Coll. Antropol. **38** (2014) Suppl. 1: 25–33
Original scientific paper

Predicting Business Opportunities and/or Threats – Business Intelligence in the Service of Corporate Security (Empirical Analysis of the Usage in the Economy of Republic of Croatia)

Mirko Bilandžić[1] and Danijela Lucić[2]

[1] University of Zagreb, Faculty of Humanities and Social Sciences, Zagreb, Croatia
[2] University of Zagreb, Faculty of Political Science, Zagreb, Croatia

A B S T R A C T

Predicting business opportunity sand risks is based on existing knowledge about them. In practice, this knowledge comes from collecting business information from the business environment, within the framework of something that is known as business intelligence (BI). Prediction of opportunities and risks is inherent in business of successful company. Corporate security as a framework for ensuring the safety of business is based on timely and accurate information that becomes foreknowledge of threats, for which prediction companies are using different tools, and business intelligence (BI) is a proven tool. The aim of using BI in company is well-timed detection of opportunities and threats in business environment that management could react in time. Implementation of BI activities in Croatia significantly differs from the world average and in applying of BI activities companies are primarily focused on business dimension of business environment, while ignoring the political and security dimensions from which threats are generated, as shown by the survey results conducted from October 2010 till April 2011 with online survey method on a sample of 1,000 largest Croatian companies by revenue.

***Key words**: corporate security, business intelligence, strategic management, Croatian economy, crisis management*

Introduction

Security is one of the basic assumptions of human life and one of the basic human needs. Therefore, the interest in this area for all aspects of human activity is a completely natural and rational phenomenon. The essence of the phenomenon of security, whose meaning is often taken as self-explanatory even ifit is one of the most used but least explained concepts[1], probably was best described by a German statesman Konrad Adenauer. Adenaur even at the beginning of the European integration process said that security is note very thing but everything is nothing without security, thus pointing out the essence of security problem. While phrases like preserving security, security establishment, security pursuit and similar characterize our everyday lives it is quite clear that security threats exist regardless of what kind and whose security we are talking about – security of individuals, countries, companies, and/or (business) organizations and collectives.

The modern world is complex in many ways. The complexity of today's world means that the process of decision-making in all sphere sand at all levels of human activity has become more complex. First of all, the world is faced with many insecurities and uncertainties about the future movement. German sociologist Ulrich Beck described that kind of world as a »risk society«[2].

Risk as an integral part of everyday life primarily results from the uncertainty created by social development. Society without risk is simply impossible. Risk is an inevitable, present and growing phenomenon within developed societies[3] and thus it is the component of the business world as society's integral part. Therefore, modern risks are not easily avoided nor controlled.

Received for publication November 29, 2013

In the Post-Cold War era and contemporary security studies term risk associated with threats and survival, increasingly takes central position instead of term security[4]. The issue of security policy has been essentially redefined: uncertainties are managed more than insecurity[5].

Moreover, analysts and experts point out the inability of modern society to cope with dangers. There are more discussions about the unknowable future than the unknown. The future world is marked as »unknown unknowns« where an attempt of objectification of »unknown« creates a new kind of threat[6]. This moreover, raises the question – could any regulatory mechanism for coping with risks (which have their true and fair dimension but which are also subjective and designed) be considered as a framework for the inevitable or »final conclusions«[7]?

Holding by Ulrich Beck, the »age of risks« is characterized by three dominant characteristics[8]. First of all, the risks are unlimited in terms of temporal and spatial mobility. Therefore total social interactions and interactions in terms of risk in a globalized world is spreading through space, and narrowing over time. Second, the destructive potential of risks is increasing. Third, traditional risks/hazards were predictable which means that they have been avoided, prevented or have been more or less effectively managed through the established regulatory mechanisms. Modern risks are unpredictable.

At this point, it is worth to emphasize that there is terminological confusion about term »risk« as this term is used for a number of concepts that have approximately similar meanings: danger, hazard, threat and so on. Risk refers to any situation in which someone or something is exposed to possible adverse outcome. The risk represents an unpredictable danger that develops during the execution of the action. This is a chance for occurrence of an event with bad consequences. This term is more accurate than the term hazard as it can be and can be used as an element in determining the degree of risk even if the hazard is used as an alternate term for the risk. Hazard is the kind of events in the environment that contains a threat in relation to the people and objects that have value to them. Threat is however unavoidable level of risk that accompanies us in the performance of some action, which is often independent of the action or from outside. Also, while considering the threat the authors stress the need of distinguishing the threat and danger. The threat is the state of actual or potential threat while the danger is feeling of the threat regardless they exist are or not[3,5].

Their fluctuations, composition and distribution are beyond the capabilities of traditional mechanisms for coping with risks and it is necessary to create new policies, strategies and institutional mechanisms for risk management.

Security strategies and modern security practice is no longer characterized by avoiding risk but rather by risk management as a permanent function. Reformulated approaches to dangers in security policies have caused risks not specific threats to occupy a dominant position in the security agendas. Therefore, the basic task of redefining the security policies is to prevent and mitigate potential damage[5].

Being aware of the fact that a security vacuum (absolute security) doesn't exist, act or stand to raise the level of security to the highest possible through identifying potential security threats. In other words they try to reduce the identified risks to the lowest possible level of threat through institutional framework. In this sense, a company can be viewed through the prism of an actor who aspires to achieve higher level of security in order to get better business results.

Business opportunities are an essential component of each company and without them, business success is unimaginable but at the same time companies are faced with many dangers that threaten their business. Opportunities and threats can be seen as two sides of the same coin and their predictions should be inherent in business of every »healthy« economic entity and it is also an integral part of the corporate security concept. This concept should especially come to the fore front in times when the economic climate in many countries around the world, including Croatia, is predominantly characterized by the crisis, uncertainty and risk and one of the basic assumptions of the corporate security concept is that awareness of the existence of threat for business subjects is not at the required level. In order to achieve key targets, companies create business strategies and use different tools and techniques where by strategic decisions need to impact business results.

Business intelligence in the context of corporate security is one of tool that has become (and is becoming) an integral part of modern business culture as well as apart of the strategies and policies of many successful companies[9]. Decision-makers are using it in order to gather and analyze the necessary business information for decision makers. And if the information is timely, accurate and pertinent in the hands of decision-makers they become a means for pursuing strategic competitive advantage of company.

In other words, business intelligence is one of the key resources for strategic management. In today's globalized world where there is a continuous struggle for competitive advantage the crucial thing for companies to find out is what is happening in the business environment?, why it is happening?, what will happen?, what to do? and finally how to do something[10]? Probably more than ever before, the Croatian economy (companies) should seek answers to these questions because of entry into the European Union in which business opportunities but also dangers and risks are greatly expanded.

Starting from the basic categorization of data included in the agenda of business intelligence – information about the environment in which companies doing business, information relating to market as well as information relating to competition[9], we argue that the most companies which operating in Croatia have limited/narrow understanding of corporate security as well as apply-

ing business intelligence activities. They primarily focus on economic dimension of environment while ignoring other dimensions (political, social, cultural and so on) from which threats are generated. Narrow understanding of security concept results in selective use of business intelligence. On the one hand, this does not contribute sufficient identifying business opportunities while on the other this does not result in detection of crisis, crisis prevention, effective functioning in times of crisis as well as the operation of the post-crisis period as the basic functions of business intelligence within the corporate security and crisis management[11]. Due to insufficient knowledge of business intelligence and its limited application, we believe that the corporate culture in the Croatian economy is at s low level which contributes to the non-competitiveness of Croatian economy and its poor economic indicators in recent years.

Corporate security

The modern corporate security concept is based on assumptions that security is not technical but strategic issue, that threats can come from internal and external business environment and concept is focused on technological and human factors. Security as an integrated concept in the modern definition and practice of corporate security refers to company's overall security.

Corporate security is faced with two intertwined challenges: supporting the growing business needs and countering increasingly sophisticated attacks against the company. The basic levels and targets of corporate security is to ensure the security of the company's business success through elimination of all risks and threats that may affect the business and business success, reducing threatening effects to a minimum, business functioning in crisis time (crisis management), and overcoming the crisis and establishment of normal functioning after crisis[12,13].

Unlike almost unique scientific/expertise understanding of corporate security according to which it is necessary for company operating and within it occupies a strategic function and thereby defines unique business system security policy as well as its unique implementation in practice, authors diverge in terms of content of corporate security concept. Gerald Kovachic and Edward Halibozek[14] incorporate security functions include the following: a) administrative security – refers to the procedures and policies, b) physical and technical security (protective security) which is focused on factories and other property, c) security of ownership and foreign partnerships (out-source/proprietary) d) personnel security concerning the protection of human health and safety at work, e) training programs and development of security awareness (security education and awareness training program) development of safety awareness, f) fire protecting for people and property; g) action in extraordinary circumstances (contingency planning); h) investigation on the programs of protection against crime, i) security of business contracted with the state structures (government security) to provide security support in relation to contracts and transactions with government, in other words, national security as part of corporate security, j) information security, k) security of managers (executive security) and l) the safety of the various business events (event security).

Croatian authors have a different understanding of the content of corporate security. According to them, the normative framework of corporate security includes IT security, personal protection, protection of intellectual property, data protection, private investigation activities, business intelligence, prevention of money laundering and terrorist financing, health and safety, fire protection, environmental protection, and rescue and defense preparations[15].

Previous analysis indicates the content of corporate security in relation to attacks on company. Even if a detailed analysis of corporate security is beyond the scope of this paper it is worth it to at least in principle note that the consideration of the content of corporate security cannot exclude illegal activities undertaken by the company against other people, companies, and even countries.

As an example of country illegal activities we can give example of transnational corporations in the U.S. and their role in government's covert actions. Using such kind of operations during the Cold War the U.S. administration crashed regimes and sovereigns around the world[16].

Gary Slapper and Steve Tombs illegal activities are calling »corporate crime«[17] and they are reflected in the following business areas: administrative area (e.g. book keeping); ecological area (environmental pollution); financial area (tax violations, illegal payments), labor-legal area (labor law requirements); production area (safety products, labels) and unfair trade (action against the competition, false advertising).

Participation of companies in cases of industrial / commercial espionage could also be counted as a corporate crime[18,19]. Here, it should be noted that the company's participation in transnational organized crime and transnational criminal enterprise can be labeled as »the continuation of business by other means«[20], as mentioned by the famous Carl von Clausewitz.

Corporate security and business information: action based on fore knowledge

Contemporary processes can be analyzed, defined and interpreted through different theoretical models. Alvin Toffler's model of the Third Wave[21] or model of technology (IT) evolution certainly is one of those which most convincingly portrays the contemporary period. This is the age of high technology and information. Its basic characteristics are rapid (positive and negative) changes in all spheres of society and human activity where high technology and information play a central role and total human knowledge is repeatedly increased while time needed to increase knowledge is less. Thus, information

and knowledge have become the dominant characteristics of the modern world.

Today's word is a world of information. In this world, information is knowledge, and not only knowledge but also the power and capital. Who owns the information has an advantage over the other. It is a powerful tool to take a superior position. In the decision-making process, information enables quality decision making, easier navigation in an unsafe and uncertain world and thus making achieving goals easier.

Manuel Castells has similar conclusions. He argues that the third technological revolution is marked on one side with management (as a dominant technology) and on the other hand with information (as a dominant product of the technological revolution). The last revolution had the greatest impact on the economic sphere so it issued to talk about a new kind of economy– information and global[22].

Corporate security is an integral part of modern business and the »new economy«. The analysis of corporate security objectives clearly indicates that it is not focused solely on the application of proactive and/or reactive security-protective measures. Prior to effective implementation of such measures is studying business environment, collecting of business information and creating knowledge about threats.

Business information and business knowledge are crucial in all phases of the risk research methodology: risk identification, risk assessment/estimation, risk evaluation and risk management[23]. Thus, point of corporate security (security operations) is largely realized in the first levels of the objectives of corporate security through eliminating all risks and threats that may affect business success and reducing threatening effects to a minimum.

Quality business information and knowledge of threats/risks based on them is the basis for quality decisions that are aimed at prevention and disabling adverse effects. It is a safe way to eliminate the possibility of business crises caused by threats where crises are seen as changes that bring a serious problem or as a condition that can cause sudden and serious harm to employees, reputation and financial results of the company[11]. When the crisis occurs, more than ever, it is necessary to collect data and information continuously[11] and convert them into business knowledge necessary to make business decisions that are oriented at ensuring the security business because crisis is a condition in which normal forces and regular operation cannot solve existing problems/threats and these crisis could causes heavy damage and casualties and in order to overcome them special solutions are required (crisis management)[24,25].

In concluding this discussion it is worth it to point out once again that information is a dominant raw material and the end product of the IT revolution or technological paradigm[24]. Information thus plays a central role in the economy of today. To achieve a competitive advantage, companies are constantly looking for new information that should be accurate, relevant and timely for achieving competitive advantage. Identifying business opportunities and risks is impossible without business information which is the basis for making strategic decisions.

Business intelligence and corporate security

The concept of business intelligence is associated with Howard Dresner who in 1989 founded the analytic (BI) department in one American consulting company. Dresner along with Stevan Dedijer are considered as pioneers of business-intelligence operations, and business intelligence in general. Notably, Dedijer used the term »social intelligence«[26]. Terminological discrepancy which dominates both, in the Anglo-Saxon-speaking world and especially in the Croatian language, beyond the scope of this paper so here we only state the terms used to denote this phenomenon: economic intelligence, market intelligence, market monitoring, business intelligence, competitive intelligence, competitor intelligence, corporate intelligence, commercial intelligence, government intelligence and so on[27–30].

As there is no universal term used to denote this activity and there is no generic definition as well, here we opted for a definition that emphasizes the action element (decision making). It is an action element which gives meaning to the preceding actions and so»... the content business intelligence includes collecting and processing of data and information, analyzing and converting them into knowledge which serves as a support for business decisions-making[9]«.

In discussion of business intelligence and corporate security, two dimensions should be emphasized. One is supportive and is related to the application of business intelligence activities which are primarily focused on the business environment in order to study any possible threat for the company. In contrast to such offensive support dimensions, defensive dimension (business counter intelligence) is the direct effect of business intelligence in corporate security. It includes activities that are focused on eliminating or reducing the impact of intelligence activities of rivals and protecting information of a company with respect to the economic (industrial) espionage.

The main goal of business counter intelligence is not eliminating threats and risks but reducing the risks of loss of company's information to a minimum. In other words, business counter intelligence system aims to establish mechanisms for managing security risks related to business information and it is based on the principle of cost-benefit analysis. Business information become interesting for companies primarily to gain competitive advantage through research potential markets, research and development of new products, take over of clients, detection strategies, etc.

Business intelligence in the Croatian economy-empirical analysis

Production of literature that is focused on business intelligence topics is quite large in the world, both professional and scientific. Significant expansion has been re-

corded in the last twenty years and that is evident from a number of review articles[31–34]. The large number of articles resulted from empirical research in different countries and on different aspects of business intelligence.

The Journal of Competitive Intelligence and Management which is published under SCIP (Strategic and Competitive Intelligence Professionals) in 2004th has released special editions[35] that discuss the use of business intelligence in countries around the world and its development mostly through case studies/country studies. The majority of empirical studies have been conducted in countries that have a high percentage of applied business intelligence activities, whether in the public or private sector.

On 2005 Global Intelligence Alliance[36] (GIA) on a sample of 287companies in18 countries around the world conducted interesting and on global scale significant study which showed that highly developed countries are leaders in usage of BI but also some developing countries[37] had good results too (Figure 1).

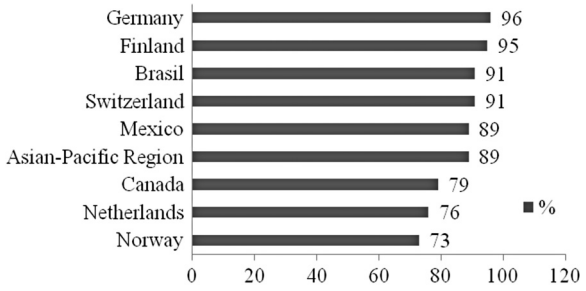

Fig. 1. National percentages of systematic business intelligence activities.

In the Croatian case there are two more studies (behind this which results are presented here) on the field of business intelligence and its usage in Croatian companies. The first of two empirical research studies has been conducted in 2005 and the results were presented in the same year by authors Ivančević and Jurišić at professional conferences[38,39]. The results showed that 9% of the total number of companies in the study at that time had a separate business intelligence department. Other empirical research has been conducted by author Zebić[40]. These results showed that 50% of the companies had business intelligence department which is intended for data collecting and analysis of business information.

Material and Methods

The last and most comprehensive research on the usage of business intelligence in Croatian companies was realized by Department of Sociology of the University of Zagreb and business weekly »Lider«.

Online survey research has taken a period of seven months (from October 2010 until April 2011). In order to achieve a representative sample, research was conducted in two stages. Target population was the largest companies that operating in Croatia. Precisely, that was population of 1,000 largest companies. This classification was made by business weekly »Lider« in 2010 where the basic criterion for creating a list was total revenue in previous year. List »Top 1000« was published in June 2010 as a special edition along with regular weekly »Lider« (No. 247). Magazine editors provided e-mail addresses of 1,000 largest companies to researchers and an online questionnaire with a statement of consent were sent to research participants.

The first stage of researching lasted from October 2010 up to half of November 2010 year. During this period, most of the answers were collected (170 of 233). After the first stage was finished, sample projection has been done in order to assess the state of the sample representativeness. One of the key representativeness parameter was the region in which company operates. Regional division was made according to NUTS II classification[41] (NUTS-Nomenclature des unités territoriales Statistiques). It is official classification of the European Union, which determines the statistical spatial units. Such classification was proposed by the Croatian Bureau of Statistics in March 2007. The European Commission confirmed the compliance of the proposal of such regional divisions with EU standards. The second parameter of representativeness was company size. Company size was determined by the number of employees (official categories) where companies with fewer than 50 employees are into category small, companies between 50 and 249 are medium-sized while those companies with more than 250 employees are in category large.

In February 2011, after the required number and profile of the company was determined, the second stage of research commenced. In this phase, the questionnaire was sent only to the addresses of those companies that satisfied the necessary criteria to achieve representativeness. In the second phase 53 responses more were collected. At the end 233 responses were collected (23.30%).

Even the profile of returned response fit the parameters of representativeness, the sample was additionally weighted in order to get more reliable conclusions on population. Within the population of the 1,000 largest companies most of them were from Northwestern region 655 (23% small, 44% medium and 33% large companies) in the Eastern region was138 companies from the list »Top 1000« (13% small, 46% medium and 41% large companies) while in the South (Adriatic) region were 207of them (11% small, 43% medium and 46% large companies).

The sample of returned responses (N=233) was composed of 168 companies from the Northwestern region, 30 from the Eastern and 35 from the South region. After the sample was weighed (on basic criteria-region and company) the most evident changes were in the South region (Tables 1 and 2)[42].

The questionnaire was composed of three thematic sections with 27 questions. In the first part, there was a knowledge test about the BI system and its usage. In this section respondents completed the test in order to check the level of knowledge in the business intelligence sys-

TABLE 1
RESPONSE STRUCTURE (UNWEIGHTED DATA)

Region	Company size			
	Small	Medium	Large	Total
	N (%)	N (%)	N (%)	N (%)
Northwestern	39 (23)	68 (41)	61 (36)	168 (100)
Eeastern*	4 (13)	13 (43)	13 (43)	30 (100)
South (Adriatic)	6 (17)	20 (57)	9 (26)	35 (100)

* percentages are rounded

TABLE 2
RESPONSE STRUCTURE (WEIGHTED DATA)

Region	Company size			
	Small	Medium	Large	Total
	N (%)	N (%)	N (%)	N (%)
Northwestern	34 (22)	61 (40)	58 (38)	153 (100)
Eeastern*	4 (13)	14 (44)	14 (44)	32 (100)
South (Adriatic)	8 (17)	27 (56)	13 (27)	48 (100)

* percentages are rounded

tem and its potential effects on the company's operations. Furthermore, in the same part of the questionnaire we checked which categories of data were collected and to which extent. We checked how and where companies collect data and investigated how companies do measuring, processing and analyzing data as well as how the BI system contributes to their business. In the second part of the questionnaire, participants were asked to answer questions about the plans related to the BI system in their company. In the last part of the questionnaire participants have answered on some general questions about the company. These answers were the basis for subsequent classification of companies in our sample. The last question in the survey was open-ended where participants were able to express their attitudes about the subject. In the following text we presented only relevant results means those related to relations of business intelligence systems and corporate security.

All data analysis in this work is done using SPSS (Statistical Package for the Social Scienece). For testing association between two variables we used Pearson's chi-squared statistic test and Cramér's V as a standard measure of association between two nominal variables. The level of statistical significance used in analysis was $p<0.05$.

Results

In this research 233 companies participated, 46 small companies (21%), 102 medium-sized companies (43%) and 85 large companies (36%) (Table 2). Nearly three-quarters (72%) of all companies from sample were based in Northwestern Croatia, 15% were based in the Adriatic region, while 13% of companies were from Eastern Croatia (Table 2). It is important to note that all analysis and results presented below are based on weighted sample.

The ownership structure of companies was as follows: 84% were privately owned, 7% were state-owned, and mixed (state and private owned) companies were 9%. From the above presented structure of the questionnaire it is quite clear that this research was conducted in order to detect situations in the biggest Croatian companies regarding knowledge in BI system, usage of BI system but we also wanted to find out plans related to possible implementation of BI and/or its further development in the usage within the company in order to give an assessment of the prospects of usage BI tools in the largest companies that operate in Croatia.

Based on the results of previous researches of this type in Croatia, that were mentioned above and based on some business indicators that were visible from the list »Top 1000« we started with the assumption that most of the Croatia's companies are not systematic in conducting business intelligence activities and that in most case there is no institutionalized department focused exclusively on activities of this type. The results showed that a large number of companies, 75% of the 233 that participated in the research conduct some kind of BI activities and only 18% stated that they do not use BI activities at all. It should be noted that only 19% (of this 75% that are using some kind of BI activities) are doing this systematically means they have institutionalized BI department within the company (Figure 2).

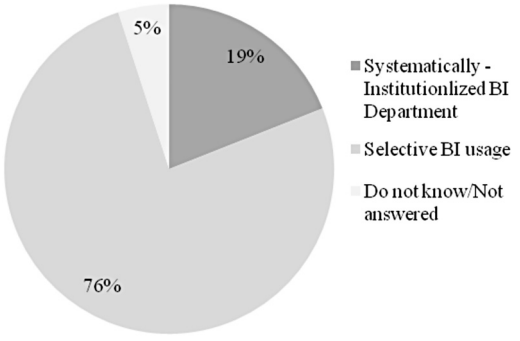

Fig. 2. Business intelligence level of usage.

Based on this we can conclude that companies in Croatia are lagging behind world leading countries as well as those that are showing significant economic progress in recent period. If we look overall, we can say that the companies are using BI techniques unsystematically. Also, these techniques are not an integral part of company's corporate culture and they are not entirely in the service of corporate security in Croatia.

The results as expected showed that the usage of business intelligence activities is related to company size. Large companies significantly more than small and medium sized companies have institutionalized department for BI activates, means that systematically applying BI activities (Table 3).

TABLE 3
COMPANY SIZE AND LEVEL OF BI ACTIVITY USAGE*

Level of usage	Company size		
	Small	Medium	Large
	(%)	(%)	(%)
Systematically / BI Department	13	11	32
Selective / No BI Department	61	59	50
No activity	26	30	18
Total	100	100	100

* χ^2=17.439, df=6, p=0.008, Cramer's V=0.180

Although between companies there is no statistically significant difference in the company activity type and usage of business intelligence (chi-square test, χ^2=17.007, p=0.711), but it is noteworthy that this tool is most used by companies in the banking and financial sector. This is an entirely expected result for several reasons. Primarily, these sectors predominantly use information as a »raw material« but also one part of answer probably lies in the fact that almost all companies in these industries are foreign owned and within them corporate security and BI exist as integral element and are indispensable part of business strategy.

When we talk about data sources, regardless of whether the company has institutionalized business intelligence departments or just applying some of BI activities, almost all companies are using open data sources that are available. The most common source is the internet, followed by their own databases, newspapers, various publications and magazines, as well as an external open database. This finding is encouraging because the base for any good business intelligence is usage of data that is available to everyone and that is very important because data are collected legally and process should result in usable business information.

Furthermore, the results showed that companies are narrowly focused on the business dimensions of the environment in which they operate-competition and business aspects of the market. And while using some BI activities they ignore broader aspects of the environment in which they operate, primarily those related to the political and security situation. This finding confirmed our initial thesis (Figure 3). Companies mostly collect information relating to their own products and services, prices of products, customers of the same, new products on the market, potential business opportunities, new customers and similar. Also, information on the socio-cultural aspects are not high on the priorities for company.

Placing the emphasis solely on the information that is closely related to the business and ignoring information concerning the security situation, general political situation and socio-cultural aspects can have negative effect on companies and their businesses. In the context of corporate security, this ignored dimension plays an important role as it is a framework from which threats are generated. These findings pointing to the low level of corporate culture means closely understanding of corporate security and lack of long-term business strategies. Country that is in the process of integration in to association with new, different, unexplored and unknown political, economic, cultural and other characteristics should focus its radar to detecting these dimensions and not exclusively have focus on itself and/or competition from its surrounding.

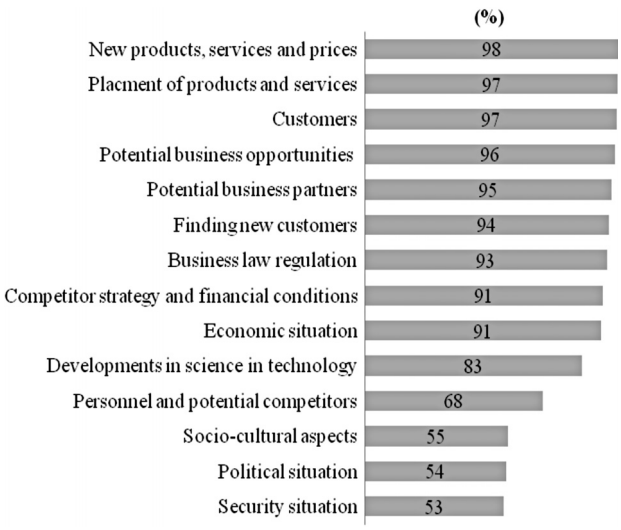

Fig. 3. Ranking/prcetnage of information type that companies collect.

There is one finding in support of our thesis about the selective collecting of information and predominantly focusing on business dimension within which are information about competitors and their products. The finding says that 81% of companies consider their competition strong regardless of whether they apply BI activities systematically, occasionally or not at all. There was no statistically significant correlation between the level of usage of BI and how some companies assess their competition (chi-square test, χ^2=6.387, p=0.381).

As empirical data generally support the thesis of the low level of corporate culture in Croatia, namely that part which is discussed in paper, this theme seeks its widening, both in theoretical and empirical sense, because the consequences of this situation on the overall state of the economy is unquestionable. Further research should go into the core of problem and do detail scan in order to draw attention to weaknesses of businesses strategies and on this way potentially provide guidance for future development to decision makers.

Also, examples of economically successful countries, in our case these are primarily countries with highly developed BI system (Figure 1), is very significant fact and at the same time should trigger further action, both scientific and practical. Necessity of providing a framework which would generate a new/different kind of corporate culture is evident from analysis and comparison of these successful countries. This new corporative culture should have significantly broader understanding of corporate

security as well as functions and capabilities of BI tools in this context. Of course, human resources/human capital are the key for this base and people need to be educated and well trained in this area which requires systematic action and cooperation between public and government institutions and the private sector.

Conclusion

Contemporary »risk society« is full of risks, threats and hazards that are an integral part of functioning in daily life which is also typical for the business world. The modern business world is faced with need not only to manage insecurities but increasingly managing uncertainties generated from a globalized hyper-competitive business environment. New circumstances have imposed tasks for national economies and companies to search for new mechanisms in order to deal with new challenges. In a hyper-competitive globalized world market there is great need for new knowledge and innovation. The key prerequisite for functioning and development in such competitive, uncertain and risky environment are innovative national, social and business activities based on knowledge.

There are two key determinants of the conditions in modern Croatia. On the one hand, this is a long-standing political, social, economic, moral and management crisis, and on the other hand the efforts and expectations of entry into the European Union today's most powerful political and economic association. Obviously, this is a context which vitally needs innovation and adoption of them. Business intelligence and corporate security are certainly innovative national-economic and business tools. In other words, these are resources which should contribute to social change, in particular, economic development and business security of Croatian companies. These are certainly an effective means for equitable and competitive Croatian fierce competition in the Euro-Atlantic market.

The use of business intelligence to detect threats for Croatian companies is an additional step in this process. The results showed that 19% of companies in Croatia have separate business intelligence departments, while 57% of companies occasionally with in other business activities are engaged in business intelligence activities. The progress has been made in relation to previous period but when the situation is compared with one in highly developed economies it is evident that this is insufficient for equal competition in the Euro-Atlantic market.

Research has also shown that most of the businesses that operate in the Croatian territory have limited/narrow understanding of corporate security and in applying business intelligence activities they are primarily focused on business dimensions of environment in which they operate while ignoring other dimensions from which threats could be generated. Narrow perception of security results in selective use of business intelligence. On one hand it does not contribute to sufficient identifying of business opportunities, while on the other hand it does not result in detection of crisis, crisis prevention, effective functioning in times of crisis as well as the functioning in the post-crisis period. And all this is part of the basic functions of business intelligence within the corporate security and crisis management. Preference of information closely related to the business over these regarding security, general political situation and socio-cultural aspects could certainly have a negative effect on business operations. These ignored dimensions play an important role as a framework from which, in narrow sense, threats are generated. If Croatian companies want to succeed in global business environment they should not ignore threats from this global environment.

Acknowledgments

The research which results are presented above was conducted in order to create final work for three students of Sociology, Faculty of Philosophy, University of Zagreb (Jelena Jakšić, Danijela Lucić and Martina Putar Novoselec). It was conducted under the supervision and cooperation with Ph.D. Mirko Bilandžić and Ph.D. Benjamin Čulig from Sociology department of Faculty of Philosophy, University of Zagreb. Authors would like to thank the all members of team as well as business weekly »Lider« which provided database for sample and helped in technical part of research.

REFERENCES

1. TATALOVIĆ S, BILANDŽIĆ M, Basis of the National Security (Ministry of the Interior, Zagreb, 2005). — 2. BECK U, Risk Society: Towards a New Modernity (Filip Višnjić, Beograd, 2001). — 3. ČALDAROVIĆ O, Towards the society of successful regulation of risks? (Croatian Sociological Association and Faculty of Humanities and Social Science, Zagreb, 2012). — 4. BUZAN B, HANSEN L, The Evolution of International Security Studies (Cambridge University Press, Cambridge, 2009). — 5. KESSLER O, DAASE C, Alternatives: Global, Local, Political, 33 (2008) 211. — 6. FUREDI F, Invitation to Terror (Naklada Ljevak, Zagreb, 2009). — 7. HENG YK, McDONAGH K, International Relations, 25 (2011) 313. — 8. MYTHEN G, WALKLATE S, Security Dialogue, 39 (2008) 221. — 9. BILANDŽIĆ M, Business Intelligence (AGM, Zagreb, 2008). — 10. PANIAN Ž, KLEPAC G, Business Intelligence (Masmedia, Zagreb, 2003). — 11. LUECKE R, Crisis Management, (Zgombić & Partners, Zagreb, 2005). — 12. BILANDŽIĆ M, Why business intelligence and corporate security operations are not implemented in Croatian companies? (Expert Conference on Corporate Security, Lider, Zagreb, 2010). — 13. IVANDIĆ VIDOVIĆ D. Process Management of Corporate Security. In: IVANDIĆ VIDOVIĆ D, KARLOVIĆ L, OSTOJIĆ L (Eds) Corporate Security (Croatian Association of Security Managers, Zagreb, 2011). — 14. KOVACICH LG, HALIBOZEK PE, The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program (Butterworth-Heinemann, Burlington, 2002). — 15. KARLOVIĆ L, OSTOJIĆ A, Normative framework for corporate security. In: IVANDIĆ VIDOVIĆ D, KARLOVIĆ L, OSTOJIĆ L (Eds) Corporate Security (Croatian Association of Security Managers, Zagreb, 2011). — 16. BILANDŽIĆ M, CIA's Covert Operationsas a component of U.S. foreign policy. MS Thesis. In Croat. (University of Zagreb, Zagreb, 1996). — 17. SLAPPER G, TOMBS

S, Corporate Crime (Longman, Essex, 1999). — 18. ONCIX – OFFICE OF THE NATIONAL COUNTERINTELLIGENCE, Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011. Office of the National Counterintelligence Executive, accesed 08.09.2012. Available from: URL: http://www.ncix.gov/publications/reports/fecie_all/index.php. – 19. POTTER E, Economic Intelligence and National Security (Carleton University Press and The Center for Trade Policy and Law, Carleton, 1998). — 20. WILLIAMS P, Organized crime, drug trafficking and trafficking in women. In: CAVELTY DM, MAUER V (Eds) The Routledge Handbook of Security Studies (Routledge Taylor & Francis Group, Abingdon/New York, 2010). — 21. TOFFLER A, The Third Wave (Bantam Books Inc., New York, 1980). — 22. CASTELLS M, The Rise of the Network Society, The Information Age: Economy, Society and Culture (Golden Marketing, Zagreb, 2000). — 23. KLAIĆ B, Thedictionary of foreign words (Zora, Zagreb, 1974). — 24. JAVOROVIĆ B, Crises and disasters. In: GROUP of AUTHORS (Eds) Crisis management (Defimi, Zagreb, 2004). — 25. GRBAVAC V, TEPEŠ B, ROTIM F, Journal for General Social Issues, 5 (2001) 858. — 26. DEDIJER S, Stevan Dedijer – The World Jumper (Zrinski d.d., Zagreb, 2000). — 27. PIRTTIMAKI V, Journal of Competitive Intelligence and Management, 4 (2007) 132. — 28. DEDIJER S, Opening Plenary Lecture (Business Intelligence – First Croatian Conference of the collecting, organization and use of business information, Bureau of Business Research, Zagreb, 1999). — 29. VRENKO I, Econimic and Competitive Intelligence – A case study of Slovenia (Business Intelligence – First Croatian Conference of the collecting, organization and use of business information, Bureau of Business Research, Zagreb, 1999). — 30. KLASAN V, Polemos, 14 (2011) 77. — 31. DISHMAN P, FLEISHER CS, KNIP V, Journal of Competitive Intelligence and Management, 1 (2004) 13. — 32. FLEISHER CS, KNIP V, DISHMAN P, Journal of Competitive Intelligence and Management, 1 (2003) 11. — 33. FLEISHER CS, WRIGHT S, TINDALE R, Journal of Competitive Intelligence and Management, 1 (2007) 32. — 34. KNIP V, DISHMAN P, FLEISHER CS, Journal of Competitive Intelligence and Management, 1 (2003) 1. — 35. Accessed 13.03. 2013. Available from: URL: www.scip.org/index.cfm. — 36. Accessed 13. 03.2013. Available from: URL: www.globalintelligence.com. — 37. PRITTIMAKI V, Journal of Competitive Intelligence and Management, 1 (2007) 146. — 38. IVANČEVIĆ D, JURIŠIĆ M, Research study: State of competitive intelligence in Croatian companies (Expert conference on Competitve Intelligence – To CI or Not to CI, Infoarena, Zagreb, 2005). — 39. JURIŠIĆ M, The State of competitive intelligence in Croatian companies (Scientific Conference – Towards the Knowledge Era, The Faculty of Management, Novi Sad, 2005). — 40. ZEBIĆ O, Business intelligence and shaping business strategy Croatian companies. Ec.S. Thesis. In Croat. (University of Zagreb, Zagreb, 2010). — 41. NARODNE NOVINE 35/07, accessed on 13.03.2013. Available from: URL: narodne-novine.nn.hr/default.aspx. — 42. BILADNŽIĆ M, ČULIG B, LUCIĆ D, PUTAR NOVOSELEC M, JAKŠIĆ J, Business Excellence, 1 (2012) 16.

M. Bilandžić

University of Zagreb, Faculty of Humanities and Social Sciences, Ivana Lučića 3, 10000 Zagreb, Hrvatska
e-mail: mbilandz@ffzg.hr

PREDIKCIJA POSLOVNIH PRILIKA I/ILI OPASNOSTI – BUSINESS INTELLIGENCE U FUNKCIJI KORPORATIVNE SIGURNOSTI (EMPIRIJSKA ANALIZA PRIMJENE U GOSPODARSTVU U REPUBLICI HRVATSKOJ)

S A Ž E T A K

Predikcija poslovnih prilika i opasnosti uvjetovana je postojanjem znanja o njima. Praktično, to znanje nastaje prikupljanjem poslovnih informacija iz poslovne okoline, a okvir za to poznat je i pod nazivom business intelligence (BI). Predviđanje prilika i opasnosti inherentno je poslovanju svakog uspješnog gospodarskog subjekta. Korporativna sigurnost kao okvir za ostvarenje sigurnosti poslovanja temelji se na pravodobnim i točnim informacijama pretočenim u prethodno znanje o ugrožavanjima za čije predviđanje poslovni subjekti koriste različite alate, a sustav upravljanja poslovnim informacijama, odnosno BI, jedan je od provjerenih alata. Cilj primjene BI-a jest pravovremeno detektiranje prilika i opasnosti iz poslovnog okruženja kako bi menadžment stigao reagirati na vrijeme. Primjena BI aktivnosti u Hrvatskoj bitno odstupa od svjetskog prosjeka, a u provođenju BI aktivnosti tvrtke su prvenstveno orijentirane na podatke usko vezane za poslovnu dimenziju okruženja u kojem posluju, ignorirajući pri tom političku i sigurnosnu situaciju, okvire iz kojih se generiraju ugroze u užem smislu što je pokazalo i istraživanje provedeno od listopada 2010. do travnja 2011. godine metodom online ankete na uzorku od 1.000, prema prihodu, najvećih hrvatskih tvrtki.