# Communicating the Economic Value of Security Investments; Value at Security Risk

Rolf Hulthén
rolf.hulthen@teliasonera.com, rolf.hulthen@telia.com

TeliaSonera AB
www.teliasonera.com

**Abstract** The information and data security communities and their individual practitioners have long experienced the pedagogical difficulties in communicating to management or funding bodies the importance and relevance of sufficient investments in information and data security. Inside these communities there is almost universal agreement that companies under invest in security.

One reason for this pedagogical failure is that the highly specialized security domain is difficult to penetrate for the average manager with a background in business administration or economics. Consequently, the entities and metrics used by the security community to evaluate security risks and their consequences usually tell very little to people involved in security investment decisions.

Historically, Return on Investment RoI has been used for this purpose. However, RoI is not an ideal entity to use, since it generates misunderstanding and misinterpretation. Companies and enterprises already have tools, methods and metrics to express risk levels and their economic consequences to support management in investment decision situations: we refer to Value-at-Risk and Value-at-Risk-type metrics.

This contribution transforms or transfers entities and metrics used by the information and data security communities into Value at Risk-type entities and metrics. This will allow management to understand, compare and evaluate security risks and their economic consequences with risks generated by other sources, strategies or investment decisions and give management a firmer and more rational basis for security investment decisions.

## *1 Introduction and Problem Situation*

There are several models aiming at answering the questions on how much to spend on security investments, and on the incentives to do so [1] – [3]. Usually the models aim at establishing a quantitative relation between investment level and the resulting vulnerability level.

The information and data security communities and their individual practitioners have long experienced the pedagogical difficulties in communicating to management or funding bodies the importance and relevance of sufficient investments in information and data security and inside these communities there is almost universal agreement that companies under invest in security. However, some rational economical support for such a strategy can be raised [3].

One reason for this pedagogical failure is that the highly specialized security domain is difficult to penetrate for the average manager with a background in business administration or economics. Consequently, the entities and metrics used by the information and data security communities to evaluate security risks and their consequences usually tell very little to people involved in security investment decisions.

Historically, Return on Investment RoI (sometimes named Return on Security Investment RoSI in our application) [1] has been used for this purpose. However, RoI is not an ideal entity to use, since it generates misunderstanding and misinterpretation: RoSI as applied is not a financial return on an investment that we can collect and register in accounting books [4], [5] but an *expected net prevented loss* due to security breaches per monetary unit invested.

Companies and enterprises already have tools, methods and metrics to express risk levels and their economic consequences to support management in investment decision situations: we refer to Value-

at-Risk (VaR) [6], [7] and Value-at-Risk-type metrics. We have already seen several such VaR-type metrics, e.g. Credit-, Cash Flow-, Revenue-, Profit-, and Market Value at Risk.

The purpose of this contribution is to add 'Value-at-Security Risk' (VaSR) to this collection by transforming or transferring the entities and metrics (such as Threat, Vulnerability, Security Risk, Breach Loss) already used by the information and data security communities into Value at Risk-type entities and metrics. This will allow management to understand, compare and evaluate security risks and their economic consequences with risks generated by other sources, strategies or investment decisions: companies may have corporate guidelines on allowed financial risk levels as a function of investment levels [14]. Credit rating agencies, such as Moody's [15] and Standard & Poor's [16], have very well defined demands on financial risk level, investment level, time span and equity capital for a company to qualify for a particular rating level.

Thus, our aim is to give to management a metric that will constitute a firmer and more rational basis for security investment decisions.

We reach the purpose in the following steps:

Section 2 introduces and lists entities to be used, and section 3 formulates our problem and defines the concept of Value-at-Risk. Section 4 gives a high-level analytic introduction to our model, whereas section 5 goes into analytic details and derives the key entity that solves our problem. Section 6 uses this entity to define and calculate the most important Value-at-Risk entities. Section 7, finally, gives some comments and conclusions.

Thus, this contribution establishes a connection between the length of an investment period, risk level and value at risk. An earlier contribution [3] established the connection between length of investment period, investment level, risk level and value to be security protected.

## *2 Background and Preliminaries*

We import from [2] and [3] the following mean value (or Expected Value in the sense of statistical theory) entities, namely

- *Threat* $T(t)$ is the number of (security) attacks per unit time at time t,
- *Vulnerability* $V(t)$ is the probability that an attack at time t will be successful,
- *Breach Loss* $\lambda(t)$ is the economic loss we make from a successful attack at time t,
- *Potential Loss per Unit Time* at time t is $T(t)\lambda(t)$; taken over an investment period $(t_j; t_{j+1})$ the *Potential Loss* is $PL(t_j; t_{j+1}) = \int_{tj}^{tj+1} T(\tau)\lambda(\tau)\, d\tau$.
- *Security Risk per Unit Time* at time t is $T(t)V(t)$; this is equal to the number of successful attacks per unit time at time t.

  Taken over an investment period $(t_j; t_{j+1})$ the *Security Risk* is $SR(t_j; t_{j+1}) = \int_{tj}^{tj+1} V(z_j; \tau)T(\tau)\, d\tau$.

  $z_j$ is the investment in monetary units that we make at investment time $t_j$ for the period $(t_j; t_{j+1})$. The resulting vulnerability is $V(z_j;t)$; it will increase during the course of time [3].

To reach our present purpose, we need to introduce the following stochastic variables:

- A is the number of (security) attacks per unit time at time t; discrete (and integer) A has power density function (pdf) $p_A(n;t) = Pr\{A = n; t\}$, i.e. the probability that A equals n at time t.

We want the expected value of A to be $E\{A\} = T(t)$ since we want to transform or transfer *Threat* $T(t)$ used by the security community into entities used by the financial risk community.

- S is the number of successful (security) attacks per unit time at time t; discrete (and integer) S has pdf $p_S(m;t) = Pr\{S = m; t\}$, i.e. the probability that S equals m at time t. We will later present a candidate model for authentic data for $p_S(m;t)$.

  With the expected value of S as $E\{S\}$, we observe that *Vulnerability* $V(t) = E\{S\}/E\{A\}$ and that $E\{S\} = T(t)V(t)$, i.e. *Security Risk per Unit Time* at time t.

- L is the economic loss we make from a successful attack at time t. Continuous L has pdf $f_L(\ell;t)$, i.e. the probability that L falls in an interval $(\ell;\ell+d\ell)$ at time t is equal to $f_L(\ell;t)d\ell$. We will later present a candidate model for authentic data for $f_L(\ell;t)$.

  We want the expected value of L to be $E\{L\} = \lambda(t)$, i.e. *Breach Loss* at time t in the terminology of the security community.

## *3 Problem Formulations; Value-at-Risk*

The core question answered by stating the Value-at-Risk is the following: *In a situation beyond our own immediate control and where value is at risk, what is the maximum loss value that, with a preset level of confidence, will not be surpassed within a defined time span?*

This value is the *Value-at-Risk.* Within Credit Risk Management, typical values can be 5 M$, 95 %, 24 hours. Depending on the application, these numbers can be quite different. We refer to [6] for an introduction to the subject.

In principle, there are two methods to arrive at the Value-at-Risk, a non-parametric- and a parametric method. The non-parametric method relies on historic data in the sense that we, from such data for the application under consideration, generate a histogram for loss within the defined time span. From this histogram we estimate VaR (and other entities of interest) at the preset confidence level. Provided we have sufficient historic data, this method is simple and quite straight forward. However, it does not generate as much insight into the underlying mechanisms to our risk situation as does the parametric method, which, on the other hand, critically depends on an accurate risk situation model and historic data to normalize our model parameters. The method also relies on the possibility to estimate the value of the resource that we want to protect, which can be very different, e.g. corporate IT infrastructure, competitive information and knowledge such as customer or product data, and brand value. We return to this issue in section **7 Comments and Conclusions; Present and Future Work.**

The parametric method derives a pdf for the loss within a defined time span. From this pdf we calculate VaR and other entities of interest. We will follow the parametric method line and state our own problem situation as follows:

*Find the pdf for the total loss $\mathcal{L}$, i.e. the value that, due to security breach attacks, is at risk during an investment period.*

This pdf will use entities already in use by the security community to calculate *Value-at-Security Risk, Expected Breach Loss, Unexpected Breach Loss,* and *Expected Tail Breach Loss;* this is done in section **6 Value-at-Security Risk Entities.**

## *4 Value-at-Security Risk Model; Assumptions*

Using the stochastic variables S and L introduced above and initially following, but generalizing and adapting to our present application, the approach in [6], chapter 19.3, we experience the individual losses $L_1, L_2, L_3,\ldots$ during a time unit at time t, so that the total loss per time unit at time t is

$$L_m = \sum_{i=1}^{m} L_i \ .$$

The generalisation we make is to introduce time dependent $\lambda(t)$ and $\nu(t)$; this is relevant since we know that Threat, Vulnerability and Breach Loss all vary with time [8].

Further, the probability that the total loss $\mathcal{L}(t)$ per time unit at time t is smaller than or equal to some value x is

$$\Pr\{\mathcal{L}(t) \le x\} = \sum_{m=0}^{\infty} \Pr\{L_m \le x \mid m\} \times p_S(m;t) =$$

$$= \sum_{m=0}^{\infty} \Pr\{(\sum_{i=1}^{m} L_i) \le x \mid m\} \times p_S(m;t). \qquad (1)$$

Here we have made the assumptions that the individual attacks, as well as their consequent breach losses, are independent. We are aware that this is not always the case and will comment on these assumptions in section **7 Comments and Conclusions**; **Present and Future Work.**

From this expression we may in principle obtain the pdf g(x) for the total loss $\mathcal{L}$ over the investment period $(t_j; t_{j+1})$ as

$$g(x) = \int_{tj}^{tj+1} [d\Pr\{\mathcal{L}(t) \le x\}/dx]\, dt \qquad (2)$$

From g(x) we may determine VaSR on the confidence level at our specification, and any additional statistical entity that we prefer under the conditions at hand, i.e. known, assumed or estimated behaviours of *Threat* T(t), *Vulnerability* V(t), and *Breach Loss* $\lambda(t)$.

We will next introduce and make concrete assumptions on these entities and develop g(x) into an operationally useful form.

## 5 Our Parametric Model

We make the assumption that the number of successful attacks per time unit at time t (i.e. the stochastic variable S) is Poisson-distributed; this is a well tested model of the number of arrival events [9]. Thus, we have

$$p_S(m;t) = (\nu(t)^m/m!) \times \exp(-\nu(t)) \ ; \ \ m \text{ integer} \ge 0 \text{ and } \nu > 0. \qquad (3A)$$

$$p_S(m;t) = 0 \ ; \ \ m \text{ integer} \ge 0 \text{ and } \nu = 0. \qquad (3B)$$

Here the event intensity $\nu(t) = E\{S\} = T(t)V(t)$, i.e. *Security Risk per Unit Time* at time t.

[6] uses a time-independent geometric distribution for the number of events per time unit, which we think is less in agreement with the actual behaviour in our application.

We next make the assumption that the economic loss L that we make from a successful attack at time t is exponential distributed with the expected value $E\{L\} = \lambda(t)$, i.e. *Breach Loss* at time t. Thus,

$$f_L(\ell; t) = \begin{cases} = (1/\lambda(t)) \times \exp(-\ell/\lambda(t)); \ \ \ell \ge 0 \text{ and } \lambda(t) > 0, \\ = 0 \ \ \text{elsewhere} \end{cases} \qquad (4)$$

[6] uses the same distribution but with time-independent parameter $\lambda$.

To proceed we need the pdf of $L_m = \sum_{i=1}^{m} L_i$ , where all $L_i$ have pdf Equ (4). It is well known [9] that the pdf for a sum of m independent expo($\lambda(t)$)-distributed stochastic variables is gamma-distributed $\Gamma(m;\lambda(t))$, i.e. $L_m$ has pdf

$$f_{Lm}(\ell; t) = \{\ell^{m-1}/[\lambda(t)^m \Gamma(m)]\} \times \exp[ - \ell/\lambda(t)] . \qquad (5)$$

$\Gamma(m)$ is the Gamma function; $\Gamma(m) = (m-1)!$ , m integer ≥ 1.

We now have

$$\Pr\{(\sum_{m=0}^{\infty} L_i) \le x \mid m\} = \int_0^x \{\ell^{m-1}/[\lambda(t)^m \Gamma(m)]\} \times \exp[ - \ell/\lambda(t)] \, d\ell + \Pr\{(\sum_{m=0}^{\infty} L_i) \le x \mid m=0\}$$

and, using Equ (3), rewrite Equ (1) to read

$$\Pr\{\mathcal{L}(t) \le x \} = \sum_{m=1}^{\infty} \{ \int_0^x \{\ell^{m-1}/[\lambda(t)^m \Gamma(m)]\} \times \exp[ -\ell/\lambda(t)] \, d\ell \, (\nu(t)^m/m!) \times \exp[ -\nu(t)] \} +$$
$$+ \exp( -\nu(t)) =$$

$$= \{ \int_0^x \exp( -\nu(t)) \times \exp[ - \ell/\lambda(t)] \, d\ell\} \times \{ \sum_{m=1}^{\infty} \{\ell^{m-1}/[\lambda(t)^m \Gamma(m)]\} [\nu(t)^m/m!)]\} +$$
$$+ \exp( -\nu(t)) , x \ge 0 \text{ and } \nu > 0. \qquad (6A)$$

$$\Pr\{\mathcal{L}(t) \le x \} = 0 \text{ for } x < 0 \text{ and for all } x \text{ when } \nu = 0. \qquad (6B)$$

The last term in Equ (6A) is important; it absorbs the case m= 0 which is not covered by the pdf of $L_m$ , $\Gamma(m;\lambda(t))$, but contributes to $\mathcal{L}(t) \le x$. We will comment on it in section **5.2 A Special Case: Constant λ and ν.**

Using the *modified Bessel function of the first kind* [10], and the fact that $\Gamma(\nu + k + 1) = (\nu + k)!$ for integer ν,

$$I_\nu(z) = \sum_{k=0}^{\infty} (z/2)^{\nu+2k}/[ k! \, (\nu + k)! ]$$

we obtain

$$\Pr\{\mathcal{L}(t) \le x \} = \sqrt{\nu(t)/\lambda(t)} \exp( -\nu(t)) \int_0^x I_1( 2\sqrt{\ell \, \nu(t)/\lambda(t)} ) \exp[ -\ell/\lambda(t)] / \sqrt{\ell} \, d\ell +$$
$$+ H(\nu) \exp( -\nu(t)),$$

i.e. the pdf of $\mathcal{L}(t)$ is

$$f_{\mathcal{L}}(x;t) = \Pr\{\mathcal{L}(t) \le x\}/dx =$$

$$= C \sqrt{\nu(t)/\lambda(t)} \exp( -\nu(t)) \, I_1( 2\sqrt{x \, \nu(t)/\lambda(t)} ) \exp[ -x/\lambda(t)] / \sqrt{x} \; +$$
$$+ C \, \delta_{x,0} \, H(\nu) \exp( -\nu(t)) . \qquad (7)$$

$\delta_{x,0}$ is the Kronecker delta and H(ν) is the Heaviside step function. Expressed as in Equ (7), this $f_{\mathcal{L}}(x;t)$ is valid for all $x \geq 0$ and for all values of $\nu \geq 0$.

C is a probability-normalization constant; using entry 11.4.31 of [10],

$$\int_0^\infty \exp(-a^2t^2)\, I_\mu(bt)\, dt = (\sqrt{\pi}/2a)\exp(b^2/8a^2)\, I_{\mu/2}(b^2/8a^2)$$

when $\mathcal{R}(\mu) > -1$ and $\mathcal{R}(a^2) > 0$, which is true in our case, and

$$I_{1/2}(z) = \sqrt{2/z\pi}\,\sinh(z),$$

we confirm that C = 1 and arrive at the pdf for the total loss $\mathcal{L}(t)$ per time unit at time t

$$f_{\mathcal{L}}(x;t) = \sqrt{\nu(t)/\lambda(t)}\,\exp[-\nu(t)] \times I_1\left(2\sqrt{x\nu(t)/\lambda(t)}\right)\exp[-x/\lambda(t)]/\sqrt{x} + \\ + \delta_{x,0}\, H(\nu)\exp(-\nu(t)) \qquad (8)$$

With no loss of generality, taking the investment period to be (0;T), we now find the pdf $g_{\mathcal{L}}(x)$ for the total loss $\mathcal{L}$ over the investment period to be

$$g_{\mathcal{L}}(x) = \int_0^T f_{\mathcal{L}}(x;t)\, dt \qquad (9)$$

This is as far as we reach with analytic techniques without making functional assumptions about λ(t) and ν(t).

### 5.1 Some Observations on $f_{\mathcal{L}}(x;t)$ and $g_{\mathcal{L}}(x)$

Using the approximation $I_\mu(z) \approx (z/2)^\mu/\Gamma(\mu+1)$, valid for $0 < z < \sqrt{\mu+1}$, we have for $x < \lambda/2\nu$

$$f_{\mathcal{L}}(x;t) = [\nu(t)/\lambda(t)\exp[-x/\lambda(t)] + \delta_{x,0}\, H(\nu)]\exp[-\nu(t)]$$

so that

$$f_{\mathcal{L}}(0;t) = [\nu(t)/\lambda(t) + H(\nu)]\exp[-\nu(t)]\,.$$

Moreover, $f_{\mathcal{L}}(x;t) \to 0$ when $x \to \infty$.

Further, for $x > 0$ and using $I_{\mu-1}(z) = dI_\mu(z)/dz + [\nu(t)/z(t)]\, I_\mu(z)$, we learn that $f_{\mathcal{L}}(x;t)$ exhibits a maximum at $x = x_{max}$ satisfying

$$I_2(z) / I_1(z) = z/2\nu(t), \qquad (10)$$

where $z = 2\sqrt{x\nu(t)/\lambda(t)}$; since $I_2(z)/I_1(z) < 1$ for all z, it is always true that $x_{max} < \nu(t)\lambda(t)$ . This is expected.

As a consequence, $g_{\mathcal{L}}(x)$ is everywhere finite for finite investment interval (0;T).

### 5.2 A Special Case: Constant λ and ν

When λ and ν are both constant (i.e. independent of time) and at least when $[2\nu(t)/z]\, I_2(z) - I_1(z) > 0$ over the entire investment period, $g_{\mathcal{L}}(x)$ also has a maximum at $x = x_{max}$ above. Figure 1 shows such a case for λ= 0.5 and ν= 3.0. In this case Equ (10) gives $x_{max} = 0.634$. This may give us some guidance

in investment decisions: $0 < x_{max} < \nu(t)\lambda(t)$ tells us that medium sized breach losses are more frequent than low- and high-cost breaches.

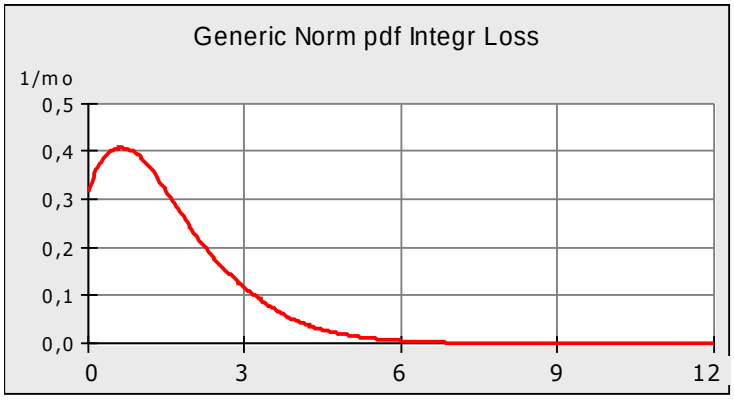



*Figure 1.* Power Density Function $g_{\mathcal{L}}(x)$ for total Breach Loss $\mathcal{L}$ over an investment period T= 1 year with constant $\lambda$ and $\nu$.

We further study the special case when $\lambda$ and $\nu$ are both constant since this gives us an opportunity to check the model in a few details:

Using Eqs (8) and (9) and the fact that $\int_{-\infty}^{\infty} f(x)\delta_{x,0}\,dx = f(0)$, we obtain the *Expected Breach Loss* over the investment period (0;T)

$$E\{\mathcal{L}\} = \int_0^{\infty} x\, g_{\mathcal{L}}(x)\,dx = T\int_0^{\infty} x\, f_{\mathcal{L}}(x)\,dx = T\sqrt{\nu/\lambda}\,\exp(-\nu)\int_0^{\infty} x^{1/2}\, I_1(2\sqrt{x\nu/\lambda})\exp(-x/\lambda)\,dx =$$

$$= \{ \text{entry 11.4.29 of [10]} \} = T\lambda\nu.$$

This is exactly what we expect: on an average $\nu$ successful attacks per time unit, each causing the average breach loss $\lambda$, will give this loss over the investment period.

We also calculate the *Breach Loss Variance* over the investment period,

$$V\{\mathcal{L}\} = E\{(\mathcal{L} - E\{\mathcal{L}\})^2\} = \int_0^{\infty} (x - T\lambda\nu)^2\, g_{\mathcal{L}}(x)\,dx = \{ \text{entry 11.4.28 of [10]} \} =$$

$$= T\lambda^2\nu\,[2 + \nu(1 - T)^2].$$

This result is of the quality that we expect: on an average $\nu$ exponentially distributed stochastic variables per time unit generate a gamma distributed stochastic variable with expected mean $\lambda\nu$ (as above) and variance $\lambda^2\nu$ [9]. A multiplicative factor is plausible from the fact that the number of exponentially distributed variables added to form the gamma distributed stochastic variable is also a stochastic variable, thus generating an additional variance beyond $\lambda^2\nu$; the $V\{\mathcal{L}\}$ expression above is confirmed by simulation.

Had we not included the isolated $\exp(-\nu(t))$ –term in Equ (6), and thereby nor the $\delta_{x,0}\exp(-\nu(t))$ –term in Equ (8), we would instead obtain

$$E\{\mathcal{L}\} = T\lambda\nu/(1 - \exp(-\nu)),$$

i.e. $E\{\mathcal{L}\} = T\lambda\nu$ only asymptotically when $\nu \to \infty$ and $E\{\mathcal{L}\} = T\lambda$ asymptotically when $\nu \to 0$, which is impossible for an obvious reason: also without successful attacks would we suffer a breach loss $T\lambda$.

Similarly, $V\{\mathcal{L}\} \to T\lambda^2\nu^2 \to \infty$ when $\nu \to \infty$ and $V\{\mathcal{L}\} = T^2\lambda^2$ asymptotically when $\nu \to 0$, which again is impossible for the same reason.

We want both $V\{\mathcal{L}\}$ and $E\{\mathcal{L}\}$ to be as small as possible but since both these entities increase monotonically in all variables contained, we instead study $V\{\mathcal{L}\}E\{\mathcal{L}\}$ as a candidate metric for optimisation. More precisely do we want to know if there is an optimal length of the investment period (0;T) and we find that $V\{\mathcal{L}\}E\{\mathcal{L}\}$ exhibits a minimum for

$$T = T_{opt} = 3/4 + \sqrt{1/16 - 1/\nu}\ , \ \nu \geq 16.$$

However, this investment period length is far below any practical interest: for $\nu = 16$ successful attacks per time unit would we have to invest at intervals 0.75 time units, and for very high-frequency successful attacks at intervals 1 time unit to enjoy optimality.

Likewise, *Normalized Breach Loss Variance* $V\{\mathcal{L}\}/E^2\{\mathcal{L}\}$ suffers from the same defect as $V\{\mathcal{L}\}E\{\mathcal{L}\}$, i.e. gives an optimal investment period length that is far below any practical interest.

We have to find economic optimality elsewhere.

## 6 Value-at-Security Risk Entities

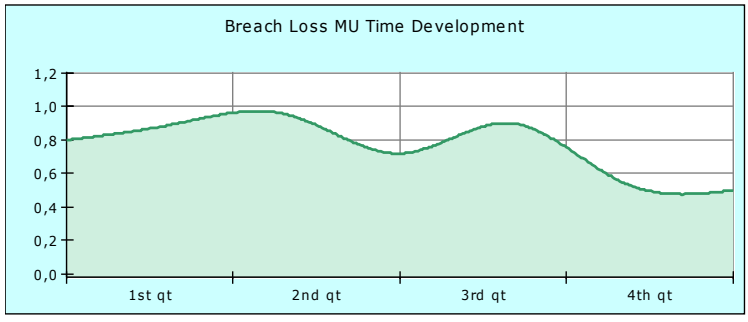
Using Eqs (8) and (9), we may derive all quantitative entities of economic and risk evaluation interest, using the entities used by the security community. We list the most important and most frequently used VaR-type entities here and give examples.

*Value-at-Security Risk*. Writing the Value-at-Security Risk = $X_{vasr}$ for short, this value is defined by the relation

$$\int_0^{Xvasr} g_{\mathcal{L}}(x)\, dx = 1 - RL,$$

where RL is our preset risk level; 1 – RL = CL, i.e. our confidence level. The explicit interpretation is a standard one: our total loss over the investment period, due to security breaches, will not exceed the value $X_{vasr}$ with probability CL.

Figure 2 shows an example with synthetic curves $\lambda(t)$ and $\nu(t)$ and the resulting $g_{\mathcal{L}}(x)$.



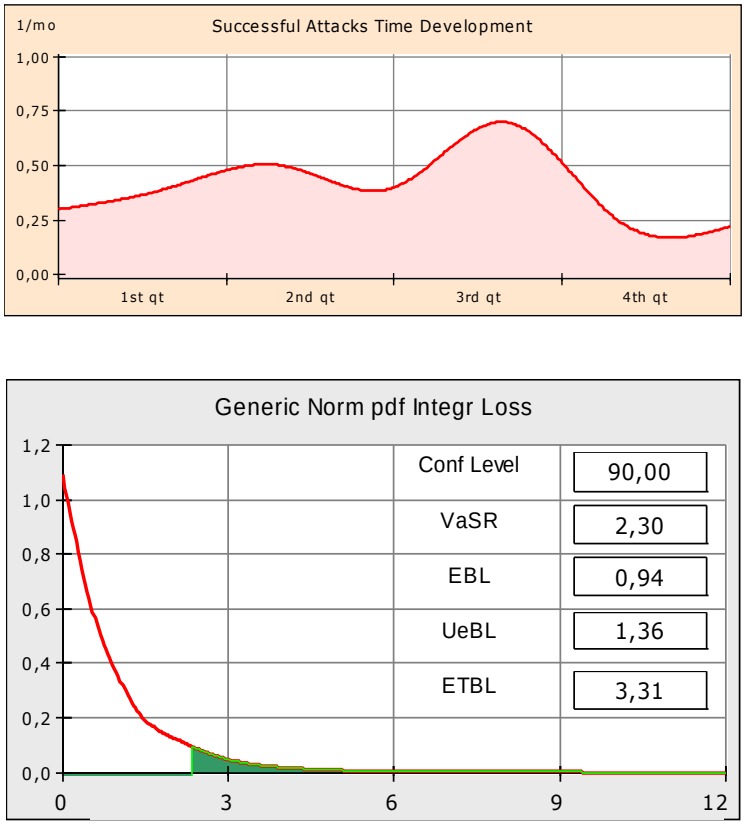



*Figure 2.* Power Density Function $g_{\mathcal{L}}(x)$ for total Breach Loss $\mathcal{L}$ over an investment period.

*Expected Breach Loss* (EBL) is

$$EBL = E\{\mathcal{L}\} = \int_0^{\infty} x\, g_{\mathcal{L}}(x)\, dx\ ,$$

and *Unexpected Breach Loss* (UeBL) is VaSR – EBL [6].

*Expected Tail Breach Loss* (ETBL) is the expected loss in case the loss exceeds VaSR, i.e.

$$ETBL = E\{\mathcal{L}\ |\mathcal{L} > X_{vasr}\} = \int_{Xvasr}^{\infty} x\, g_{\mathcal{L}}(x)\, dx \,/\, \int_{Xvasr}^{\infty} g_{\mathcal{L}}(x)\, dx$$

*Security Risk* over the investment period (0;T) is

$$SR(0;T) = \int_0^T \nu(t)\, [\sum_{m=0}^{\infty} p_S(m;t)]\, dt = \{\text{ Equ (3) }\} = \int_0^T \nu(t)\, dt\ .$$

This expression agrees with the equivalent expression in use by the security community.

To calculate the values of these entities, we have to resort to computer simulations.

## 7 Comments and Conclusions; Present and Future Work

An assumption made was that the individual attacks as well as their consequent costs are independent; this is not always true since some attacks come in bursts. A typical example is successful virus attacks, where many computers and servers become infected by the same virus. Thus, bursts are usually independent but attacks within a burst are correlated.

The present approach can harbour this situation by modelling breach loss $\lambda(t)$ and attack intensity $\nu(t)$ to have coinciding periods with varying combinations of breach loss level and attack intensity level, e.g. frequent low breach loss attacks or rare high breach loss attacks. Figure 3 shows such a situation with synthetic data.

We are presently modifying the model and the simulation implementation to include a situation with varying and stochastic burst time lengths. We are further collecting and analyzing our historic authentic data with the intention of using it as input to our simulations.

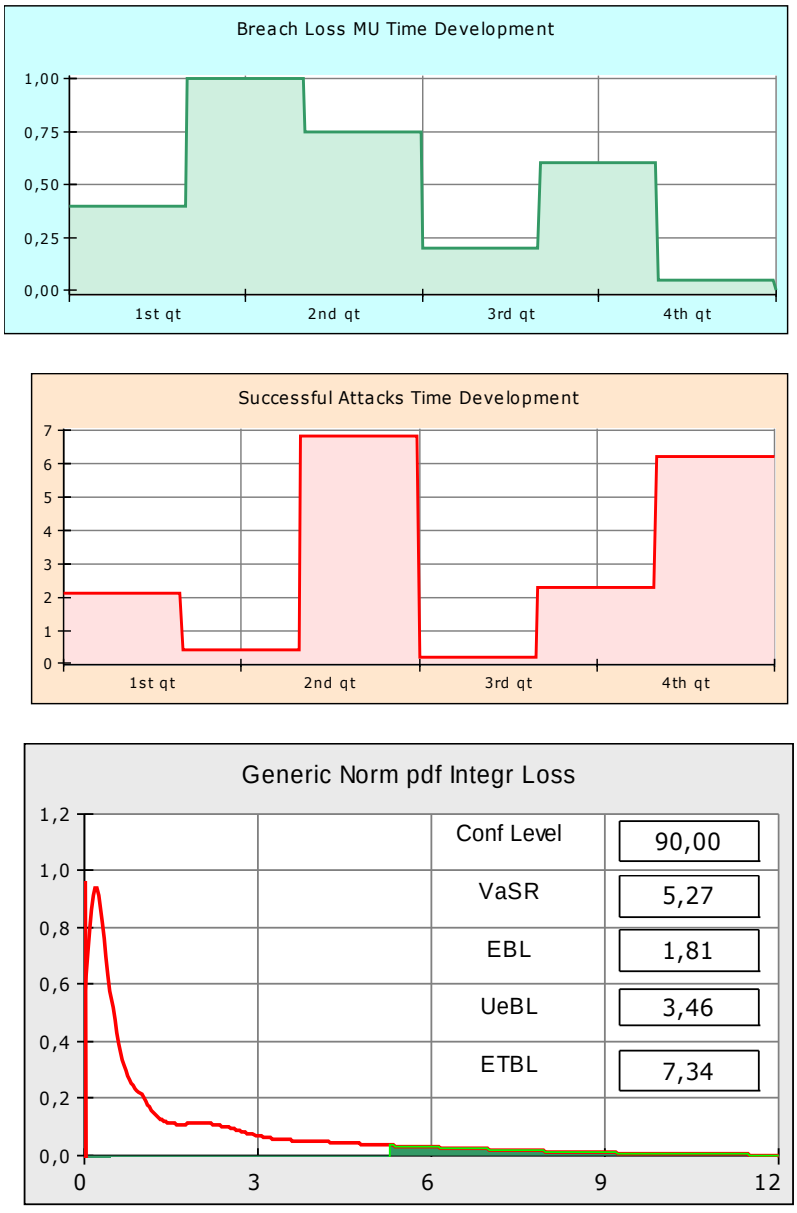



*Figure 3.* Power Density Function $g_{\mathcal{L}}(x)$ for Total Breach Loss $\mathcal{L}$ over an investment period with Average Breach Loss $\langle\lambda\rangle = 0.5$ and Average Successful Attack Intensity $\langle\nu\rangle = 3$; $\langle\lambda\rangle\langle\nu\rangle = 1.5$ and $\langle\lambda\,\nu\rangle = 1.345$ and EBL = $E\{\mathcal{L}\} = 1.811$.
Compare with *Figure 1*, where $\lambda = 0.5$ and $\nu = 3$.

Another critical assumption is that we can estimate the values of the resources to be protected so that we have a fair estimate of breach loss $\lambda(t)$. Admittedly this is a hard and uncertain activity [11], [12]

and several practitioners within the information and data security communities have strong reservation against the principal possibility of doing so. [13] is one of them. Despite his explicit rejecting position, the author repeatedly gives good examples of metrics that can be useful for such endeavours. Moreover, individual managers or resource responsible people do make such estimates for specific applications or situations, e.g. by estimating costs caused by virus attacks. These costs include manpower costs for clean-up operations and stand-still time, license costs and sometimes loss of brand value. The estimates may not cover all costs or losses, but they can serve as a floor in security investment decisions.

We make the observation that the model presented does not use the individual entities Threat T(t) and Vulnerability V(t), but their product. As far as Threat and Vulnerability are known individually we may gain additional insight into our security situation, but the present model does not need them such, at least if we do not want to calculate the equivalent of Potential Loss; then we will need the pdf of a stochastic variable Threat T(t) that measures the number of attack attempts per time unit at time t. Potential Loss is substituted by VaSR, EBL, UeBL and ETBL (and others) as defined here, which are much more informative than Potential Loss. With them, we can address management in a terminology that management is familiar with.

## References


[1] http://www.geocities.com/amz/links.html#ROI_ALE lists an abundance of papers and links on *ROI & Economics of Information Security*

[2] *The Economics of Information Security Investments,* L A Gordon & M P Loeb, ACM Transactions on Information and System Security, **5**$^{No4}$, November 2002

[3**]** *The Gordon-Loeb Investment Model Generalized: Time Dependent Multiple Threats and Breach Losses over an Investment Period,* R Hulthén, Workshop on the Economics of Information Security, 2007-06-07—08. Rump Session presentation (available from the author)

[4] *Microeconomics,* R S Pindyck & D L Rubinfeld, Prentice Hall International, Inc; 2001

[5] *Financial Statements. A Step-by-Step Guide to Understanding and Creating Financial Reports*, T Ittelson, Career Press, 1998

[6] *Value at Risk. The New Benchmark for Managing Financial Risk,* P Jorion, 3rd Edition, McGraw-Hill, International Edition 2007

[7] *Risk Management Publications* available at http://www.riskmetrics.com/

[8] *The CSI Survey 2007. The 12th Annual Computer Crime and Security Survey,* R Richardson. Can be downloaded from www.GoCSI.com

[9] *Simulation Modeling and Analysis,* A M Law & W D Kelton, McGraw-Hill, 1982

[10] *Handbook of Mathematical Functions*, Abramowitz and Stegun, http://www.math.sfu.ca/~cbm/aands/

[11] http://www2.sims.berkeley.edu/resources/infoecon/ The Economics of the Internet, Information Goods, Intellectual Property and Related Issues. Compiled by Hal R. Varian

[12] *The Statistical Value of Information,* Luther Martin, Workshop on the Economics of Security Investment Implications, 2006-10-23- -24

[13] *Security Metrics. Replacing Fear, Uncertainty, and Doubt*, A Jaquith, Addison-Wesley, 2007

[14] CFO TeliaSonera AB, Private Communications (Company Internal Document)

[15] http://www.moodys.com/cust/default.asp

[16]http://www2.standardandpoors.com/portal/site/sp/en/us/page.my_homepage?lid=us_topnav_mypage