A MODIFIED MEAN VALUE APPROACH TO ASSESS SECURITY RISKS

Albin Zuccato
Karlstad University, Department of Computer Science
Universitetsgatan 1, 651 88 Karlstad, Sweden
albin.zuccato@kau.se

Abstract As eCommerce security risk assessment, where the conventional methods of risk analysis are implemented, have lead continuously to problems, it is reasonable to assume that a faster and more business centric method to assess security risk can be helpful. In this paper, a modified mean value approach, which is supposed to be quickly conducted and understandable also for business people, is proposed. The approach is based on a mean value decision scenario enhanced with risk attitudes and consolidated to reflect the time behavior requirements. Economic research has proven that different risk attitudes are to expect for different risk scenarios, and therefore we give an example of the flexibility of the approach working with these different attitudes during one assessment session.

Keywords: risk analysis, risk assessment, mean value, risk attitude

1. INTRODUCTION

As mentioned in (Moses, 1992), risk analysis and assessment have the problem that they never are finished in time. An extreme scenario is presented, where the risk analysis was finished when the product already had retired. For electronic- and mobile-commerce (e/mCommerce) with its short time-to-market requirements the consequences are even worse. However, this is not restricted to e/mCommerce: also the conventional industry has the goal of coming closer to the costumer in shorter time with help of computer systems, and needs therefore a fast process to assess the involved security risks.

Another problem, often heard from practitioners, is that a lengthy risk analysis delivers results that have to be explained to the decision maker, who often enough is a senior manager with business background. Also this requires additional time.

All these problems lead Gerber/vanSolms (Gerber and von Solms, 2000) to the conclusion that risk analysis is not the single sufficient tool for security preparation. However, they postulate that risk analysis could supply a decision support capability.

This information brings us to the conclusion that a risk assessment tool has to enforce the following requirements:

- direct decision support
- understandable results
- fast applicability

This paper intends to propose an approach that fulfill these criteria. For beeing able to meet the first two requirements we will refer to the mean value approach and its enhancements which have their roots in business science – see for example (Gordon, 1983). As the security risk management can be considered as different from a conventional risk decision, some modifications are proposed to meet the third requirement – the speed. These modifications are presented in an own section and constitute the modified mean value approach for information security. To see how this works a simple eCommerce situation will be analyzed using the approach.

2. BUSINESS DECISION SYSTEM

The economic management means that corporations, managers and employees always have to make their own decisions. To make a decision understandable and reconstructible, a methodic way of conducting it is required, otherwise the consequence would be a chaotic and ineffective business. That would be a hindrance to maximize the profit.

A risk management decision is one of the most important decisions in an organization. Economics has therefore taken great effort in research and in formalizing this kind of decision making processes.

The range of methods is wide, and a description of them all is beyond the scope of this work. Instead this work focuses on a simple method - the mean value approach - and modifies it in a way that may satisfy the needs of information security management.

In this section we investigate the prerequisites for the modified mean value approach. The first area of investigation will be the conventional formula for the mean value, and an example of usage will be given. To understand how to overcome one of the deficits of the mean value approach – the ignorance of risk attitude – a short presentation of preference functions will be presented. This is then going to be used to

motivate a way of finding the risk attitude of the decision maker[1] and of taking it into account.

2.1. MEAN VALUE APPROACH

It can be assumed that a rational human beeing[2] always would choose a situation with the highest profit – or for security with the smallest costs. The question is now how to find the optimal alternatives out of the many availiable[3] ones. Firstly some kind of comparison criteria have to be chosen. One of the simplest ways is to calculate the mean value (μ) of the alternatives by multiplying the effect (e_{ik}) with the probability (p_i) – as seen in equation 1 – , and to take that with the highest value (assuming that positive numbers represent profit and negative loss) – see (Gordon, 1983).

$$\mu_i = \sum_{k=1}^{n} p_k \times e_{ik} \tag{1}$$

To see how this works, lets calculate the following situation. A person wants to travel from A to B. Depending on the weather and on the way of travelling – by car (alternative 1 – A_1) or by motorcycle (A_2) – , different travelling times (effects – e) are expected by the person. Unfortunately the person has to decide today how to act, and cannot wait until tomorrow when s/he knows the weather. By looking on the weather forecast the person learns that it is going to rain (situation 1 – S_1) with 40 % ($p_1 = 0.4$) likelihood and, with 60 % ($p_2 = 0.6$) the sun is going to shine (S_2). This is represented in table 1.

Table 1 Example for the mean value approach

	Rain - S_1 $p_1 = 0.4$	Sun – S_2 $p_2 = 0.6$	μ
Travel by car – A_1	80 min	70 min	74 min
Travel by motorcycle – A_2	90 min	50 min	66 min

Based on the mean value the person decides to choose alternative A_2 because on the average less travel time is to expect.

2.2. ABOUT PREFERENCE FUNCTIONS

A decision, solely based on the mean value, neglects people's or organizations perception of risk situations. Dependent on the overall risk attitude, a person or an organization reacts differently on risks. A situ-

ation, where an unlikely risk can have strong negative influence on the economic situation, can be worse for a decision maker than a risk which only means small but regular loss.

To represent this fact, economic science (Eatwell et al., 1987) proposes the use of preference functions. Such a preference function shows in a transitive, irreflexive way the preferable alternatives compared to the other ones. Alternative 1 $\prec$ Alternative 2 means that 2 is to prefer to 1, whereas Alternative 3 $\sim$ Alternative 4 means an indifference between those alternatives. Considering the dilemma of the decision maker from above, we can say that a person, as mentioned above, prefers a likely small loss over an unlikely huge loss.

Now the question is how to represent the risk attitude formally. Lets assume that we compare a saving where we certainly get the interests(A_1) of 100 against a lottery/bet(A_2) where we can loss 1000 of win 1200. The example is shown in table 2 shows two situations that are equally based on their mean values. However, we can see that the standard deviation is different. So the standard deviation[4] can be used to see how much fluctuation we can expect.

Table 2 Example for a standard deviation approach

	S_1	S_2	μ	σ
	$p_1 = 0.5$	$p_2 = 0.5$		
A_1	100	100	100	0
A_2	-1000	1200	100	1100

Using this in the security area means that the standard deviation can be used to express the uncertainty of the event – see for example (Dockner et al., 1999). To reflect the risk attitude the standard deviation (σ) has to be incorporated in the individual preference function $\Phi = \Phi(\mu, \sigma)$.

To be able to solve the decision problem it is necessary to formulate a risk attitude function. The function needs to include the standard deviation σ and a weighting factor α. However, the influence of the standard deviation can vary. Therefore this behavior should be expressed in a function of the standard deviation $\alpha f(\sigma)$.

Depending on the risk attitude (see (Dockner et al., 1999)), α usually takes different values. Note that the presented risk attitude functions are used in economics and do therefore not reflect the intention of modelling security risks.Their normal usage is to compare win situations with

eachother instead of loss situations – as required for security modelling. We distinguished between the following attitudes:

risk neutral Alternatives with the same mean value are equal, independent of the standard deviation – this is actually the mean value approach which therefore can be considered as the special case.

$$\Phi(\mu, \sigma) = \mu + \alpha f(\sigma), \alpha = 0 \Rightarrow \Phi(\mu, \sigma) = \mu \tag{2}$$

risk aversion The higher the risk is, the higher the average return (based on the mean value) has to be.

$$\Phi(\mu, \sigma) = \mu + \alpha f(\sigma), \alpha < 0 \tag{3}$$

risk loving The mean value is negatively correlated to the standard deviation.

$$\Phi(\mu, \sigma) = \mu + \alpha f(\sigma), \alpha > 0 \tag{4}$$

For each alternative decision the equation is calculated and a ranking carried through. The result is a vector of alternatives ordered by preference.

3. A MODIFIED MEAN VALUE APPROACH

As already mentioned in the introduction, a risk assessment approach has to fulfill two features: they have to be understandable and quick. The second criterion, the speed, becomes even more important if considering eCommerce environments where short time-to-market is a key criterion for success. However, the speed of the process alone is not sufficient if the results can not be easily applied by the business decision makers.

The last criterion is one of the driving factors for using a mean value approach: the business people are used to it – see for example (French, 1993), (Gordon, 1983). In almost every book and curriculum about economics you find a part about mean value based decisions. However, as presented in the last section, the simple mean value approach is not entirely designed for security. Therefore modifications are necessary, to reflect information security needs. To reflect the speed requirement some simplifications are recommended. However, it is not permitted to reduce the quality visibly.

3.1. THE APPROACH

When looking at the mean value function some modifications for an effective use for security risk assessment seem to be necessary. First

we can assume that there is only one condition (the loss situation) for which we calculate the risk. This simplification relaxes the amount of data necessary with an acceptable loss of accuracy. This is due to the fact that for risk assessment the win situation has a profit[5] of 0 – in other words: a vulnerability, leading to a risk, is not exploited there is no profit. So we can simplify to

$$\mu = p \times e \tag{5}$$

If we further assume that the process is conducted by experts with a risk attitude represented via $\alpha f(\sigma)$ we can conclude that

$$p_{modified} = p + \alpha f(\sigma) \tag{6}$$

and

$$e_{modified} = e + \alpha f(\sigma) \tag{7}$$

It can also be assumed that both values need to be modified. In the result, existing countermeasures and their potential usefulness have been taken into account. Additionally: the frequency also represents how much the expected risk is feared. By involving the risk attitude the effect values also include the kind of assumed damage.

Note that due to the simplification of only observing the loss situation, the slope (α) needs to be multiplied with -1. This leads to the opposite interpretation as presented in section 2.2. Figure 1 shows the indifference curves for (a) a risk averse decision maker and (b) a risk loving decision maker. All points on an indifference curve are equally good for the decision maker, whereas an indifference curve closer to 0 is preferable against one further away from the center.

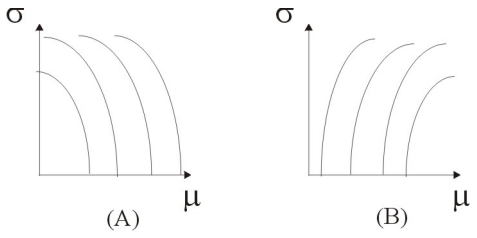

Figure 1 Indifference functions representing the risk attitude

Aggregating the simplification and the modification leads us to the simple equation

$$\Phi(\mu, \sigma) = \mu_{modified} = p_{modified} \times e_{modified} \tag{8}$$

to calculate a risk.

3.2. INPUT DATA

The main input data for the calculation is the probability and the effect(impact). The identification of risks and the assignment of the initial values is out of the scope of this paper[6]. Only the further processing of those data by experts is investigated. For efficiency reasons it is recommended only to calculate an overall value for a risk, and not to split it in the categories of confidentiality, integrity and availability as suggested for example by CRAMM (CRA, 1996).

However, to make the data more usable a standardization between 0 and 1 is suggested. For the probability values this should not be especially difficult, as they are usually expressed as a percentage of likelihood.

For the effects the standardization needs some explanation. To express damage of an asset between 0 and 1 we need to find a characteristic that can be used for every asset under consideration. The proposal of the ALE - FIPS 65 (FIP, 1975) is a table representing damage in money values and giving mappings to abstract representation of these values. This seems to be unsuitable, at least if we consider that this approach should be usable for qualitative risk assessment as well.

It would therefore be more suitable to express a damage potential in the percentage of destruction of the asset. 0 means that the asset is not harmed at all, while 1 means the complete destruction of the asset. An example for 0 is a port scan, which has (nearly) no destructive influence on an asset[7]. Whereas the erasure of a database with no back-up would be a complete destruction of the asset and therefore 1. Note that from an objective viewpoint the values 0 and 1 are unimaginable because such a "pure" situation is very unlikely in reality.

3.3. WHAT RISK ATTITUDE FOR SECURITY?

As seen from the final equation (see equation 8) the risk attitudes are represented in modified values. But how do you determine them? Economics suggests the alternative to offer the decision makers some lotteries compared with a certain payments ($\mu = e$ is equal, better or worse than $\mu\sigma = p_1e_2 + p_2e_2$) and then to aggregate the answers to a risk attitude function.

In security risk assessment and decisions we could assume a risk averse behavior in almost all situations. In most cases the values of p and e will then be increased to reflect the risk according to the decision makers attitudes.

However, research in economics shows that a decision maker, even if s/he tends to be risk averse, under some circumstances is becoming risk loving. In the security field this could for example happen if we can expect a likely risk with minor effect – such as the already described port scan. A risk loving behavior is consequently possible for those risks. The result would be that the values – here mainly the p – are reduced.

3.4. INTERPRETING THE RESULT

There are two different interpretation methods in the assessment approach, the qualitative one and the quantitative one. If the approach is a qualitative one the calculated risk values themselves can be used. For a quantitative approach the risk values are multiplied with the monetary value of the asset under consideration.

The first approach assumes that the risks are calculated and then ordered into a vector according to their severity. With this ordering also the order of processing becomes obvious. This is due to the fact that it sounds reasonable to process higher risks earlier. By expressing the residual risk with a risk value it could also be determined to which extent the risks have to be considered. The independence from asset values enables also the reuse of the risk values for different assets with the same risk characteristic.

For the quantitative approach the calculated damage value can define the amount of investigations for countermeasures. The residual risk can here be expressed as an monetary amount which has to be reached with countermeasures.

4. SCENARIO

The following scenario assumes that only three risks need to be calculated. This is of course a very narrow scenario, far away from reality, but still capable of showing how the modification and simplification can be carried through. Even if the scenario could be seen as independent from an application area for the motivation of the modification, it should stay in mind that here a web based eCommerce service is analyzed.

Three scenarios are investigated, as presented in figure 3. Scenario one (S_1) assumes an event which is likely but have small effect – this could for example be a port scan that reduces availability to a small extent. The objective risk values represent that the possible risk often occurs (95 % likelihood), but do not do any harm. The decision maker has the feeling that such risks are overreflected. He has a loving risk attitude in concern of such small risks. S/he calculates the modified values by assuming that the probability is lower than the analysis has shown. The

risk attitude function for that specific risk returns that 0.25 has to be subtracted from the objective value. Note that now this attitude can be used for equivalent assets without any recalculation.

The next scenario assumes an average risk – for example when a database integrity becomes uncertain and an investigation becomes necessary. Here the decision maker is satisfied with the analyzed values and acts risk neutral. S/he therefore does not modify the values.

In the last scenario the decision maker faces a situation where s/he is really afraid of – the compromission of costumer data which would reduce the trust to the service and probably interrupt the eCommerce activities. The decision maker assumes that this event could destroy the company's operations and needs therefore special consideration. The risk averse attitude here leads to an increase of the likelihood and the effect. Note that from an attitude viewpoint an effect (or equivalent likelihood) of 1 is allowed.

Table 3 Scenarios for a modified mean value approach

Scenario	p	e	$Risk$	p_m	e_m	$Risk_m$
S_1	0.95	0.10	0.095	0.70	0.10	0.07
S_2	0.50	0.18	0.090	0.50	0.18	0.09
S_3	0.05	0.95	0.045	0.20	1.00	0.20

After calculating the risks, the decision maker sees an order that suggests that he/she should react first on 3, then on 2 and finally on 1. Compared with the pure mean value approach the order has completely changed due to the attitude of the decision maker.

5. CONCLUSION

Making risk decisions in a way that other people can understand and reconstruct is a difficult task. The proposed method is supposed to enable the inputs for making such decisions based on a formal calculation. The modified mean value approach assumes that a decision maker has his/her preferences and experiences, and knows how to deal with risks. This knowledge is formulated and represented in the risk attitude function.

Due to the simplicity of the method, it is reasonable to expect a fast performance of this method. This simplicity also solves a common problem in security risk management - the lack of a broad data base. The method can work even with very vague information and still deliver sufficient results. These facts are supported by practical experiences

gained by the author during usage of the method in an large Austrian bank, where the method was used to guide the security management activities for the internet banking system.

As one of the most difficult parts of the proposed method we can consider the determination of the risk attitude. However, the risk attitude can be analyzed formally – as proposed with a lottery/certain payment situation – or simply guessed and conducted by feelings (as practitioners often do).

It might bet criticized that a decision maker – especially if s/he is the proposed senior manager – will not have time to take part in the risk assessment. This problem can be solved by delegating the preparation and decision of minor risks to subalterns providing them a risk attitude function (or risk attitude guidelines).

To take use of the method in a more intuitive way, as further research, the development of effect/damage examples can be proposed. Those damage examples should describe a scenario in detail and express why a risk generates a certain potential to destroy an asset. The result could then be used to map it to actual situations which are comparable to the model case.

After all this approach is considered to meet the, in the introduction described, quality criteria of speed, understandability and business orientation.

Acknowledgments

Part of this work has been funded by the HumanIT research programm at Karlstad University. We therefore want to thank HumanIT for their support. We also want to thank Prof. Simone Fischer-Hübner and Stefan Lindskog for there helpful comments and Linda Martinson for here support.

Notes

1. Note that this includes the organizational decision making process or an individual decision.

2. Rational behavior is the maximation of self interest. (GAB, 1997)

3. The mean value approach assumes that the possible situations are known – so does the method, presented in this paper.

4. The Standard deviation is represented by: $\sigma_i^2 = \sum_{k=1}^{n} p_k(e_{ik} - \mu_i)^2$

5. Note that here the potential savings of countermeasures are not taken into account. This is done because it seems questionable if it is possible to assign a value without knowing which countermeasures that are going to be used. The proposal of countermeasures is namely the result of the risk analysis process.

6. Imaginable methods are statistical time line analysis, simulation or expert guesses.

7. Not assumed any performance loss, disk space requirement due to log file size or what so ever.

References

(1975). *FIPS 65, Guidelines for Automatic Data Processing Risk Analysis, withdrawn Aug. 1995.* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology.

(1996). *CCTA Risk Analysis and Management Method*. Central Computer and Telecommunication Agency, United Kingdom, user manual edition.

(1997). Gabler Wirtschaftslexikon. CD-ROM edition.

Dockner, E., Vetschera, R., and Gaunersdorfer, A. (1999). Skriptum Betriebswirtschaftliche Entscheidungen. Universitt Wien.

Eatwell, J., Milgate, M., and Newman, P., editors (1987). *The New Palgrave: A Dictionary of Economics*, volume 3. The Macmillan Press Limited.

French, S. (1993). *Decision Theory - An Introduction to the Mathematics of Rationality*. Ellis Horwood Limited.

Gerber, M. and von Solms, R. (2000). From risk analysis to security requirments. *Computer & Security*, 20(7):577 – 584.

Gordon, G. (1983). *Quantitative Decision Making for Business*. Prentice-Hall Inc.

Moses, R. H. (1992). *Risk Analysis and Management*, volume Computer secuirty reference book, chapter 21, pages 227 – 263. Butterworth Heinemann.