How to Estimate a Technical VaR Using Conditional Probability, Attack Trees and a Crime Function

Wolfgang Boehmer

How to estimate a technical VaR using conditional probability, attack trees and a crime function

Wolfgang Boehmer

Technische Universität Darmstadt, Morneweg Str. 30,
CASED building, D-64293 Darmstadt, Germany
wboehmer@cdc.informatik.tu-darmstadt.de

Abstract. According to the Basel II Accord for banks and Solvency II for the insurance industry, not only should the market and financial risks for the institutions be determined, so should the operational risks (opRisk). In recent decades, Value at Risk (VaR) has prevailed for market and financial risks as a basis for assessing the present risks. Occasionally, there are suggestions as to how the VaR is to be determined in the field of operational risk. However, existing proposals can only be applied to an IT infrastructure to a certain extent, or to parts of them e.g. such as VoIP telephony. In this article, a proposal is discussed to calculate a technical Value at Risk (t-VaR). This proposal is based on risk scenario technology and uses the conditional probability of the Bayes theorem. To determine the threats, attack trees and threat actors are used. The vulnerabilities have been determined empirically for an insurance company in 2012. The attack trees are weighted by a function that is called the criminal energy. To verify this approach the t-VaR was calculated for VoIP telephony for an insurance company. It turns out that this method achieves good and sufficient results for the IT infrastructure as an effective method to meet the Solvency II's requirements.

Keywords: Conditional probability; Bayes theorem; attack trees; threat actor; crime function; risk scenario technology

1 Introduction

In the early days of protecting IT, i.e. in the early 90s, the focus was purely on technical security, because it was recognized that the IT is vulnerable. These often expensive safeguarding measures were not always bound by economic considerations and only a rudimentary relationship to the business processes was established. Therefore the Basel II Accord in 2004 represents a cornerstone, because it placed the operational risk (opRisk) equal to the market and financial risks. In the implementation of Basel II / Solvency II requirements for operational risks, it was recognized immediately that they should be treated differently than the market and financial risks. For while the market and financial risks can reference historical data, this is not possible for operational risk due to lack of data. Thus many projects have failed that tried to create a loss database in order to provide a database for operational risk. Additionally, for the operational risks, attempts have been made in several theoretical models to determine appropriate parameters for the VaR, which have never prevailed in practice. Consequently, the qualitative

and the quantitative risk procedures developed that still stand side by side today. The German Baseline Protection Manual, with his hazard analysis, can be considered a representative of the qualitative method and, to name a few examples for the quantitative method, there is the standard ISO 27005 or the standard ISO 31000. What the methods above have in common is that these do not calculate a VaR or similar parameter that is compatible with the parameters of the market and financial risks.

An important feature in the calculation of risk between the market and financial risks on the one hand and the operational risks on the other hand is the fact that the area of operational risk, the IT infrastructures are dominated by threats and existing vulnerabilities. Thus in the market and financial risks, the widespread approach of a Monte Carlo simulation to determine the probability distribution leads to unsatisfactory results when used for operational risks.

In general, the risk analysis is the consideration of two distributions. The first distribution describes the occurrence probability of risk events, and the second distribution represents the impact or outcome (consequence) of the risk event, if the risk is faced. Then the two distributions are convolved. This convolved distribution is a new distribution, the distribution of risk. If, for example, a 5% quantile (α - quantile as a confidence level) of this risk distribution is defined as the expected loss, the VaR is determined. But the question remains, how realistic input distributions are found. Furthermore, the type of the input distribution determines a specific part of the operational risk. The Basel II framework includes the operational risk (opRisk) and defines *opRisk as the risk of losses resulting from inadequate or failed internal processes, people and systems, or external events*. In this definition, legal risk is included. Strategic and reputational risks are excluded. Without entering into details, the main difference with market and credit risk is that, for opRisk, we only have losses, as P. Embrecht et al. argued in his paper [1].

The contribution of this paper is the development of a VaR for the system, or in detail, for the technical infrastructure, the t-VaR, that considers the characteristics of an IT infrastructure and is part of the opRisk, but is placed on a par with the VaR for the market and financial risks.

The rest of the article is organized as follows. In the next section, the underlying model is discussed. In section III, the data collection for the identification of vulnerabilities, threats, and the application of the model to calculate the t-VaR is discussed using the VoIP telephony of an insurance company. In section IV, the relevant literature is discussed. The article concludes with a brief summary, continuing considerations and proposals for further studies.

2 The Model

2.1 Basic equations

Starting from the general linear relationship between the risk ($\mathcal{R}$), the probability (Pr) and the monetary outcome (impact) (I), as expressed in the equation 2.1,

$$\mathcal{R} = Pr \times I \ \ [\mathbb{R}], \tag{2.1}$$

which is not used in this paper. We use instead 2.1 the loss distribution approach and the Lower Partial Moment, *cf.* Fig. 2, as expressed for a system Ψ in equation 2.2. Because

only the negative result for a system is considered, the Loss $[\mathbb{R}^-]$, as is typical in the area of operational risk (see [1]).

$$\mathcal{R} = \left(Pr_E \times L \right) [\mathbb{R}^-] \ \mapsto \Psi \tag{2.2}$$

In equation 2.2 for the probability (Pr) of an event (E) the most frequent probability is not used, the conditional probability (Pr_E) in accordance with Bayes' Theorem is.

According to the Bayesian statistics, a hypothesis is created that says here, that a vulnerability only can be exploited on the condition (|) if a threat exist with a matching threat agent. Or vice versa, that a threat with a threat agent can develop only if a corresponding vulnerability exists. The threat is indicated by (Thr) and the vulnerability by (Vul). Thus the equation 2.2 can be transformed into the equation 2.3.

$$\mathcal{R} = \left(Pr_E \left(Vul \,|\, Thr \right) \times L \right) [\mathbb{R}^-] \ \mapsto \Psi \tag{2.3}$$

Thus, the conditional probability that an existing vulnerability is exploited by a threat with a matching threat agent is described in equation 2.4

$$Pr_E(Vul \,|\, Thr) = \frac{Pr_E \left(Thr \cap Vul \right)}{Pr_E \left(Thr \right)}. \tag{2.4}$$

Hence the numerator describes in the equation 2.4 the intersection between the set of threats and set of vulnerabilities in the plane of the probability Pr_E (*cf.* Fig. 1). In this context, the vulnerability, the following definition is used.

Definition 2.1.01 *(Vulnerabilities) are real (existing) and represent a weakness of an asset or represent a point at which the asset (component, system, process, employee) is technically or organizationally vulnerable. Vulnerability is a property of an asset and the security services of assets can be changed, circumvented or deceived (*cf. *ISO 27000:2012, p. 11).*

Definition 2.1.02 *(Threats) are not real (hypothetically) and aim at an asset (system or component) to exploit one or more weaknesses or vulnerabilities to a loss of data integrity, liability, confidentiality or availability. Threats can interact with an asset actively or passively (*cf. *ISO 27000:2012, p. 10).*

The Figure 1 shows the conditional probability on a two dimensional level and the set of threats and vulnerabilities as well as their intersection. If now the equation (2.4) is used in the Def 2.2, the following equation (2.5) results for the system Ψ. Equation (2.5) states that the risk ($\mathcal{R}$) to face a loss (L $[\mathbb{R}^-]$) depends of the event (E), and a conditional probability (Pr) for the occurrence of the intersection of vulnerability (Vul) and threat (Thr) for the system Ψ.

$$\mathcal{R} = \left(\frac{Pr_E \left(Thr \cap Vul \right)}{Pr_E \left(Thr \right)} \right) \times L \, [\mathbb{R}^-] \ \mapsto \Psi. \tag{2.5}$$

From equation (2.5) individual risk scenarios $\mathcal{R} = \{R_{sz1}, ..., R_{szn}\}$ the Loss ($L = \{l_1, ..., l_n\}$) can be developed for different systems $\Psi = \{\psi_1, ..., \psi_n\}$, such as shown by the

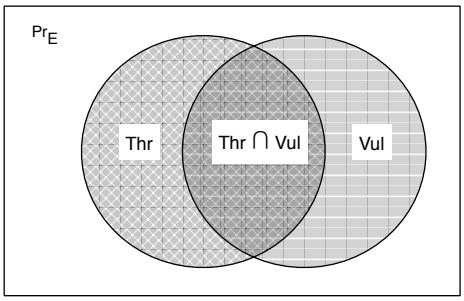

Fig. 1: Section and intersection of the set of threats and the set of vulnerabilities

following equations (2.6) to (2.9).

$$R_{sz1} = PrE_{p1}(Vul_1 \,|\, Thr_1) \cdot l_1 \mapsto \psi_1 \tag{2.6}$$
$$R_{sz2} = PrE_{p2}(Vul_2 \,|\, Thr_1) \cdot l_2 \mapsto \psi_2 \tag{2.7}$$
$$R_{sz3} = PrE_{p3}(Vul_2 \,|\, Thr_2) \cdot l_3 \mapsto \psi_2 \tag{2.8}$$
$$\vdots$$
$$R_{szn} = PrE_{pn}(Vul_j \,|\, Thr_k) \cdot l_n \mapsto \psi_n \tag{2.9}$$

Summing up risk scenarios $R_{sz1}, ..., R_{szn}$ for an infinitely long period of time gives the maximum possible loss, such as the equation (2.10) expresses. For shorter periods e.g. for a fiscal year (T) a summation does not make sense; the risks must be aggregated as discussed in section (V).

$$\sum_{i=1}^{n} R_{sz_i} = PrE_{pi}\left(\sum_{Vul_{k=1}}^{n} \,|\, \sum_{Thr_{j=1}}^{n}\right) \cdot l_i \tag{2.10}$$

While vulnerabilities are real, threats are hypothetical. To obtain a quantitative assessment of the risk situation of a company, it is necessary to analyze the threats more accurately, because not every threat has an immediate and direct effect. It also assumes that behind every active threat, an actor must be present. Historically, the concept of the threat tree was first discussed in 1991 by J.D. Weis [2]. This concept is based on the theory of fault trees (Fault Tree Analysis, Event Tree Analysis FTA and ETA).

With risk (Eq. 2.3) as a measure, it is associated as a universal measure of a probability space and is strongly related to the Loss Distribution Approach (LDA). The Loss Distribution Approach has been widely used in the financial and insurance industry for several decades and is as used for share portfolios. Thus it is natural to use this loss approach in the area of operational risk, but not for an equity portfolio, but for the value chain (production). In the literature, the topic is widely studied; significant work in this area has been performed by P. Embrecht et al. [1], M. Leipold and P. Vanini [3] and K. Böcker and C. Klüppelberg [4].

2.2 LDA Approach

The Loss Distribution Approach (LDA) refers to the bottom (marked in gray) part of Figure 2, which is the lower partial moment (LPM). For risk analysis, this means that two distributions are determined for a time period (T). First is the distribution of losses (Loss (T), *cf.* 2.2) and second is the probability distribution of events (Pr_E(T), *cf.* 2.2) which were mathematically composited in the grey dashed line in Figure 2 and is a joint distribution of risk according to the equations (2.6) to (2.9). The joint distribution is interpreted, which lead more often to minor losses and rarely major losses. This distribution is required to determine the VaR and the confidence level.

In the article by K. Böcker and C. Klüppelberg [4], a general summary of the standard LDA approach is given on page 6/7, which we follow here roughly.

1. The severities process $(l_k)_{k \in N}$ are positive independent and identically distributed (iid) random variables describing the magnitude of each loss event.
2. The number $N(x)$ of loss events (l_i) in the time interval $[t_1, t_2]$ for $t_2 \geq t_1$ is random (see Fig. 2). The resulting counting process $(N(x)_{t_2 \geq t_1})$, is generated by a sequence of points $(x_n)_{t\, n \geq 1}$ of non-negativ random variables, and
3. The severity process and the frequency process are assumed to be independent.
4. The aggregate loss process:
   The aggregate loss $L(x)$ up to time T constitutes a process

$$L(T) = \sum_{i=1}^{N(x)} l_i, \quad x \geq 0 \tag{2.11}$$

2.3 Value at Risk

Illustrated in the equation 2.2, the risk represents the Lower Partial Moment (LPM), which as a downside risk measure only refers to a part of the total probability density (see Fig. 2). This covers only the negative deviations from a target size (e.g. a plan value of the reachability of the insurance company for their customers in a time interval) and evaluates all of the information of the probability distribution (up to the theoretically possible maximum outage). The random variable in the example in Figure 2 presents the reachability of the insurance company for their costumers in the unit of time. The reachability varies only in a small range $1 - \alpha$ for the planned insurance service and is shown as a random variable (X) for the period t_1, t_2. Figure 2 shows the normal distribution of the exogenous density function that results from the random variable (X). For this discrete random variable (X), the values $x_i, i =, 1, 2, 3$ and $x_i \neq x_j$ for $i \neq j$. The expected value (E_w^T) is defined for the discrete random variable (X) as the sum of their possible values, weighted by the respective probability. In the example of Figure 2, for the time period $t_1 \leq T \leq t_2$, this is represented by probability $1 \rightarrow \infty$ with

$$E_w^T = \sum_{i=1}^{\infty} x_i \cdot Pr\,(X - x_i). \tag{2.12}$$

For the random variable (X) as a placeholder, we can use the three protection goals of information security. These are defined e.g. in the standard ISO/IEC 27001:2005 as confidentiality (C), integrity (I), availability (A) [5]. Often referred to as the CIA Triad.

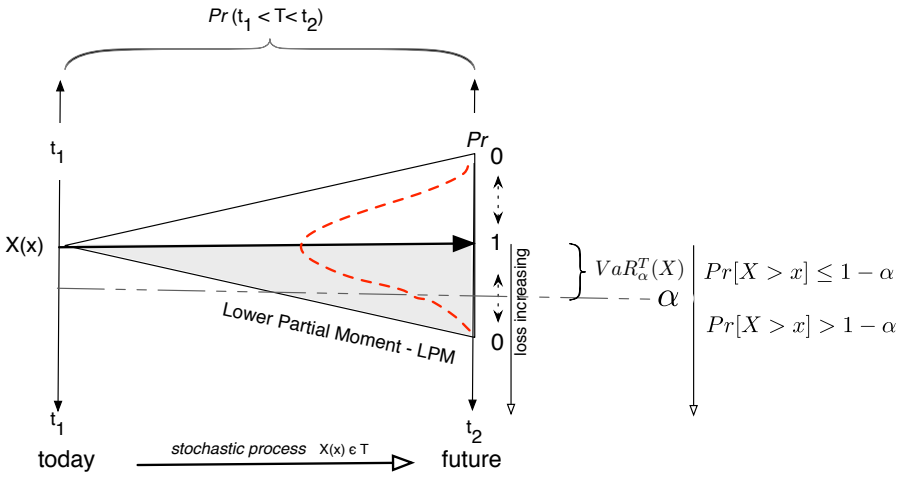

Fig. 2: Expected value of random variable (X), opVaR and opES

The statistical spread (σ) is the expectation of (E_w) expressed in the discrete case with the variance (Var), as shown in equation 2.13

$$Var(X) = \sigma_X^2 = \sum_{i=1}^{\infty} (x_i - E_w(X))^2 \cdot Pr\,(X = x_i). \tag{2.13}$$

The variance (Var) represents the average of the squared deviations from the mean of the random variable (X). The standard deviation is defined as the square root of the variance. The Discrete result values in the time interval T have been approximated by a normal distribution, so that in the Figure 2, the continuous course of the random variable is shown with density $f(x)$, so the expected value is obtained in this case E_w^T, as shown in equation 2.14

$$E_w^T = \int_{-\infty}^{+\infty} x \cdot f(x)\, dx. \tag{2.14}$$

In Fig. 2, the $opVaR_\alpha^T(X)$ and the $opES_\alpha^T(X)$ have been illustrated. This is where a VaR is a α-quantile. The α-quantile q_α of a distribution function $F(x)$ is the value of the $\alpha\%$ below the mass of the probability mass that separates the upper $1 - \alpha\%$ from the probability mass. The random variable (X) with probability α then takes on a value less than or equal to q_α.

The formal definition of the α-quantile is shown as in infimum function in equation 2.15 with

$$q_\alpha = F^{-1}(\alpha). \tag{2.15}$$

F^{-1} it is the inverse function of the distribution function.

The *Value at Risk, VaR* is thus the α-quantile of a loss distribution. If a random variable (X)is given, the *OpVaR* for a time interval T is shown in the following equation 2.16

$$opVaR_{\alpha}^{T}(X) = inf\{x \in \mathbb{R} \mid P[X > x] \leq 1 - \alpha\}. \tag{2.16}$$

$opVaR_{\alpha}^{T}(X)$ expresses that the smallest loss (for the example it would be the availability of the VoIP telephony of the insurance company) that corresponds to a lower limit and exceeds the loss with a probability of $(1 - \alpha)$. Hence the crucial probability for the calculation of $(opVaR_{\alpha}^{T}(X))$ is determined by the α confidence level. To hold the energy production in the range of $opVaR_{\alpha}^{T}(X)$ for the open system of the value chain, a control circuit based ISMS is used to react accordingly to the disturbances with respect to the protection goals.

2.4 Expected shortfall

The Expected Shortfall (ES), often referred to as the *Conditional VaR*, ($CVaR$), as a coherent risk measure, was already addressed in 1997 by Artzner et al. [6]. The ES is defined as the expected loss in the event that the VaR is actually exceded. Thus, this is the probability-weighted average of all losses that are higher than the VaR. For Figure 2, the OpES for the random variable (X) with probability α for a time interval T is given in the equation 2.17.

$$opES_{\alpha}^{T}(X) = E_{w}^{T}[X \mid X \geq opVaR_{\alpha}^{T}(X)] \tag{2.17}$$

The expected value E_{w}^{T} for the time period T shown in Equation 2.17 corresponds to a conditional expectation of the random variable (X), for the case that $X \geq opVaR_{\alpha}^{T}(X)$ occurs. A risk scenario is understood under the conditional expectation of the random variable (X). For the very rare deviations of the extreme values of E_{w}^{T} a control circuit based Business Continuity Management System (BCMS) is used.

A major difference between the analysis of financial and market risks and operational risks, is that there are, firstly, no goals and no security protection concepts concerning the protection goals exist in the field of finance and mark risks, and secondly, there are no management systems that can respond to exogenous disturbances. Only the approach of H. Markowitz [7] in 1959 suggesting a risk diversification of a portfolio could, therefore, be considered as a measure to protect the invested capital (availability of capital), but for operational risks it would only be helpful in rare situations.

In the previous sections, the VaR and the OpVaR have been discussed along with application scenarios. The argument here, however, is that these considerations of VaR and the OpVaR could be transferred to information technology and information processing, but not easily, if at all.

One of the main differences is that the information technology of a company is exposed to, among other technical damage, passive and active threats, vulnerabilities and attacks. The literature in the field of OpVaR has barely considered these facts at all. Against this background, a technical VaR is proposed (t-VaR), which addresses the concerns of information technology and information processing as well as the demonstrated passive and active threats, vulnerabilities and attacks. This is based on the definition of risk, according to equation (2.2).

2.5 Attack trees and threat agent

Equation (2.5) illustrated the Baysian view of a risk situation for a system Ψ. Exogenous knowledge is required for the intersection of vulnerability (Vul) and threat (Thr) for the Bayesian statistics. This required exogenous knowledge is filled with the attack trees, attack actors and a crime function. With this exogenous knowledge makes it possible to estimate the conditional probability of the intersection, as we will show in this section.

The idea of the attack trees goes back to the article by Weis in 1991 [2]. In this article he describes *threat logical trees*. Generally, attacks are modelled with graphical, mathematical, decision trees. A few years later, the idea of the threat trees was taken up by B. Schneier, among others, and developed [8]. This work by B. Schneier led to extensive additions and improvements to this technology, such as that published by A.P. Moore et al. [9]. Several tools have been developed and published; representative here of the work is [10, 11]; the authors provide an overview of the techniques and tools. The contribution of S. Mauw and M. Oostdijk [12] in 2005 formalize the concepts informally introduced by Schneier [8]. This formalization clarifies which manipulations of attack trees are allowed under which conditions. The commonality of attack trees and game theory has been elaborated on in 2010 by Kordy et al. [13]. Thus, a similar approach for the threat scenarios and threat agent are performed using the game theory.

In this work, we expand the idea of T. R. Ingoldsby [11] with conditional probability and the t-VaR. Threat trees generally have a root or target. Different branches (nodes) can lead to this target that are to be regarded as parts of goals and each start of a leaf. Each leaf is initiated by an attacker with different motives. The leaves and branches are weighted and equipped with an actor [12]. The weighting corresponds to the criminal energy (Criminal power, Cp), and contain three functions. The assessment of these three functions reflect the exogenous knowledge which is required in the Bayesian statistics (see equation (2.4)).

Already in 1985, A. Mosleh et al. pointed out the two main distributions for a risk analysis on the Bayesian statistic [14]. On the one hand, it is the probability distribution of the event occurring. Since these are rare events, the Poisson distribution is proposed here, which is later used by many other authors. The one-parameter Poisson distribution does a good job of providing the assessment, that small deviations occur more frequently than larger deviations, such as is expressed in Figure 2 with the lower partial moment (LPM). The challenge now is to get a good estimation of the parameters of the distribution. This assessment is made in this paper on the threats and attack trees in combination with the function of the criminal energy.

On the other hand, in the article by A. Mosleh et al. [14], the loss distribution is approximated by the log normal distribution. This distribution also corresponded to the idea that small losses occur more frequently than large losses for a long time. This idea has been revised by the Black Swan Theory [15] (extreme value theory) and is now often replaced by a Generalized Pareto Distribution (GPD).

Often, the loss distribution is easier to determine than the frequency distribution, if the loss is related to the value chain.

The function of the criminal energy (Cp), which in turn is composed of three additive functions, represents the expert knowledge for the Bayesian risk analysis (see equation (2.6 - 2.9)). The criminal energy is represented by the cost function (cost of attack

cf. Fig. 3), the technical feasibility function (technical function, *cf.* 4) and the noticeability function, *cf.* Fig. 5. The three functions are mentioned by T. R. Ingoldsby [11] and have to be adjusted to the relevant inspection. The following Figures 3 - 5 describe the exogenous knowledge that focuses on the objective of VoIP telephony. This exogenous knowledge is important for the Bayesian approach.

Fig. 3 states that a threat agent (actor) for an attack on the VoIP telephony of the insurance company is willing to spend money on tools. This willingness varies between 0 - 1 (axis of ordinates) and decreases with increasing costs (axis of abscissae). This can be explained simply because on the internet there are a number of free tools that are all well-suited to threaten a VoIP telephony.

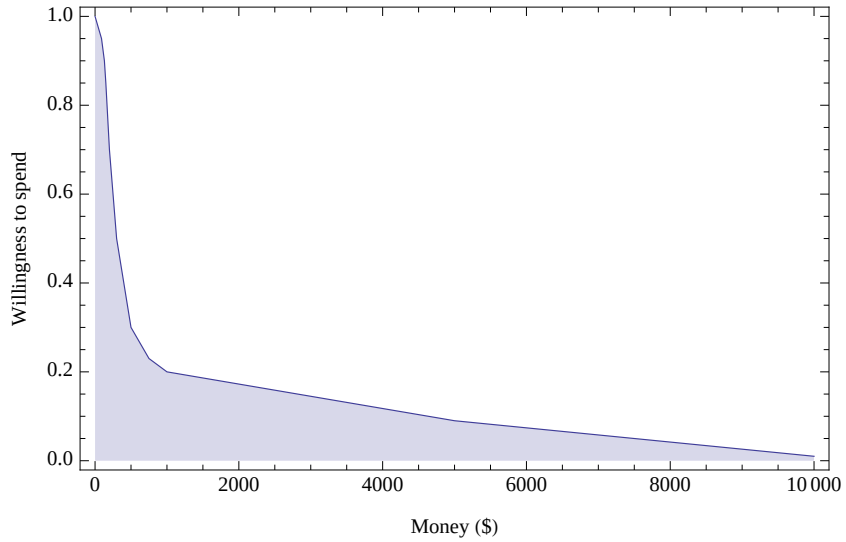

Fig. 3: Cost function

Figure 4 indicates how the tools are used and the technical possibilities that exist. It is a statement about the complexity of the tools and the willingness to make use of this complexity. The curve indicates that the greater the technical possibilities and the complexity of the tools, the more the willingness drops. I.e. it simple tools are preferred with simple operation.

Figure 5 shows the noticeability function expressing how an actor wants to disguise his attack, so that he could not be discovered. From of these three functions, the threat of an attack is determined more precisely. This is called the criminal energy. These functions must be adapted to each situation and reflect the exogenous knowledge again, which is necessary for the conditional probability.

As an example, we can estimate the technical ability rating of 5 (out of 10), and expose the miscreant at a 0.3 noticeability.

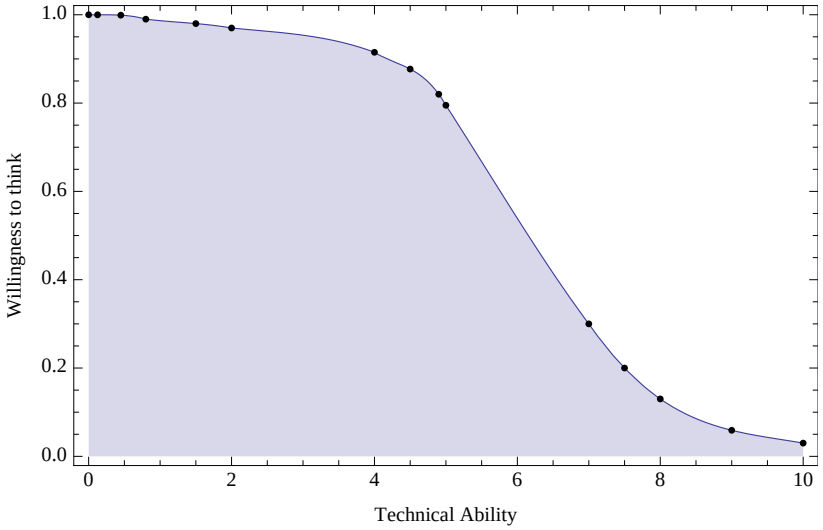

Fig. 4: Technical function

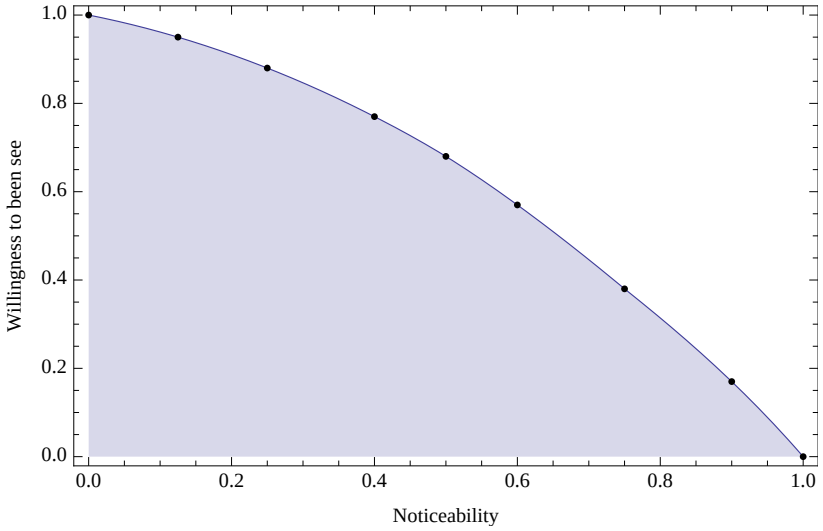

Fig. 5: Noticeability function

Using the utility functions shown, we discover that

$$f_{cost}\,(25) = 0.9 \tag{2.18}$$

$$f_{tech\,ability}\,(05) = 0.9 \tag{2.19}$$

$$f_{noticeabiity}\,(0.3) = 0.85 \tag{2.20}$$

and therefore the criminal energy with

$$CE = f_{cost} \cdot f_{tech\,ability} \cdot f_{noticeabiity} \tag{2.21}$$

$$CE = 0.6885 = 0.9 \cdot 0.9 \cdot 0.85 \tag{2.22}$$

With this function of the criminal energy, we could estimate the threat profile in conjunction with a specific threat agent (actor). The three functions of Figures 3 - 5 do not explain anything about the motivation and benefit of the threat agent, but the threat agent's motivation is correlated to attack benefits. These must also be taken into account in order to understand how desirable an attack appears to an adversary. The discussion of the motivation and benefits of a threat agent is not really covered in this article, due to lack of space. But, typically the largest benefit of the threat agent is associated with achieving the tree's root node, or with side benefits occurring at the various intermediate nodes. Different threat scenarios run through different paths among leaf nodes and root node (cfg Fig. 7). The threat agent's benefits may differ considerably depending on the threat scenario used. We will discuss different threat scenarios and different paths between leaf nodes and root in the next section.

3 Data acquisition

According to the model (cfg section 2), data acquisition regarding vulnerabilities is handled in this section and matched to the attack-tree with the associated threat agent (actor) and analyzed to develop risk scenarios according to the equations 2.6 to 2.9. Here, ψ represents the VoIP telephony. Other systems are not investigated and consequently $\Psi = \psi$. This means that in this real-world case study, all the vulnerabilities, threats and risk scenarios relate to ψ = VoIP telephony of the insurance company.

Figure 6 is a rough sketch of the VoIP telephony of the insurance company. There are two locations indicated with A and B. The two locations (A, B) are connected to a non-public network (MPLS cloud) and the switch at the location A and B are both used for data traffic as well as for voice traffic. This means that two locations are not connected to the internet. The MPLS cloud is maintained by a service provider which supplies the insurance company in addition to other customers in its MPLS cloud. The customers (the insured) of the insurance company choose from outside the softphone to get in touch with the employees. In addition to uptime (availability), the confidentiality of the conversations is a security objective for the insurance company.

3.1 Vulnerability analysis

The empirical study in 2012 for the insurance company had to analyze the current target vulnerabilities within the scope of VoIP telephony. These weaknesses are discussed as an example in this section to show the procedure of the model. This analysis was carried out in two steps. In the first step, the VoIP module (B 4.7) of the baseline protection manual from the BSI was used [16, 17]. The technical department was interviewed. In the second step, a white box penetration testing was conducted to verify the statements and to find other vulnerabilities. It is worth mentioning that there is no connection between the VoIP telephony and the Internet.

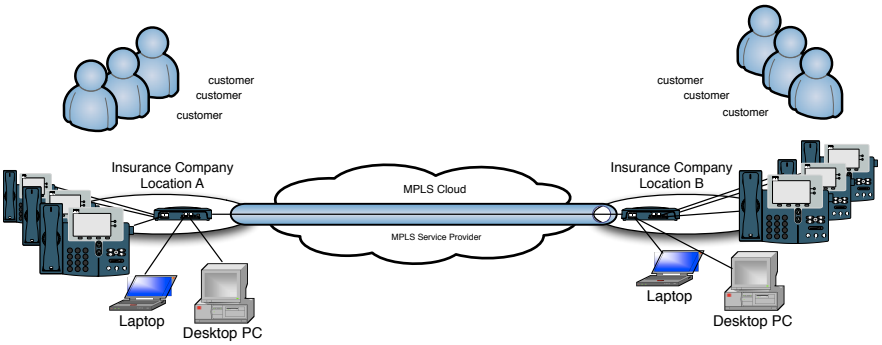

Fig. 6: VoIP Architecture

In our investigation in 2012 it was recognized, inter alia, that the voice data (RTP stream) transmitted without encryption and the ports at the Softphones and patch socket in the premises were not secured against unauthorized use (IEEE 802.1x, Port Based Network Control PBNC). Furthermore, we identified that there was no firewall between the MPLS network and the LAN of the insurance company and also the voice data was transmitted unecrypted in the MPLS network.

Based on these findings, the following threat analysis was performed.

3.2 Threat analysis

The threat analysis is based on the identified vulnerabilities and contains three elements: the threat scenarios, the matching threat agent and the function of the criminal energy.

In our threat analysis, we show as an example, how the protection target – in this case, the confidentiality of VoIP Telephony – is given in the current threat situation for the insurance company. Confidentiality for VoIP telephony means that the phone calls between the employees of the insurance company and its insured cannot be intercepted. Similarly, the phone calls between sites A and B will be kept confidential, because the interception could have negative implications for the insurance company.

Figure 7 shows the potential threat paths for the insurance company from the leaf to the root. Between the paths are either "or" or "and" connections. The "and" connection means that the two paths connected with the "and" must be met in order to reach the next sub-goal. Between the sub-goals the function of the criminal energy will change. The individual leaves represents the threat agent and the root represents the target of the attack (interception of voice traffic). The numbers represent the function of the criminal energy and therefore the exogenous knowledge. The index (I) = Impossible and (P) = Possible differentiates possible paths that are possible or not possible due to policies or structural circumstances. The equations 2.18 - 2.20 were determined for each threat attack and different threat agent with a specific crime function (*cf.* 2.21). Inserting a set of risk scenarios for the VoIP-Telephony in the given situation into the set of equations 2.6 - 2.9 created equations 3.1 - 3.4.

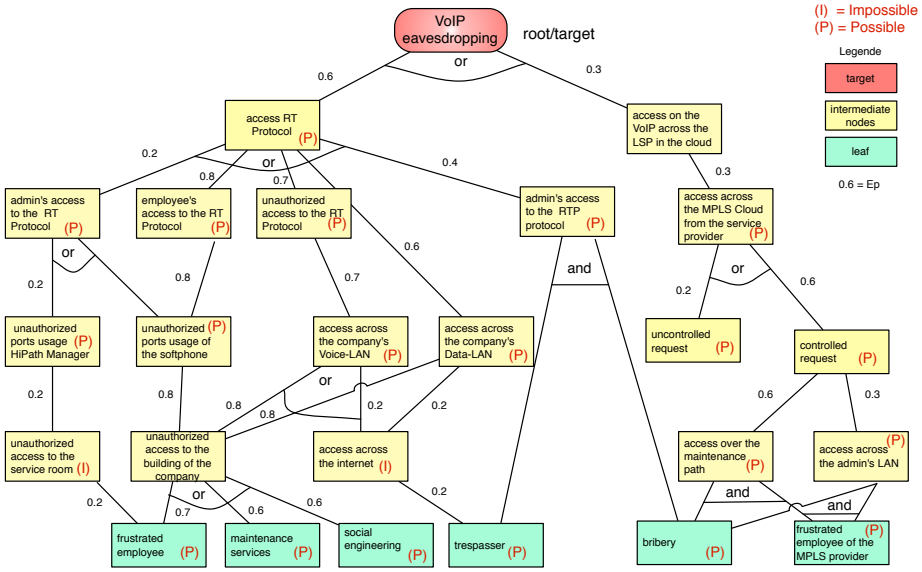

Fig. 7: Attack tree with the criminal energy

The actual risks of wiretapping the voice traffic in the real-world case study was estimated with risk scenarios (cfg equations 3.1 - 3.4) according to the Bayesian statistics, with the attack trees, the threat agent and the criminal function (CE). As a threat agent, an intruder from the inside the insurance company was postulated, because the unencrypted voice traffic is only in the LAN of the insurance company and is also transmitted unencrypted in the cloud provider's MPLS. However, no Internet connection exists for voice traffic to the insurance company and the MPLS cloud is also not connected to the Internet. Thus, as insiders only someone from the insurance company is eligible out of the environment (priviledged person) of the MPLS cloud providers.

The threat was assumed to be the interception (Thr_1) of sensitive voice data of the insurance company that could be performed by an internal perpetrator (threat agent). Likewise, the threat agent could also be represented by service personnel (Thr_2) or a trespasser (Thr_3). For each threat tree and threat agent a separate criminal function from Fig. 3, Fig. 4 and Fig. 5 is estimated with the equation 2.21. The leaves in Figure 7 represent the different threat agents. The behavior of insiders has already been addressed in a number of published articles, representative here is the article by I. J. Martinez-Moyano et al. [18]. ψ_1 denotes the VoIP infrastructure and refers to the vulnerability of the non-encrypted voice data with Vul_1.

The possible damage resulting for insurance company caused by insiders is the associated reputational damage if the intercepted voice data is given to the public. Given to the reputational damage for the voice data scenario, we made an assumption that 25 customers terminate their contract in the current year. The loss by termination is indicated with l_{25c}. The loss of 25 insurance contracts in a one-year period is also well

above the normal turnover rate between 8 - 11 ($l_{8c} - l_{11c}$) contracts per year (T) and hence higher than the expected value of E_w^T (cfg Eq. II.12).

We can use the equations 2.6 - 2.9 to express the risk scenarios $R_{sz1} - R_{szn}$ (3.1 - 3.4) with the potential loss of 25 contracts (l_{25c}) under consideration of Eq. 2.21 for the threat agents and the attack trees for our real-world case study of ψ = VoIP telephony of the insurance company:

$$R_{sz1} = PrE_{p1}(Vul_1 \,|\, Thr_1) \cdot l_{25c} \mapsto \text{VoIP-Telephony} \tag{3.1}$$

$$R_{sz2} = PrE_{p2}(Vul_1 \,|\, Thr_2) \cdot l_{25c} \mapsto \text{VoIP-Telephony} \tag{3.2}$$

$$R_{sz3} = PrE_{p3}(Vul_1 \,|\, Thr_3) \cdot l_{25c} \mapsto \text{VoIP-Telephony} \tag{3.3}$$

$$\vdots$$

$$R_{szn} = PrE_{pn}(Vul_n \,|\, Thr_n) \cdot l_{25c} \mapsto \text{VoIP-Telephony} \tag{3.4}$$

The probability $PrE_{p1} - PrE_{pn}$ is estimated as described above with the conditional probability of Eq. 2.4.

In addition to safeguarding the confidentiality and the risk scenarios as described with $R_{sz1} - R_{szn}$ (3.1 - 3.4), we also worked out the risk scenarios for the other two protection goals: the availability and integrity. Thus, for the protection of target availability and integrity, analogous threat trees were developed with appropriate threat agents and criminal functions in order to then determine the conditional probability and therefore the risk scenarios. Due to space limitations in this article, these analogous considerations will not be pursued further.

4 Results

In this section, we will discuss the results from the VoIP-Telephony investigation for our real-world case study.

The business success of a insurance company can be determined, inter alia, by the amount of insurance policies ($|C|$). The number of insurance policies ($c_i \in C$) fluctuates with 8 to 11 policy terminations. The target is expected to lose no more than 8 insurance policies per year, however, if the loss of 11 insurance policies occurs, this is also acceptable and the α value is achieved. Thus, the expected value of $E_w^T(C)$ for one year is 8 insurance policies and corresponds to the target value "1" in Figure 8. The period is one year (T).

The equation4.1 describes the negative variation around the target value of 1 ((l_{c8} = 8 lost contracts). The possible new customers per year are not considered in our real-world case study. For this reason, only the lower distribution (LPM) is considered. The scattering width is 3 contracts and partly achieves the loss of 11 contracts per year. The equation 4.1 now describes the influence of the technical infrastructure with the control objectives (Confidentiality, Integrity, Availability) to the cardinality of the set of contracts $|C|$.

$$\text{t-Var(C)} = \sigma_C^2 = \sum_{i=1}^{|C|} (c_i - E_w^T(C))^2 \cdot Pr\,(C = c_i). \tag{4.1}$$

This experience of the turnover is derived from observations from the last 10 years.

For the insurance company, availability for your customers is very important. If customers cannot express their concerns over the phone, they are angry and are ready to switch to another insurance company in the current year.

The loss of confidentiality creates reputational damage for the insurance company and a number of customers cancel. There is an internal investigation of the insurance company, which proves this fact. This is one of reasons why the risk analysis was performed. It has been shown that, due to the risk scenarios in our real-world case study, there is the possibility losing a lot more contracts than expected. Figure 9 shows the

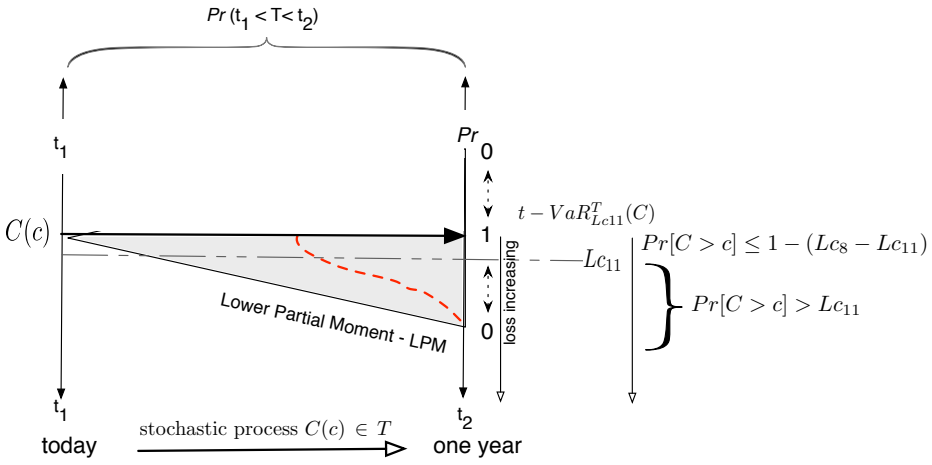

Fig. 8: Technical Value at Risk for the insured contracts

distribution of the LPM in a different presentation. This presentation is done very often for loss considerations instead of Figure 8. These are the discrete values of the risk scenarios that have been analyzed in our real-world case study. It can be shown that the expected loss of 8 to 11 insurance polices has been clearly exceeded. It is therefore an unexpected loss.

In conclusion, it can be said for our real-world case study that the insurance company has decided to take appropriate countermeasures in the field of encryption in the LAN and in the connection in the MPLS cloud. It was ensured that the cost of action does not exceed the potential unexpected losses.

5 Related work

The concept of risk and its various considerations is a discussion of the past few decades in the literature as shown in the article 1980 of S. Kaplan and J. Garrick [19]. Also, the authors distinguish between risk and hazard. While the risk (R) contains the three

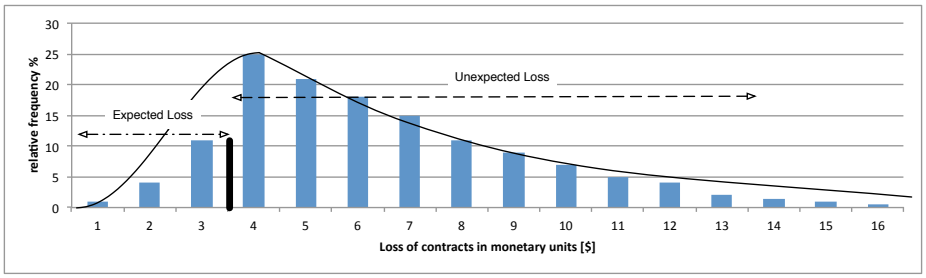

Fig. 9: Loss distribution for the contracts c_i due to breaches of confidentiality of the VoIP-Telephony

items, the set of scenarios (S), probability (p) and loss (x), in a linear combination $R = \{\langle S_i, p_i, x_i\rangle\}$, the concept of hazard (H) contains only two items, the set of scenarios (S) and the loss (x) in a linear combination $H = \{\langle S_i, x_i\rangle\}$. Furthermore, the authors [19] pointed out the difference between the probability according to the frequentist view of Laplace and the conditional probability of the Bayesian theory. For both of these views, there are a number of publications. Widespread is also the approach of Bayes. For this view, there are different ideas, to name a few: [14, 20–22].

Representative of many contributions to the provision of operational risk is the work of P. Embrecht et al. [1] or by K. Boecker and C. Klüppelberg [4]. The discussion about the coherent version of VaR was initiated by P. Atzner et al. [6]. In the area of operational risk, additional work should be mentioned that is related to this paper. Thus, the present paper follows broadly the doctoral thesis from 2010 of N. Poolsappasit [22] but expands on his idea, however, to the actor model and a weight function, which represents the criminal energy. Finally, it can be summarized that one unique way does not yet exist to satisfy answers to determine the operational risk.

6 Conclusion and further investigation

Over the past two decades the VaR and the coherent variant C-VaR have established themselves as a value for determining the risks associated with market and financial risks. According to BASEL II and/or Solvency II the operational risks should be determined in an appropriate manner. Once the standard approach to a loss database proved infeasible and unsuccessful, many institutes and industrial companies tried to follow BASEL II. However, the process of determining the VaR in the market and financial risks cannot be directly transferred to the technical infrastructure. In our view, the operational risk of the individual VaR must be assembled for systems, processes, people and external events. Therefore, in this article we present a method based on the Bayesian statistics, vulnerabilities, attack trees, an actor model and the function of criminal energy, that determines a technical VaR that is an appropriate response to the specific protection targets (confidentiality, integrity, availability) of an IT infrastructure. The real-world case study of VoIP telephony in an insurance company verified t-VaR for the

protection target of confidentiality. As a result, it can be shown that the t-VaR is an appropriate method to determine the VaR for the IT infrastructure under operational risks. Other considerations now aim to determine a t-VaR for other areas of the IT infrastructure, and then conduct a risk aggregation to determine the overall risk in the technical area.

References

[1] P. Embrechts, H. Furrer, and R. Kaufmann, Quantifying regulatory capital for operational risk, Derivatives Use, Trading and Regulation, vol. 9, pp. 217 – 233, 2003.

[2] J. D. Weis, A system security engineering process Proceedings of the 14th National. Computer Security Conference, 1991.

[3] M. Leippold and P. Vanini, The quantification of operational risk (november 2003).

[4] K. Böcker and C. Klüppelberg, Operational var: A closed-form approximation, December 2005.

[5] SC27, ISO/IEC 27001:2005, information technology - security techniques - information security management systems - requirements. Beuth-Verlag, Berlin, 10 2005.

[6] P. Artzner, F. Delbaen, J.-M. Eber, and D. Heath, Coherent measures of risk, Math. Finance, vol. 9, no. 3, pp. 203 – 228, 2001.

[7] H. M. Markowitz, Portfolio Selection: Efficient Diversification of Investment. Blackwell Publishers Ltd, Oxford, 1991, Originally published in 1959 by John Wiley & Sons, Inc., New York, 1991.

[8] B. Schneier, Attack trees, Dr. Dobb' s Journal, vol. 24, no. 12, pp. 21– 29, 1999.

[9] A. P. Moore, R. J. Ellison, and R. C. Linger, Attack modeling for information security and survivability, Technical Note CMU/SEI-2001- TN-001, Carnegie Mellon University, 2001.

[10] O. Sheyner and J. Wing, Tools for Generating and Anaylzing Attack Graphs, pp. 344 – 371. FMCO 2003, LNCS 3188, Springer-Verlag Berlin Heidelberg, 2004.

[11] T. R. Ingoldsby, Fundamentals of Capabilities-based Attack Tree Analysis. Amenaza Technologies Limited, 406 – 917 85th St SW, m/s 125.

[12] S. Mauw and M. Oostdijk, Foundations of attack trees, in International Conference on Information Security and Cryptology – ICISC 2005. LNCS 3935, pp. 186 – 198, Springer, 2005.

[13] B. Kordy, S. Mauw, M. Melissen, and P. Schweitzer, Attack-defense trees and two-player binary zero-sum extensive form games are equivalent, in Proceedings of the First international conference on Decision and game theory for security, GameSec'10, (Berlin, Heidelberg), pp. 245 – 256, Springer-Verlag, 2010.

[14] A. Mosleh, E. R. Hilton, and P. S. Browne, Bayesian probabilistic risk analysis, ACM SIGMETRICS – Performance Evaluation Review, vol. 13, June 1985.

[15] N. N. Taleb, The Black Swan. The Impact of the Highly Improbable. Random House Inc., 2008.

[16] Federal Office for Security in Information Technology, Baseline Protection Guide Germany. Bundesanzeiger, 2006.

[17] Federal Office for Security in Information Technology, IT Baseline Protection Handbook, Bundesanzeiger, Cologne, 2003 – 2005.

[18] I. J. Martinez-Moyano, E. Rich, S. Conrad, D. F. Andersen, and T. R. Stewart, A behavioral theory of insider-threat risks: A system dynamics approach, ACM Transactions on Modeling and Computer Simulation, vol. 18, April 2008.

[19] S. Kaplan and B. J. Garrick, On the quantitative definition of risk, Risk Analysis, vol. 1, July 1980.

[20] L. Dalla Valle and P. Giudici, A bayesian approach to estimate the marginal loss distributions in operational risk management, Comput. Stat. Data Anal., vol. 52, no. 6, pp. 3107 – 3127, 2008.

[21] C. Alexander, Bayesian methods for measuring operational risk, Discussion Papers in Finance, 2000.

[22] N. Poolsappasit, Towards an Efficient Vulnerability Analysis Methodology for better Security Risk Management. PhD thesis, Colorado State University, July 2010.