ZORAN KEKOVIĆ, VESNA NIKOLIĆ

SECURITY ANALYSIS AND MAPPING RISKS

As business actions and risks related with them put on like necessity, basic question isn't should we risk, already: are we aware of risk, why we risk, how much we risk and when we risk most. In the business integral access of mapping risks is recommended like a part of unique process risks management. It is shown identification process, process of measures and monitoring security risks of major significance for success or failure in company business. On these basics it is possible to get down to integrating these risks in separate and common map of risks and realize their individual and common effects on company on the whole.

INTRODUCTORY CONSIDERATIONS

Deciding for business projects, management of company choose between two solutions related with risks: stagnating or progress as risk! Increase competition, client's request, increase the speed of technological progress, almost, do not leave a place for dilemma: stagnating or progress.

Strategy choice isn't just a thing of subjective appraisal and compromise of people who presents management. When we appreciate objective sources and indexes, result of risks is a "acceptable" or "unacceptable" risk. On the other hand, consciousness about risk should not discourage inovations and energetic temperament. In any case, surprises will be reduced, because accent will be put on "proactive" instead of "reactive" management.

In connection with strategy determination "progress as risk", there are a few question: do we risk, why we risk, how much we risk and when we risk most. Giving answers on these questions have an aim to produce appropriate suppositions for making a correct, timely and real decisions. How pass it from risky to less risky plan and reduce expenses, without imperilling aims of company, is key for making a decision.

Risks management, as a process that should make possible to predict future events and check them, overcome a few connected, successive phases: coordinating goals, identification hazards and other category linked to risks, analysis and estimate risks, selection the best strategy and current monitoring.

In all these phases, it is necessary that we are aware of huge advantages which offers so-called risks mapping, what it relates to analysis and estimate risks specially. When is at stake security risks, it is very important that their analysis and estimate would be a part unique process of risks management, what is necessary to precede understanding goals of organisation security.

AIMS OF RISKS MANAGEMENT IN SECURITY

New business opportunity in the context technical-technological inovations, modern business risks and linked to them security risks influence on need systematic access to uncertainty and risks management. That means that goals some business units must be coordinated with goals and business politics of company. On the other hand, risk's phi-

losophy requires that company's aims would be determined from aspect of risk and profit. What do in mentioned context present a rational aim for security? Is it avoidance all losses linked to security risks?

Reaction to any threat linked to possible losses isn't optimal solution, whether it is about giving up business actions or use countermeasure that, when are risks at stake, must not channel narrowly only on fixed business functions. That access will result different answer to be exposed risks. In that way, security aim should not have been to avoid all risks. Another extreme would lead to avoidance analysis total risks of organisation which doesn't take into consideration security strategy of organisation. That speculative access, based on experience or appraisal, probably would not have as result effective use all available resources of organisation.

From aspect higher management, it expects from management of security to do maximal effort and with their aims and strategy risks management insure to not be extremme surprises. Higher management can decide to accept risk, but with maximal consciousness about possible consequences. Conclusion is simple, goal of security should have been risk management based on gathering data and predicting probability events and on that base limitation to be exposed risk which can damage organisation.

Complexity, unpredictability, dynamism and often immeasurability and secrecy security phenomena and events influence on preciseness their foreseeing – especially when it is at stake unusual events as terroristic events and unrepeatability conditions in which they appear. Measurement answers on these and other questions crucial influent on quality analysis and appraisal risks. Performing these complex analysis risks is very discussible from aspect costs and savings – profitability analysis, why it practices to use by high-risky events. Like that are security events according to definition, because of insufficient understanding for questions security and preventive imperil in organisations, these analyses are used rarely.

METHODOLOGY OF RISK ANALYSIS

In spite of existence important number of methods and technique analysis of risks security, permanent changes in security, from local level, through region and state, to international level, requires development new methods and techniques.

In study it is described possibility use SARA methodology on risk analysis (*Scaning Analyses Response Assessment model*), up to now use mostly in area community policing. Process of analysis is iterative, so cycles scanning, analysis, answer and reviewing can repeat, all to satisfaction set goal. Model offers possibility of usen feedback information, that is results were attained in the first iteration, because of correction used answer, repeated reviewing, or repetition complete cycle if used answers aren't satisfactory.

SCANNING PHASE

IDENTIFICATION AREA OF IMPERILLING, RISKS SECURITY AND CONSEQUENCES

Security analysis offer primary support in process identification area in which exist risk, in regard to existence weaknesses, by establishing concrete risks, as well as establishing possible correlation between them. Analytic methods offer possibility systematic realization encirclement from interest for analysis, establishing risk classification, appointment risks, give the base for further risks appraisal. In process identi-

fication it is used company's documentation, in other words documentation of system security incidents, as well as reports, reviews and statistics of Ministry of Internal Affairs and other medias for informations wich posses relevant data.

In addition, it comes after independent analyst's investigation, as questionnaires, interviews, meetings and conversations because of realization kontext in which security phenomena from interest are going.

It is used methods of intuitive (heuristic) and objective (detailed) analyses. In this part of process risks management the most suitable are methods factographic and factological informing, elements of description statistics, combined with reports, reviews, expertises (for example Delphy method).

After preparation adequate number of elements for concluding, it is possible to establish areas in which organisation is exposed risk, as well as threat. Clasification of threats mean controlled and uncontrolled threats, after that they are identified individually. List of threats follows list of weak points, as well as risks. In the field of risks management, SWOT analysis (Strengths Weaknesses Opportunities and Threats analysis) is useful – use matrix risks for dokumentation threats, risks and expose. It is necessary to establish tolerance for risk, in other words acceptance certain level of risk, usually in domain where organisation is strongest.

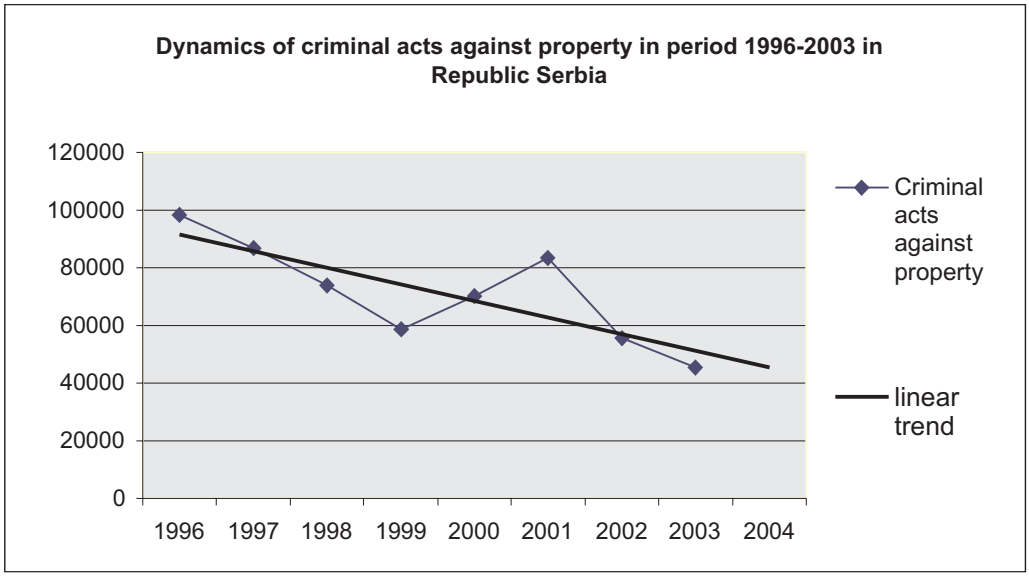
One of the basic characteristics of security risks is possibility their direct or indirect, crucial or potential, immediate or postponed influence on other (unsecurity) risks. The best way to make possible complete understanding profile security of organisation, hers weaknesses and adventages, predictability and expose to different risks, is these risks connect to other which don't have a primary security nature.

Complexity connections and relations between security and other risks require to establish nature of these connections, considering different conditionality and indirectness of security phenomenon in sociable, natural and technical phenomena and influence. In addition, it is needed and considering small risks whose interaction can get into different consequences.

If question is what basic risks some productional or commercial organisations are, usual answers are attacks on property with elements forcible criminality. If this answer wasn't accidental, Table 1 shows a review state of public security in Republic Serbia, in period 1996-2003. In Table 1, it can see that these kind of crime are most representative, in all period of observation. On Picture 1, it is shown a number of crime against property with trend's line and with the prognosticated period. From there it can conclude that a number of crime that kind goes down, with expected number of crime from 51297 in the next year, what is 13% higher than a number of crime in 2003. So mentioned facts speak in favor of that to determinate risk's factor arisen by damages which are commited crime against property, should give this risk high rate, if it is about organisation on territory of Republic Serbia.

Table 1
Review state of public security in Republic Serbia in period 1996-2003

Field of criminal acts, territory of Republic Serbia, period 1996-2003.								
	1996.	1997.	1998.	1999.	2000.	2001.	2002.	2003.
Participation of criminal acts in bussines area in altogether criminal acts	66%	64%	66%	63%	66%	69%	59%	51%
Participation of criminal acts in bussines area in common criminal acts	74%	73%	75%	74%	76%	77%	69%	58%



Picture 1
Dynamics of criminal acts against property in period 1996-2003 in Republic Serbia

ANALYSIS PHASE

ANALYSIS AND ASSESSMENT OF SECURITY RISKS

Security analysis and assessments can be realised for individual events, for one aim or for more busssines goals. Like result of that process arrise different strategies and necessity to accord them.

Analysis and assessment methods involve jobs – ranking risks, creating risk matrix, risk (threats and advanteges) cartography, creating risk portfolio, making correlation between risks and creating dynamic financial analysis.

Withal named methods representing tools for decision making. Analysis proces comprise decisions on strategic, tactical and operational level, therefore nacional, regional, public and private, group and individual decisions. For that purposes risk assessment uses decision support systems – multicriteria systems, web based systems, spatial and group systems.

Principles of heuristic consideration give us the simplest way to present calculated risks within a system, shown in equation below:

$$RF \text{ (risk factor)} = \sum Ki*Ri = \sum Ki*Fi(xi) = K1*f1(xi) + K2*f2(xi) + ...+ Kn*fn(xi),$$

where K is weighted factor, R is probability of individual risk wich depends on different factors named f(x).

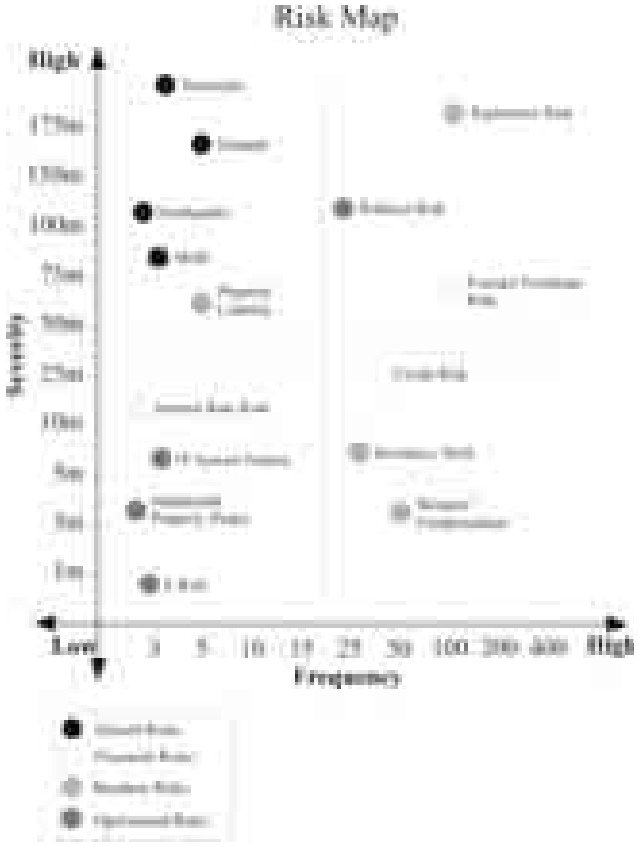
According to designed aims of company, expertise indicates on weighted factor for certain risk, also on likelihood of occurency. Extremly useful in that process are integrated information systems, wich conjoins informations from unhomogeneous areas, with possibility to incorporate analytical methods by programming, scenario-simulat-

ing, online reporting and of course cost benefit analysing solutions. In text below risk mapping process is emphasized, like break point of analysis phase.

RISK MAPPING AND RISK MAPS

Risk maps represent the model for graphic presentation of all risks, not only for those wich are connected with individual bussines sections. This visual medium provide different possibilities - to see a risk groupping and understood connections between them.

Identification of all risks, corelation between them and relationship with risk management solutions process initiated Department for risk management in Microsoft company to create the Risk mapping software system. Integral risk map for some company shows frequency dynamics and risk level, in regard each identified risk. Risk map from Picture 2 shows then E-risk (electronic technology risks) or IT (Information and Communication Technology) system crash represents lowfrequent and low-level risks, but that conclusion should be treated with reserve and only if company doesn't depend on technology. In this case we treat operational risks, in regard usually busines activities.



Picture 2 Risk map-Example[1]

Risks depend on each other. Interested example is risk called lost of reputation. One deadlock in reatailer's chain could cause undelivered stuffs or services, or with unappropriate quality and that event can threat company reputation and contract disrupt.

On the other hand, reputation collaps effects on long period of recovering and revitalizing busssines activities.

Indirect losses maded by teroristic act are caused by bussines interruption in postcrisis period. In example above, there is strong correlation between terorism and bussines processses interuption. Large fire causes not only an property losses or death, even influence on interuption in bussines.

Positive an negative corelation between risks can be used in integral risk management package, using organisation advantages. Therefore, probability of appearance – so and the management strategy for all separate risks depend on each other.

Often managers are not concious then risks correlate for each other. Especialy from security point of view, harmonizing group aims is very complex. Profit drives companies to invest there where conditions are prosperous, but where the hazards are bigest. In that situation, role of security management add up on risk identification and analysis. Possession of informations about risk probability and level and possible losses eliminates incertitude, but not and risk. Comprehend risk scenarious enable us to compute and classificate part of security risks in overall risk structure. Thereby yield to comprehension of acquirement certain aims overall probability, connected with bussines propositions, so risk map is necessary tool in that process.

Risk estimation is important tool too, in organisations wich pay security services or products related with them, becose that estimations provide adequate quality of contracts, assurances contracs and client aims and needs realization.

Risk examination by risk mapps enable creating of consistent risk management strategy. When we discuss about individual operations, risk effects haven't be obvious, but little problem in one department can cause big in other, or little risks with large frequency could become unacceptable in all .

RESPONSE PHASE

DESIGN STRATEGY, IMPLEMENTATION AND INTEGRATION IN BUSSINES PROCESSES

Work on strategy imply variants named avoidance, transfer, reduction and acceptance of risks. Depend on established goals in risk analyses process, apropos status of the security system indicators wich should be set on desirable level, we determine propose for concrete actions. Propose - action plan, contains deferent methods and tehniques, from preventive to repressive actions, from developing infrastructure for risk management, security culture of employees, education and training for employees on security system and finalysed with integrated information system for risk management and decision support system development (examples like *COBRA, INFOGuard, Risk Watch...).*[2]

Irremissible part of actions are recommendations, profiled like regulations and manuals for employyes/organisation, for effective risk management, appropose for emphasize system security. Regulations have the goal named ISO standards in security

field, wich are configured in recommendations like *ISO17799 and Quality Management certified ISO 9001:2000.*

ASSESMENT PHASE

MEASURING AND MONITORING EFFECTIVITY

After the integration of applyed actions in bussines processes, measure indicators of system performanses is necessary, meaning assess new established state. That means then concrete indicators, determined and scaled in scanning and analyses phase, should bring feeedback information about quality of apllied actions. After the new system assessment is maintained, the SARA model phases could be repeated, with goal – to update final system assessment on desirable level. If is necessary (new system assesment is not satisfactory), we may repeat complete process.

This phase comprehend and reporting to competent instituion managers too, becose is necessary for them to be completely informed about the situation and make further decisions.

RISK MAPPING SIGNIFICANCE FOR CURRENT MONITORING

Analyses and assessment quality is very oblique on cognitive attributes of security system. With new risks in security field, we may expect investments in new technology, new placements for peoples, encreasing service and stuff offers etc. This and other reasons have influence on risk management evaluation process necessity, wich could provide information about the following conclusions. Are the incidents was surprise in regard on incipient assessments. Eleven september 2001. incident is represent for drastic deviation from all predicted "worst scenarious".

Risk acceptance assessments are based on incipient estimations, but in the mean time different deviations from acceptable risk level are possible. Named reasons means then identification and estimation are realised and after decision and aplliying risk management strategy. In this phase too, role of risk mapping is multiple.

For comparing purposes (Picture 3) we can use risk map, made for ilustrating frequency and level of losts, before and after adopting risk management solutions.

Risk map can be connected and with current risk management. Particularly, each of early presented risks is graficaly presented in regard on implemented strategies. When we compare two maps, become explicitly then applied strategies aren't coordinated with risk acceptancy level (Picture No. 1). How current evaluation important is, shows example with employee compensation. Until this costs are negligible, risk manager will advise then work contuses should be payed by company (final decision of course is on top management). But when costs, caused with risk frequency, grown too large, risk need to be transfered by insuring.

Risk map can be used for following and recognition rest risks. Representing total company's risks spectrum, wich exists after risk management strategies applied, provide new threats recognition. In this context we can categorised risks on – inacceptable, hardly acceptable and relative negligible. From that point of view, priority in bussines processes and risk tolerancy level recognition, could be realised.

Picture 3 Current risk handling - Example[3]

CONCLUSIONS

Security system in organisation/company would'nt be efficient and developed if is based only on planning specimen experiences and subjektive estimations. Security, together with other bussines processses, must become part of risk management and risk evaluation paradigm.

Risk magement is dynamic process, not the project ! Risk maps are one of the necessary tools wich provide that, as security analysis must make them cognizable to security management. Athwart, this important function will lost main meaning.

ABOUT THE AUTHORS

Zoran Kekovic is assistant professor at Faculty of Civil Defence University of Belgrade and researher in certain division in Police College, Belgrade. He has participated in different projects, conferences and congressses and is author of many articles. Most of project and articles are about industrial security and relationships between private and public sector in their roles in joint security. His interests are oriented in developing risk management process in security fields. He is a member of Center for Security Management, Faculty of Civil Defence, University of Belgrade.

Contact details: Pollice College, Belgrade, tel: +381 11 3107208,

e-mail: zoran@vsup.edu.yu or zorankekovic@yahoo.com .

Vesna Nikolić is engineer of telecommunications, graduate student in field Information Systems. Works in CyberEducation and Development Center within Police College in Belgrade, like Head of Department for Modern Education. She is responsible for Police College Information System planning, developing and evaluating. Also teaches a course on "Information System of the Ministry of Internal Affairs". Her areas of interests are security analysis and e-learning.
Contact details: Pollice College, Belgrade, +381 11 3107173,
e-mail: vesnan@vsup.edu.yu or kess@yubc.net

ENDNOTES

1 See Ref. No. 1

2 See Ref. No. 8, 12 and, respectively

3 See Ref. No. 1

This paper has been peer reviewed by: professor Dr. sc. Ozren Dzigurski, Faculty of Civil Defence, University of Belgrade.

REFERENCES

1) Baranoff, E. (2004). Risk management and insurance. Danvers, USA:Wailey.

2) Kenedi, P. (1997). Priprema za 21. vek. Beograd: Sluzbeni list SRJ.

3) Marez, T. (2000). Police and private security: What the future hold?. Otawa, Canada: Association of chiefs of police.

4) Stamatovic-Djuric, O.,Vidojkovic, D., Savic, J. (2003). Informatika u organima unutrašnjih poslova. Beograd: Visa skola unutrasnjih poslova.

5) Stamatovic-Djuric, O.,Vidojkovic, D., Savic, J. (2000). Savremeno operativno informisanje. Beograd: Visa skola unutrasnjih poslova.

6) Taylor, M., Horgan, J. (2003).Terorizam u buducnosti. Zagreb: Golden marketing.

References from World Wide Web:

7) American Institute of Certified Public Accountants. (2004). American Institute of Certified Public Accountants. Retrieved March 25, 2004, from the World Wide Web: .

8) C&A Systems Security Limited. (2004). C&A Systems Security Limited. Retrieved May 10, 2004, from the World Wide Web: /.

9) Cho, S., Ciechanowitz, Z. (6/16/2001). Selection of systems for detailed risk analysis in combined risk analysis approach. Information Security Group, Royal Holloway, University London. Retrieved May 10, 2004, from the World Wide Web: http://www.cs.kau.se/~simone/ifip-wg-9.6/scits2/Cho.pdf .

10) Community Policing Consortium.(2004). Community Policing Consortium.Retrieved May 15, 2004, from the World Wide Web: http://www.communitypolicing.org/.

11) IEMSs - the International Environmental Modelling and Software Society Retrieved. (2003). IEMSs - the International Environmental Modelling and Software Society Retrieved. Retrived June 7, 2004, from the World Wide Web: 257_carlon.pdf.

12) InfoGuard AG. (2003). InfoGuard AG. Retrieved June 9, 2004, from the World Wide Web: http://www.infoguard.com/.

13) International Association of Crime Analysts. (2001). International Association of Crime Analysts. Retrieved March 20, 2004, from the World Wide Web: http://www.iaca.net/.

14) Patrick, M. (11/8/2002). Proving the SARA model: A problem solving approach to street crime reduction in the London Borough of Lewisham. Retrieved March 17, 2004, from the World Wide Web: http://wwwojp.usdoj.gov/nij/maps/Conferences/02conf/Patrick.doc.

15) Police Information Technology Organisation. (2002). Police Information Technology Organisation. Retrieved March 25, 2004, from the World Wide Web: http://www.pito.org.uk/.

16) Risk Management and Human Capital Consulting - Aon Corporation. (2001). Risk Management and Human Capital Consulting - Aon Corporation. Retrieved May 28, 2004, from the World Wide Web: http://www.aon.com/.

17) Sensors Research Consulting, Inc. (1998). Sensors Research Consulting,Inc. Retrieved June 10, 2004, from the World Wide Web: http://wwwsensors-research.com/.

18) RiskWatch.(1998). RiskWatch. Retrieved June 10, 2004, from the World Wide Web: http://www.riskwatch.com/.