Scientific Research Publishing

Journal of Information Security, 2021, 12, 115-136
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Information Segmentation and Investing in Cybersecurity

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

Robert H. Smith School of Business, University of Maryland, College Park, USA
Email: lagordon@umd.edu, mploeb@umd.edu, lzhou@umd.edu

How to cite this paper: Gordon, L.A., Loeb, M.P. and Zhou, L. (2021) Information Segmentation and Investing in Cybersecurity. *Journal of Information Security*, **12**, 115-136.
https://doi.org/10.4236/jis.2021.121006

Received: November 12, 2020
Accepted: January 16, 2021
Published: January 19, 2021

Abstract

This paper provides an analysis of how the benefits of information segmentation can assist an organization to derive the appropriate amount to invest in cybersecurity from a cost-benefit perspective. An analytical model based on the framework of the Gordon-Loeb Model ([1]) is presented that provides a set of sufficient conditions for information segmentation to lower the total investments in cybersecurity and the expected loss from cybersecurity breaches. A numerical example illustrating the insights gained from the model is also presented.

Keywords

Cybersecurity Investments, Information Segmentation, Economics of Information Security

1. Introduction

In today's interconnected world of digital computer-based communication systems, a fundamental question confronting organizations is: How much should an organization invest in cybersecurity related activities?[1] The answer to the above question is far from straightforward. Indeed, deriving the appropriate amount an organization should invest in cybersecurity is essentially a resource allocation decision that is best resolved in terms of cost-benefit analysis.

The primary objective of this paper is to provide an analysis of how information segmentation can assist an organization to derive the appropriate amount to invest in cybersecurity from a cost-benefit perspective. While many benefits of

[1] Cybersecurity is concerned with protecting the confidentiality (C), integrity (I), and availability (A) of information transmitted via the Internet or any other computer-based network. The above three aspects of cybersecurity are often referred to as the CIA of cybersecurity, where authentication and nonrepudiation are part of the A (availability).

information segmentation have been well-documented (e.g., [2] [3] [4]), the benefits of segmentation in selecting the appropriate amount to invest in cybersecurity have largely been unexplored. Wang [5] and Xu, Li and Fu [6] analyze the cybersecurity investment decisions for given segments, but do not discuss or analyze whether information segmentation is beneficial to the overall organization's cybersecurity investment decisions. The void in the literature raises two questions that are addressed in this paper: 1) Can information segmentation assist an organization in deriving the appropriate amount to invest in cybersecurity? 2) When does information segmentation result in reducing the overall organization's cybersecurity investment expenditures and reducing the expected losses from cybersecurity breaches? In addressing these two questions, we show how the cost-benefit analysis framework underlying the Gordon-Loeb Model (originally proposed in [1]) is well suited for incorporating information segmentation into the decision process to derive the appropriate amount to invest in cybersecurity.[2]

The remainder of this paper proceeds as follows. In the next (*i.e.*, second) section of the paper we provide a brief review of the literature on cybersecurity investments.[3] In the third section of the paper we provide a discussion of information segmentation, with an emphasis on the benefits of information segmentation in deriving the appropriate amount an organization should invest in cybersecurity related activities. The fourth section of the paper provides a model and example that illustrates the use of the Gordon-Loeb Model for deriving the appropriate amount to invest in cybersecurity related activities. The example is based on an organization that has segmented its information into three subsets of information. The fifth section of the paper provides some concluding comments and suggestions for future research.

2. Literature Review on Cybersecurity Investments

Although cybersecurity is a fundamental concern for organizations, they cannot devote all of their resources to cybersecurity. Indeed, as with all resource allocation decisions, investments in (*i.e.*, expenditures on) cybersecurity related activities need to be viewed in the context of cost-benefit analysis.[4] That is, in addressing the fundamental question concerning the right amount to invest in cybersecurity, organizations need to consider the costs and benefits associated with such investments.

[2] Technically speaking, the Gordon-Loeb Model focuses on solving for the optimal amount to invest in cybersecurity. Since the Model relies on various estimates (as discussed in the next section of the paper), the focus in this paper is on solving for the appropriate amount to invest in cybersecurity (*i.e.*, an estimate of the optimal amount).

[3] The term cybersecurity investments, as used in this paper, refers to the internal investments made by an organization to improve the firm's cybersecurity. This view of the term should not be confused with investments in the stock of individual firms that provide cybersecurity-related services or investing in a cybersecurity exchange-traded fund (ETF), such as CIBR (*i.e.*, First Trust Nasdaq Cybersecurity ETF).

[4] In the accounting literature, a distinction is usually made between investments and expenditures. For purposes of this paper, the terms investments and expenditures are considered interchangeable.

There is a large, and growing, body of literature addressing issues related to cybersecurity investments. The focus of this literature is, however, quite varied. For example, one stream of this literature focuses on the trade-offs among different combinations of security related expenditures (e.g., expenditures on such things as access controls, encryption, firewalls, employee training, intrusion prevention and detection systems, computer hardware, etc.). Generally speaking, this stream of literature is concerned with deciding on how to efficiently allocate the funds that have been budgeted for cybersecurity related activities. Papers by Bodin, Gordon and Loeb [7], Smeraldi and Malacaria [8], and Zhuo and Solak [9] fall into this category.

A second stream of literature addressing issues related to cybersecurity investments focuses on expenditures related to cybersecurity insurance as a way of transferring the risk associated with cybersecurity breaches. Of course, expenditures on cybersecurity insurance are indirectly investments in cybersecurity. Papers by Gordon, Loeb and Sohail [10], Böhme and Schwartz [11], Herath and Herath [12], Marotta, Martinelli, Nanni, Orlando and Yautsiukhin [13], the U.S. Department of Homeland Security [14] and Bodin, Gordon, Loeb and Wang [15] fall into this category.

A third stream of the literature addressing issues related to cybersecurity investments focuses on deriving the optimal amount an organization should invest in cybersecurity activities. This stream of literature implicitly assumes the investment in cybersecurity related activities will be allocated in the most efficient manner. Papers by Hoo [16], Gordon and Loeb [1], Cavusoglu, Mishra and Raghunathan [17], Tanaka, Matsuura and Sudoh [18], Hausken [19], Huang, Hu and Behara [20], Gordon, Loeb, Lucyshyn and Zhou [21] [22], Fielder, Panaousis, Malacaria, Hankin and Smeraldi [23], Gordon, Loeb and Zhou [24] [25], Wang [5] and Xu, Li and Fu [6] fall into this category. Section 6 of the paper by Wang ([5], p. 9) examines the optimal cybersecurity investment allocations to multiple segments of data assets. Xu, Li and Fu [6] also examine the optimal allocation to segments, where the segments are the headquarters and the divisions of a multidivisional firm. The papers by Wang [5] and Xu, Li and Fu [6], unlike this paper, do not discuss or present a model demonstrating the benefits of information segmentation.

All of the above noted streams of literature have a bearing on answering the question: How much should an organization invest in cybersecurity related activities? However, the papers addressing issues related to the optimal amount an organization should invest in cybersecurity are explicitly concerned with answering the above question. The most widely referenced economic model for deriving the optimal amount to invest in cybersecurity activities in the academic literature is the Gordon-Loeb Model [1] (hereafter referred to as the GL Model). The GL Model explicitly considers the costs and benefits associated with cybersecurity investments. Besides being widely referenced in the academic literature, the GL Model is frequently mentioned in practitioner-oriented articles and featured in various news media outlets (e.g., The Wall Street Journal). Furthermore, various research reports refer to, and recommend the use of, the GL Model (e.g., [26]).[5] Most importantly for the purposes of this paper, the GL Model provides a general framework that can assist organizations during the process of making decisions concerning the derivation of the appropriate amount to spend on cybersecurity related activities. As noted by the U.S. Council of Better Business Bureaus, in its Report on the "2017 State of Cybersecurity Among Small Businesses in North America":

> Since the threat of cybersecurity is real, and action is important, a fundamental question organizations answer is: How much should they invest in cybersecurity? Gordon and Loeb developed a model based on cost-benefit analysis to help answer this question. Their framework provides a useful guide for organizations trying to find the right level of cybersecurity investment ([26], p. 20).

The general framework provided by the GL Model is based on three fundamental factors. These three factors are: 1) the value of the information being protected, which represents the potential loss from a cybersecurity breach and is denoted as *L*, 2) the probability that the information will suffer a cybersecurity breach, denoted as $v\ (0 < v < 1)$,[6] and 3) the productivity of the investment in cybersecurity activities, referred to as the security breach probability function and denoted as $S(z,v)$, where z represents the investment. Note that $S(0,v) = v$ (*i.e.*, v represents the probability of a breach when $z = 0$). Given the above, the expected loss before an additional investment in cybersecurity activities is equal to *vL*. The productivity function for an investment, $S(z,v)$, provides a revised measure of the probability that an information set will be breached after some level of investment in cybersecurity. The GL Model assumes that the benefits from increasing cybersecurity investments are derived from decreasing the expected loss, $S(z,v)L$, associated with a cybersecurity breach. The model also assumes that these benefits are increasing at a decreasing rate (*i.e.*, there are positive, but diminishing, returns to increasing cybersecurity investments). In other words, increased investments in cybersecurity reduce $S(z,v)$, and in turn $S(z,v)L$ (*i.e.*, the expected loss), but this reduction in the expected loss occurs at a decreasing rate. A convenient feature of the GL Model is that it easily incorporates the information segmentation concept discussed above. The GL Model is summarized in a set of equations provided in the Appendix to this paper.

[5] For a good discussion of the widespread use of the GL Model, see [27].

[6] The probability that a cybersecurity breach will occur can be thought of as the combination of the information set's vulnerability and the threat of attack to the information set. To be precise, the variable v is the probability of a breach occurring conditional on the realization of a threat (*i.e.*, conditional on the probability of a threat equaling one). Equivalently, vL can be thought of as the information set's expected loss conditional on the realization of a threat. Following [1] (p. 442), we assume that the threat probability remains constant and is unaffected by an organization's investment in cybersecurity. For ease of exposition, we refer to v as the vulnerability of the information set and as the probability that the information set will suffer a successful cyberattack.

3. Information Segmentation

3.1. Basic Concept

Firms often have several segmented computer networks and multiple segmented databases within a given network.[7] Both network segmentation and database segmentation facilitate limiting the access of information to specific individuals. Database segmentation and network segmentation result in what we refer to as information segmentation (*i.e.*, subsets of segmented information). Firewalls, access controls, encryption, and dedicated computers are among the ways to facilitate information segmentation. Network segmentation is also a useful mechanism for keeping some information disconnected from the Internet, which is a critical portal for cybersecurity breaches. Information segmentation could be based on a variety of factors, including business functions (e.g., accounting/finance, production, marketing), business subunits (including wholly-owned subsidiaries), customer characteristics, geographic location of sales and/or operations, government regulations, point of sales characteristics (e.g., retail store sales, e-commerce sales), secret formulas, etc.

The amount a firm should be willing to invest in cybersecurity-related activities to protect a specific information segment should be directly related to the potential benefits (*i.e.*, potential reduction in the expected loss) resulting from the cybersecurity investment in the information segment. That is, decisions regarding the amount to invest in cybersecurity for a specific information segment should be based on a segment-specific cost-benefit analysis. Based on the GL Model, this means that the optimal amount (z_i^*) to invest in a specific information segment *i* depends on the value (L_i) of the information contained in the *i*th information segment, the vulnerability to cybersecurity breach of that information segment (v_i), and the productivity of additional investments in cybersecurity for that information segment, $S_i(z_i, v_i)$. Based on the assumption that additional investments in cybersecurity reduce the probability of incurring a cybersecurity breach, the benefits from such an additional investment can be derived by multiplying the reduction in the probability of breach times the potential benefits (*i.e.*, $[v_i - S_i(z_i, v_i)]L_i$). To illustrate the above point, assume a firm has a cybersecurity breach to an information segment that contains sensitive customer information (e.g., credit card numbers, and/or social security numbers). Such a breach could result in a major loss to the firm due to its potential negative impact on future revenues and potential class-action lawsuits. A large investment in cybersecurity related activities to protect that information segment by reducing the probability of a breach to that information segment may be warranted. In contrast, a cybersecurity breach to a publicly available segment of information (e.g., a listing and description of government regulations used for compliance purposes) is unlikely to result in a major loss to a firm. In this latter

[7] "A *computer network* is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections (data links) between nodes…The best-known computer network is the Internet" (https://en.wikipedia.org/wiki/Computer_network).

case, a large investment in cybersecurity related activities to protect that information segment seems unjustified.

In addition to the fact that different segments of information within a given firm may have different values, the probability of a cybersecurity breach to different information segments would likely be an increasing function of the value of the information being protected. Generally speaking, the more valuable an information segment, the greater the amount of effort and dollars a hacker would be willing to spend on illegally obtaining such information. That is, hackers also conduct a cost-benefit analysis when targeting information to steal.[8] Thus, there is a game-theoretic cost-benefit type of analysis going on between those protecting an information segment and those trying to illegally gain access to the same information segment. On the one hand, the owners of an information segment consider the cost-benefit aspects of protecting the information. On the other hand, potential hackers are considering the cost-benefit aspects of conducting a successful hack of the information.

Achieving 100% cybersecurity is essentially impossible from a technical perspective. Furthermore, from an economics perspective, an organization should stop investing in cybersecurity activities once the incremental costs from an incremental investment exceed the expected incremental benefits from such an investment. The expected incremental benefits from increasing cybersecurity investments are primarily derived from avoiding the costs (*i.e.*, cost savings or what some call cost avoidance) associated with cybersecurity breaches. In other words, by avoiding a cybersecurity breach an organization saves the amount it would have lost due to the breach.[9] The amount an organization would expect to lose from a cybersecurity breach is based on the value of the information being protected and the probability that a successful breach was to occur. Thus, the expected incremental benefits from an incremental investment in cybersecurity activities equal the expected loss from a cybersecurity breach that would be avoided as a result of the additional cybersecurity investment. Assuming that cybersecurity investments reduce the probability of a breach, these benefits would equal the reduction in the probability of a breach due to the investment multiplied by the value of the information being protected (see Equation [A1] in the Appendix).

The four steps associated with implementing the GL Model, when multiple segments (*i.e.*, subsets) of information exist, are as follows:[10]

Step 1: Estimate the value, L_i, associated with each information segment i

[8] See [28].

[9] Although beyond the scope of this paper, it is possible for an organization to gain revenues (*i.e.*, benefits) from cybersecurity expenditures by gaining market share due to improved security relative to its competitors. Where such revenues occur, they would be added to the benefits derived from the cost savings from investing in cybersecurity. These latter benefits, however, are generally not significant relative to the cost savings that result from cybersecurity investments.

[10] For purposes of this discussion, we ignore any externalities (see Appendix for a discussion of extending the GL Model to include externalities) associated with a cybersecurity breach in this discussion of the four steps. For an entertaining three-minute video that describes the below four steps, see https://www.youtube.com/watch?v=cd8dT0FuqQ4.

being protected.

Step 2: Estimate the probability, v_i, of a breach associated with each information segment *i*. As pointed out above, the probability of a breach would likely vary for different information segments.

Step 3: Estimate the productivity of investments in cybersecurity $\left[S_i\left(z_i, v_i\right)\right]$ to protect each specific information segment.

Step 4: Derive the optimal investment level, z_i^* for each information segment *i*, (*i.e.*, z_i^* minimizes $\left[S_i\left(z_i, v_i\right)L_i + z_i\right]$). The sum of the investments, $z_{seg}^* \equiv \sum_i z_i^*$ is the optimal total investment level, under the assumption that the information segments are independent of each other.[11]

3.2. Benefits of Information Segmentation for Deriving Cybersecurity Investments

By deriving the appropriate amount to invest in cybersecurity for each information segment based on the GL Model, and aggregating these amounts, an organization is able to answer the question: How much should our organization invest in cybersecurity related activities? More to the point, assuming independent information segments, the answer to the question is that the overall level of cybersecurity investment should be the sum of the amounts derived for each segment (as shown in step 4 above).

There are at least seven potential benefits that information segmentation provides an organization concerning its cybersecurity investment level.[12] First, information segmentation facilitates limiting the access of information to specific individuals (internal, as well as external, to the organization), based on need and security clearance. Thus, for a given cybersecurity investment level, there should be an improvement in the overall security of the information contained within an organization's entire computer-based information system. Alternatively, for a given level of overall cybersecurity, an organization should be able to invest less than would be necessary in the absence of information segmentation.

Second, and closely related to the first benefit noted above, information segmentation minimizes the cascading effect of a cybersecurity breach that actually occurs within an organization. Minimizing the cascading effect is accomplished by decoupling information into disconnected (*i.e.*, independent) segments or strongly separated (e.g., via firewalls, access controls, encryption, etc.) information segments. In other words, the goal is to minimize the connectivity of information segments such that a cybersecurity breach to one segment of information

[11] It should be noted, however, that for information segments that are interdependent, the total cost of protecting the information segments may lower or higher than correcting a breach where the information segments are independent of each other depending on the interactive effects of the information segments. Although beyond the scope of this paper, connectivity of information segments requires an estimate of the connectivity in order to estimate the appropriate amount to invest in protecting against a cybersecurity breach and the appropriate amount to invest for correcting a breach that has occurred.

[12] The seven benefits to be discussed are benefits gross of the implementation costs of segmentation. Of course, in order for segmentation to be economical, the benefits must exceed the implementation costs.

can be contained to that subset of information. Where connectivity among information segments exist, however, an estimate of the interactive effect needs to be made. Here again, for a given level of overall cybersecurity, information segmentation (especially where the information segments are independent from one another) should facilitate an organization's ability to invest less than would be necessary in the absence of any information segmentation.

Third, the decoupling of information segments means that the effort, and in turn investment, involved in detecting a cybersecurity breach should be much lower than in a situation where the breach affects an organization's entire information system. Furthermore, by focusing on specific segments of information, once an actual cybersecurity breach is detected, the required investment to recover from the breach should be more focused, and in turn lower, than the required investment where a cybersecurity breach has affected the organization's entire information system.

Fourth, information segmentation also facilitates more focused policies and decentralized accountability regarding the protection of an organization's information. The decentralization of information accountability and more focused policies concerning an organization's cybersecurity is especially important for large (e.g., multinational) organizations. More focused policies and decentralized accountability should also facilitate a more efficient allocation of funds budgeted for cybersecurity related activities. The above should translate into reducing cybersecurity breaches and, in turn, the overall investment required for cybersecurity related activities.

Fifth, Information segmentation should also improve the reliability of the estimates of the value of information needing protection, the probability of a breach to an information subset, and the productivity of investments in cybersecurity to protect the specific information subset. In other words, information segmentation should improve the estimates required to implement the framework underlying the GL Model for cybersecurity investments. This improvement in estimates is accomplished by shifting the focus from a large heterogeneous computer-based information system to segments of information that are more aligned with specific organizational tasks. Improved estimates should result in more cost-efficient cybersecurity investments.

Sixth, information segmentation should also improve the efficiency (*i.e.*, performance) of the overall information system by reducing congestion (*i.e.*, the problem associated with a network node inefficiently handling data). By improving the overall efficiency of an organization's information system, the investment required to secure the system at a particular level should also be reduced. Alternatively, for a given level of investment in cybersecurity, an organization should be able to achieve a higher overall level of cybersecurity than possible in the absence of information segmentation.

Seventh, information segmentation should also improve the feedback control process associated with cybersecurity investments. More specifically, cybersecurity investments are best thought of as part of an organization's planning and control process. The planning phase of the process begins by identifying opportunities and potential problems related to cybersecurity and developing a strategy to improve the organization's cybersecurity by taking advantage of these opportunities and addressing the potential problems. Implementation of the strategy involves the actual investment (*i.e.*, expenditures) to carry out the cybersecurity strategy. Decisions concerning the amount of cybersecurity investments (expenditures) that should be included in an organization's operating and capital budgets are part of an organization's overall financial planning process. The control phase of the cybersecurity investment process begins by comparing the actual investments with the budgeted (*i.e.*, planned) expenditures for cybersecurity activities. Any difference between the budgeted and actual cybersecurity expenditures should be analyzed so as to improve future financial planning concerning cybersecurity. In addition, the control phase of the cybersecurity investment process includes comparing the actual results (*i.e.*, benefits) with the anticipated results from the investments. In this latter regard, the following question needs to be addressed: Did the investments in cybersecurity yield the anticipated reduction in cybersecurity breaches? Analyzing the difference between the actual and planned investments on cybersecurity, as well as comparing the actual results from the investments with the anticipated results, involves what is usually referred to as a feedback control system. Information segmentation should help to facilitate this feedback control process in terms of focus, accuracy, and timeliness. A well-designed feedback control system based on information segments, compared to an organization's entire information system, should improve the efficiency of future planning for cybersecurity investments.

Although our discussion treated each of the seven benefits derived from information segmentation as being independent of each other, in reality they will likely interact with one and other. For example, increased clarity of an organization's policies and lines of accountability related to cybersecurity will clearly impact the reliability of the estimates of the value of information needing protection (L_i), the probability of a breach to that information subset (v_i), and the productivity of investments in cybersecurity to protect the information subset $\left[S_i\left(z_i, v_i\right)L_i\right]$. **Figure 1** summarizes the seven benefits derived from information segmentation.

4. Model and Numerical Example

In this section, we present an analytical model based on the framework of the Gordon-Loeb Model to provide a set of sufficient conditions for information segmentation to lower the total investments in cybersecurity and the expected loss from cybersecurity breaches. The model examines the impact of information segmentation on the optimal level of cybersecurity investments and the resulting expected loss from cybersecurity breaches. A numerical example is also provided in this section to illustrate the insights gained from the model.

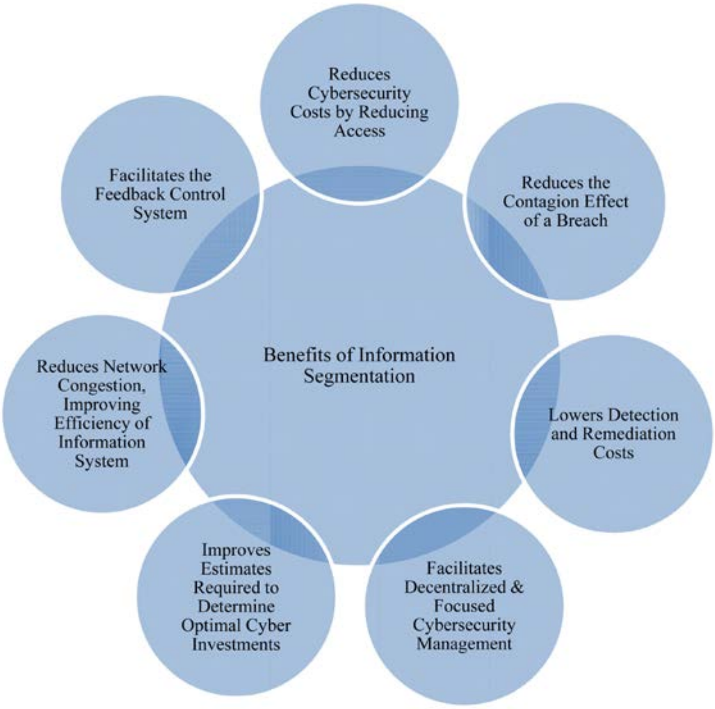
Reduces Cybersecurity Costs by Reducing Access
Reduces the Contagion Effect of a Breach
Lowers Detection and Remediation Costs
Facilitates Decentralized & Focused Cybersecurity Management
Improves Estimates Required to Determine Optimal Cyber Investments
Reduces Network Congestion, Improving Efficiency of Information System
Facilitates the Feedback Control System
Benefits of Information Segmentation

Figure 1. Benefis of information segmentation.

4.1. Model

As previously noted, the GL Model denotes an organization's value of information set as *L*, the vulnerability of the information set as *v*, the investment in cybersecurity as *z*, and the security breach probability function as $S(z,v)$. As discussed in Gordon and Loeb (2002), before any additional cybersecurity investments, the security breach probability equals to the vulnerability of the information set *i.e.*, $S(0,v)=v$. In addition, the security breach probability function should satisfy conditions $\frac{\partial S}{\partial z}=S_z(z,v)<0$ and $\frac{\partial^2 S}{\partial z^2}=S_{zz}(z,v)>0$. That is, as the investment in cybersecurity increases, the probability of the organization being breached is reduced, but at a decreasing rate.

Suppose the organization's information set can be divided into *N* segments. For $i=1,2,\cdots,N$, we denote the value of information in segment *i* as L_i, the vulnerability of the segment *i* information set as v_i ($0<v_i<1$), the cybersecurity investment in segment *i* as z_i and the security breach probability for segment *i* as $S_i(z_i,v_i)$. To focus on the impact of information segmentation on cybersecurity investment decisions, we assume that information segmentation does not change the organization's value of information. That is, for the whole organization, the total value of information with or without the information segmentation is the same. Formally stated, we have

$$L=\sum_{i=1}^{N}L_i. \tag{1}$$

Since the organization's information set is assumed to have been divided into

N segments, we assume the expected loss from cybersecurity breaches (before any additional cybersecurity investments) with segmentation to be no greater than the expected loss without segmentation. That is,

$$\sum_{i=1}^{N} S_i\left(0, v_i\right) L_i \leq S\left(0, v\right) L, \tag{2}$$

i.e.,

$$\sum_{i=1}^{N} v_i L_i \leq vL. \tag{3}$$

To demonstrate the benefits of segmentation, we look at the case where there is no initial benefit to segmentation. That is, at the initial investment levels, the organization's expected loss from breaches to the non-segmented information equals the sum of the expected losses to all segments. Stated formally, we assume:

$$vL = \sum_{i=1}^{N} v_i L_i. \tag{4}$$

Note that Equation (4) can be rewritten as

$$v = \frac{\sum_{i=1}^{N} v_i L_i}{L}. \tag{5}$$

In other words, the organization vulnerability without segmentation is a weighted average of the vulnerability of individual segments. The weight on the vulnerability of a segment is the ratio of the segment's value of information to that of the whole organization.

Since each information segment is only a subset of the organization's information set, we expect the same amount of cybersecurity investment will be more effective in protecting a segment than protecting the whole information set. For simplicity, we assume: 1) each segment's security breach probability function (*i.e.*, the productivity of the investment in cybersecurity activities) takes the same functional form as the organization's breach probability function, and 2) the effectiveness of cybersecurity investment in a segment is inversely related to the proportion of value of information in that segment to the organization's total value of information. Formally stated, the breach probability function for segment i ($i = 1, 2, \cdots, N$) is assumed to be

$$S_i\left(z_i, v_i\right) = S\left(\frac{z_i}{L_i / L}, v_i\right) \tag{6}$$

In this setup, the more valuable the segment's information relative to the whole information set, the more similar the segment's security breach probability function is to the organization's breach probability function without information segmentation. When there is no information segmentation (*i.e.*, $L_i / L = 1$), the above function reverts to $S\left(z, v\right)$.

Without information segmentation, the organization invests in cybersecurity activities to minimize the sum of the expected loss from cybersecurity breaches and the investment in cybersecurity for the single organizational wide information set, *i.e.*,

$$\min_{z}\left[S\left(z,v\right)L+z\right]. \tag{7}$$

The optimal investment in cybersecurity (z^*) needs satisfy the first order condition

$$S_z\left(z^*,v\right)L+1=0. \tag{8}$$

In addition, we denote security breach probability resulting from the optimal investment as $S^*=S\left(z^*,v\right)$ and the expected loss from cybersecurity breaches as $S^*L=S\left(z^*,v\right)L$.

With information segmentation, cybersecurity investments in each segment are determined separately. Hence, each segment will minimize the segment's total cybersecurity costs as below

$$\min_{z_i}\left[S\left(\frac{z_i}{L_i/L},v_i\right)L_i+z_i\right]. \tag{9}$$

The segment *i* optimal investment (z_i^*) can be solved using the following first order condition:

$$\frac{1}{L_i/L}S_z\left(\frac{z_i^*}{L_i/L},v_i\right)L_i+1=0, \tag{10}$$

i.e.,

$$S_z\left(\frac{z_i^*}{L_i/L},v_i\right)L+1=0. \tag{11}$$

Hence, for segment *i*, the security breach probability resulting from the optimal investment is $S_i^*=S\left(\frac{z_i^*}{L_i/L},v_i\right)$ and the expected loss from cybersecurity breach is $S_i^*L_i=S\left(\frac{z_i^*}{L_i/L},v_i\right)L_i$.

With information segmentation, the total investment in cybersecurity is $\sum_{i=1}^{N}z_i^*$, and the total expected losses from security breaches based on the optimal segmental investment is $\sum_{i=1}^{N}S_i^*L_i=\sum_{i=1}^{N}S\left(\frac{z_i^*}{L_i/L},v_i\right)L_i$.

Based on the characteristics of the initial condition [*i.e.*, Equation (4)] and the characteristics of the security breach functions [*i.e.*, Equation (6)], we will present two propositions that provide sufficient conditions for information segmentation to reduce the optimal level of cybersecurity investments and lower the expected loss from cybersecurity breaches for an organization. In the process of proving each proposition, we will first state and prove a corresponding lemma.

Lemma 1: when all information segments in an organization have equal vulnerability, the sum of optimal investments in cybersecurity with information segmentation is equal to the optimal investments in cybersecurity without information segmentation. That is, if $v_i = v_j$ for all *i* and *j*, then $\sum_{i=i}^{N} z_i^* = z^*$.

Proof: Based on first-order conditions (8) and (11), the optimal investments in cybersecurity is a function of the vulnerability. In other words, we can write the optimal investment in cybersecurity without information segmentation as $z^*(v)$, and optimal cybersecurity investment segment *i* as $z_i^*(v_i)$. Given that $S_z < 0$ and $S_{zz} > 0$, from Equation (11), we have

$$z_i^*(v_i) = \frac{z^*(v_i)L_i}{L}. \tag{12}$$

When $v_i = v_j$ for all *i* and *j*, $v_i = v$ for all *i*. Hence,

$$\sum_{i=i}^{N} z_i^*(v_i) = \sum_{i=i}^{N} \frac{z^*(v_i)L_i}{L} = \sum_{i=i}^{N} \frac{z^*(v)L_i}{L} = z^*(v). \tag{13}$$

Q.E.D.

Proposition 1: When an organization's information set contains information segments of different vulnerability, the sum of optimal investments in cybersecurity with information segmentation is less than the optimal investment in cybersecurity without information segmentation if the optimal investment in cybersecurity is concave in vulnerability. That is, when there exists two segments, *i* and *j*, such that $v_i \neq v_j$, $\sum_{i=1}^{N} z_i^* < z^*$ if $\frac{\partial^2 z^*}{\partial v^2} < 0$.

Proof: Let $\theta_i = L_i / L$ for $i = 1, 2, \cdots, N$. Note that $0 \le \theta_i \le 1$ and $\sum_{i=1}^{N} \theta_i = 1$. This allows us to rewrite Equation (5) as

$$v = \sum_{i=1}^{N} \theta_i v_i. \tag{14}$$

Based on Equation (12), we can write the total cybersecurity investment with information segmentation as

$$\sum_{i=1}^{N} z_i^*(v_i) = \sum_{i=1}^{N} \frac{z^*(v_i)L_i}{L} = \sum_{i=1}^{N} \theta_i z^*(v_i). \tag{15}$$

Since there exists two segments, *i* and *j*, such that $v_i \neq v_j$, by Jensen's Inequality and Equation (14), it follows that $\sum_{i=1}^{N} \theta_i z^*(v_i) < z^*(v)$ if $\frac{\partial^2 z^*}{\partial v^2} < 0$.

Q.E.D.

The sufficient condition in **Proposition 1** will hold if the optimal investment in cybersecurity increases in vulnerability at a decreasing rate.

Lemma 2: When all information segments in an organization have equal vulnerability the sum of expected losses from cybersecurity breaches with information segmentation is equal to the expected loss from cybersecurity breaches without information segmentation. That is, if $v_i = v_j$ for all *i* and *j*, then $\sum_{i=1}^{N} S_i^* L_i = S^* L$.

Proof: Recall that the optimal investment in cybersecurity can be written as a function of vulnerability, *i.e.*, $z^*(v)$ or $z_i^*(v_i)$. Hence, we can also write the resulting expected loss from security breaches without segmentation as a function of the organization's vulnerability, *i.e.*, $S^* = S\left[z^*(v), v\right]L = S^*(v)L$.

The expected loss from security breaches based on the optimal segmental cybersecurity investment is

$$S_i^* L_i = S\left(\frac{z_i^*(v_i)}{L_i/L}, v_i\right) L_i. \tag{16}$$

Combined with Equation (12), we have $S_i^* L_i = S\left[z^*(v_i), v_i\right] L_i$, which can also be written as a function of the segmental vulnerability, *i.e.*,

$$S_i^* L_i = S\left[z^*(v_i), v_i\right] L_i = S^*(v_i) L_i. \tag{17}$$

When $v_i = v_j$ for all *i* and *j*, $v_i = v$ for all *i*. Hence,

$$\sum_{i=1}^{N} S^*(v_i) L_i = \sum_{i=1}^{N} S^*(v) L_i = S^*(v) L.(18) \tag{18}$$

Q.E.D.

Proposition 2: When an organization's information set contains information segments of different vulnerability, the sum of expected losses from cybersecurity breaches with information segmentation is less than the expected loss from cybersecurity breaches without information segmentation if the security breach probability based on the optimal cybersecurity investment is concave in vulnerability. That is, when there exist two segments, *i* and *j*, such that $v_i \neq v_j$, $\sum_{i=1}^{N} S_i^* L_i < S^* L$ if $\frac{\partial^2 S^*}{\partial v^2} < 0$.

Proof: Given Equation (17), the total expected loss from cybersecurity breaches with information segmentation is

$$\sum_{i=1}^{N} S_i^* L_i = \sum_{i=1}^{N} S^*(v_i) L_i. \tag{19}$$

Since there exist two segments, *i* and *j*, such that $v_i \neq v_j$, by Jensen's Inequality and Equation (14), we have

$$\sum_{i=1}^{N} S^*(v_i) \frac{L_i}{L} < S^*(v), \tag{20}$$

if $\frac{\partial^2 S^*}{\partial v^2} < 0$. In other words, $\sum_{i=1}^{N} S^*(v_i) L_i < S^*(v) L$ if $\frac{\partial^2 S^*}{\partial v^2} < 0$.

Q.E.D.

The sufficient condition in **Proposition 2** will hold if the security breach probability resulting from the optimal investment in cybersecurity increases in vulnerability at a decreasing rate.

Taken together, our model shows that for all information segments sharing a broad class of security breach probability functions and when the information segments do not have equal vulnerability, information segmentation results in a reduction in both the optimal level of cybersecurity investments and the expected loss of cybersecurity breaches for an organization.[13]

[13] Note that a class of security breach probability functions given by [1] (p. 446) in their Equation (5) satisfies the conditions of **Propositions 1** and **2**.

4.2. Numerical Example

We develop a hypothetical example for a small, publicly traded, US-based jewelry firm called ZLG (hereafter referred to as ZLG). ZLG has annual revenues of approximately $500 Million a year, and roughly 1100 employees. The ZLG consists of 20 retail stores, each one located in a different Metropolitan area on the East Coast of the U.S.

The computer-based information system for ZLG consists of wide area networks (WANs) that segment its information into the following three organizational functions: customers (including credit card information and other personal data related to customers), internal operations (including employee information and financial information required for preparing financial statements and meeting tax requirements), external operations (including advertising and supply chain partners). The three information segments are physically separated from one another via routers and switches, thus the segments are considered to be independent of each other (*i.e.*, a cybersecurity breach to an information segment is confined to that information segment).[14] A schematic diagram of the ZLG's computer-based information system is provided in Figure 2.[15]

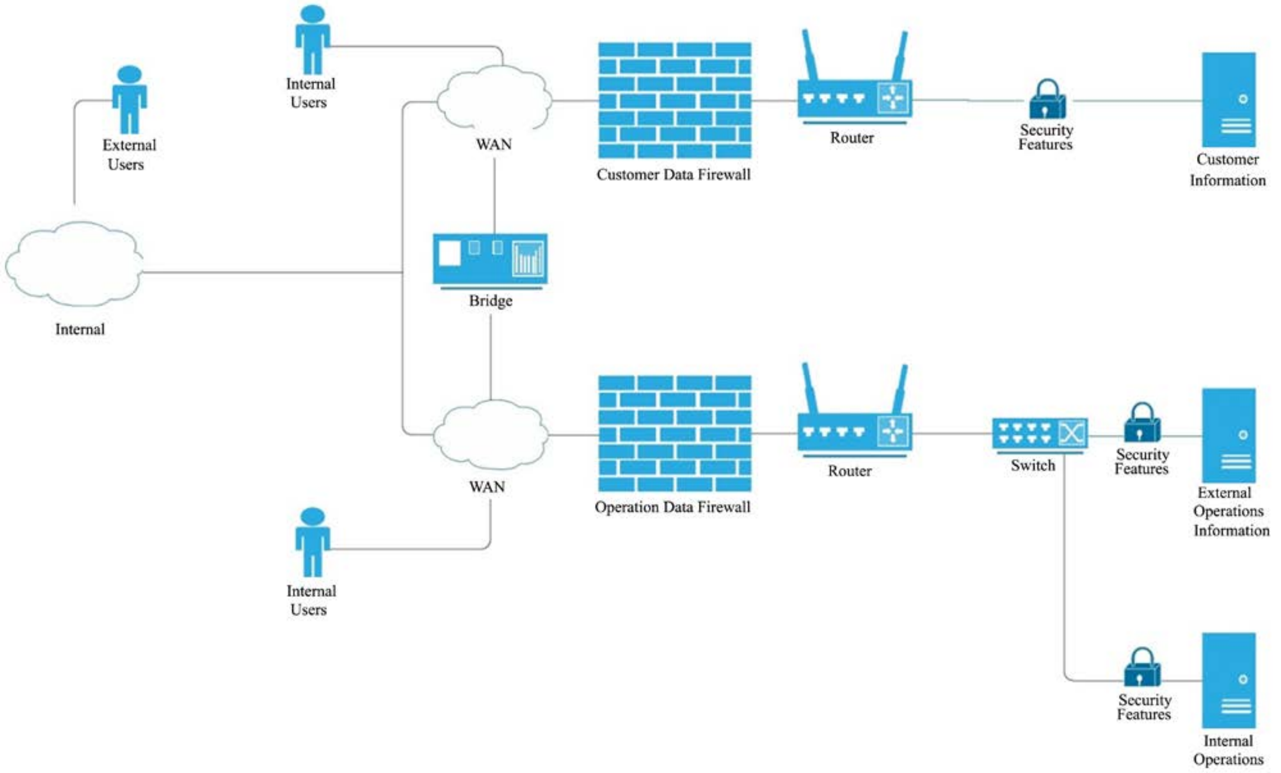

Figure 2. Schematic diagram of ZLG's computer-based information system.

[14] Of course, each information segment can be further divided into various sub-categories (e.g., the customer database is further segmented by the geographical location of each jewelry store). In this example, we focus on the single layer segmentation of customers, internal operations and external operations to demonstrate the impacts of information segmentation.

[15] As indicated in Figure 2, a bridge is used to create a single aggregate network from the network segments at ZLG.

Up until this point in time, the CIO (Chief Information Officer) and her staff (which includes a CISO [Chief Information Security Officer]) have taken care of the firm's cybersecurity related issues. Although ZLG has not had a cybersecurity breach (at least not one of which the firm is aware), the CIO and CISO have become aware of an increasing number of cybersecurity breaches in small businesses in North America. Accordingly, the CIO and CISO, in cooperation with the firm's CFO (Chief Financial Officer), decided it was time to make an additional investment in cybersecurity activities. In order to get an estimate of the amount of the new investment, the CIO, CISO and CFO decide that ZLG will follow the U.S. Council of Better Business Bureaus' recommendation and use the framework underlying the GL Model for cybersecurity investments ([26], p.20).

The CIO and CFO of ZLG are fully aware of the fact that the net benefits from any additional cybersecurity investment derived from the GL Model is best viewed as an estimate. However, they believe that initially viewing the investment decision from a sound economics perspective is a good starting place because it forces the firm to consider the cost-benefit factors that underlie cybersecurity investment decisions. Ultimately, the investment amount derived based on the GL Model will be modified based on the combined business judgment of ZLG's CIO, CISO and CFO.

As discussed in Section III of this paper, there are four basic steps that need to be taken in deriving the additional amount that ZLG Jewelry should invest in cybersecurity activities, based on the framework underlying the GL Model. The first step is to estimate the value (*i.e.*, L_i) for each of the three (*i.e.*, customers, internal, and external) information segments being protected. The second step is to estimate of the probability (*i.e.*, v_i) that a cybersecurity breach will occur for each of the three information segments, assuming no additional investment in cybersecurity. The third step is to estimate the productivity of an additional investment in cybersecurity ($S_i\left[z_i, v_i\right]$) to protect each specific information subset. The fourth step is to derive the optimal investment level for each information segment. In other words, the L_i, v_i, and $S_i\left[z_i, v_i\right]$ in the GL Model need to be estimated for each of the three (*i.e.*, customers, internal, and external) information segments. In essence, the plan is to estimate the optimal amount of additional investment in each of the three information segments and then sum these amounts to arrive at an initial total estimate for additional cybersecurity investments by ZLG Jewelry.

Table 1 provides the data associated with the above noted estimates. As illustrated in **Table 1**, the CIO, CISO and CFO, after talking to the firm's legal staff concerning potential liabilities resulting from cybersecurity breaches, estimate that the value of the information segments (*i.e.*, the estimated cost to the firm if a successful breach occurred to the information segments) to be $120,000,000, $60,000,000, and $20,000,000, for the three information segments (*i.e.*, customers information segment, the internal operations information segment, and the external operations information segment, respectively). Hence, the total value of information of the firm is $200,000,000. The CIO and CISO estimate that the

Table 1. The Information segments of ZLG and cybersecurity investments[a].

	With Segmentation				Without Segmentation	Economic Benefits of Information Segmentation
	Customers	Internal Operations	External Operations	Total		
Value of Information	$120,000,000	$60,000,000	$20,000,000	$200,000,000	$200,000,000	
Vulnerability	40%	20%	10%		31%	
Expected Loss Before Additional Investment	$48,000,000	$12,000,000	$2,000,000	$62,000,000	$62,000,000	
Optimal Investment	$2,280,000	$788,528	$180,000	$3,248,528	$3,321,363	$72,835
Expected Loss with Optimal Investment	$2,400,000	$848,528	$200,000	$3,448,528	$3,521,363	$72,835
Total Cybersecurity Costs	$4,680,000	$1,637,056	$380,000	$6,697,056	$6,842,726	$145,670

[a] The numbers of optimal investment, expected loss with optimal investment and total cybersecurity costs are generated based on security breach probability function $S(z,v)=\frac{v}{1+z/200000}$, where the optimal investment is $z^{*}=\sqrt{200000vL}-200000$, and rounded to the nearest dollars.

current probability of a breach (*i.e.*, without an additional investment in cybersecurity activities) to be 40%, 20%, and 10%, respectively for the three information segments.[16] Without information segmentation, the vulnerability is 31% (*i.e.*, the same as the weighted average of the vulnerability of all segments: $\left[(\$120000000\times 40\%+\$60000000\times 20\%+\$20000000\times 10\%)/\$200000000\right]$). The CIO and CISO together estimate the breach probability function for ZLG without information segmentation would be $S(z,v)=\frac{v}{1+\frac{1}{200000}z}$. With information segmentation, breach probability functions for the three information segments are $\frac{40\%}{1+\frac{1}{200000}\times\frac{z}{0.6}}$, $\frac{20\%}{1+\frac{1}{200000}\times\frac{z}{0.3}}$, and $\frac{10\%}{1+\frac{1}{200000}\times\frac{z}{0.1}}$. As shown in Table 1, solving for the optimal investments for each information segment, we get $2,280,000, $788,528 and $180,000 for the three information segments, respectively. The total cybersecurity investment from all segments is $3,248,528, which is less than the optimal investment in cybersecurity without segmentation ($3,321,363). The total expected losses from cybersecurity breach-

[16] The differences in the probability of a breach for the three information segments is due to the value of the information to potential hackers (*i.e.*, we assume that the value of an information segment is positively associated with the motivation and effort a hacker is willing to expend on stealing such information).

es with segmentation are $3448.528, which is less than the expected loss from cybersecurity breaches without segmentation ($3521.363). Thus, information segmentation leads to both lower total optimal investments in cybersecurity and lower expected losses from cybersecurity breaches.

5. Concluding Comments

Cybersecurity breaches have become a major concern to modern organizations operating in today's interconnected world of digital computer-based communication systems. In order to prevent, as well as recover, from these breaches, organizations need to invest in cybersecurity related activities. Given the exponential growth of developments related to the "Internet of Things (IoT)," the importance of investing in cybersecurity will only increase over the foreseeable future. Accordingly, a fundamental resource allocation question that needs to be addressed is: How much should our organization invest in cybersecurity?

Unfortunately, a simple, unequivocal, answer to the above question does not exist. Using cost-benefit analysis, however, is the best approach for determining the appropriate amount to invest. The main arguments presented in this paper have been that information segmentation can assist an organization derive the appropriate amount to invest in cybersecurity from a cost-benefit perspective and that the Gordon-Loeb Model provides a logical cost-benefit framework for incorporating information segmentation into cybersecurity investment decisions.

It is important for organizations to understand that investing in cybersecurity is best viewed as a process that focuses on preventing breaches where possible and minimizing the damage from breaches that occur. This process includes identifying the cybersecurity risks, the potential losses that may occur as a result of a breach and determining the appropriate actions and investments that are most likely to minimize any damage that could result from cybersecurity breaches. Since 100% security is unrealistic, especially from an economics perspective, a part of cybersecurity investments should be devoted to a recovery plan. Indeed, a critical component of an organization's efficient cybersecurity investment plan should be its plan for recovering from potential cybersecurity breaches.

There are, of course, many issues not discussed in this paper that have an effect on deriving the right amount to invest in cybersecurity. For example, if a company was doing business with the U.S. federal government, approaching cybersecurity risk in a manner that is consistent with the NIST Cybersecurity Framework ([29]) is essential [25]. Another issue that would directly affect the required level of cybersecurity investments would be various international, federal, state, and municipal compliance regulations. In this latter regard, if an organization was involved in business in Europe, compliance with the European's GDPR (General Data Protection Regulation) would be required (see [30]). While the model presented provided some insights concerning the benefits of information segmentation, a more comprehensive model of cybersecurity segmentation investments awaits further research. For example, a more general model would 1) take into account that segmentation may directly affect the organization's value of information and the expected losses from cybersecurity breaches, 2) explicitly consider the costs of implementing the segmentation of data, 3) consider the interactive effects among the segments due to their connectivity. Moreover, a general model of information segmentation would not treat the segments as exogenous, but determine the specification of the segments endogenously. The above limitations notwithstanding, we believe that the analysis and example discussed in this paper provide valuable insights that can go a long way in assisting organizations get a better handle on deriving the right amount to invest in cybersecurity related activities.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

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. https://doi.org/10.1145/581271.581274

[2] Dosal, E. (2019) What Are the Benefits of Network Segmentation? https://www.compuquip.com/blog/4-security-benefits-of-network-segmentation

[3] TrustNet (2020) Network Segmentation: Security Benefits and Best Practices. https://www.trustnetinc.com/network-segmentation/

[4] Velimirovic, A. (2020) 7 Network Segmentation Security Best Practices. https://phoenixnap.com/blog/network-segmentation-security

[5] Wang, S. (2017) Optimal Level and Allocation of Cybersecurity Spending: Model and Formula. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3010029 https://doi.org/10.2139/ssrn.3010029

[6] Xu, L., Li, Y.H. and Fu, J. (2019) Cybersecurity Investment Allocation for a Multi-Branch Firm: Modeling and Optimization. *Mathematics*, **7**, 587. https://doi.org/10.3390/math7070587

[7] Bodin, L.D., Gordon, L.A. and Loeb, M.P. (2005) Evaluating Information Security Investments Using the Analytic Hierarchy Process. *Communications of the ACM*, **48**, 78-83. https://doi.org/10.1145/1042091.1042094

[8] Smeraldi, F. and Malacaria, P. (2014) How to Spend It: Optimal Investment for Cyber Security. *Proceedings of the* 1*st International Workshop on Agents and Cyber-Security*, Paris, May 2014, Article No. 8. https://doi.org/10.1145/2602945.2602952

[9] Zhuo, Y.R. and Solak, S. (2014) Measuring and Optimizing Cybersecurity Investments: A Quantitative Portfolio Approach. *IIE Annual Conference. Proceedings*, Institute of Industrial and Systems Engineers, Peachtree Corners.

[10] Gordon, L.A., Loeb, M.P. and Sohail, T. (2003) A Framework for Using Insurance for Cyber-Risk Management. *Communications of the ACM*, **46**, 81-85. https://doi.org/10.1145/636772.636774

[11] Böhme, R. and Schwartz, G. (2010) Modeling Cyber-Insurance: Towards a Unifying Framework. https://www.econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf

[12] Herath, H. and Herath, T. (2011) Copula-Based Actuarial Model for Pricing Cyber-Insurance Policies. *Insurance Markets and Companies*: *Analyses and Actuarial Computations*, **2**, 7-20.

[13] Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A. (2017) Cyber-Insurance Survey. *Computer Science Review*, **24**, 35-61. https://doi.org/10.1016/j.cosrev.2017.01.001

[14] U.S Department of Homeland Security (2012) Cybersecurity Insurance Workshop Readout Report. National Protection and Programs Directorate, Washington DC. https://www.cisa.gov/sites/default/files/publications/November%202012%20Cybersecurity%20Insurance%20Workshop.pdf

[15] Bodin, L.D., Gordon, L.A., Loeb, M.P. and Wang, A. (2018) Cybersecurity Insurance and Risk-Sharing. *Journal of Accounting and Public Policy*, **37**, 527-544. https://doi.org/10.1016/j.jaccpubpol.2018.10.004

[16] Hoo, K.S. (2002) How Much Is Enough? A Risk Management Approach to Computer Security. *Workshop on the Economics of Information Security*. http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/06.doc

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

[18] 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. https://doi.org/10.1016/j.jaccpubpol.2004.12.003

[19] Hausken, K. (2006) Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment. *Journal of Accounting and Public Policy*, **25**, 629-665. https://doi.org/10.1016/j.jaccpubpol.2006.09.001

[20] Huang, C.D., Hu, Q. and Behara, R.S. (2008) An Economic Analysis of the Optimal Information Security Investment in the Case of a Risk-Averse Firm. *International Journal of Production Economics*, **114**, 793-804. https://doi.org/10.1016/j.ijpe.2008.04.002

[21] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2014) Externalities and the Magnitude of Cyber Security 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

[22] 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. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

[23] Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. and Smeraldi, F. (2016) Decision Support Approaches for Cyber Security Investment. *Decision Support Systems*, **86**, 13-23. https://doi.org/10.1016/j.dss.2016.02.012

[24] 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

[25] Gordon, L.A., Loeb, M.P. and Zhou, L. (2020) Integrating Cost-Benefit Analysis into the NIST Cybersecurity Framework via the Gordon-Loeb Model. *Journal of Cybersecurity*, **6**, tyaa005. https://doi.org/10.1093/cybsec/tyaa005

[26] Fanelli, B., Pessanha, R., Gwiazdowski, A., Chng-Castor, A. and Auger, G. (2017) 2017 State of Cyber Security among Small Businesses in North America, 1-24. https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf

[27] Haapamäki, E. and Sihvonen, J. (2019) Cybersecurity in Accounting Research. *Managerial Auditing Journal*, **34**, 808-834. https://doi.org/10.1108/MAJ-09-2018-2004

[28] Schechter, S.E. and Smith, M.D. (2003) How Much Security Is Enough to Stop A Thief? *International Conference on Financial Cryptography*, Guadeloupe, 27-30 January 2003, 122-137. https://doi.org/10.1007/978-3-540-45126-6_9

[29] National Institute of Standards and Technology (2018) National Institute of Standards and Technology. Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[30] European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC. http://data.europa.eu/eli/reg/2016/679/oj

Appendix: Summary of Gordon-Loeb Model

The equations described below, and the description of the variables used in these equations, are the same as those in the Gordon and Loeb (2002), and Gordon *et al.* (2016). The first equation is a representation of the expected benefits of an investment in information security (*i.e.*, cybersecurity), denoted as EBIS. The firm's EBIS results from reducing the probability of a breach based on the productivity function for an investment, *z*, as shown below:

$$\text{EBIS}(z) = \left[v - S(z,v)\right]L. \qquad \text{[A1]}$$

Since v and L are parameters for a given information set, z is the firm's only decision variable, and EBIS is written above as a function of *z*. The second equation represents the expected net benefits from an investment in information security, ENBIS, and equals EBIS less the amount of the cybersecurity investment, *z*, as shown below:

$$\text{ENBIS}(z) = \left[v - S(z,v)\right]L - z\,. \qquad \text{[A2]}$$

Denote $z^* = \arg\max\left\{\left[v - S(z,v)\right]L - z\right\} = \arg\min\left[S(z,v)L + z\right]$. That is, the investment z^* that maximizes ENBIS minimizes the total expected cost of a cybersecurity breach (*i.e.*, the revised measure of v after investing *z*, plus the plus amount of the cybersecurity investment, *z*). The optimal investment, z^* is characterized in Equation [A3], where the expected marginal benefits from investing in cybersecurity (*i.e.*, left hand side of [A3]) is equal to the expected marginal cost of the investment (right hand side of [A3]).[17]

$$-S_z\left(z^*,v\right)L = 1 \qquad \text{[A3]}$$

Gordon and Loeb (2002) proved (Proposition 3, p. 451) that for two broad classes of security breach probability functions, the optimal level would be less than or equal to *vL*/*e*, or roughly 37% of the expected loss from a security breach, as shown in Equation [A4] below:

$$z^*(v) \le \left(\frac{1}{e}\right)vL. \qquad \text{[A4]}$$

The GL Model was extended to include externalities in Gordon *et al.* (2014). Let L^P represent the private costs to an organization from a cybersecurity breach, L^E represent the cost of externalities to other organizations and individuals from the firm's cybersecurity breach, and L^{SC} represent the total social costs from the firm's cybersecurity breach. Thus, $L^{SC} = L^P + L^E$. Gordon *et al.* (2014, p. 8)) demonstrate the revised version of [A4] for the social optimal cybersecurity level considering externalities, denoted as z^{SC}, as shown in Equation [A5] below:

$$z^{SC}(v) \le (1/e)\left[1 + \left(L^E/L^P\right)\right]vL^P \qquad \text{[A5]}$$

[17] There are no fixed costs in the GL Model's analysis and z represents cybersecurity investment in dollars. The price of each unit of z is equal to $1.