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.

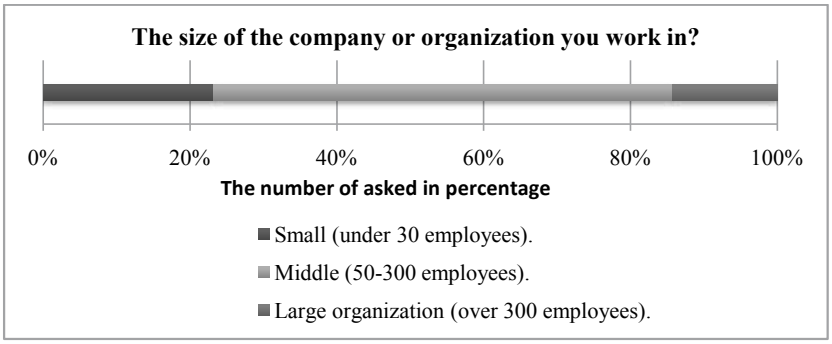


Figure 1: The size of the company or organization where the asked are employed

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).

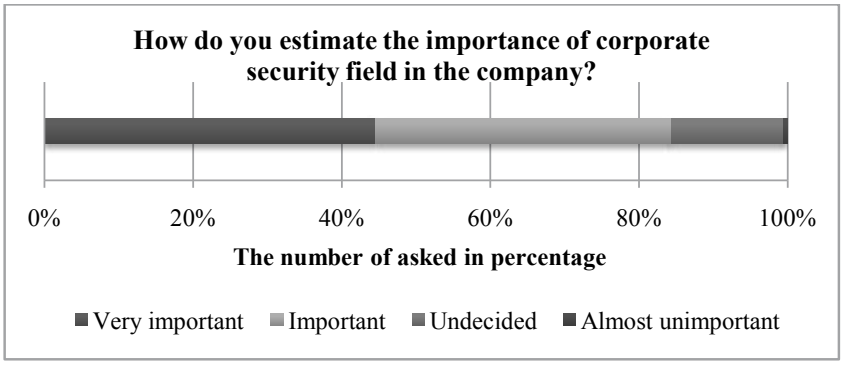


Figure 2: Estimation of the importance of corporate security field (Androić, 2013: 54)

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)

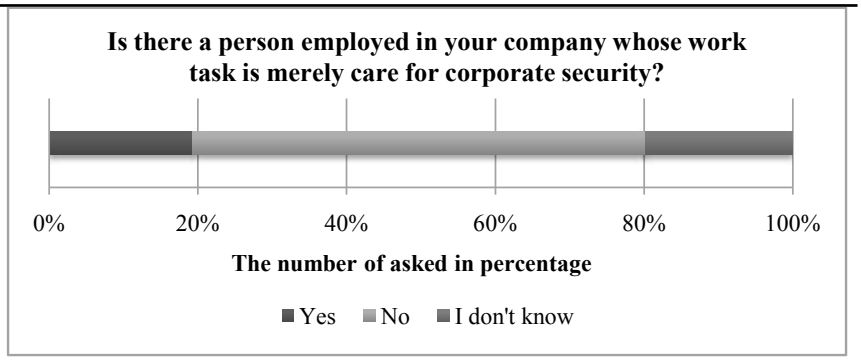


Figure 4 below shows that the majority of Slovenian companies take care of technical protection of the building by outsourcing for the whole field. This answer was chosen by 37%. They are followed by companies that provide technical protection of the building with their own personnel and equipment. This 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

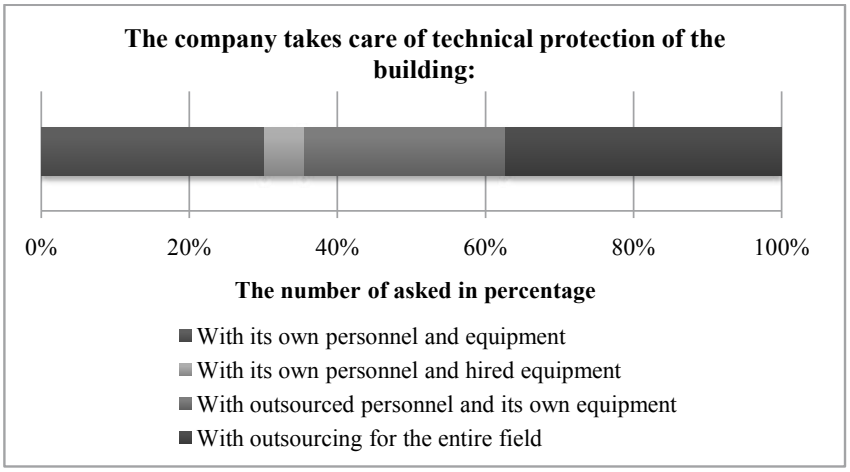


Table 1 shows the distribution of answers regarding the frequency of use of individual types of security surveillance, about which we inquired by means of question Q31. Video surveillance and alarm devices are used the most frequently, each occupying a 17% share among enumerated types of security surveillance. 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

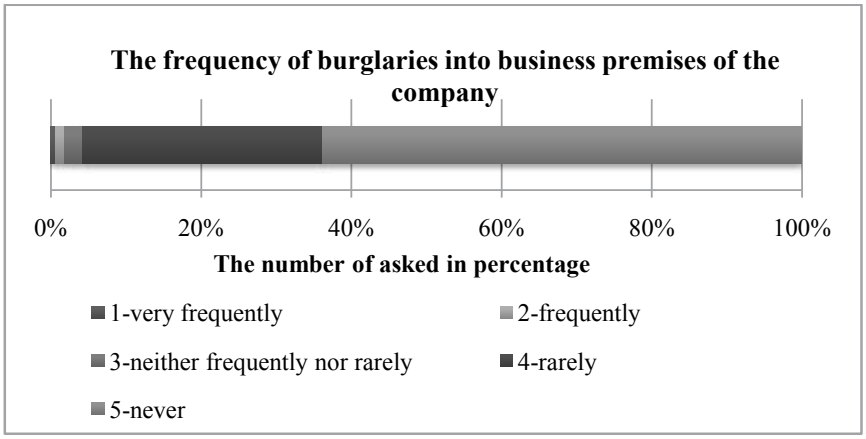
burglary (e.g. smoke screen), electronic key holes and recording telephone calls. Only a 1% share is occupied by biometry. Specifics of individual shares of answers are seen in the table below. Based on the answers received, we can infer that companies take good care of property protection, and indirectly 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)

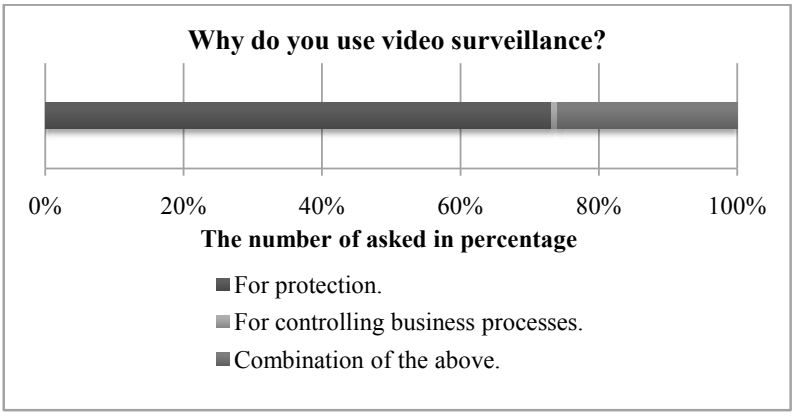
By using a 5-point Likert scale (1-very frequently, 2-frequently, 3-neither frequently nor rarely, 4-rarely, 5-never) respondents were asked to estimate the frequency of burglaries of the business premises of the company. Figure 5 shows that the most (64%) estimated that burglary never happens, while 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.

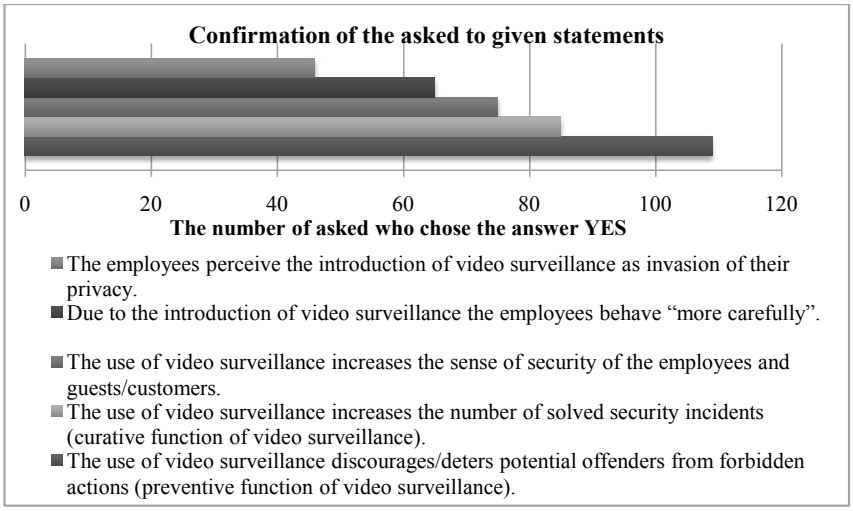


Figure 7: Confirmation of the asked to given statements referring to the use of video surveillance

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.

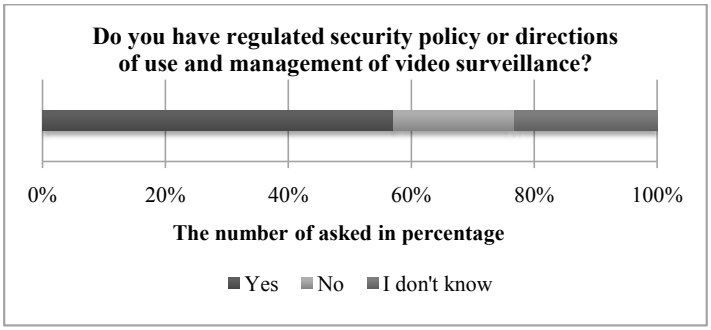


Figure 8: Security policy or directions of use and management of video surveillance

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

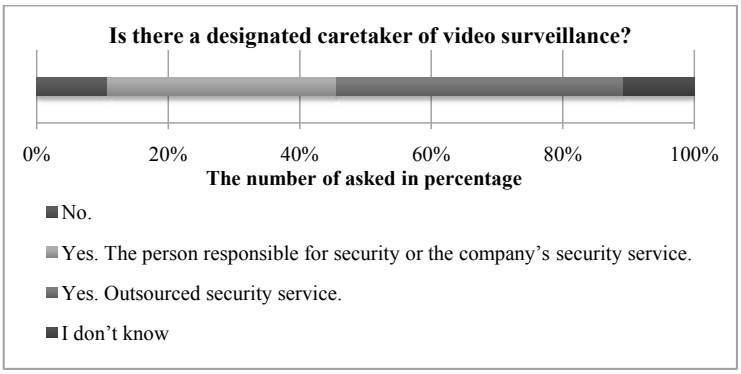
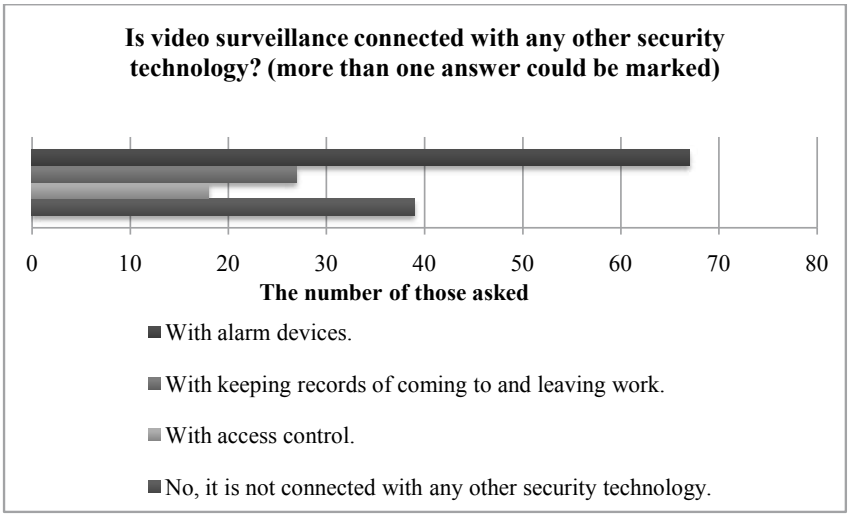


Figure 10 shows answers to the question »Is video surveillance connected with any other security technology? (more than one answer can be selected)«. We can see that most of the respondents, as many as 60%, think that video surveillance in the company is connected with alarm devices. This answer includes 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.