Research of Threat Estimate Criterion in Managing Business with Cash Money and Valuables

Darko Palačić*

Abstract: In article are presented results of empiric research in threat estimate criterion, by which is determined 15 criterions that are indispensably graded during performing the threat estimate. Correct choice of threat estimate criterion is basic condition to contemplate source and type of threat in managing business with cash money and values. Research is conducted among companies authorized for threat estimate performance. Therefore, the results of this research represent contribution to defining threat estimate methodology in managing business with cash money and values.

Keywords: criterion, financial institutions, security, threats estimate

JEL Classification: C13, D81

Introduction

European countries have united their interests in bank institutions and founded European Banking Federation (Federation Bancaire de L'Union Europeenne - FBE). European Banking Federation (2005) momentarily has 28 full members and 7 associate members. Among the associate members is the Republic of Croatia also. Data about number of robberies committed in certain countries per million inhabitants from FBE report (2002, 2004, 2005) are presented in Chart 1. The largest number of robberies happens in Italy and this country significantly differs from others. After Italy follows Germany and Austria. They have slightly bigger number of robberies than transitional countries. According to presented data Slovenia and Croatia essentially do not stand out from countries around them.

The risk, that is according to FBE defined as probability of attack on bank offices (total number of offices divided by number of committed robberies), is growing, and

---

* Darko Palačić is at Alzas Alarms d.o.o., Čakovec, Croatia.

at the moment in Europe the rate is 1:35, to be exact, the robbery is committed in one out of 35 bank offices.

Figure 1: Number of robberies per million inhabitants
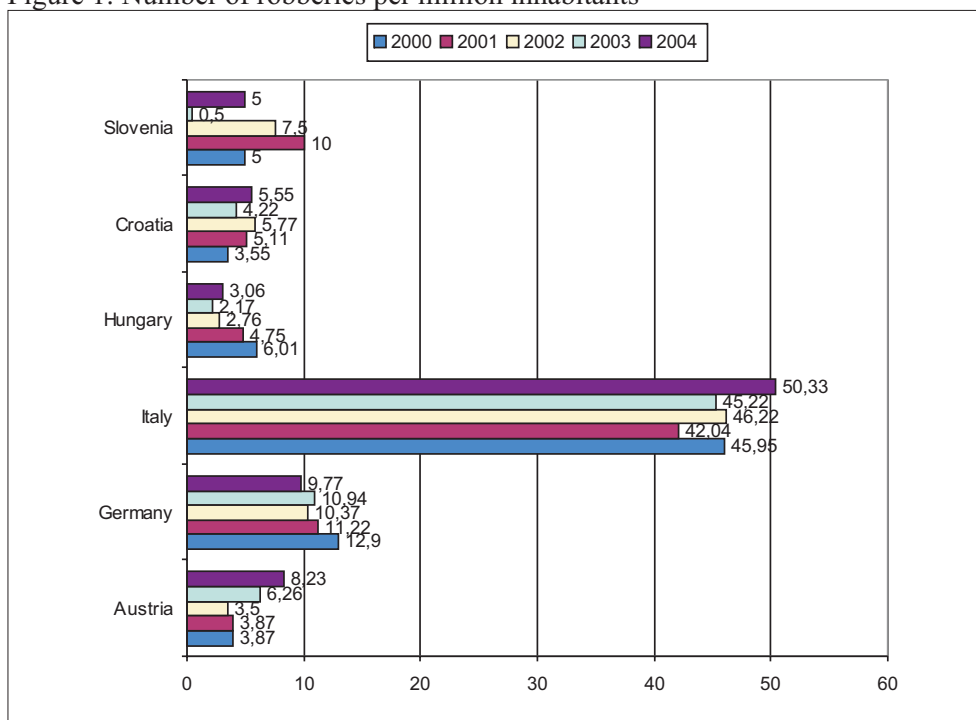
Of great concern is the growth of attack on cash money and valuable's transport vehicles. In those attacks often army weapons are used. On the basis of conducted research in FBE report (2005), it is concluded that the balance between expected robbery and risk in principle has an impact on growth or diminishing certain type of criminal act. For example, burglaries into money institutions which expect large loot are in correlation with applying army weapons and type of attack. Information about large loot has an impact on preparation, organization and equipping criminal groups.

Conception and Purpose of Threat Estimate

Efficient managing of potential loss and damage in conducting business with cash money and valuables is one of conditions for successful realization of business results in this line of work. For that reason safety and risk management in dealing

with cash money and valuables must be integrated in entire business of financial institution.

According to Lamoreaux (2005), the goal of safety process and safety system that is managed, is realization of acceptable state of safety in which risks are identified, assessed, and diminished or completely removed. Reinstatement of safety system, its bringing up to date and development is based upon threat estimate by which sources and type of threat are defined, then critical places in business process, consequences of threat and optimal measures of protection from determined threats. (e.g. Dworken et al., 2003).

Considering the frequency of appearance, financial institutions are at the highest threat point in robberies. Reason for that is found in easy availability to larger amounts of money and relatively short time needed for a criminal act to be executed (e.g. Palačić and Hutinski, 2006).

Threat estimate is procedure of probability of events and estimate which represents possible danger and threat to people, money and valuables, as well to business processes. To estimate, it means to make judgments, gradation and assessment. Procedure of estimate and assessment will result with right outcome only if it is based on relevant data. The point of making a threat estimate is recognizing source and type of danger, determining the risk level, in other words probability of event emergence that represents danger to people, property and business processes, for-seeing probability and frequency of its emergence, determining risk size, and diminishing the risk through setting optimal measures of protection and raising up defense capabilities.

There are number of distinct approaches to threat and risk analysis. However, these essentially break down into two types: quantitative and qualitative (e.g. Turner, Gelles et al., 2003). Quantitative Risk Analysis approach employs two fundamental elements; the probability of an event occurring and the likely loss should it occur. Qualitative Risk Analysis is the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements (e.g. Vidalis, Blyth et al., 2002). Key elements for quantitative threat estimate are determining estimate criterion and its significance.

Determining the sample

Research criterion of threat estimate is conducted in companies that deal in private protection business in Croatia. Those companies are authorized for making threat estimates in financial institutions. By that the aimed population is identified. On January 1st 2006 in Croatia, 234 authorized businesses for private protection were

registered. The frame for sample selection is alphabetical list of authorized businesses for private protection, which for research needs provided by the Croatian Security Association.

Random sample is chosen out of basic group, and is determined with help of table of random numbers (e.g. Žugaj, Dumičić, Dušak et al., 1999). By setting the sample, the method of sample selection without repetition is applied. To be precise, elements for sample are chosen by order, and same have after selection remained in the basic group and by that procedure took part in selection of the next element for sample.

The size of a sample is based upon two judgmental decisions, on reliability level and on permitted error in sampling. The subject of research is safety of people and property, therefore, the 1,28 coefficient of trust is set, which is given in chosen probability assessment of 80%, with allowed error of ±10% and coefficient in population variation of 50%. Determined size of simple random sample (n = 41) represent total number of authorized businesses for private protection (sample unit) that are included in empiric research, while, the research unit is person that conducts threat estimates. The sample is representative and probable. Relatively speaking, the sample makes 17.52 % of main group, and it can be concluded that the contained population is representative. Representative sample is achieved by correct random election of elements in basic group, basic characteristics of those elements that are similar to basic group, than by reliability level and allowed error.

Research Methodology

For research needs Likert type of survey questionnaire has been composed. Research has been conducted through e-mail during month of May 2006. With the help of survey the opinions of participants is searched, for their viewpoints and significance of criterion thus being determined. For determining threat estimate criterion, methods of analytical statistics are being used to enable on basis of data, conclusions about characteristics of entire population.

Characteristics of Examinees

Regarding the question about their own knowledge of threat theory, the acquired opinion of the examinees on their own knowledge of the subject one declared having to know the theory of threat. Total of 14.3% examinees think to know the threat theory poorly, 40% of examinees, good, 34.3% think to know very well, and 11.4% think to know very well.

Figure 2: Personal knowledge in threat theory
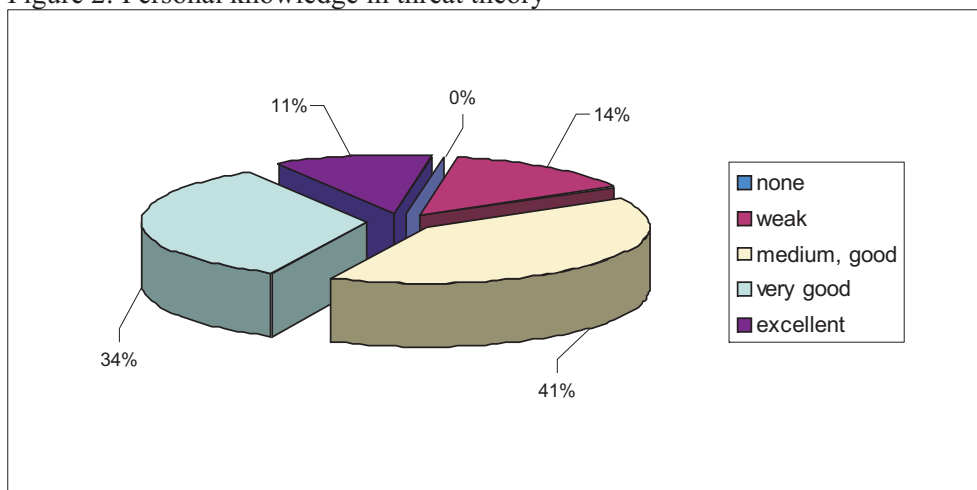
In group that declared to know the threat theory very well, first half has work experience from 3 to 5 years, and other half from 11 to 20 years. Total of 20% of examinees have work experience from 11 to 20 years and grade their threat theory knowledge very good.

Regarding the data combined in Table 1. it has been conducted χ^2 test of independence of peculiarity of work experience in field of technical protection and threat estimate knowledge according to which it is considered by zero hypotheses that all classifications are mutually independent.

With level of coincidental appearance probability p = 0.05 and χ^2 = 3.4 it is determined that the difference among classifications is not statistically significant, in fact the difference is coincidental. So it is concluded that there is no mutual dependence in work experience on field of technical protection and knowledge in threat theory. Considering that the difference is not statistically significant, connection degree does not need to be calculated. The fields that contain the data of 0.0% means that there is no examinees with mentioned feature.

Although percentage part of people with single characteristics varies from 2.9 - 20% statistically significant difference among classifications is not found. Majority of examinees, depending on work experience (37.1%) falls in category from 11 to 20 years, and 40% of examinees declares to know the threat theory well (good). Statistically significant difference is determined among good and excellent knowing the threat theory with coincidental appearance probability less then 5%.

Table 1: Contingence in threat theory knowledge regarding work experience

		Knowledge in threat theory					Total %
		None %	Weak %	Medium, well %	Very well %	Excellent %	
Work experience in technical protection	up to 2 years	0.0	2.9	2.9	8.6	0.0	14.3*
	from 3 to 5 years	0.0	0.0	8.6	11.4	5.7	25.7*
	from 6 to 10 years	0.0	11.4	8.6	2.9	0.0	22.9*
	from 11 to 20 years	0.0	0.0	20.0	11.4	5.7	37.1*
Total %		0.0	14.3*	40.0**	34.3*	11.4*	100.0

*p<0.05, **p<0.01

Results in Threat Estimate Criterion Research

Considering, that there is no unique threat estimate system, the research had a goal to determine the criterion on basis of which the threat is being estimated. Therefore, in conducted research the examinees have declared on the basis of implementation of certain threat estimate criterion in managing business with cash money and valuables in their own practice. Valuing vulnerability, as a threat estimate criterion is least applicable in practice (35.9% examinees do not value vulnerability). Even 25% of examinees during estimate do not grade the reaction speed of security officers and police, 16% of examinees do not grade applying organizational protection measures, and 18% availability of cash money and valuables to perpetrators.

By Pearson coefficient of linear correlation between measured applicable and inapplicable appearance of certain threat estimate criterion, it is determined that correlation of mentioned features is weak.

By analysis of given results, with probability of coincidental appearance less than 5%, it is defined that in threat estimate are used criterion from table 2.

Table 2: Implementation of threat estimate criterion

	Criterion that are being graded during threat estimate	Graded %	Not graded %
1	Data about facility and location	100.0	0.0
2	Exposure of facility and location to threat	100.0	0.0
3	Data about business process	100.0	0.0
4	Type and number of users	100.0	0.0
5	Work regime and way of facility usage	100.0	0.0
6	Applying technical protection measures	100.0	0.0
7	Applying organizational protection measures	82.1	17.9**
8	Availability of money and values to perpetrators	83.3	16.7**
9	Speed of reaction from security officers and police	75.0	25.0**
10	Total efficiency of existing protection	78.9	21.1**
11	Data about harmful events up to now	97.5	2.5**
12	Valuing the property	90.0	10.0**
13	Valuing certain type of threat	88.9	11.1**
14	Valuing the vulnerability	64.1	35.9
15	Valuing the risk	100.0	0.0
	Average	90.7**	9.3

**p<0.01

The estimate criterion 'applying organizational protection measures' totally 17.9% examinees do not grade, from which 42.9% examinees that have declared to know the threat theory very good and 14.3% examinees that know the threat theory poorly (weak). By conductig χ^2 test, with the coincidental appearance probability level p = 0.01 and value χ^2 = 12.6 it is concluded that the difference between applicability and inapplicability of criterion is statistically significant, to be exact, not coincidental.

The estimate criterion 'availability of money and values to perpetrators', 16.7% examinees do not grade, from which 20% examinees that excellent know the threat theory, 40% examinees know the threat theory, very good and 20% examinees that know the threat theory good and weak. Through the χ^2 test, with coincidental appearance probability level p = 0.01 and value χ^2 = 15.11 we learn that the difference between applicability and inapplicability of criterion is statistically significant, to be exact, not coincidental.

The estimate criterion 'speed of reaction from security officers and police' does not grade 25% examinees, from which 33.3% examinees that have declared to know the threat theory very good, 55.6% examinees that have declared to know the threat theory good and 11.1% examinees that know the threat theory poorly (weak). From conducted χ^2 test, with coincidental appearance probability level p = 0.01 and value $\chi^2 = 8.25$ it is concluded that the difference between applicability and inapplicability of criterion is statistically significant, to be exact, not coincidental.

The estimate criterion 'total efficiency of existing protection' does not grade totally 21.1% examinees, from which 25% examinees that have declared to know the threat theory very good, 62.5% examinees that have declared to know the threat theory good i 12.5% examinees that know the threat theory poorly (weak). Conducted χ^2 test, with coincidental appearance probability level p = 0.01 and value $\chi^2 = 10.31$ shows clearly that the difference between applicability and inapplicability of criterion is statistically significant, to be exact, it is not coincidental.

The estimate criterion 'data about harmful events up to now' does not grade 2.5% examinees, and only one of examinees had declared to have week knowledge about threat theory. The χ^2 test, with coincidental appearance probability level p = 0.01 and value $\chi^2 = 31.1$ it is concluded that the difference between applicability and inapplicability of criterion is statistically significant, to be exact, it is not coincidental.

The estimate criterion 'valuing the property' does not grade totally 10% of examinees, from which 25% examinees that have declared to know the threat theory very good, 50% examinees that have declared to know the threat theory good and 25% examinees that know the threat theory poorly (weak). By conducted - test, with coincidental appearance probability level p = 0.01 and value χ^2 test = 20.8 concluds that the difference between applicability and inapplicability of criterion is statistically significant, to be exact, it is not coincidental.

The estimate criterion 'valuing certain type of threat' does not grade 11.1% examinees, from which 25% examinees that know the threat theory excellent, 25% examinees that have declared to know the threat theory good and 50% examinees examinees that know the threat theory poorly (weak). Conducted χ^2 test, with coincidental appearance probability level p = 0.01 and value $\chi^2 = 20.8$ it is evident that the difference between applicability and inapplicability of criterion is statistically significant, to be exact, it is not coincidental.

The estimate criterion 'valuing the vulnerability' does not grade totally 35.9% examinees, from which 14.3% examinees that have declared to know the threat theory very good, 64.3% examinees that have declared to know the threat theory good and 21.4% examinees examinees examinees that know the threat theory poorly (weak). In conducted χ^2 test, with coincidental appearance probability level p = 0.05 and value $\chi^2 = 1.4$ it follows that the difference between applicability and

inapplicability of criterion is not statistically significant, to be exact, it is coincidental.

Discussion

By conducting empirical research via representative sample of authorized companies, 15 threat estimate criterion in managing cash money and valuables we conclude that these need to be graded so that adequate protection measures can be set. Considering that in Croatia there is no one unique threat estimate system in managing business with cash money and valuables, the results of this research is a step forward into the field of defining unique threat estimate system and work methodology. Results of this research are statistically processed and for each criterion statistical difference between applicability and inapplicability in practice is determined.

Regarding the characteristics of examinees that have participated in this research, in fact, their knowledge of threat theory, acceptance of mentioned threat estimate criterion in managing business with cash money and valuables we propose a continuance of research in the field.

At the end we can say that results of such research enables the setting of a unique model of threat estimate in managing business with cash money and valuables supported by computers that will help achieve security growth of financial institutions.

REFERENCES

European Banking Federation, (2005), Bank Robberies & other Bank Raids in Europe, http://www.fbe.be (17.02.2006.).

European Banking Federation, (2002), Eleventh Report on Bank Robberies and Other Bank Raids, Banking Federation of The European Union, Brussels: Working group on physical security, http://www.fbe.be (17.02.2006.).

European Banking Federation, (2004), Thirteenth FBE Report on Bank Robberies and other Bank Raids, Banking Federation of The European Union, Brussels: Working group on physical security, http://www.fbe.be (17.02.2006.).

Dworken, J. T., (2003), Threat Assessment,. *Alexandria*, Institute for Public Research.

Hutinski, Ž., Palačić, D., (2006), Sustav upravljanja sigurnošću novčarskih institucija, in I. Konferencija 'Menadžment i sigurnost 2006', (Čakovec: HDIS).

Lamoreaux, D.J. (2005). Business Loss prevention Techniques, http://www.pimall.com/nais/nloss. prev.html (21.03.2006.).

Palačić, D., Hutinski, Ž., (2006). Security Management System in Financial Institutions: How to reduce the likelihood of robbery, burglary and larceny, in Čišić,D., Hutinski, Ž., Baranović, M. and Sandri, R. (ed.) MIPRO 2006, 29th International Convention (Opatija: MIPRO).

Turner, J. T., Gelles, M. G., (2003), Threat Assessment-A Risk Management Approach (London: The Haworth Press), http://www. haworthpress.com (22.03.2006.).

U.S. Department of Justice, (2005), Protective Intelligence – Threat Assessment Investigations, http://www.atapusa.org/downloads/PAITI170612.pdf (22.03.2006.).

Vidalis, S., Blyth, A., (2002), Understanding and Developing a Threat Assessment Model, School of Computing, University of Glamorgan, http://www.comp.glam.ac.uk (21.03.2006.).

Žugaj, M., Dumičić, K., Dušak, V. (1999). Temelji znanstvenoistraživačkog rada (Varaždin: FOI).