# Extending the Gordon&Loeb Model for Information Security Investment

Jan Willemson
Cybernetica
Aleksandri 8a, 51004 Tartu, Estonia
Email: jan.willemson@gmail.com

***Abstract*—In this paper we study the information security investment model proposed by Gordon and Loeb [1]. We argue that the original model is missing at least one important restriction concerning monotonicity of the remaining vulnerability viewed as a function of original vulnerability level, and propose adding the respective condition. We present a new family of remaining vulnerability functions satisfying all the conditions and generalizing all the currently known example function families.**

***Index Terms*—Gordon&Loeb model, information security investment**

## I. Introduction

When some digital or physical property is to be safeguarded, we usually face an investment problem. On one hand, no protection measures are for free, and on the other hand, each of the measures has its own return in terms of prevented loss. However, security investments differ from capital investments. In case of the latter ones, return can be measured directly by the amount of income obtained within some time period. But in case of security investments, how are we supposed to evaluate the amount of loss that actually never occurs?

This is indeed a complicated question, to which no single correct answer has been found and probably will never be. Over the years, several approaches have been proposed trying to estimate the cost-benefit balance for security investments, e.g. Annual Loss Expected (ALE) and several ALE enhancements like Exposure/Impact analysis [4], Return on (Security) Investments (RO(S)I) [6] and Security Savings and Benefit [3]; see [5] for a good overview and comparison of several related methodologies.

Even though being quite general and well-proven in practical situations, these approaches mainly give us means to reason whether some security investment is reasonable (worth its cost), but they hardly help us in finding the optimal level of investments. In order to achieve this kind of functionality, one has to introduce methods allowing more analytical tools.

A suitable framework was proposed by Gordon and Loeb in 2002 [1]. First they assumed all the essential parameters (like decrease in vulnerability as a function of investment) to be continuous and enough differentiable (which they generally aren't, but this simplification is still reasonable to achieve an analytic model). Next they made some natural assumptions concerning the behavior of these parameters and used standard calculus to study a few example situations. Later this model has been experimentally evaluated by Tanaka and Matsuura [7] and extended in several directions by Hausken [2] and Willemson [8].

The current paper builds on our previous research [8] and is organized as follows. First, in Section II we summarize the general principles of Gordon&Loeb model. In Section III we argue that an important condition is missing from the original model and propose including it, presenting a very general class of functions satisfying all the current conditions and generalizing all the known example functions in Section IV. Finally, Section V draws some conclusions and sets directions for further work.

## II. The Model of Gordon and Loeb

In order to estimate the optimal level of information security investment for protecting some information set, Gordon and Loeb consider several parameters of the set in [1], and we will accept similar, though a bit more formal notation.

First, let $L$ denote the *potential loss* associated with the threat against the information set, i.e. $L = t\lambda$, where $t$ is the probability of the threat occurring and $\lambda$ is the (monetary) loss suffered. Further, let $v$ denote *vulnerability*, i.e. the success probability of the attack once launched; $vL$ is then the total *expected loss* associated with the threat against the information set.

If a company invests $z$ dollars into security, the remaining vulnerability (called *security breach probability* in [1]) will be denoted by $S(z, v)$. The expected benefit from the investment can then be computed as $(v - S(z, v))L$ and the expected net benefit as $(v - S(z, v))L - z$. Under suitable differentiability assumptions, we can see that the optimal level of investment can be found by computing the local optimum $z^*$ of the expected net benefit, i.e. by solving the first order equation

$$\frac{\partial}{\partial z}[(v - S(z, v))L - z] = 0$$

and obtaining the following condition for $z^* = z^*(v)$:

$$-\frac{\partial}{\partial z}S(z^*, v)L = 1. \qquad (1)$$

Of course, the remaining vulnerability function can not be arbitrary. Clearly, since $S(z, v)$ is a probability, we must have $0 \leq S(z, v) \leq 1$. Its first argument is an investment and the second one another probability, so $0 \leq z$ and $0 \leq v \leq 1$. Besides that, the following assumptions are defined in [1]:

**A1** $\forall z\, S(z,0) = 0$, i.e. if initially the attack success probability is $0$, it stays so after every possible investment.

**A2** $\forall v\, S(0,v) = v$, i.e. if we invest no money, there will be no change in the attack probability.

**A3** The function $S(z,v)$ is continuously twice differentiable and for $0 < v < 1$

$$\frac{\partial}{\partial z} S(z,v) < 0 \quad \text{and} \quad \frac{\partial^2}{\partial z^2} S(z,v) > 0.$$

Additionally,

$$\forall v \lim_{z \to \infty} S(z,v) = 0.$$

The last item is postulating that with increasing investments it is possible to decrease the vulnerability level, but at a decreasing rate. Nevertheless, investing larger and larger amounts it is possible to make the attack probability arbitrarily small.

An interesting detail to note in assumption **A3** is the restriction $v < 1$. Does this mean that if the vulnerability level is originally $v = 1$ (i.e. if an attack is launched, it will inevitably succeed) then no matter how much money we invest, we may not be able to decrease this vulnerability? This would very much counter our intuition about information set defense, thus from now on we will consider the assumption **A3** to hold for all $v \in (0,1]$.

It seems that the reason why Gordon and Loeb originally introduced the somewhat artificial restriction $v < 1$ is the example family $S^{II}(z,v) = v^{\alpha z+1}$, $(\alpha > 0)$ given in [1] which for $v = 1$ would be constantly equal to 1. Thus considering the remark above we argue that this family in its vanilla form can not really correspond to any real threat scenario. On the other hand, Tanaka and Matsuura claim in their paper [7] to have found empirical evidence supporting the family $S^{II}$ considering the case of computer viruses spread by email. However, Tanaka and Matsuura only compare the family $S^{II}$ to the family $S^{I}(z,v) = \frac{v}{(\alpha z+1)^\beta}$, $(\alpha > 0, \beta \geq 1)$ and the real claim they make is that the family $S^{II}$ *fits more*. They do it by considering the (relative) effect of security investments

$$E(z_a, z_b; v) = \frac{S(z_a, v)}{S(z_b, v)} \quad (z_a < z_b)\,.$$

Thus the evidence to support the family $S^{II}$ is rather remote. First, it may happen that some non-considered family (e.g. some of the families considered by Hausken [2] or Willemson [8]) would fit much more than $S^{II}$ of Gordon and Loeb, and second, the same expression $E(z_a, z_b; v)$ can be obtained from several different functions $S(z,v)$. We conclude that more empirical evidence must be collected and analyzed before we can say anything in the favor of some concrete family of the remaining vulnerability functions.

In the rest of the paper we will on one hand restrict the original Gordon and Loeb model by adding another assumption, and on the other hand generalize it by proposing a general functional form for the functions $S(z,v)$ covering all the currently proposed concrete function families.

## III. The New Assumption

Out of the original restrictions **A1**–**A3** of Gordon and Loeb, **A1** and **A2** are boundary conditions and **A3** states the behavior of $S(z,v)$ as the function of the investment $z$. However, there is no restriction regarding the behavior of $S(z,v)$ as the function of the original vulnerability $v$. In fact, it is possible to find functions $S(z,v)$ satisfying all the assumptions **A1**–**A3**, but still contradicting the intuition about security investments.

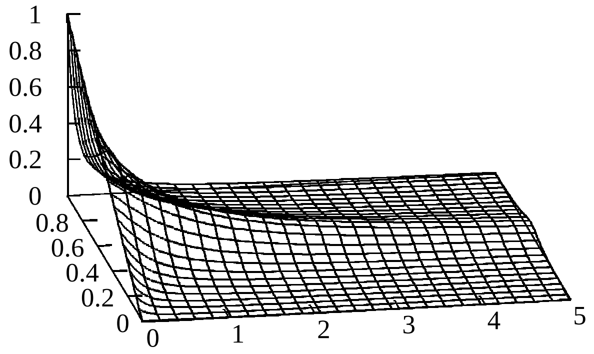
In particular, we argue that the remaining vulnerability function should be monotone in $v$ as well. Otherwise, for some investment $z$ we could have initial vulnerability levels $v_1 < v_2$ such that after investing the amount $z$ we would get $S(z,v_1) > S(z,v_2)$. This contradicts the original intuition of Gordon and Loeb, however, the assumptions **A1**–**A3** do not prohibit such a situation.

Consider for instance the family of functions

$$S^\sharp(z,v) = v \cdot \left(1 - \frac{\arctan((\alpha \cdot (v-\beta)^2 + 1) \cdot z)}{\frac{\pi}{2}}\right),$$

where $\alpha > 0, 0 < \beta < 1$. The example for $\alpha = 50$ and $\beta = \frac{1}{2}$ is depicted in Figure 1.

Fig. 1. Graph of the function $S^\sharp(z,v)$ for $\alpha = 50$ and $\beta = \frac{1}{2}$



Since

$$\arctan((\alpha \cdot (v-\beta)^2 + 1) \cdot z) \in [0, \frac{\pi}{2}),$$

we have $0 \leq S^\sharp(z,v) \leq 1$.

*Proposition 1:* The function $S^\sharp(z,v)$ satisfies the assumptions **A1**–**A3**, but is not monotone in $v$ for any value $z > 0$.

*Proof.* The conditions **A1** and **A2** are straightforward to verify. We compute the partial derivatives of $S^\sharp(z,v)$ for the condition **A3**.

$$\begin{aligned}
\frac{\partial}{\partial z} S^\sharp(z,v) &= -\frac{2(\alpha(v-\beta)^2+1)v}{\pi((\alpha(v-\beta)^2+1)^2 z^2+1)} < 0,\ (v > 0) \\
\frac{\partial^2}{\partial z^2} S^\sharp(z,v) &= \frac{4(\alpha(v-\beta)^2+1)^3 vz}{\pi((\alpha(v-\beta)^2+1)^2 z^2+1)^2} > 0,\ (v > 0)
\end{aligned}$$

It is clear that all these derivatives are continuous and also that if $z \to \infty$ then $\arctan((50 \cdot (v - \frac{1}{2})^2 + 1) \cdot z) \to \frac{\pi}{2}$ and thus $\lim_{z\to\infty} S^\sharp(z, v) = 0$.

On the other hand, considering $S^\sharp(z, v)$ as a function of $v$ we evaluate it for $v = 0$, $v = \beta \in (0, 1)$ and $v = 1$. We see that

$$(\alpha\cdot(0-\beta)^2+1)\cdot z > (\alpha\cdot(\beta-\beta)^2+1)\cdot z < (\alpha\cdot(1-\beta)^2+1)\cdot z$$

which due to monotonicity of $\arctan$ implies

$$S^\sharp(z, 0) < S^\sharp(z, \beta) > S^\sharp(z, 1)$$

for any $z > 0$. □

It is clear that the functions behaving like $S^\sharp(z, v)$ should not be considered when talking about returns on security investments. In order to rule them out, we propose adding a new assumption to the three originally stated by Gordon and Loeb, namely:

**A4** The function $S(z, v)$ is differentiable as a function of $v$ and for all $z$

$$\frac{\partial}{\partial v} S(z, v) > 0\,.$$

## IV. A GENERAL CLASS OF FUNCTIONS SATISFYING A1–A4

Even though the original Gordon and Loeb model is too relaxed and does not contain enough restrictions to capture the full intuition concerning security investments, all the currently known examples of the remaining vulnerability function families ([1], [2], [8]) are rather specific. The purpose of this section is to present a more general family of functions satisfying the assumptions **A1**–**A4** and generalizing all the previous examples.

The general family we propose to consider can be defined as follows:

$$S^{\diamondsuit}(z, v) = v^{p(z)}q(z),$$

where $p, q : \mathbb{R} \to \mathbb{R}$ are twice continuously differentiable functions satisfying the following conditions:

$$\begin{array}{rcl} p(0) & = & 1 \\ q(0) & = & 1 \\ p'(z) & \geq & 0 \\ p''(z) & \leq & 0 \\ q'(z) & < & 0 \\ q''(z) & > & 0 \\ \lim\limits_{z\to\infty} q(z) & = & 0 \end{array} \tag{2}$$

Note that these conditions imply that $p(z)$ and $q(z)$ obtain only positive values, more precisely, for every value of $z$ we have $p(z) \geq 1$ and $0 < q(z) \leq 1$.

*Proposition 2:* All the functions of the family $S^{\diamondsuit}(z, v)$ satisfy the assumptions **A1**–**A4**.

*Proof.* For the condition **A1** we compute

$$S^{\diamondsuit}(z, 0) = 0^{p(z)}q(z) = 0$$

and for the condition **A2** we find

$$S^{\diamondsuit}(0, v) = v^{p(0)}q(0) = v^1 \cdot 1 = v.$$

For the conditions **A3** and **A4** we note that $S^{\diamondsuit}(z, v)$ is continuously twice differentiable as a function of $z$ and continuously differentiable as a function of $v$. We evaluate the derivatives as follows.

$$\frac{\partial}{\partial z} S^{\diamondsuit}(z, v) = v^{p(z)}(q'(z)) + v^{p(z)} \log(v)q(z)(p'(z)) < 0\,,$$

since the first term is $< 0$ and the second one $\leq 0$.

$$\begin{array}{rcl} \frac{\partial^2}{\partial z^2} S^{\diamondsuit}(z, v) & = & v^{p(z)}q''(z) + \\ & + & 2v^{p(z)} \log(v)p'(z)q'(z) + \\ & + & v^{p(z)} \log(v)q(z)p''(z) + \\ & + & v^{p(z)} \log(v)^2 q(z)(p'(z))^2 > 0\,, \end{array}$$

since the first term is $> 0$ and the others are $\geq 0$. Since $\lim_{z\to\infty} q(z) = 0$ and $v \leq 1$, we must also have

$$\lim_{z\to\infty} S^{\diamondsuit}(z, v) = \lim_{z\to\infty} v^{p(z)}q(z) = 0\,.$$

The derivative of $S^{\diamondsuit}(z, v)$ as a function of $v$ can be estimated as

$$\frac{\partial}{\partial v} S^{\diamondsuit}(z, v) = v^{p(z)-1}p(z)q(z) > 0\,,$$

since all the multiplied terms are positive as well. □

Next we consider some of the currently proposed examples of remaining vulnerability functions and show to which extent and how they can be represented as special cases of the family $S^{\diamondsuit}(z, v)$. We note that similar arguments hold essentially for every example family presented in [1], [2], [8]. Verification of the conditions given by equations (2) is straightforward and is therefore omitted.

- The family $S^{I}(z, v) = \frac{v}{(\alpha z+1)^\beta}$ ($\alpha > 0$, $\beta \geq 1$) of Gordon and Loeb [1] can be obtained from $S^{\diamondsuit}(z, v)$ by taking $p(z) = 1$ and $q(z) = \frac{1}{(\alpha z+1)^\beta}$.
- The family $S^{II}(z, v) = v^{\alpha z+1}$, ($\alpha > 0$) of Gordon and Loeb [1] can be obtained from $S^{\diamondsuit}(z, v)$ by taking $p(z) = \alpha z + 1$ and $q(z) = 1$. We note that such a choice does not satisfy the requirement $\lim_{z\to\infty} q(z) = 0$, but as noted in Section II, the family $S^{II}(z, v)$ does not satisfy the requirement $\lim_{z\to\infty} S^{II}(z, v) = 0$ for $v = 1$ either.
- The family $S^{III}(z, v) = \frac{v}{1+\gamma(e^{\phi z}-1)}$ ($\gamma > 0$, $\phi > 0$) of Hausken [2] can be obtained from $S^{\diamondsuit}(z, v)$ by taking $p(z) = 1$ and $q(z) = \frac{1}{1+\gamma(e^{\phi z}-1)}$. One can see that the first derivative of $q(z)$ is not monotone, and as a consequence, $S^{III}(z, v)$ does not satisfy the assumption **A3** as noted already by Hausken.
- The family

$$S^{V}(z, v) = \left\{ \begin{array}{rl} v(1 - \frac{z}{b})^k, & \text{if } 0 \leq z < b \\ 0, & \text{if } z \geq b \end{array} \right. \quad (b > 0, k > 1)$$

of Willemson [8] can be obtained from $S^{\diamondsuit}(z,v)$ by taking $p(z)=1$ and

$$q(z)=\begin{cases} (1-\frac{z}{b})^k, & \text{if } 0\leq z<b \\ 0, & \text{if } z\geq b \end{cases} \quad (b>0,k>1)\,.$$

The first and second derivatives of $q(z)$ are not strictly different from zero, but in [8] we discuss the method of removing the strictness constraint by modifying the "tail" of this function as well.

In general, most of the current examples of the remaining vulnerability function have $p(z)=1$, with the only notable exception of $S^{II}(z,v)=v^{\alpha z+1}$, $(\alpha>0)$ of Gordon and Loeb [1]. At the same time, the only existing evidence (even though very remotely) hints that $S^{II}(z,v)$ may describe the reality the best [7]. Thus it seems that considering more complex functions in the position of $p(z)$ may be the key for future understanding of security investment behavior.

## V. Conclusions and Further Work

In this paper we developed the original model of Gordon and Loeb in two directions. First, we restricted the class of possible remaining vulnerability functions by adding another assumption and second, we generalized all the known examples by stating simple functional (rather than scalar) constraints to the family. It is easy to see that not all possible functions satisfying the assumptions **A1**–**A4** are covered by the family $S^{\diamondsuit}(z,v)$, for example we may consider the function

$$S(z,v)=\frac{v^{1+zv}}{1+z}\,.$$

Thus one of the further research direction is to try to find more natural restrictions to the class of remaining vulnerability functions.

Another prospective research direction is opposite to the previous one – trying to find even more general forms of function families. Ideally, both of the directions should converge to the point where we on one hand have defined a reasonable list of restrictions and on the other hand are able to fully constructively describe all the members of the family determined by these restrictions.

When studying the way how the family $S^{\diamondsuit}(z,v)$ generalizes all the previously known specific examples, we noted that even though most of these examples use the trivial exponent for $v$ being equal to 1, it may actually happen that non-trivial exponents (like defined for the family $S^{II}$ by Gordon and Loeb [1]) reflect the reality much better. Thus understanding the role of this exponent may be one of the key factors for better application of Gordon&Loeb model in practice.

All these directions together with wider experimental evaluations of the model remain the subjects for future research efforts.

## VI. Acknowledgments

This research has been supported by Estonian Science Foundation grant no. 7081.

## References

[1] Lawrence A. Gordon and Martin P. Loeb. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5:438–457, November 2002. Reprinted in *Economics of Information Security*, 2004, Springer, Camp and Lewis, eds.

[2] Kjell Hausken. Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. *Information Systems Frontiers*, 8(5):338–349, 2006.

[3] Kevin J. Soo Hoo. *How Much Is Enough? A Risk-Management Approach to Computer Security*. PhD thesis, Stanford University, June 2000.

[4] James W. Meritt. A method for quantitative risk analysis. In *Proceedings of the 22nd National Information Systems Security Conference*, 1999.

[5] Stuart E. Schechter. *Computer Security Strength & Risk: A Quantitative Approach*. PhD thesis, Harvard University, 2004.

[6] Wes Sonnenreich, Jason Albanese, and Bruce Stout. Return On Security Investment (ROSI) – A practical quantitative model. *Journal of Research and Practice in Information Technology*, 38(1):55–66, February 2006.

[7] Hideyuki Tanaka and Kanta Matsuura. Vulnerability and Effects of Information Security Investment: A Firm Level Empirical Analysis of Japan. In *International Forum of Financial Information Systems and Cybersecurity: A Public Policy Perspective*, College Park, MD, May 26 2005.

[8] Jan Willemson. On the Gordon & Loeb Model for Information Security Investment. In *Proceedings of The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, 2006.