Calibration of the Gordon-Loeb Models for the Probability of Security Breaches

Maurizio Naldi
Dpt. of Civil Engineering and Computer Science
University of Rome Tor Vergata
Rome, Italy
Email: maurizio.naldi@uniroma2.it

Marta Flamini
Faculty of Engineering
International Telematic University Uninettuno
Rome, Italy
Email: m.flamini@uninettunouniversity.net

***Abstract*—Security breaches provoke increasingly high economic losses, requiring higher investment in security. The models by Gordon and Loeb are the most prominent tool employed to assess the impact of security investments on the probability of security breaches, but the estimation of their parameters remains an elusive issue. In this paper the impact of the investment productivity parameters in both Gordon-Loeb models is investigated, and a method is proposed for their estimation. The method employs a least-squares procedure and requires the amount of investments in security over period and the corresponding observed loss due to security breaches.**

***Keywords*–Security; Data Breaches; Gordon-Loeb Model; Investment**

I. Introduction

The economic impact of data breaches is a growing concern among companies and individuals: according to the latest investigation by the Ponemon Institute, the average total cost of a data breach for a company has increased from $3.79 to $4 million in 2016 [1]. Similar results, which show security incidents on the rise, are reported in [2]. Though expenses to secure data are no longer considered as costs, but, correctly, as investments, the problem of relating their amount with the benefit they provide (i.e., reducing the probability of data breaches) is relevant. Many efforts have been devoted to define the return on security investments [3], [4], [5]. The most prominent model relating the investment on security with the security breach probability is the couple due to Gordon and Loeb (hereafter referred to as the GL1 and GL2 model, or GL models for short) [6]. After their introduction, the GL models have been the subject of several extensions and refinements [7], [8], [9], [10], [11] and have been employed to evaluate the applicability of sanctions as incentives to investing in security [12], [13], [14], [15].

However, the actual application of the Gordon-Loeb models requires its parameters to be known (two for GL1 and one for GL2). Gordon and Loeb have proposed some values for both in their seminal paper [6], but no significant support has been provided in the literature for specific values. In the absence of either reliable indications as to the values of those parameters or a method to set those parameters, the GL models may not be applicable in a specific context.

In this paper, we aim to understand the role and impact of the GL model parameters and obtain an estimator for them. After describing the GL models in Section II, we provide the following contributions:

- we introduce the quasi-elasticity function to examine the sensitivity of the security breach probability to each parameter in the GL models (Section III);
- we propose a numerical estimator for the parameters of both GL models, based on a least-squares approach, which requires some observations of the investment in security and the corresponding loss (Section IV);
- for the GL2 model only, we propose an approximate formula to estimate its parameter (Section IV).

II. Gordon-Loeb security breach probability models

In this section we describe the two models proposed by Gordon and Loeb in [6] for the relationship between the investment I in security and the probability P that a data breach occurs in the case of an attack. Incidentally, we note that Huang and Behara derived two models in [16] to describe that relationship in the case of opportunistic and targeted attacks, obtaining the same mathematical shape as Gordon and Loeb, so that the arguments developed in the following are valid for Huang and Behara models as well.

Gordon and Loeb actually proposed two broad classes of security breach functions. Though in their paper the loss is considered to be suffered by the company responsible for data protection, this assumption encompasses the case where the loss is suffered by the customer and the company holding the data is held liable for that loss. The functions proposed by Gordon and Loeb are respectively

$$\begin{aligned} P_{\mathrm{GL1}} &= \frac{V}{(\alpha I + 1)^{\beta}} \\ P_{\mathrm{GL2}} &= V^{\gamma I + 1}, \end{aligned} \tag{1}$$

where $\alpha > 0$, $\beta \geq 1$, and $\gamma > 0$ are measures of the productivity of information security investments (in the following we refer to them as investment productivity parameters), and V is the probability of loss in the absence of investments. The probability of a security beach is therefore a decreasing function of the amount invested in security (under both GL1 and GL2 models), which is the decision variable controlled

978-1-5386-2735-8/17 $31.00 © 2017 IEEE
DOI 10.1109/UKSim.2017.18

TABLE I
MODEL REFERENCE VALUES, EXTRACTED FROM [8]

Parameter	Value
V	0.64
L	$4 \cdot 10^5$
I	$6 \cdot 10^4$
α	10^{-5}
β	1
γ	10^{-5}

by the company holding the data. For any couple (V, I), the probability of loss decreases as we increase either α, β, or γ, which means that those parameters control the extent of the benefits of increased investments in security.

III. SENSITIVITY OF SECURITY BREACH PROBABILITY MODELS

Before proposing a method to estimate the investment productivity parameters, in this section we investigate how each of them impacts on the security breach probability, i.e., the sensitivity of the security breach probability to changes in the models' parameters.

We first examine the impact of varying the investment in security. We measure the sensitivity through the quasi-elasticity of the security breach probability function with respect to the investment:

$$\epsilon_I^* = \frac{\partial P_*}{\partial I/I} = I\frac{\partial P_*}{\partial I}, \tag{2}$$

where the asterisk means that we can apply the same formula to the GL1 as well as to the GL2 model, by employing the pertaining security breach probability function (respectively P_{GL1} and P_{GL2}). We adopt the quasi-elasticity since the dependent variable (the security breach probability) is naturally normalized to 1. In order to obtain the change in the security breach probability due to a 1% increase in the investment, we need to multiply the quasi-elasticity by 100.

If we consider the GL1 model, we obtain

$$\epsilon_I^{(\text{GL1})} = I\frac{\partial P_{GL1}}{\partial I} = -\alpha\beta\frac{VI}{(\alpha I+1)^{\beta+1}} \tag{3}$$

We immediately recognize that the quasi-elasticity is negative, as expected: the security breach probability decreases when we increase our investment in security. For the time being, we consider a generic value of the investment, rather than the optimal one. The impact of the investment is modulated by α and β. In order to examine the impact of the two parameters separately, we fix one of them (using the value extracted from [8] and reported in Table I) and let the other vary. When we let α vary as an independent variable, we obtain the graph shown in Figure 1.

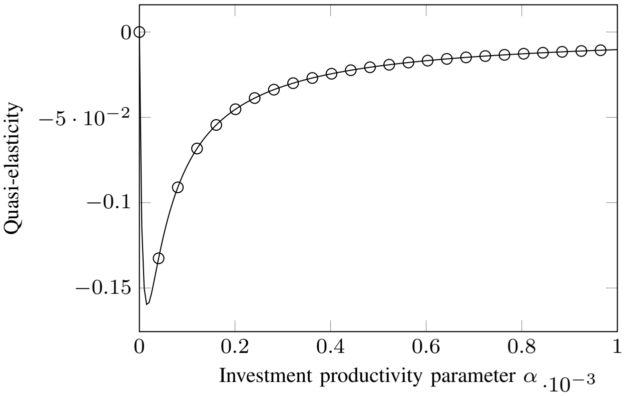

Figure 1. Impact of α on the sensitivity of the breach probability (quasi-elasticity) to the investment in the GL1 model

We see that there is a specific value of the productivity parameter α for which the sensitivity is maximum (the absolute value of the quasi-elasticity is maximum). However, for very large values of α, the security breach probability is less and less dependent on the security investment.

In the same way, if we let instead β vary in Equation (3), we obtain the similar graph shown in Figure 2, but with a somewhat dilated x-scale. In fact the range considered in the two plots is $[0, 10^{-3}]$ for α, but $[1, 10]$ for β (which includes values quite far from the typical value reported in Table I). For the values of β around that reported in Table I, the quasi-elasticity would lie in the nearly linear decay portion of Figure 2.

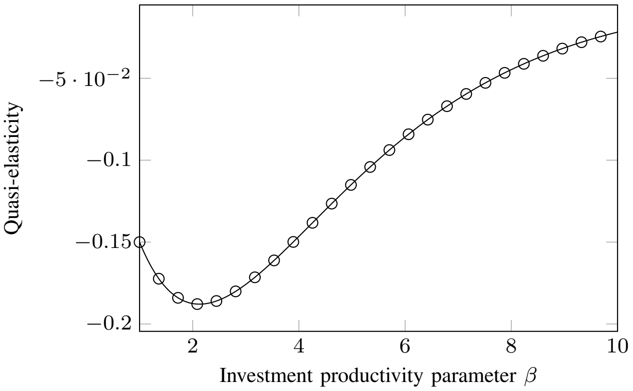

Figure 2. Impact of β on the sensitivity of the breach probability (quasi-elasticity) to the investment in the GL1 model

Similarly, for the GL2 model the quasi-elasticity is

$$\epsilon_I^{(\text{GL2})} = I\frac{\partial P_{GL2}}{\partial I} = I\gamma V^{\gamma I+1}\ln V, \tag{4}$$

which is, as expected, negative (since $\ln V < 0$).

For the values of Table I, we obtain the graph in Figure 3, which resembles those already obtained for α and β.

So far, we have considered the investment as an independent variable, which the company may set quite regardless of any other constraint. Actually, the models proposed by

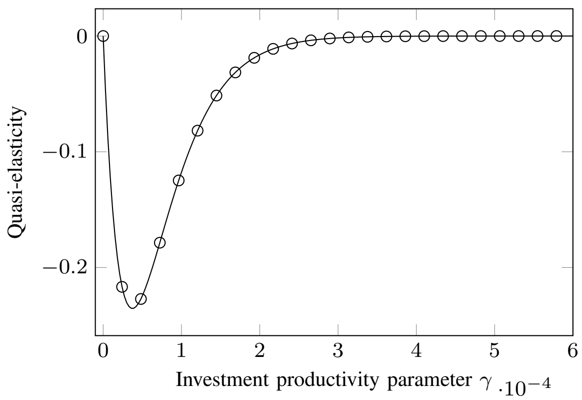

Figure 3. Quasi-elasticity in the GL2 model

Gordon and Loeb allow to derive the optimal amount to invest as that amount that maximizes the ENBIS, i.e. the net benefit from investing in security:

$$\text{ENBIS} = (V - P_*)L - I, \tag{5}$$

where L is the potential loss resulting from a data breach, and the asterisk again represents either model to use for the security breach probability.

Gordon and Loeb themselves derived the optimal investments in [6]. Though the derivation has been reformulated to take into account specifically both internal and external losses in [8], the actual formula remains equal if we aggregate all the losses in L. For the two models we obtain respectively the optimal investments

$$\begin{aligned} \hat{I}_{\text{GL1}} &= \frac{(\alpha\beta VL)^{\frac{1}{\beta+1}} - 1}{\alpha} \\ \hat{I}_{\text{GL2}} &= \frac{\ln\left(-\frac{1}{\gamma VL\ln V}\right)}{\gamma \ln V}. \end{aligned} \tag{6}$$

Since it is rational for the company to invest such an optimal amount, we can assume that it does so and compute the resulting probability of breach corresponding to the optimal investment. For the two models, after recalling Equations (1) and (6), we obtain respectively

$$\begin{aligned} \hat{P}_{\text{GL1}} &= P_{\text{GL1}}(\hat{I}_{\text{GL1}}) = \frac{V}{\left[\alpha\frac{(\alpha\beta VL)^{\frac{1}{\beta+1}}-1}{\alpha} + 1\right]^{\beta}} \\ &= \frac{V}{\left[(\alpha\beta VL)^{\frac{1}{\beta+1}}\right]^{\beta}} = \frac{V^{\frac{1}{\beta+1}}}{(\alpha\beta L)^{\frac{\beta}{\beta+1}}} \\ \hat{P}_{\text{GL2}} &= P_{\text{GL2}}(\hat{I}_{\text{GL2}}) = V^{1+\gamma\frac{\ln\left(-\frac{1}{\gamma VL\ln V}\right)}{\gamma\ln V}} \\ &= V \cdot V^{\frac{\ln\left(-\frac{1}{\gamma VL\ln V}\right)}{\ln V}} = V \cdot e^{\ln V\frac{\ln\left(-\frac{1}{\gamma VL\ln V}\right)}{\ln V}} \\ &= -\frac{1}{\gamma L \ln V} \end{aligned} \tag{7}$$

Since the investment is not an independent variable any longer, we can now analyze the sensitivity of the security breach probability directly with respect to the invesrment productivity parameters α, β, and γ.

For the GL1 model the quasi-elasticity with respect to α is

$$\begin{aligned} \hat{\epsilon}_{\alpha} &= \alpha\frac{\partial \hat{P}_{\text{GL1}}}{\partial\alpha} = \alpha\frac{V^{\frac{1}{\beta+1}}}{(\beta L)^{\frac{\beta}{\beta+1}}}\frac{\partial}{\partial\alpha}\alpha^{-\frac{\beta}{\beta+1}} \\ &= -\alpha\frac{V^{\frac{1}{\beta+1}}}{(\beta L)^{\frac{\beta}{\beta+1}}}\frac{\beta}{\beta+1}\alpha^{-\frac{\beta}{\beta+1}-1} \\ &= -\frac{1}{\beta+1}\frac{(\beta V)^{\frac{1}{\beta+1}}}{(\alpha L)^{\frac{\beta}{\beta+1}}} \end{aligned} \tag{8}$$

Equation (8) shows that the sensitivity of the security breach probability to the investment productivity parameter α is a function of α as well as β. We can see the effect of both parameters in Figure 4 (plotted for $V = 0.64$ and $L = 4 \cdot 10^5$). Since the quasi-elasticity is negative, the regions of highest sensitivity are those where the surface shows a dip, which happens for the lowest values of α and β.

For the GL1 model the quasi-elasticity with respect to β (plotted in Figure 5) is

$$\begin{aligned} \hat{\epsilon}_{\beta} = \beta\frac{\partial \hat{P}_{\text{GL1}}}{\partial\beta} &= \beta\left\{V^{\frac{1}{\beta+1}}\ln V\frac{-1}{(\beta+1)^2}(\alpha\beta L)^{\frac{-\beta}{\beta+1}}\right\} + \\ &+ \beta V^{\frac{1}{\beta+1}}\frac{(\alpha\beta L)^{\frac{-\beta}{\beta+1}}\left[\frac{-1}{(\beta+1)^2}\ln(\alpha\beta L) - \frac{L\alpha\frac{\beta}{\beta+1}}{\alpha\beta L}\right]}{(L\alpha\beta)^{\frac{2\beta}{\beta+1}}} = \\ &= \beta\left\{\frac{-\ln V}{(\beta+1)^2}V^{\frac{1}{\beta+1}}(\alpha\beta L)^{\frac{-\beta}{\beta+1}}\right\} + \\ &- \beta V^{\frac{1}{\beta+1}}(\alpha\beta L)^{\frac{-\beta}{\beta+1}}\left(\frac{\ln(\alpha\beta L)}{(\beta+1)^2} + \frac{1}{\beta+1}\right) = \\ &= -\beta V(\alpha\beta L)^{\frac{-\beta}{\beta+1}}\left[\frac{\ln V}{(\beta+1)^2} + \frac{\ln(\alpha\beta L)}{(\beta+1)^2} + \frac{1}{\beta+1}\right] = \\ &= -\frac{\beta V^{\frac{1}{\beta+1}}(\alpha\beta L)^{\frac{-\beta}{\beta+1}}}{(\beta+1)^2}\left[\ln(\alpha\beta VL) + \beta + 1\right] \end{aligned} \tag{9}$$

Again, the shape of the sensitivity to β resembles the sensitivity to α. The greatest sensitivity is achieved for the lowest values of the two parameters, i.e., when α gets closer to 0 and β gets closer to 1. Their estimation correspondingly becomes most critical in that range, since small uncertainties in the parameter values may give rise to large changes in the predicted security breach probability.

It is to be noted that lower values of α and β corresponds to higher values of the security breach probability for the same investment, i.e., to less productive investments in security. Therefore the estimation of the investment productivity parameters is more critical for less productive investments.

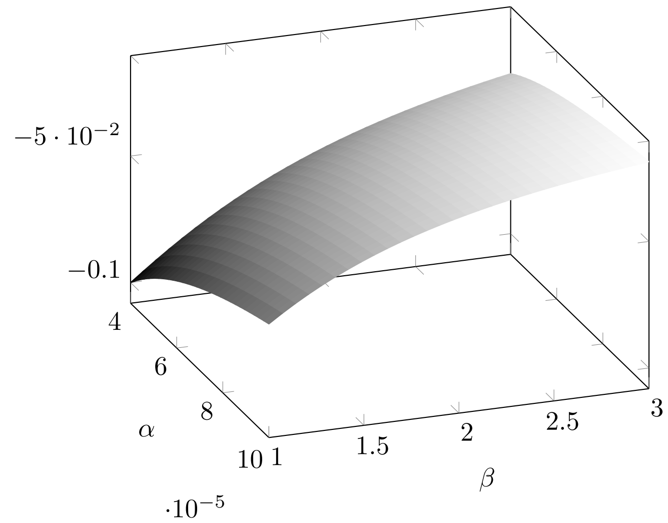

Figure 4. Sensitivity of the security breach probability (quasi-elasticity) to α as a function of both investment productivity parameters

Finally, for the GL2 model the quasi-elasticity with respect to γ is

$$\begin{aligned}\hat{\epsilon}_\gamma &= \gamma\frac{\partial \hat{P}_{\text{GL2}}}{\partial\gamma} = \gamma\frac{1}{L\ln V}\frac{1}{\gamma^2} \\ &= \frac{1}{\gamma L\ln V}\end{aligned} \tag{10}$$

and is plotted in Figure 6, exhibiting a monotone behaviour, with a sharp dip as γ gets below 1. Since, again, the highest values of the security breach probability correspond to the lowest values of the productivity parameter (γ), that behaviour confirms the reasoning already exposed for α and β in the GL1 model: the estimation of γ is more critical for less productive investments.

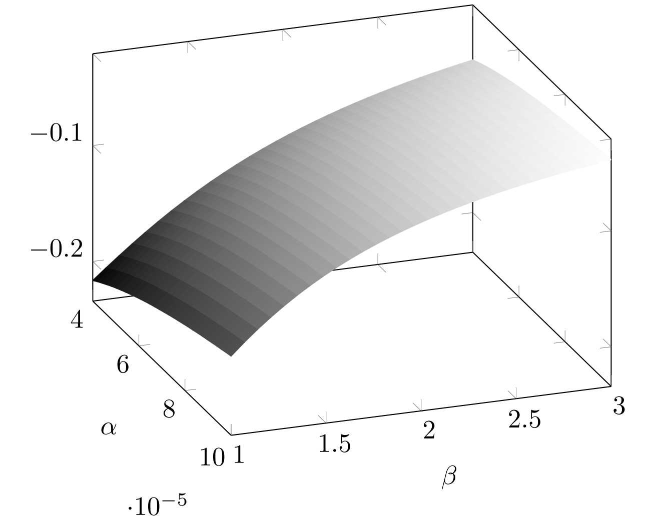

Figure 5. Sensitivity of the security breach probability (quasi-elasticity) to β as a function of both investment productivity parameters

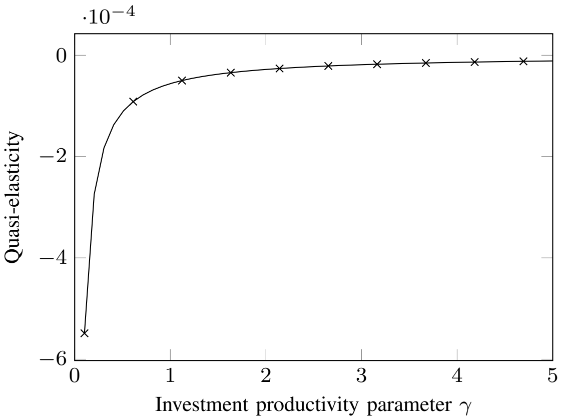

Figure 6. Sensitivity of the security breach probability (quasi-elasticity) to γ in the GL2 model

IV. Estimation of model parameters

Either Gordon-Loeb model is completely specified just if we can calibrate them for our specific case, i.e., if we can assign specific values to the investment productivity parameters (α and β for the GL1 model and γ for the GL2 one). However, this has proven rather difficult so far. Gordon and Loeb themselves provided values for those parameters, but just as an example, without showing any supporting evidence (the values used by Gordon and Loeb are reported in Table I) [6]. Several examples of unreliable and misused statistics concerning information security are reported in [17], which witness the difficulty of getting reliable estimates.

In this section we propose a method to estimate those parameters, which relies on the assessment of the annual investments in security and the annual loss from security breaches. Both quantities should be within the reach of any company. We expect any company to keep a record of its investments, and therefore of its investments in security as well. And the losses due to security breaches are being assessed more and more precisely (see, e.g., [18], [19], [20], [21], [22], [23], [24]).

Let's suppose we have the time series of losses due to security breaches, so that l_j represents the security breach loss in year j (though we choose the year as our recording frequency, the model can be applied with a different recording frequency, e.g. over semesters or quarters). The overall loss over a year can be obtained simply by adding the losses incurred upon all the security incidents taking place in that year. Similarly, we indicate by I_j the investment in security made in year j. If our records extend over n years, we have n couples (I_j, l_j), $j = 1, 2, \ldots, n$. Since the expected loss is $L \cdot P_*$, where the asterisk again denotes either of the two models by Gordon and Loeb, we can fit either GL

TABLE II
CASES FOR THE CALIBRATION EXAMPLE

Case	Ex-ante breach probability V	Maximum loss L
1	0.9	10^6
2	0.5	10^6
3	0.9	$5 \cdot 10^5$
4	0.5	$5 \cdot 10^5$

TABLE III
ESTIMATES OF α AND β IN THE GL1 MODEL

Case	α	β
1	$5.026 \cdot 10^{-5}$	1
2	$4.031 \cdot 10^{-5}$	1.07
3	$4.752 \cdot 10^{-5}$	1
4	$4.00 \cdot 10^{-5}$	1.13

model to the data we have recorded by the least-squares (LS) approach, so that

$$\alpha, \beta = \underset{\alpha,\beta}{\text{argmin}} \sum_{j=1}^{n} \left[l_j - L \cdot P_{\text{GL1}}\right]^2 . \tag{11}$$

$$\gamma = \underset{\gamma}{\text{argmin}} \sum_{j=1}^{n} \left[l_j - L \cdot P_{\text{GL2}}\right]^2 . \tag{12}$$

In order to examine the procedure's performance, we consider the four cases of Table II. For each case we compute the expected loss following the GL models, and then generate a synthetic dataset by imposing a random component outputting a loss value in the $\pm 15\%$ range around the expected loss. The least squares minimization through a numerical approach provides the estimates of Table III and the curves shown in Figure 7 for the GL1 model and in Figure 8 for the GL2 model, along with the synthetic dataset used as an input to the LS parameter estimation. We see that the fit is quite good for all cases.

For the GL2 model, instead of adopting a numerical minimization procedure, we can resort to a linear proxy of Equation (12). Some algebraic passages transform the nonlinear relationship between the expected loss $\bar{L}$ and the investment into a linear dependence on the investment. By taking logarithms we have

$$\begin{aligned} \bar{L} &= LV^{\gamma I+1} \\ \ln \bar{L} &= \ln L + (\gamma I + 1) \ln V \\ \ln \bar{L} &= \ln(VL) + \gamma \ln VI \\ z &= a + bI, \end{aligned} \tag{13}$$

which can be used as a linear regression formula relating the transformed variable $z = \ln \bar{L}$ and the investment I, with $a = \ln(VL)$ being known and $b = \gamma \ln V$ to be determined by a least squares minimization procedure.

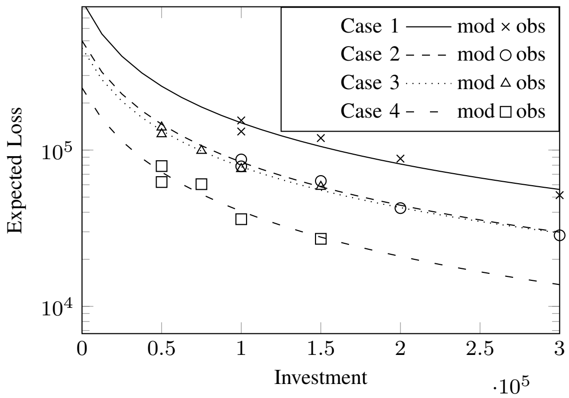

Figure 7. Best fit curves in the GL1 model

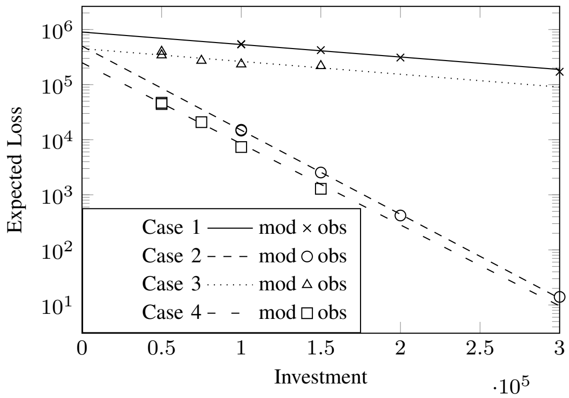

Figure 8. Best fit curves in the GL2 model (numerical LS procedure)

If we consider the n couples (I_i, z_i), $i = 1, 2, \ldots, n$, where $z_i = \ln l_i$, the least squares estimate of b is

$$b = \frac{\sum_{i=1}^{n} I_i z_i - a \sum_{i=1}^{n} I_i}{\sum_{i=1}^{n} I_i^2} . \tag{14}$$

After obtaining b, it is straightforward to get $\gamma = b / \ln V$.

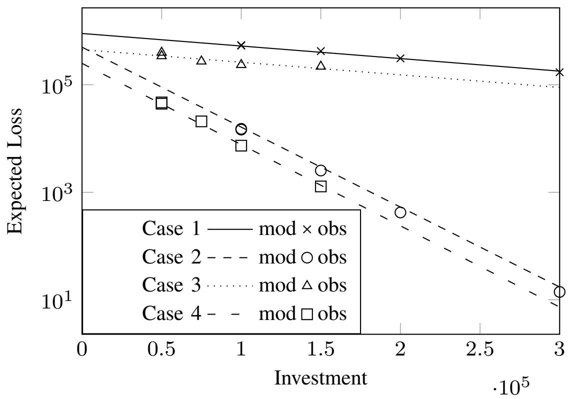

Figure 9. Best fit curves in the GL2 model (linear regression)

The resulting comparison between the observations and the model obtained through the linear regression formula is

TABLE IV
ESTIMATES OF γ

Case	Numerical LS	Linear regression
1	$4.95 \cdot 10^{-5}$	$5.10 \cdot 10^{-5}$
2	$5.07 \cdot 10^{-5}$	$4.94 \cdot 10^{-5}$
3	$5.12 \cdot 10^{-5}$	$5.08 \cdot 10^{-5}$
4	$4.89 \cdot 10^{-5}$	$5.02 \cdot 10^{-5}$

shown in Figure 9. Again, as in the numerical procedure, we observe a fairly good approximation in all cases, showing that the linear regression formula can be used for a quick estimate in place of the exact numerical procedure. The parameter estimates obtained with the two methods are shown in Table IV. The linear regression estimates are quite close to those obtained with the exact numerical procedure: the maximum difference over the four cases is 3%.

V. Conclusion

In both Gordon-Loeb models the investment productivity parameters influence most the security breach probability when they are in their lowest range. Since security investments are less productive in that range, the estimation of the investment productivity parameters gets more and more critical as the investment gets less and less productive.

The numerical least-squares approach proposed for their estimation relies on input data that are easily collected: the investment itself and the loss from data breaches observed in the same period (e.g., over a year). For the GL2 model we can use a quick formula that provides the investment productivity parameter in close agreement with the numerical LS minimization. In all cases the fit with the observed values is quite good. The method can therefore be applied to calibrate either Gordon-Loeb model to the specific context in which the company operates.

References

[1] The Ponemon Institute, "2016 Cost of Data Breach Study: Global Analysis," The Ponemon Institute, Tech. Rep., June 2016.

[2] Symantec, "Internet Security Threat Report," Symantec, Tech. Rep., April 2016.

[3] A. Davis, "Return on security investment–proving it's worth it," *Network Security*, vol. 2005, no. 11, pp. 8–10, 2005.

[4] W. Sonnenreich, J. Albanese, and B. Stout, "Return on security investment (ROSI)-a practical quantitative model," *Journal of Research and practice in Information Technology*, vol. 38, no. 1, pp. 45–56, 2006.

[5] D. Dor and Y. Elovici, "A model of the information security investment decision-making process," *Computers & Security*, vol. 63, pp. 1–13, 2016.

[6] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.

[7] J. Willemson, "On the Gordon & Loeb model for information security investment." in *WEIS*, 2006.

[8] L. A. Gordon, M. P. Loeb, W. Lucyshyn, L. Zhou *et al.*, "Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model," *Journal of Information Security*, vol. 6, no. 01, p. 24, 2014.

[9] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "Increasing cybersecurity investments in private sector firms," *Journal of Cybersecurity*, vol. 1, no. 1, pp. 3–17, 2015.

[10] S. Farrow and J. Szanton, "Cybersecurity investment guidance: Extensions of the Gordon and Loeb model," *Journal of Information Security*, vol. 7, no. 02, p. 15, 2016.

[11] L. A. Gordon, M. P. Loeb, and L. Zhou, "Investing in cybersecurity: Insights from the Gordon-Loeb model," *Journal of Information Security*, vol. 7, no. 02, p. 49, 2016.

[12] G. D'Acquisto, M. Flamini, and M. Naldi, "A game-theoretic formulation of security investment decisions under ex-ante regulation," in *27th IFIP International Information Security and Privacy Conference*, ser. IFIP Advances in Information and Communication Technology, vol. 376. Springer, 4-6 June 2012.

[13] ——, "Damage Sharing May Not Be Enough: An Analysis of an Ex-ante Regulation Policy for Data Breaches," in *9th International Conference, TrustBus 2012, Vienna, Austria, September 3-7, 2012. Proceedings*, ser. Lecture Notes in Computer Science, vol. 7449. Springer, 2012, pp. 149–160.

[14] M. Naldi, M. Flamini, and G. D'Acquisto, *Economics of Grids, Clouds, Systems, and Services: 10th International Conference, GECON 2013, Zaragoza, Spain, September 18-20, 2013. Proceedings*. Springer International Publishing, 2013, ch. Information Security Investments: When Being Idle Equals Negligence, pp. 268–279.

[15] ——, "A revenue-based sanctioning procedure for data breaches," in *The 7th International Conference on Network and System Security NSS 2013*, ser. Lecture Notes in Computer Science. Madrid: Springer, June 3-4, 2013.

[16] C. D. Huang and R. S. Behara, "Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints," *International Journal of Production Economics*, vol. 141, no. 1, pp. 255 – 268, 2013.

[17] J. Ryan and T. I. Jefferson, "The use, misuse, and abuse of statistics in information security research," in *Proceedings of the 2003 ASEM National Conference, St. Louis, MO*, 2003.

[18] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in *11th Annual Workshop on the Economics of Information Security, WEIS 2012, Berlin, Germany, 25-26 June, 2012*, 2012.

[19] L. A. Gordon, M. P. Loeb, and L. Zhou, "The impact of information security breaches: Has there been a downward shift in costs?" *Journal of Computer Security*, vol. 19, no. 1, pp. 33–56, 2011.

[20] A. M. Algarni and Y. K. Malaiya, "A consolidated approach for estimation of data security breach costs," in *Information Management (ICIM), 2016 2nd International Conference on*. IEEE, 2016, pp. 26–39.

[21] P. Choong, E. Hutton, P. Richardson, and V. Rinaldo, "Assessing the cost of security breach: A marketer's perspective," in *Allied Academies International Conference. Academy of Marketing Studies. Proceedings*, vol. 21, no. 1. Jordan Whitney Enterprises, Inc, 2016, p. 1.

[22] R. Layton and P. A. Watters, "A methodology for estimating the tangible cost of data breaches," *Journal of Information Security and Applications*, vol. 19, no. 6, pp. 321–330, 2014.

[23] S. Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity*, p. tyw001, 2016.

[24] K. L. Gwebu, J. Wang, and W. Xie, "Understanding the cost associated with data security breaches." in *PACIS*, 2014, p. 386.