–140). Zagreb: Fakultet za fizičku kulturu.

Bosnar, K. , Sertić, H., & Prot, F. (1999). Razlike u stavu djevojčica i dječaka, učenika viših razreda osnovne škole, prema borilačkim sportovima. In D. Milanović (Ed.), *Zbornik radova međunarodne znanstvene konferencije »Kineziologija za 21. stoljeće«* (pp. 123–125). Zagreb: Fakultet za fizičku kulturu.

Diener, E. (2000). Subjective well-being: The science of happiness and a proposal for a national index. *American Psychologist*, *13*(2), 34–43.

Diener, E., & Biswas-Diener, R. (2000). New directions in subjective well-being: The cutting edge. *Indian Journal of Clinical Psychology*, *27*(3), 21–33.

Diener, E., Suh, E., & Oishi, S. (1997). Recent findings on subjective well-being. *Indian Journal of Clinical Psychology*, *12*(4), 124–128.

Diener, E., Emmons, R. A., Larsen, R. J., & Griffin, S. (1985). The satisfaction with life scale. *Journal of Personality Assessment*, *49*(2), 71–75.

Jukić, I., Vučetić, V., Aračić, M., Bok, D., Dizdar, D., Sporiš, G., et al. (2008). *Dijagnostika kondicijske pripremljenosti vojnika.* Zagreb: Kineziološki fakultet.

Masten, R., Dimec, T., Ivanovski Donko, A., & Tušak, M. (2010). Motives for sports participation, attitudes to sport and general health status of the Slovenian armed forces employees. *Kinesiology*, *42*(2), 153–163.

Mišigoj-Duraković, M. (2003). *Telesna vadba in zdravje: znanstveni dokazi, stališča in priporočila*. Ljubljana: Zveza društev športnih pedagogov Slovenije, Fakulteta za šport, Zavod za šport Slovenije. Zagreb: Kineziološka fakulteta.

Mraković, M. (1970). *Tjelesno vježbanje kao faktor redukcije maloljetničke delikvencije* (Doctoral dissertation). Beograd: Fakultet za fizičko vaspitanje

Myers, D. G., & Diener, E. (1995). Who is happy? *Psychological Science*, *6*(1), 10–19.

Prot, F., & Bosnar, K. (2000). Stavovi prema sportu studenata jednog kineziološkog fakulteta. In V. Findak (Ed.), *Zbornik radova 9. ljetne škole pedagoga fizičke kulture Republike Hrvatske* (pp. 180–182). Zagreb: Kineziološki fakultet.

Prot, F., & Mraković, M. (1988). Metric properties of time-resistant scale measuring the level of sport engagement. In L. M. Ruiz, J. E. Duran, & J. L. Hernández Álvarez (Eds.), *Proceedings of International Congress Humanismo y nuevas technologias en la educacion fisica y eldeporte* (pp. 607–611). Madrid: INEF.

Prot, F., Bosnar, K., & Sertić, H. (1999). Metrijske karakteristike skale stava prema borilačkim sportovima kod dječaka viših razreda osnovne škole. In V. Findak (Ed.), *Zbornik radova međunarodne znanstvene konferencije "Kineziologija za 21. stoljeće"* (pp. 461–463). Zagreb: Fakultet za fizičku kulturu.

Picarielo, J. M. (2000). Battle-focused physical training: A career-long commitment. In K. Mophuting (Eds.), *International scientific symposium, Gaborone, 23–27 Oct. 2000* (pp. 11–13). Gaborone.

Smolander, J., Louhevaara, V., & Oja, P. (1984). Policemen's physical fitness in relation to the frequency of leisure-time physical exercise. *International Archives of Occupational and Environmental Health, 54*(4), 295–302.

Sorensen, L., Smolander, J., Louhevaara, V., Korhonen, O., & Oja, P. (2000). Physical activity, fitness and body composition of Finnish police officers: A 15-year follow-up study. *Occupational Medicine, 50*(1), 3–10.

About the Authors:

Damir Lauš, mag. cin, Ministry of Internal Affairs, Police Department Bjelovarsko-Bilogorska, Ph.D. student at the Faculty of Kinesiology in Zagreb. E-mail: damir.laus@bj.t-com.hr

Goran Ribičić, Ph.D., mag. cin, Ministry of Internal Affairs, Police College, Zagreb. E-mail: gribicic1@gmail.com

Tatjana Badrov, M.Sc., lecturer of Communication Skills and Vice Dean of the Technical College in Bjelovar. E-mail: tbadrov@vtsbj.hr