Journal of Information Security, 2016, 7, 49-59
Published Online March 2016 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2016.72004

Investing in Cybersecurity: Insights from the Gordon-Loeb Model

Lawrence A. Gordon, Martin P. Loeb, Lei Zhou

Robert H. Smith School of Business, University of Maryland, College Park, USA
Email: lgordon@rhsmith.umd.edu, mloeb@rhsmith.umd.edu, lzhou@rhsmith.umd.edu

Received 19 January 2016; accepted 20 March 2016; published 23 March 2016

Copyright © 2016 by authors and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

Given the importance of cybersecurity to the survival of an organization, a fundamental economics-based question that must be addressed by all organizations is: How much should be invested in cybersecurity related activities? Gordon and Loeb [1] presented a model to address this question, and that model has received a significant amount of attention in the academic and practitioner literature. The primary objective of this paper is to discuss the Gordon-Loeb Model with a focus on gaining insights for the model's use in a practical setting.

Keywords

Economics of Information Security, Cybersecurity Investment

1. Introduction

Cybersecurity is a critical concern in today's interconnected digital world.[1] In fact, the major industrialized countries throughout the world now consider having a cybersecurity strategy as a national policy priority (OECD, 2012). Private sector organizations are equally concerned about cybersecurity, especially in light of the recent wave of high visibility corporate breaches.[2]

Given the importance of cybersecurity to the survival of an organization, a fundamental economics-based question that must be addressed by all organizations is: How much should be invested in cybersecurity related

[1] For purposes of this paper, the term *cybersecurity* refers to "the protection of information that is accessed and transmitted via the Internet or more generally, through any computer network" ([2], p. 10).

[2] For example, in the U.S., Target Corporation had a major cybersecurity breach in 2013 (see Target's 10-K Report for the fiscal year ending February 1, 2014, filed with the U.S. Securities and Exchange Commission at: https://corporate.target.com/annual-reports/pdf-viewer-2013?cover=6725&parts=6727). JP Morgan Chase & Co. had a major cybersecurity breach in 2014 (see JP Morgan Chase & Co.'s 8-K Report filed on October 2, 2014 with the U.S. Securities Exchange Commission at https://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm).

How to cite this paper: Gordon, L.A., Loeb, M.P. and Zhou, L. (2016) Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security*, **7**, 49-59. http://dx.doi.org/10.4236/jis.2016.72004

activities? Since organizations have finite resources, answering the above question essentially involves a resource allocation decision. As with all resource allocation decisions, a good starting place is to assess the costs and benefits (*i.e*., conduct a cost-benefit analysis) associated with cybersecurity investments.[3] That is, as long as the expected incremental benefits exceed the expected incremental costs from additional cybersecurity investments, an argument can be made for increasing additional cybersecurity investments. Mathematically speaking, the optimal level of cybersecurity investment for an organization is at the point where the expected marginal investment costs equal the expected marginal benefits derived from the investment.[4] Finding this optimal level of investment in cybersecurity is, in essence, the Holy Grail that is at the heart of economic aspects of cybersecurity.

One approach for deriving an organization's optimal level of cybersecurity investment, which has received a significant amount of attention in the academic and practitioner literature, is referred to as the *Gordon-Loeb Model* (hereafter as the GL Model).[5,6] The primary objective of this paper is to discuss the GL Model, as well as some extensions to the model, with a focus on gaining insights for utilizing the GL Model in a practical setting. In other words, although the GL Model is based on a set of mathematical formulas, the focus of this paper is to show that the intuition underlying the model's key components, as well as the model's findings, provide a useful framework for guiding organizations in their quest for deriving the right level of cybersecurity investment.

The remainder of this paper will proceed as follows. In the next (second) section of the paper, we briefly review the GL Model. The third section of the paper focuses on the general insights that can be gleaned from the model. Based on these insights, the third section of the paper also provides a set of steps an organization could take to derive its optimal (or at least an appropriate) level of cybersecurity investment. In the fourth section of the paper, we provide a hypothetical example of how an organization can derive its cybersecurity investment level. The example also illustrates how to allocate the investment to various information sets, based on the steps provided in the third section of the paper. The fifth, and final, section of the paper provides some concluding comments, as well as limitations of the GL Model and directions for future research.

2. The Gordon-Loeb Model

Following is a brief review of the GL Model. This review is based, in large part, on the original article [1]. The purpose of this review is to highlight the key components of the model, as well as the key findings from the model. The emphasis will be placed on the intuition underlying the model's key components and findings, rather than the mathematics upon which the model is based. As such, this paper builds and expands upon [7]. We refer readers interested in delving more deeply into the mathematics of the model to the original article [1], as well as the follow-up article [8].

The basic assumptions of the GL Model are as follows. First, information sets of organizations are vulnerable to cyber-attacks. This vulnerability, denoted as v $(0 \leq v \leq 1)$, represents the probability that a breach to a specific information set will occur under current conditions.[7] Second, if an information set is breached, the value of the information set represents the potential loss (*i.e*., the cost of the breach) and can be expressed as a monetary value, denoted as L. Thus, vL is equal to the expected loss prior to an investment in additional cybersecurity activities.[8] The third assumption is that an investment in cybersecurity, denoted as z, will reduce v based on the productivity of the cybersecurity investment. The GL Model defines $s(z,v)$ as the *security breach probability function*. More to

[3] Although a cost-benefit analysis is a good starting place with all resource allocation decisions, other considerations, many of which cannot be quantified, also need to be considered when deciding on how much to spend on cybersecurity activities. More will be said about this point in the final section of this paper.

[4] The primary benefits from cybersecurity investments are the cost savings associated with cybersecurity breaches that were prevented due to investments. In some cases, however, cybersecurity investments could give an organization a competitive advantage that could generate additional benefits (e.g., increased revenues).

[5] While there is a broad literature dealing with cybersecurity investment (e.g., [3]-[5]), the Gordon-Loeb Model has been referred to as the "gold standard" for deriving the amount an organization should invest on cybersecurity activities (e.g., see the Appendix A to [6]).

[6] In the original paper, the GL Model used the term *information security* rather than cybersecurity. Given the role of the Internet in storing and transmitting information in today's interconnected digital economy, for purposes of this paper the two terms are considered to be interchangeable.

[7] Our notion of $v$as the probability that a successful breach will occur incorporates the threat that an information set will experience a cybersecurity attacked, as well as the information set's vulnerability to a cybersecurity breach. Gordon and Loeb [1], for expositional ease, held the threat probability constant so that v was interpreted as the probability of a breach for the given threat level.

[8] Although not explicitly stated in [1], the GL Model considers situations where some level of cybersecurity already exists within an organization and thus the concern is to derive the optimal amount of additional investment. Also, note that measuring the actual loss from a cyber breach is not straightforward. One method used in the cybersecurity economics literature is to measure the effect of the announcement of a cyber breach on the value of firm's stock. See, for example, [9].

the point, $s(z,v)$ specifies a function that considers the productivity of different levels of cybersecurity investments and thus provides a revised measure of the probability of an information set's vulnerability after some level of investment in cybersecurity. The model also assumes that $s(z,v)$ is twice continuous differentiable and strictly convex, such that the benefits from increasing cybersecurity investments related to a specific information set are increasing at a decreasing rate (*i.e.*, there are positive, but diminishing, returns to additional investments in cybersecurity), as shown in **Figure 1**. The model also assumes that, if some level of vulnerability exists for an information set, additional investments in cybersecurity can bring the probability of a cybersecurity breach arbitrarily close to zero, but not zero.

Given the assumption discussed above, the GL Model can be summarized in a set of equations published in [1] (p. 444). These equations are provided below, where the price of a unit of investment, z, is equal to one. In these equations, the *expected benefits of an investment in information security* are denoted as EBIS, and are equal to the reduction in the firm's expected loss attributable to the extra security, as shown in Equation (1) below:

$$EBIS(z) = \left[v - S(z,v)\right]L \tag{1}$$

EBIS is written above as a function of z, since the investment in information security is the firm's only decision variable (v and L are given parameters for a given information set). The *expected net benefits* from an investment in information security are denoted ENBIS, and equal EBIS less the cost of the investment, as shown in Equation (2a) below:

$$ENBIS(z) = \left[v - S(z,v)\right]L - z\,. \tag{2a}$$

Maximizing Equation (2a) is equivalent to minimizing the expression shown in (2b) below:

$$S(z,v)L + z\,. \tag{2b}$$

The interior maximum at $z^* > 0$, is characterized by the first-order condition for maximizing Equation (2a), and is shown in Equation (3) below:

$$-s_z\left(z^*,v\right)L = 1\,. \tag{3}$$

From (3) above, it becomes clear that the optimal level of investment, z^*, in cybersecurity takes place where the expected marginal benefits from investing in cybersecurity is equal to the expected marginal cost of the investment.[9] This optimal level of cybersecurity investment is illustrated in **Figure 1**, at the investment level of z^*. Gordon and Loeb [1] were able to show that, for two broad classes of security breach probability functions, the optimal level would not exceed vL/e, or roughly 37% of the expected loss from a security breach, vL.[10] Following [1] (p. 451), this result is expressed as:

$$z^*(v) < (1/e)vL\,. \tag{4}$$

Mathematicians Lelarge [10] [11] and Baryshnikov [12] generalized the results of the GL Model to a large array of security breach probability functions. When the assumptions given by Lelarge are violated, the papers of Willemson [13] and Hausken [14] provide demonstration that the 37% rule does not always hold. Gordon *et al.* [8] extended the GL Model to include externalities, which were not considered in the original model. The revised formulation for the social optimal cybersecurity level considering externalities, denoted as z^{SC}, is shown as the inequality (5) below (see page 8 of [8]):

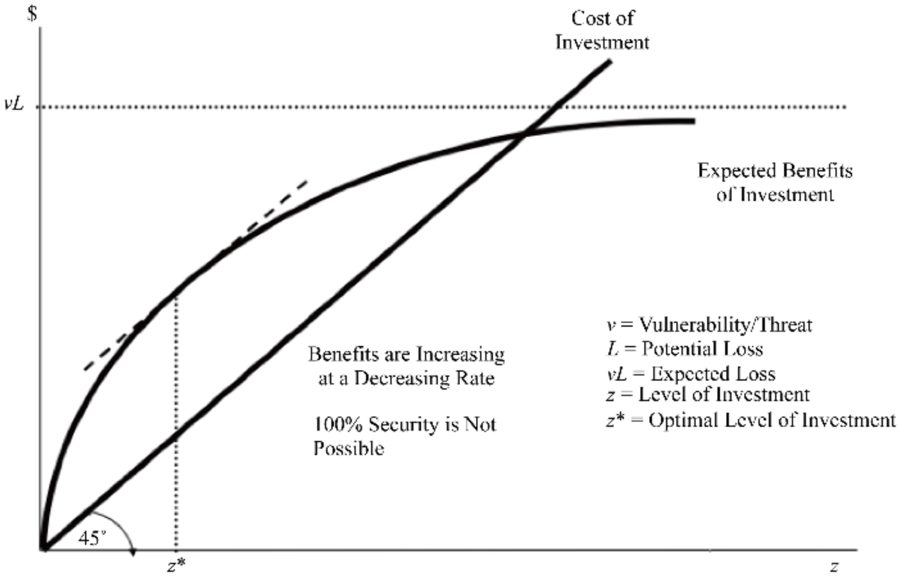
$$z^{SC}(v) < (1/e)\left[1 + \left(L^E/L^P\right)\right]vL^P \tag{5}$$

where L^P represents the private costs to an organization from a cybersecurity breach, L^E represents the cost of externalities to other organizations and individuals from the firm's cybersecurity breach, and L^{SC} represents the total social costs from the firm's cybersecurity breach (*i.e.*, $L^{SC} = L^P + L^E$).[11]

[9] It should be recalled that the price of a unit of z is equal to 1. Furthermore, there are no fixed costs in the analysis, which means that that the investment curve in **Figure 1** is a 45-degree linear curve.

[10] Although the GL Model discussed$L$ and$z$ in terms of a single breach, the analysis would be the same if L and$z$ were considered in terms of multiple breaches within a single time period without corrections after each breach (*i.e.*, ignoring the interdependencies among breaches during the time period).

[11] Because the socially optimal level of investment is greater than the private optimal level of investment, additional incentives are required to motivate private firms to invest more. Gordon *et al.* [15] [16] look at ways in which private firms may be incentivized to increase their cybersecurity investments.



Adapted from [1] (Figure 1, p. 445)

Figure 1. Benefits and costs of an investment in cyber/information security.

3. Insights from the Gordon-Loeb Model

The GL Model provides important insights regarding the way organizations can derive the appropriate level of cybersecurity investment and the best way to allocate this investment to various information sets. These insights are most clearly seen in terms of the model's key components and findings.

There are three key components underlying the way the model derives the optimal amount to invest in cybersecurity. The first component has to do with identifying and valuing an organization's information sets. The value of each set represents the potential loss if the information set were to experience a cybersecurity breach. Since segmentation of information sets (via network segmentation) is an important part of cybersecurity, firms are likely to have several sets of information to protect.[12]

Once the organization's information sets are established and valued, the second component of the GL Model has to do with estimating the vulnerability to a cybersecurity breach for each information set. That is, the organization should estimate the probability that an information set will experience a cybersecurity breach, for each information set identified.

The third underlying component of the GL Model has to do with the way and investment in cybersecurity will reduce an information set's vulnerability to a cybersecurity breach (*i.e.*, the productivity of a cybersecurity investment). Estimates of this investment productivity will likely vary for different information sets, depending on the specific concerns surrounding a particular information set. In addition, as noted above, it is assumed that the benefits from cybersecurity investments will increase at a decreasing rate. In fact, the finding from the GL Model that firms should generally invest an amount that is less than, or at most equal to, roughly 37% of the expected loss that could result from a cybersecurity breach to an information set is directly related to the assumption that the benefits of cybersecurity investments increase at a decreasing rate. Furthermore, it is assumed that cybersecurity investments are allocated to cybersecurity activities based on the declining marginal productivity of the investments.

Another finding from the GL Model is that the optimal level of cybersecurity investment does not always increase with the level of vulnerability.[13] For example, it may pay for a firm to spend more on protecting an information set that has a medium level of vulnerability than one with a high level of vulnerability. Again, this general finding is linked to the productivity of incremental investments in cybersecurity.

The above discussion can be summarized in terms of four steps. These steps are provided below. In the next section, an example based on these steps is provided.

[12] Each set would contain various pieces of information based on some logical grouping of the relevant information for an organization.
[13] Tanaka *et al.* [17] empirically verify this finding.

Step 1: *Estimate the Value*, *and thus the potential Loss* (*L*), *for each information set in the organization*. This step recognizes the fact that the value of the information sets that you wish to protect may differ. It also recognizes the fact that segmentation of information sets is an important component of cybersecurity.

Step 2: *Estimate the probability that an information set will be breached based on the information set's vulnerability*. This step explicitly considers the likelihood of a successful cyber-attack on each information set within the organization.

Step 3: *Create a grid of all possible combinations of steps* 1 *and* 2 *above*. The grid resulting from this step should range from Low Value/Low Vulnerability to High Value/ High Vulnerability information sets. Each cell in the grid represents the expected loss (*L*) without any additional investment in cybersecurity. The expected loss is, in essence, the potential benefit (*i.e.*, cost savings) from additional cybersecurity investments. The net benefit (discussed in the previous section of this paper) would be the difference between the benefit and investment cost.

Step 4: *Derive the level of cybersecurity investment by allocating funds to protect the information sets*, *subject to the constraint that the incremental benefits from additional investments exceed* (*or are at least equal to*) *the incremental costs of the investment*. Assuming the investments in cybersecurity will have different levels of productivity based on the levels of vulnerability associated with each information set, the optimal amount to invest in different information sets will vary and not necessarily increase with increases in the vulnerability of an information set. Furthermore, it is assumed that cybersecurity investments are allocated to cybersecurity activities based on the declining marginal productivity of the investments.

4. Example for Deriving the Investment Level

In this section we provide a hypothetical example of how to use the insights from the GL Model discussed in the previous section of this paper. Our approach is to focus on the four steps of the GL Model that were discussed at the end of the previous section of this paper.

The example is for the GLZ Corporation, a U.S. based manufacturing company that sells its products in several different countries as well as throughout the U.S. The company, which manufactures household appliances, has two manufacturing plants in the U.S. and one manufacturing plant in Canada.

The GLZ Company has 12,000 employees, of which 10,000 are located in the U.S. and another 1500 in Canada. The remaining 500 employees are located in a variety of other countries (*i.e.*, other than the U.S. or Canada) and focus largely on sales related issues. The GLZ Company has patents for several of its products and has several key business partners in the U.S., Canada, China, and throughout Europe. These business partners are from various points throughout the entire supply chain, including firms that provide raw materials to the corporation and large retail stores that sell its final products.

In an effort to protect its information from cybersecurity breaches, as well to minimize the impact of any cybersecurity breaches that actually occur, the firm has been diligent in segmenting its databases (*i.e.*, data segmentation). For example, the firm has segmented its databases according to countries, business partners, customer related information, employee information and market-based data. In addition, highly sensitive data (e.g., employee social security numbers) is separated from less sensitive data (e.g., employee names). In deriving the firm's overall level of spending, the firm has decided to follow the four steps suggested by the GL Model that were outlined in the previous section of this paper. The firms' approach to following these steps is provided below.

Step 1: For each separate database, what the company refers to as information set, the GLZ Corporation provides a rough estimate of the total monetary value in terms of the maximum potential loss (*L*) the firm would incur if the information set were to experience a cybersecurity breach. Stated in terms of dollars, the firm decides on five discrete categories of monetary value for purposes of grouping information sets. These five categories are $20 million, $40 million, $60 million, $80 million, and $100 million. Different information sets could have the same monetary value. These dollar values represent the potential maximum cost of a cybersecurity breach and include such things as the cost of detecting and correcting the cybersecurity breach. In addition, these dollar values include the potential costs associated with lost revenues due to the negative reputation effects of a cybersecurity breach and the potential costs associated with successful lawsuits filed against the firm as a result of the breach.

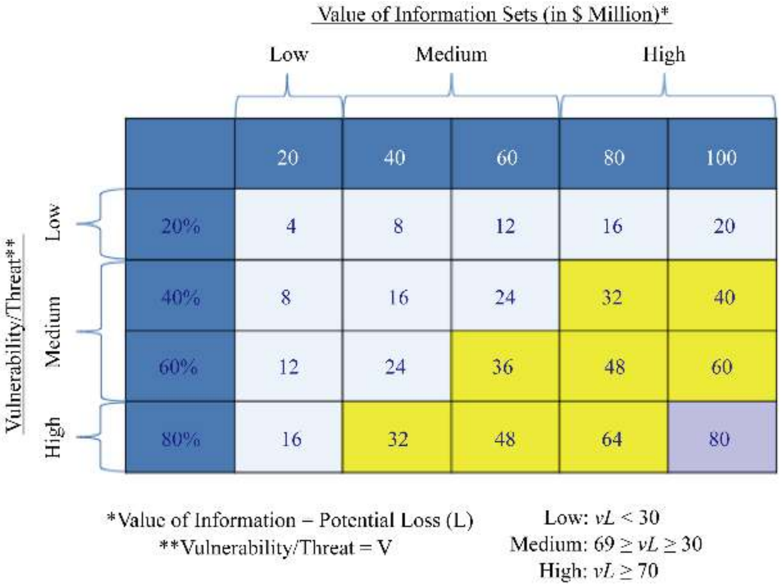
Step 2: The next step in GLZ Corporation's decision process for deriving its cybersecurity spending is to assign a vulnerability (*v*) score to each information set. For illustrative purposes, it is assumed that GLZ corporations assign a vulnerability score of either 0.2, 0.4, 0.6 or 0.8 to each information set. Assigning an information set a score of 0.2, 0.4, 0.6 or 0.8 means there is a 20%, 40%, 60% or 80% probability that the information set will incur a cybersecurity breach. The fact that more than one information set has the same monetary value, or in essence the same potential loss (L), does not mean that these sets will have the same probability of being breached. In fact, the probability that an information set may experience a breach is largely the result of the anticipated threats confronting the information set. In other words, the firm has decided that each level of potential loss (L) should be further segmented into the four categories of vulnerabilities (v), thereby generating 20 distinct information sets (*i.e.*, five categories of information value, with each of these categories sub-divided into four categories of vulnerabilities).

Step 3: The next step is for the firm to develop a grid that combines steps 1 and 2 above. This grid, which is illustrated in **Figure 2**, contains the expected losses that the firm would incur due to a cybersecurity breach of a particular information set. The cells in yellow in **Figure 2** represent the medium level of expected losses (*i.e.*, low: $vL < 30$, medium: $69 \geq vL \geq 30$, high: $vL \geq 70$).

Step 4: The final step in the process of deciding on how much to spend on cybersecurity activities is to consider the cost-benefit aspects of investing additional funds on each information set. Executing this step requires knowledge of the potential expected loss from each information set, but it also requires knowledge of the expected productivity derived from incremental cybersecurity investments. Using $1 million as our unit of investment in cybersecurity activities, this step essentially comes down to asking the following question: How much costs will our firm save, in terms of the reduction in the expected loss, by investing another $1 million on the information set under consideration? If the firm expects to save more (less) than $1 million by making an additional $1 million investment, it pays (does not pay) to make the additional investment from a strictly economics perspective. At a cost savings of $1 million, for an additional $1 million cybersecurity investment, the firm would be indifferent to investing the additional funds.

As noted above, knowledge concerning the productivity of additional investments is crucial to carrying out the fourth step. Although there is no absolute procedure for obtaining this knowledge, we do know (or at least assume) that rational economic decision makers will generally select investment opportunities in descending order. In other words, they generally select investment opportunities that provide the largest benefits first and work their way down to opportunities with smaller benefits. This approach will essentially result in a curve that exhibits increasing benefits at a decreasing rate (as shown in **Figure 1**, and discussed the previous section of this paper). Exactly how the benefits curve will look is, however, a function of the specifics productivity of the investment.

For purposes of completing the fourth step in our example, we assume that investments are generally more productive where the vulnerabilities are greatest. This assumption is based on the general principle that "low hanging fruit" are easiest to pick and therefore provide a higher return for a given level of effort. Accordingly, for our three levels of vulnerabilities (*i.e.*, the probability that a cybersecurity breach will occur), we assume that the



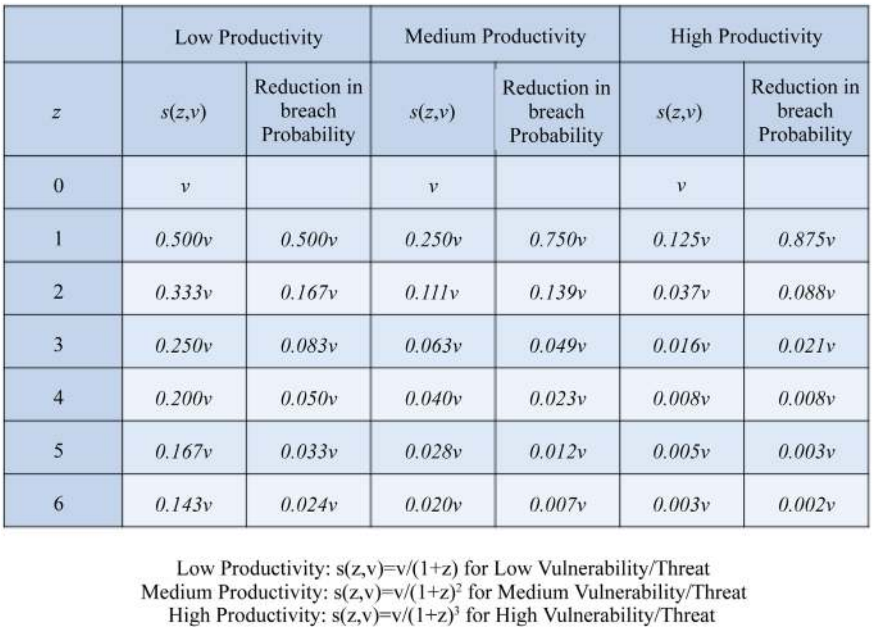
		Value of Information Sets (in $ Million)*				
		Low	Medium		High	
Vulnerability/Threat**		20	40	60	80	100
Low	20%	4	8	12	16	20
Medium	40%	8	16	24	32	40
	60%	12	24	36	48	60
High	80%	16	32	48	64	80

*Value of Information = Potential Loss (L)
**Vulnerability/Threat = V

Low: $vL < 30$
Medium: $69 \geq vL \geq 30$
High: $vL \geq 70$

Figure 2. Expected loss from information security breach.

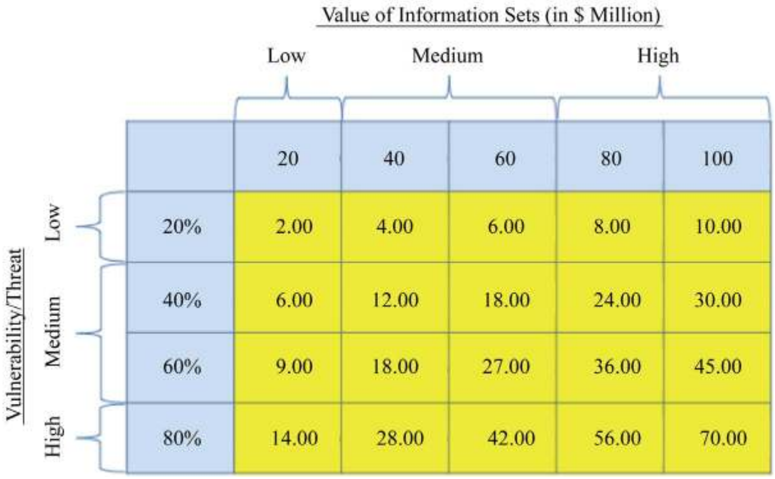
productivity of adding an additional $1 million dollars of investment (z) will reduce the vulnerabilities [*i.e.*, $s(v,z)$] from Equation (3) above by $v/(1 + z)$ where v is 0.2, $v/(1 + z)^2$ where v is 0.4 or 0.6, and $v/(1 + z)^3$ where v is 0.8. **Figure 3** provides a summary of the reduction in$v$ due to incremental investments of the 1st million, 2nd million, 3rd million, and 4th million dollars for each level of v shown in that figure. Applying the results shown in **Figure 3** to **Figure 2**, we can derive **Figures 4-7**. The cells in yellow in **Figures 4-7** represent the information sets where it is still beneficial to make the next $1 million additional investment. **Figure 8** illustrates the final amounts to invest to all of the information sets. As shown in **Figure 8**, the maximum amount to invest in any information set is $4 million (the final cells in yellow). More to the point, for the cells showing that z is $1 million means that after investing $1 million, the savings from the next $1 million investment would be less than the investment cost. A similar interpretation would apply for the other cells shown in **Figure 8** (*i.e.*, where $2 million, $3 million, $4 million are invested, the savings from investing the next $1 million would be less than the investment cost). As shown in **Figure 8**, the only information sets to receive a $4 million in investment in our hypothetical example would be the information sets with a $100 million value (or potential loss, L) and a vulnerability (v) score of 20% and 60%, and the information set with an $80 million value and a vulnerability score of 60%.



	Low Productivity		Medium Productivity		High Productivity	
z	*s(z,v)*	Reduction in breach Probability	*s(z,v)*	Reduction in breach Probability	*s(z,v)*	Reduction in breach Probability
0	*v*		*v*		*v*	
1	*0.500v*	*0.500v*	*0.250v*	*0.750v*	*0.125v*	*0.875v*
2	*0.333v*	*0.167v*	*0.111v*	*0.139v*	*0.037v*	*0.088v*
3	*0.250v*	*0.083v*	*0.063v*	*0.049v*	*0.016v*	*0.021v*
4	*0.200v*	*0.050v*	*0.040v*	*0.023v*	*0.008v*	*0.008v*
5	*0.167v*	*0.033v*	*0.028v*	*0.012v*	*0.005v*	*0.003v*
6	*0.143v*	*0.024v*	*0.020v*	*0.007v*	*0.003v*	*0.002v*

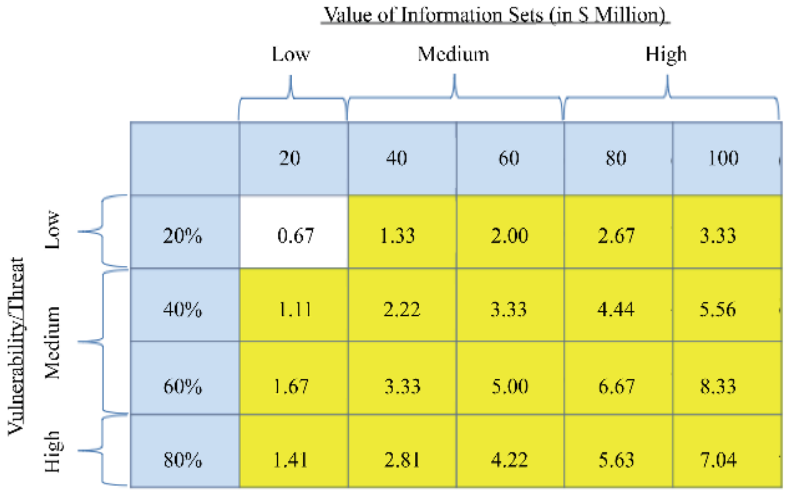
Low Productivity: $s(z,v)=v/(1+z)$ for Low Vulnerability/Threat
Medium Productivity: $s(z,v)=v/(1+z)^2$ for Medium Vulnerability/Threat
High Productivity: $s(z,v)=v/(1+z)^3$ for High Vulnerability/Threat

Figure 3. Productivity of investments in cybersecurity.



		Value of Information Sets (in $ Million)				
		Low	Medium		High	
Vulnerability/Threat		20	40	60	80	100
Low	20%	2.00	4.00	6.00	8.00	10.00
Medium	40%	6.00	12.00	18.00	24.00	30.00
	60%	9.00	18.00	27.00	36.00	45.00
High	80%	14.00	28.00	42.00	56.00	70.00

Figure 4. Cost savings from 1st million dollar investment.

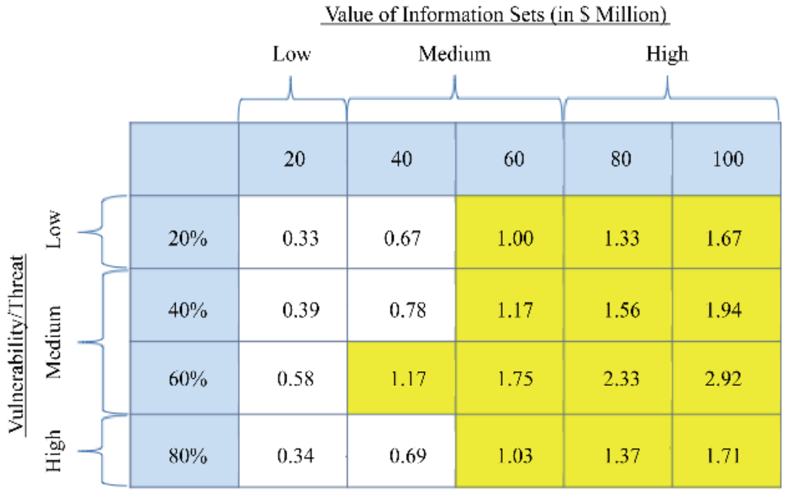


Value of Information Sets (in $ Million)

Vulnerability/Threat

		Low	Medium		High	
		20	40	60	80	100
Low	20%	0.67	1.33	2.00	2.67	3.33
Medium	40%	1.11	2.22	3.33	4.44	5.56
	60%	1.67	3.33	5.00	6.67	8.33
High	80%	1.41	2.81	4.22	5.63	7.04

Figure 5. Cost savings from 2nd million dollar investment.

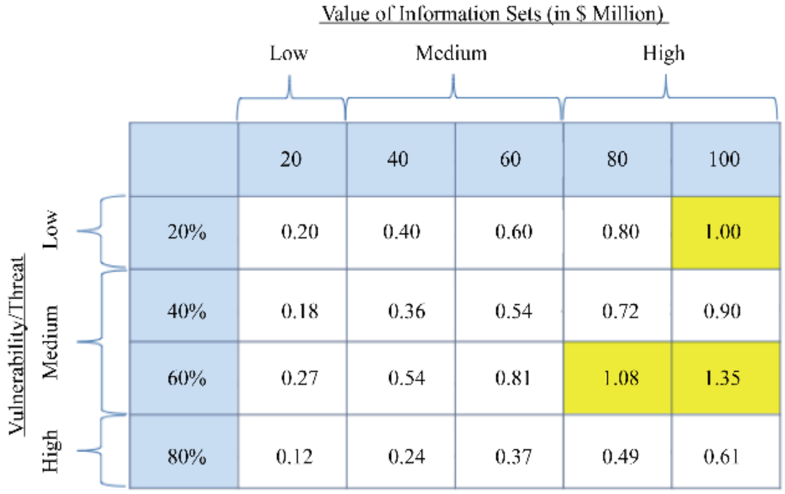


Value of Information Sets (in $ Million)

Vulnerability/Threat

		Low	Medium		High	
		20	40	60	80	100
Low	20%	0.33	0.67	1.00	1.33	1.67
Medium	40%	0.39	0.78	1.17	1.56	1.94
	60%	0.58	1.17	1.75	2.33	2.92
High	80%	0.34	0.69	1.03	1.37	1.71

Figure 6. Cost savings from 3rd million dollar investment.

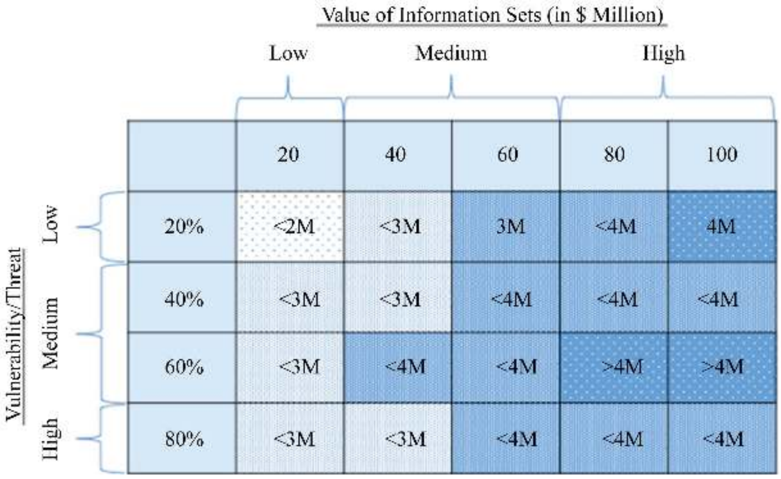


Value of Information Sets (in $ Million)

Vulnerability/Threat

		Low	Medium		High	
		20	40	60	80	100
Low	20%	0.20	0.40	0.60	0.80	1.00
Medium	40%	0.18	0.36	0.54	0.72	0.90
	60%	0.27	0.54	0.81	1.08	1.35
High	80%	0.12	0.24	0.37	0.49	0.61

Figure 7. Cost savings from 4th million dollar investment.



		Value of Information Sets (in $ Million)				
		Low	Medium		High	
Vulnerability/Threat		20	40	60	80	100
Low	20%	<2M	<3M	3M	<4M	4M
Medium	40%	<3M	<3M	<4M	<4M	<4M
	60%	<3M	<4M	<4M	>4M	>4M
High	80%	<3M	<3M	<4M	<4M	<4M

Figure 8. Investment amounts.

The actual GL Model is based on continuous investment functions, whereas our hypothetical example is based on discrete investments of $1 million per unit of investment. Consequently, the investment level in our example would only serve as an estimate of the mathematical optimum. In any case, comparing, the numbers in **Figure 8** with 1/e times the numbers in **Figure 2**, cell by cell, the example is consistent with the GL rule that the optimum investment is less than 37% of the expected loss.[14]

5. Concluding Comments

Today's interconnected digital world has changed the way organizations, as well as people, operate and interact. Indeed, we now live in a world that many describe as an *on-demand economy* (*i.e.*, a marketplace that allows consumer demands for goods and services to be immediately met via digital communication through various sorts of electronic devices). This new kind of economy has created a business model that is characterized by large quantities of information being instantaneously transmitted through cyberspace and stored in a variety of electronic devices.[15] Although the interconnected digital world has resulted in many benefits to businesses, as well as individuals, a downside of this new way of operating and interacting with one and other has been the rapid growth of cybersecurity breaches. Unfortunately, no organization is immune to potential cybersecurity breaches. Accordingly, organizations need to make investments in cybersecurity activities so as to protect themselves against the negative effects of cybersecurity breaches. A fundamental question that must be asked, in this regard, is: How much should be invested in cybersecurity related activities?

The primary objective of this paper has been to explain how the GL Model can be used by organizations to answer the above question. More to the point, this paper has provided a conceptual explanation, accompanied by an illustrative example, of how organizations can use the Gordon-Loeb Model to derive their appropriate level of cybersecurity investment.[16]

As shown in this paper, despite its mathematical underpinnings, the GL Model provides an intuitive framework that lends itself to an easily understood set of steps for deriving an organization's cybersecurity investment level. These steps are: (1) to estimate the value, and thus the potential Loss (L), for each information set in the organization; (2) to estimate the probability that an information set will be breached based on the information set's vulnerability; (3) to create a grid of all possible combinations of steps 1 and 2 above; and (4) to derive the level of cybersecurity investment by allocating funds to protect the information sets, subject to the constraint that the in-

[14] The maximum to invest (in increments of one million) were shown in **Figure 8**, for all cells with the exception of the two cells (row 4, column 5) and (row 4, column 6). Although we did not carry out the example to the point where one would not wish to invest more for those information sets, one can easily carry out the example to verify that one would want to invest less 37% of the expected loss for those sets as well.

[15] The term *cyberspace* refers to the environment where digital communication, especially via the Internet and other computer networks, takes place.

[16] For a 3-minute-and-34 second YouTube video providing a succinct overview of the Gordon-Loeb Model, see: https://www.youtube.com/watch?v=cd8dT0FuqQ4.

cremental benefits from additional investments exceed (or are at least equal to) the incremental costs of the investment.

Although not a panacea, the use of the intuitive framework provided by the GL Model can go a long way toward improving the decision process concerning the way organizations should go about deriving the appropriate amount to invest in cybersecurity activities. In other words, it provides a rational economic procedure for firms to use in deciding on how much to spend on cybersecurity, in light of the cybersecurity risk confronting the firm.

As with the use of all approaches to making investment decisions, there are limitations to using the above noted framework for deciding on the appropriate level of cybersecurity spending. The two most prominent of these limitations are the imprecision associated with valuing the information sets the firm is trying to protect and estimating the probability that a given information set will be breached. However, we believe that making rational, systematic, estimates of these factors is preferred to some completely *ad hoc* approach to considering them in the process of making cybersecurity investment decisions. Another limitation of the approach described in this paper for deriving the cybersecurity investment level is the fact that it does not explicitly consider the qualitative aspects of the decision. However, as noted in footnote 3 of this paper, we believe that using a cost-benefit approach (which is essentially what the GL Model does) is a good starting place for cybersecurity investment decisions. Qualitative concerns (e.g., the organizations overall strategy toward cybersecurity spending) should be considered before making any final decisions regarding the appropriate level of spending on cybersecurity activities. In other words, we strongly believe that economic models should be used as complement to, not as substitute for sound business judgment.

Future research could extend the analyses provided in this paper in several ways. For example, a simulation varying the number of information sets, the values for each information set, and the probabilities associated with potential breaches, could be conducted to assess the sensitivity of the resource allocation decision to these factors. In addition, the quantitative analysis provided by the GL Model could be combined with qualitative techniques for considering cybersecurity investment decisions. In this latter regard, the probabilities of potential cybersecurity breaches used in step 2 from the GL Model could be derived via an AHP (Analytical Hierarchy Process) technique, which allows for consideration of both quantitative and qualitative issues (see [18]).

References

[1] Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, **5**, 438-457. http://dx.doi.org/10.1145/581271.581274

[2] Gordon, L.A. and Loeb, M.P. (2006) Managing Cybersecurity Resources: A Cost-Benefit Analysis. McGraw-Hill, Inc., New York.

[3] Rue, R. and Pfleeger, S.L. (2009) Making the Best Use of Cybersecurity Economic Models. *IEEE Security & Privacy*, **7**, 52-60. http://dx.doi.org/10.1109/MSP.2009.98

[4] Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) A Model Evaluating IT Security Investments. *Communications of the ACM*, **47**, 87-92. http://dx.doi.org/10.1145/1005817.1005828

[5] Wang, J., Chaudhury, A. and Rao, H.R. (2008) Research Note—A Value-at-Risk Approach to Information Security Investment. *Information Systems Research*, **19**, 106-120. http://dx.doi.org/10.1287/isre.1070.0143

[6] AFCEA (Armed Forces Communications and Electronics Association) Cyber Committee Report (2013) The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment.

[7] Gordon, L.A. and Loeb, M.P. (2011) You May Be Fighting the Wrong Security Battles. *The Wall Street Journal*, 26September.

[8] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015) Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, **6**, 24-30. http://dx.doi.org/10.4236/jis.2015.61003

[9] Gordon, L.A., Loeb, M.P. and Zhou, L. (2011) The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs? *Journal of Computer Security*, **19**, 33-56.

[10] Lelarge, M. (2012) Coordination in Network Security Games. In: Greenberg, A.G. and Sohraby, K., Eds., *INFOCOM*, *IEEE*, 2856-2860. http://dx.doi.org/10.1109/infcom.2012.6195715

[11] Lelarge, M. (2012) Coordination in Network Security Games: A Monotone Comparative Statics Approach. *Selected Areas in Communications*, *IEE Journal*, **30**, 2210-2219. http://dx.doi.org/10.1109/JSAC.2012.121213

[12] Baryshnikov, Y. (2012) IT Security Investment and Gordon-Loeb's 1/e Rule. Workshop on Economics and Informa-

tion Security, Berlin. http://weis2012.econinfosec.org/papers

[13] Willemson, J. (2006) On the Gordon & Loeb Model for Information Security Investment. *The Fifth Workshop on Economics of Information Security* (*WEIS*), University of Cambridge. http://www.econinfosec.org/archive/weis2006/docs/12.pdf

[14] Hausken, K. (2006) Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. *Information Systems Frontiers*, **8**, 338-349. http://dx.doi.org/10.1007/s10796-006-9011-6

[15] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015) The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective. *Journal of Accounting and Public Policy*, **34**, 509-519. http://dx.doi.org/10.1016/j.jaccpubpol.2015.05.001

[16] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015) Increasing Cybersecurity Investments in Private Sector Firms. *Journal of Cybersecurity*, **1**, 3-17. http://dx.doi.org/10.1093/cybsec/tyv011

[17] Tanaka, H., Matsuura, K. and Sudoh, O. (2005) Vulnerability and Information Security Investment: An Empirical Analysis of e-Local Government in Japan. *Journal of Accounting and Public Policy*, **24**, 37-59. http://dx.doi.org/10.1016/j.jaccpubpol.2004.12.003

[18] Bodin, L., Gordon, L.A. and Loeb, M.P. (2008) Information Security and Risk Management. *Communications of the ACM*, **51**, 64-68. http://dx.doi.org/10.1145/1330311.1330325