JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2020, 1–8
doi: 10.1093/cybsec/tyaa005
Research paper

Research paper

Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model

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

Department of Accounting and Information Assurance, Robert H. Smith School of Business, University of Maryland, College Park, MD, 20742-1815, USA

*Correspondence address. Department of Accounting and Information Assurance, Robert H. Smith School of Business, University of Maryland, College Park, MD, 20742-1815, USA. Tel: 301-405-2209; E-mail: mloeb@rhsmith.umd.edu

Received 10 September 2019; revised 14 December 2019; accepted 23 January 2020

Abstract

The National Institute for Standards and Technology (NIST) Cybersecurity Framework has rapidly become a widely accepted approach to facilitating cybersecurity risk management within organizations. An insightful aspect of the NIST Cybersecurity Framework is its explicit recognition that the activities associated with managing cybersecurity risk are organization specific. The NIST Framework also recognizes that organizations should evaluate their cybersecurity risk management on a cost–benefit basis. The NIST Framework, however, does not provide guidance on how to carry out such a cost–benefit analysis. This article provides an approach for integrating cost–benefit analysis into the NIST Cybersecurity Framework. The Gordon–Loeb (GL) Model for cybersecurity investments is proposed as a basis for deriving a cost-effective level of spending on cybersecurity activities and for selecting the appropriate NIST Implementation Tier level. The analysis shows that the GL Model provides a logical approach to use when considering the cost–benefit aspects of cybersecurity investments during an organization's process of selecting the most appropriate NIST Implementation Tier level. In addition, the cost–benefit approach provided in this article helps to identify conditions under which there is an incentive to move to a higher NIST Implementation Tier.

Key words: NIST Cybersecurity Framework; cybersecurity investments; cybersecurity economics

Introduction

The development of the Internet and other interconnected digital computer networks has transformed the interactions among people, organizations, and countries. Although most would probably agree that this transformation has been positive, on balance, a clear downside of the world of interconnected digital communications systems has been the varied problems associated with actual and potential cybersecurity breaches.[1,2] Accordingly, cybersecurity risk management has become a critical concern to nations, organizations, and societies around the world. In the USA, this concern has been clearly recognized by the last three Presidents. President Bush, for example, initiated the US National Strategy to Secure Cyberspace in 2003 [6]. President Obama recognized the importance of cybersecurity in his Executive Order (EO) 13636, issued on 12 February 2013, formally titled "Improving Critical Infrastructure Cybersecurity" [7]. As noted in Section 1 of EO 13636:

> The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical

1 For the purposes of this article, the term "cybersecurity" refers to the protection of information transmitted and stored over the Internet or any other computer-based network.

2 Although beyond the scope of this article, a large body of literature has evolved that addresses the impact of cybersecurity breaches (in terms of stock market returns and other costs) on organizations and people (e.g., see [1–5]).

> infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil rights.

One of the key components of EO 13636 is the requirement that the US National Institute for Standards and Technology (NIST), which is part of the US Department of Commerce, develop a Cybersecurity Framework that includes "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks" (Section 7, part [a]). NIST was tasked with publishing this Cybersecurity Framework within 1 year from the date of EO 13636. NIST published Version 1.0 of the Cybersecurity Framework (formally entitled the "Framework for Improving the Critical Infrastructure Cybersecurity," but usually referred to as the "NIST Cybersecurity Framework") on 12 February 2014 [8]. The fundamental concern underlying the NIST Cybersecurity Framework is managing cybersecurity risk in a cost–benefit manner. Furthermore, the Framework explicitly recognizes that different organizations have different cybersecurity risk management needs that result in requiring different types and levels of cybersecurity investments.

President Trump gave the NIST Cybersecurity Framework a tremendous boost when he issued EO 13800 entitled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," on 11 May 2017 [9]. In Section 1, part (c), under (ii), EO 13800 states that "Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk." By requiring government agencies to use the NIST Cybersecurity Framework, President Trump made the Framework the law of the land for federal government agencies. In addition, since an information system is only as strong as its weakest link, federal agencies realize that even if they were using the NIST Cybersecurity Framework, unless their contractors (i.e., firms doing business with the federal government agencies) were managing their cybersecurity risk in a manner that is consistent with the NIST Cybersecurity Framework, their compliance with EO 13800 could be jeopardized. Thus, an externality (i.e., spillover effect) of EO 13800 is that companies wanting to conduct business with the US federal government need to either use the NIST Cybersecurity Framework or use an alternative cybersecurity risk management framework that is consistent with the NIST Framework. Indeed, companies not using a cybersecurity risk management framework that is consistent with the NIST Cybersecurity Framework may find themselves being excluded from receiving government contracts.

On 16 April 2018, NIST published Version 1.1 of the Cybersecurity Framework (NIST, 2018). As noted in the 1.1 Version of the NIST Cybersecurity Framework ([10], p. 2):

> The Framework is not a one-size fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customized practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

As pointed out in the next section of this article, the NIST Cybersecurity Framework has been widely adopted by companies and government agencies in the USA, as well as around the world. Indeed, the NIST Cybersecurity Framework has rapidly become one of the, if not the, most widely accepted approaches to facilitate cybersecurity risk management within organizations.

The NIST Cybersecurity Framework is intentionally broad and flexible. In essence, it provides a macro overview of how organizations should approach cybersecurity risk management, leaving the details of the implementation of the Framework to each firm. This latter point is especially true in terms of how a firm should consider the cost–benefit aspects of cybersecurity risk management when deciding on the organization's appropriate Framework Implementation Tier. Although the NIST Framework notes that organizations should maximize the impact of each dollar spent, it lacks specificity and thus is ambiguous in terms of guidance on how to carry out this investment prioritization. Instead, NIST leaves it up to each organization to decide how to maximize the impact of the dollars spent on cybersecurity risk management. The above notwithstanding, NIST clearly recommends that organizations should maximize the impact of the dollars spent on their cybersecurity investments based on cost–benefit analysis.[3]

The objective of this article is to provide a logical approach for integrating cost–benefit analysis into the NIST Cybersecurity Framework. The recommended approach is based on the Gordon–Loeb Model (hereafter referred to as the GL Model) for cybersecurity investments [11, 12]. Since the Implementation Tiers discussed in the NIST Cybersecurity Framework provide organizations with a blueprint for addressing cybersecurity risk management, the specific focus in carrying out the above-noted objective will be to show how the GL Model can help organizations integrate cost–benefit analysis into the process of selecting the most appropriate NIST Implementation Tier level. As a result, the relationship between the NIST Implementation Tier levels and a firm's appropriate level of spending on cybersecurity activities becomes much clearer. To our knowledge, this is the first study to explicitly integrate a cost–benefit model into the NIST Cybersecurity Framework. Thus, the major contribution of this article is that it helps eliminate, or at least reduce, the ambiguities associated with maximizing the impact of dollars spent on cybersecurity risk management.

The remainder of this article proceeds as follows. In the "Literature review" section of the article, we briefly review the relevant literature, including the NIST Cybersecurity Framework, and the GL Model for cybersecurity investments. "Integrating the GL Model into the NIST Framework" section focuses on integrating cost–benefit analysis via the GL Model into the NIST Cybersecurity Framework and provides a numerical example that demonstrates this integration. "Concluding comments" section of the article provides some concluding comments.

Literature review

Cybersecurity risk management

Cybersecurity risk refers to the probability (or possibility) that a potentially harmful event will result from deficient cybersecurity. Cybersecurity risk management is concerned with the process of managing cybersecurity risk. There is a large and growing body of

3 More will be said about this point in the next section of this article.

literature that addresses issues related to cybersecurity risk management. Given the pervasive impact of digital computer-based information systems on every conceivable discipline, the discussions on the topic of cybersecurity risk management vary widely. Indeed, these discussions have focused on such issues as defining cybersecurity risk [13], developing a taxonomy of cybersecurity risk [14, 15], developing a framework for cybersecurity risk management [8, 10, 16], information security policy [17, 18], and the economics of managing cybersecurity [19–25]. Of course, a comprehensive approach to cybersecurity risk management requires an understanding of all the issues noted above and therefore it is not surprising that many of the aforementioned references address several of the issues underlying cybersecurity risk management.

The emphasis of the analysis contained in this article is focused on the economics of cybersecurity risk management applied to the NIST Cybersecurity Framework. This focus is particularly relevant and timely due to the fact that the NIST Cybersecurity Framework has become one of the most widely accepted approaches to cybersecurity risk management among organizations in both the private and public sectors of the US economy. As noted in the Introduction of this article, US federal government agencies are required to use the NIST Cybersecurity Framework, and companies wanting to do business with these agencies need to approach cybersecurity risk management in a manner consistent with the NIST Framework. This framework has also been well-received among organizations in countries other than the US, as noted in the subsequent subsection.

NIST Cybersecurity Framework[4]

When President Trump issued EO 13800, the NIST Cybersecurity Framework became the law of the land for US federal government agencies and firms wishing to do business with these agencies. Since then, the impact of the NIST Framework has been expanding [26]. According to NIST (see: https://www.nist.gov/industry-impacts/cybersecurity), "Companies from around the world have embraced the use of the Framework, including JP Morgan Chase, Microsoft, Boeing, Intel, Bank of England, Nippon Telegraph and Telephone Corporation, and the Ontario Energy Board." Many government agencies in countries other than the USA have also embraced the NIST Cybersecurity Framework.

The overall focus of the NIST Cybersecurity Framework is to assist organizations to carry out the process of cybersecurity risk management. The three major components of the Framework are the Core, Implementation Tiers, and Profiles. The Core consists of a set of cybersecurity activities that are intended to result in specific cybersecurity outcomes. These activities are specified in terms of the following five basic functions: Identify, Protect, Detect, Respond, and Recover. The Profiles refer to the "the alignment of the Functions, Categories and Subcategories with the business requirements, risk tolerance, resources of the organization" ([10], p.11). Profiles provide the required plan for reducing an organization's cybersecurity risk.

The Framework's Implementation Tiers summarize the way "... an organization views its cybersecurity risk and the processes in place to manage such risk" ([10], p. 8). Organizations can be at one of the following four-tier levels: Tier 1 (Partial), Tier 2 (Risk Informed), Tier 3 (Repeatable), and Tier 4 (Adaptive). As stated by NIST ([10], p. 8), "Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices." In other words, the rigor and sophistication of an organization's risk management process increase as it moves from Tier 1 toward Tier 4.

Organizations at Tier 1 (Partial) do not have a formalized integrated cybersecurity risk management process and tend to be reactive rather than proactive toward cyber risk management. In addition, organizations at Tier 1 tend to have little interaction with other firms and/or professional cybersecurity groups (e.g., an Information Sharing Analysis Center) concerning cybersecurity risk management. Organizations at Tier 2 (Risk Informed) tend to have a formal, loosely integrated, risk management process, but enforcement of the process as an organization-wide policy is lacking. Tier 2 organizations also tend to have limited interactions with other firms and/or professional cybersecurity groups concerning cybersecurity risk management.

Tier 3 (Repeatable) organizations have formal, integrative risk management processes, as well as formal channels of communication with other firms and professional cybersecurity groups concerning cybersecurity risk management. These organizations are proactive, as well as reactive, in terms of their cybersecurity risk management. Tier 4 (Adaptive) organizations also have formal, integrative risk management processes, as well as formal channels of communication with other firms and professional groups concerning cybersecurity risk management. In addition to the proactive and reactive approaches, Tier 4 organizations take an adaptive approach to cybersecurity risk management. Thus, these organizations are continuously monitoring changes in the cybersecurity threats confronting them and revising their recovery plans to accommodate these changes. The financial and operating implications of the requisite changes in the recovery plans are also explicitly considered by organizations at Tier 4.

The four Tiers associated with the NIST Cybersecurity Framework provide organizations with an overview of how to view their cybersecurity risk management process and what needs to be done to move to a higher tier. The Tiers also provide a vehicle for analyzing the financial commitments associated with an organization's approach to cybersecurity risk management. As stated by NIST ([10], p. 15), "The tier selection process considers an organization's current risk management practices, business/mission objectives, supply chain cybersecurity requirements, and organizational constraints."

Although higher Tiers indicate a higher level of rigor and an increased level of sophistication of cybersecurity risk management, it does not necessarily follow that all organizations should strive to be at the highest Tier level. The benefits derived from reaching a higher Tier are not costless. In other words, there are clearly higher costs associated with moving to a higher Tier level. Thus, the appropriate Tier is organization-specific and dependent on the cost–benefit aspects of the cybersecurity risk management process for an organization. As NIST ([10], p. 8) clearly notes, "Progression to higher Tiers is encouraged when cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk." For small firms (defined in terms of revenues, employees, and online transactions), Tier 1 or 2 may be the right tier from a cost–benefit perspective. In contrast, large, publicly traded firms would likely want to reach Tier 3 or 4. The size distinction becomes apparent when one considers the fact that getting to Tier 3 or

4 This overview of the NIST Cybersecurity Framework is based on Version 1.1 of the Framework [10].

4 would likely involve adding a large amount of fixed costs (e.g., hiring a Chief Information Security Officer in addition to a Chief Information Officer) that would likely to be too costly for a small firm.[5]

GL Model

NIST's recommendation that organizations should consider the cost–benefit aspects of progression to a higher Tier level is essentially suggesting that organizations need some sort of economic model or framework to answer the following question: How much should be invested in cybersecurity risk management? One economic model that directly addresses this question and that has received wide acceptance among practitioners and academicians concerned with cybersecurity is the GL Model. In 2011, e.g., the GL Model was featured in *The Wall Street Journal* [27]. In discussing this Model, AFCEA International Cyber Committee [28] noted that "the Gordon-Loeb model has become the 'gold standard' in the cyber economic models." The 2017 report by the US Council of Better Business Bureaus concerning issues surrounding cybersecurity in small businesses in North America concluded that the GL Model is a "useful guide for organizations trying to find the right level of cybersecurity investment" ([29], p. 20). In their game-theoretic analysis of how uncertainties related to cybersecurity risk affect cybersecurity investments, Fielder *et al.* ([30], p. 2) noted that "The seminal work of Gordon and Loeb presents an economic model that determines the optimal amount to invest to protect a given set of information." Iannacone and Bridges ([31], p. 11), in their discussion of economic models focused on cost–benefit analysis of cybersecurity measures, referred to the GL Model as being "the most influential model."[6]

The GL Model assumes that organizations are vulnerable to cybersecurity breaches (i.e., 100% security is not possible from a practical perspective) and this vulnerability (denoted as v), is essentially the probability of a breach to an organization's information.[7] Since the GL Model is a one-period model, v represents the probability of a breach over a fixed time period such as 1 year. The value of an organization's information represents the potential monetary loss (denoted as L) to the organization that could result from a cybersecurity breach. Thus, vL represents the expected loss from a cybersecurity breach. However, investments in cybersecurity (denoted as z), can reduce the probability of a beach and, in turn, the expected loss from a breach. The "security breach probability function" [denoted as $s(z,v)$] represents the revised vulnerability after some level of cybersecurity investment (z). Accordingly, there are three major components that underlie the GL Model: (i) the value of the information being protected, L, (ii) the vulnerability (including threats) or probability that an organization's information will experience a cybersecurity breach before any additional cybersecurity investments, v, and (iii) the productivity function underlying the way investments in cybersecurity-related activities reduce the vulnerability that a cybersecurity breach will occur, $s(z,v)$. A basic assumption of the GL Model is that, for a given vL, the benefits derived from additional investments in cybersecurity (i.e., the reduction in expected loss from a cybersecurity breach) are increasing at a decreasing rate (i.e., $s_z = \frac{\partial s(z,v)}{\partial z} < 0$ and $s_{zz} = \frac{\partial^2 s(z,v)}{\partial z^2} > 0$).

Based on the above, the expected benefits from an investment (z) in cybersecurity, denoted as $EBC(z)$, can be generically denoted as shown in Equation (1) below:

$$EBC(z) = [v - s(z,v)]L. \quad (1)$$

The expected net benefits from an investment in cybersecurity can be generically denoted as shown in Equation (2) below:

$$ENBC(z) = [v - s(z,v)]L - z. \quad (2)$$

As shown in Gordon and Loeb (2002) for two broad classes of security breach probability functions, the optimal level of investment in cybersecurity, z^*, for a given information set, can be described by inequality (3) shown below[8]:

$$z^*(v) \leq (1/e)vL. \quad (3)$$

Since e is equal to 2.7182, Gordon and Loeb [11] were able to show that organizations should generally invest less than 37% of the expected loss from a cybersecurity breach. In addition, they were able to show that the optimal level of cybersecurity investment does not always increase with the level of vulnerability.

The following four-step approach can be used to implement the GL Model.

Step 1: Estimate the value of the information being protected, which also represents the potential loss (L).

Step 2: Estimate the probability that the information will be breached (i.e., estimate the information's vulnerability [v] to a successful attack).

Step 3: Combine the first two steps such that the expected loss is derived.

Step 4: Allocate cybersecurity investments to the information to be protected, based on the productivity of the investments and the cost of the investments (i.e., based on cost–benefit analysis).[9]

5 In a large publicly traded firm, it is possible to think of different subunits of the firm as having differing cybersecurity risk management needs. Accordingly, Tier 1 or 2 may provide enough cybersecurity protection for the information set in one subunit of a firm, whereas for another subunit it may be desirable to reach Tier 3 or 4 in terms of cybersecurity protection of the information set of that subunit. For simplicity, our discussion assumes that there is one appropriate Implementation Tier level for the entire firm (see Footnote 9 below) for more on the issue of information set segmentation.

6 There are other ways of computing the cost–benefit aspects of progressing from one NIST Tier level to a higher Tier level. However, in addition to being the most widely recognized cybersecurity investment model, the GL Model is directly linked to cybersecurity risk management in that it considers how cybersecurity investments reduce the vulnerability (or probability) of a cybersecurity breach.

7 Technically speaking, the probability of a breach is derived from the combination of the vulnerability and the threat of a breach. However, for notational simplicity, the GL Model allows the vulnerability of a breach to incorporate the notion of threat.

8 Baryshnikov [32] and Lelarge [33, 34] generalized the results by Gordon and Loeb [11] to a large array of security breach probability functions.

9 For a quantitative illustration of using the GL Model based on the above four steps [12]. Although the article that contains the original development of the GL Model (i.e., [11]) did not consider the potential interdependencies associated with an organization having multiple information sets, the follow-up article [12], illustrated the four steps for the generalized case where an organization's information set is segmented into information subsets. Such segmentation is beneficial when deriving the amount to invest in cybersecurity. The four steps described above for implementing the GL Model would be slightly different for the case with multiple subsets of information. Specifically, Step 1 would involve estimating the values associated with the various subsets of the information being protected. Step 2 would involve estimating the probabilities that the different information subsets would be breached. These probabilities would likely vary for different subsets of information. Step 3 would involve combining the first two steps such that a grid would be derived that is made up of expected losses, ranging from low value, low probability, of a breach to high value, high probability of a breach. Step 4 would involve allocating cybersecurity

Integrating the GL Model into the NIST Framework

Concepts

The fundamental question addressed in the GL Model is: How much should be invested in cybersecurity? Deciding on the appropriate NIST Tier level utilizing cost–benefit analysis essentially requires answering the same question. Following Gordon and Loeb [11, 12], we denote the value of the information being protected as L, the probability of a cybersecurity breach as v, investment in cybersecurity as z, and the security breach probability function as $s(z, v)$. Consequently, the expected loss from a cybersecurity breach is equal to vL.

The NIST Framework described in "Literature Review" section includes four Tiers, where the rigor and sophistication of an organization's risk management process increase as the organization moves from Tier 1 to Tier 4. We denote the cybersecurity investment required to adopt Tier i as z_{T_i}, where $i = 0,\ 1,\ 2,\ 3,\ 4$, respectively.[10] Since the level of investment in cybersecurity activities will have to increase as the rigor and sophistication of an organization's risk management process increases (i.e., cybersecurity investments are an increasing function of the Tier level), for a given firm we can state that: $0 = z_{T_0} < z_{T_1} < z_{T_2} < z_{T_3} < z_{T_4}$.

The Tier level a firm adopts should be a decision based on cost–benefit analysis, as pointed out by NIST ([10], p. 8). More to the point, for a firm to move from a particular T_i to the next tier T_{i+1}, the incremental benefits must be greater than the incremental costs. Since the incremental benefits come from the reduction in expected loss from security breaches $\left[s(z_{T_i}, v) - s(z_{T_{i+1}}, v)\right]L$, and the incremental costs come from the additional investment $(z_{T_{i+1}} - z_{T_i})$, a firm should only move to the next Tier if: $\left[s(z_{T_i}, v) - s(z_{T_{i+1}}, v)\right]L \geq z_{T_{i+1}} - z_{T_i}$. Rearranging this inequality yields inequality (4) below:

$$L \geq \frac{z_{T_{i+1}} - z_{T_i}}{\left[S(z_{T_i}, v) - S(z_{T_{i+1}}, v)\right]}. \tag{4}$$

We thus see that L (i.e., the value of the firm's information) is a critical element of a firm's decision to move to a higher Tier.

Define L_i as the minimum value of information necessary for a firm to move from Tier $i-1$ to Tier i, i.e.,

$$L_i = \frac{z_{T_i} - z_{T_{i-1}}}{\left[s(z_{T_{i-1}}, v) - s(z_{T_i}, v)\right]},\ \text{where}\ i = 1,\ 2,\ 3,\ 4. \tag{5}$$

Proposition: Assume $s_z = \frac{\partial s(z,v)}{\partial z} < 0$ and $s_{zz} = \frac{\partial^2 s(z,v)}{\partial z^2} > 0$ (i.e., the benefits derived from additional investments in cybersecurity are increasing at a decreasing rate), then

$$L_4 > L_3 > L_2 > L_1.$$

Proof:

Since $z_{T_{i-1}} < z_{T_i} < z_{T_{i+1}}$, we can write z_{T_i} as

$$z_{T_i} = tz_{T_{i-1}} + (1-t)z_{T_{i+1}} \tag{6}$$

for some $t \in (0, 1)$.

Given that $s_{zz} > 0$, it follows that

$$s(z_{T_i}, v) < ts(z_{T_{i-1}}, v) + (1-t)s(z_{T_{i+1}}, v). \tag{7}$$

We can rewrite Equation (6) as

$$\begin{aligned} tz_{T_i} + (1-t)z_{T_i} &= tz_{T_{i-1}} + (1-t)z_{T_{i+1}}, \\ t(z_{T_i} - z_{T_{i-1}}) &= (1-t)(z_{T_{i+1}} - z_{T_i}). \end{aligned} \tag{8}$$

Similarly, we can rewrite inequality (7) as

$$ts(z_{T_i}, v) + (1-t)s(z_{T_i}, v) < ts(z_{T_{i-1}}, v) + (1-t)s(z_{T_{i+1}}, v).$$

Given $s_z < 0$, it follows that

$$t\left[s(z_{T_{i-1}}, v) - s(z_{T_i}, v)\right] > (1-t)\left[s(z_{T_i}, v) - s(z_{T_{i+1}}, v)\right] > 0. \tag{9}$$

Combining Equations (8) and (9), we have

$$\frac{z_{T_{i+1}} - z_{T_i}}{\left[s(z_{T_i}, v) - s(z_{T_{i+1}}, v)\right]} > \frac{z_{T_i} - z_{T_{i-1}}}{\left[s(z_{T_{i-1}}, v) - s(z_{T_i}, v)\right]}. \tag{10}$$

i.e., $L_{i+1} > L_i$. Hence, $L_4 > L_3 > L_2 > L_1$. ■

The Proposition shows that, for a specific v, the value of the information must be sufficiently large for a firm to move to a higher Tier. The more valuable the information, the more likely that it is cost–beneficial for a firm to move to a higher Tier.

More generally, the above results show that a firm's decision to move to a higher Tier level in the NIST Cybersecurity Framework, based on cost–benefit analysis, is dependent on v and L for a given security breach probability function. The firm's optimal level of investment, denoted as z^*, depends on the nature of the security probability function at the initial vulnerability level, v. In particular, the value of z^*depends on the productivity (effectiveness) of investments at the initial vulnerability level.[11]

Define $T(z^*)$ as the NIST tier level achieved when the firm invests z^*. For $T(z^*)$ with Tier values 0, 1, 2, or 3, define $T^+(z^*)$ as the Tier level immediately above $T(z^*)$. If a firm is investing z^* and hence operating at Tier $T(z^*)$, the firm should only increase investment to achieve Tier $T^+(z^*)$ if there are additional benefits incentivizing the firm to achieve the next higher NIST Tier level. For example, there may be potential supply chain partners, other businesses, government agencies, and individuals who would only deal with firms that have achieved a NIST Tier level that is higher than the initial optimal Tier level associated with z^*. In other words, a firm would estimate the value of the expected increase in benefits from added business from achieving the next highest Tier level. Denote this increase in expected benefits as B. More specifically, the firm would make the investment to move up to the next Tier level when:

$$\left[s(z^*, v) - s(z_{T^+(z^*)}, v)\right]L + B > z_{T^+(z^*)} - z^*. \tag{11}$$

investments to the subsets of information to be protected based on the productivity of the investments (i.e., the benefits derived from additional investments) related to each subset of information and the costs of the investments being allocated to each information set (i.e., based on cost–benefit analyses).

10 Although the NIST Framework only has four Implementation Tiers, for notational convenience, we denote T_0 as a firm's inherent cybersecurity status without any uniquely focused cybersecurity investments. It follows that $z_{T_0} = 0$, and $s(z_{T_0}, v) = s(0, v) = v$.

11 For a class of exponential power security probability functions, Wang [35] defines an explicit effectiveness index. The value of this index has implications for the selection of z^* and consequently for the selection of a NIST Tier level. As pointed out in Wang [35], one would expect the value of the effectiveness index of smaller firms to be high. The high value reflects a compelling reason for these firms to increase investment in cybersecurity activities as basic cybersecurity measures would represent low-hanging fruit.

Table 1. Optimal cybersecurity investments (z^*) in millions for different values of L and v

Value of information set (L) (in millions)	Vulnerability (v)		
	0.1	0.3	0.5
1	0	0	0
10	0	0.45	1.16
20	0.00	1.46	2.47
30	0.45	2.24	3.48
40	0.83	2.90	4.32
50	1.16	3.48	5.07
60	1.46	4.00	5.75
70	1.74	4.48	6.37
80	2.00	4.93	6.94
90	2.24	5.35	7.49
100	2.47	5.75	8.00
110	2.69	6.12	8.49
120	2.90	6.49	8.95
130	3.10	6.83	9.40
140	3.29	7.17	9.83
150	3.48	7.49	10.25

Rearranging terms in Equation (11), gives:

$$B > \; z_{T^+(z^*)} - z^* - \left[s(z^*, v) - s(z_{T^+(z^*)}, v)\right] L \; . \tag{12}$$

That is, if the value of the expected increase in benefits from added business from achieving the next highest Tier level is greater than the right-hand side of Equation (12), the firm is motivated to increase their investments in cybersecurity activities to achieve the next highest Tier level. Thus, the NIST Framework may be able to incentivize firms to increase their investment in cybersecurity.

Example

We now provide a numerical example of the above approach. In this example, we assume that $s(z, v) = \frac{v}{(1+\frac{z}{2})}$, which is one of the two security breach probability functions examined in Gordon and Loeb [11] and the one illustrated in Gordon *et al.* [12]. Accordingly, we can minimize the total expected costs $\frac{v}{(1+\frac{z}{2})} L + z$ to obtain the optimal cybersecurity investment level (z^*). It can be easily be shown that $z^* = \sqrt{2vL} - 2$ is the optimal cybersecurity investment value.[12] For the purpose of this example, let us assume that $z_{T_1} = \$0.1M$, $z_{T_2} = \$1M$, $z_{T_3} = \$3M$ and $z_{T_4} = \$7M$.

Table 1 presents the levels of optimal cybersecurity investment (z^*), when $v = 0.1$, 0.3, or 0.5 and L ranges from \$1M to \$150M. When both v and L are small, e.g., $v = 0.1$ and $L = \$1M$, the optimal investment in cybersecurity is 0, because the benefits from such investments do not outweigh the costs. As v and L increase in this example, the expected loss from a cybersecurity breach (vL) and the optimal investment amount (z^*) also increase.

Figure 1 illustrates the information provided in Table 1. As can be seen from the figure, for a given v, as L increases, z^* also increases. It is also clear that the optimal investment levels generally fall between two different NIST Tier levels. In our example, the expected loss from a breach would have to be equal to, or greater than, \$40.5M (i.e., for $v = 0.5$, $L \geq \$81M$, for $v = 0.3$, $L \geq \$135M$, for $v = 0.1$, $L \geq \$405M$) to justify the firm investing \$7M to reach the NIST Tier 4 level of cybersecurity. Figure 2 illustrates the minimum level of L for different Tier levels, at $v = 0.3$.

From a cost–benefit perspective, it would not be appropriate for a firm to strive to reach a Tier level that is above the optimal level of investment $[T(z^*)]$ without sufficient additional benefits being generated by achieving the next higher Tier level. For a given combination of v and L, we can calculate the additional benefits needed to incentivize a firm achieving the next Tier level. For example, when $v = 0.3$ and $L = \$72.6M$, the optimal cybersecurity investment $z^* = \$4.6M$. This puts the firm at NIST Tier 3 since $z_{T_3} < z^* < z_{T_4}$. Without additional benefits due to reaching a higher tier level, it is not cost-beneficial for the firm to spend \$7M to reach NIST Tier 4. The additional benefits needed to achieve NIST Tier 4 are:

$$B > \$7M - \$4.6M - \left(\frac{0.3}{1+4.6/2} - \frac{0.3}{1+7/2}\right)\$72.6M \approx \$0.64M.$$

In other words, if the firm estimates that achieving NIST Tier 4 would result in at least \$0.64M additional benefits, it should invest the \$7M to reach NIST Tier 4.

The values for v and L in the example (i.e., 0.1, 0.3, 0.5 for v, and values between \$1M and \$150M for L) were chosen for illustrative purposes. Of course, other values could have been selected. However, this example demonstrates the process by which a firm could conduct a simulation around different values of v and L so as to provide a clearer picture of the appropriate NIST Tier level of cybersecurity for a firm.

The above example illustrates the fact that the appropriate cost-effective NIST Implementation Tier level for a firm is dependent on the same three major components that underlie the GL Model. More specifically, the cost-effective Tier level is dependent on: (i) the value of the information being protected (L), (ii) the vulnerability (or probability of a cybersecurity breach to that information [v]), and (iii) the productivity of the investments in cybersecurity activities [$s(z, v)$].

If budget constraints prevent an organization from spending the optimal amount for a given vL, the organization may have to settle for less than its ideal Tier level (at least until additional funds could be allocated to cybersecurity activities). Resource constraints are particularly relevant for small businesses. In fact, based on its study of small businesses in North America, the Report by the Better Business Bureau ([29], p. 12) pointed out that the "...lack of resources is the number one challenge these businesses face in adopting cybersecurity practices."

Concluding comments

Managing cybersecurity risk has taken center stage in organizations within the private and public sector of industrialized economies around the world. Indeed, in today's interconnected digital world, managing cybersecurity risk has become a critical component of an organization's enterprise risk management program. The NIST Cybersecurity Framework has been instrumental in providing a common language and approach for organizations to use as they strive to improve the way they manage cybersecurity risks.

12 We derive the optimal cybersecurity investment amount, for the productivity function $s(z, v) = \frac{v}{(1+\frac{z}{2})}$, by minimizing the sum of expected loss from a security breach and the cost of investment. That is,

$$\min_z \frac{v}{(1+\frac{z}{2})} L + z.$$

The first order condition is

$$\frac{\partial \frac{v}{(1+\frac{z}{2})} L}{\partial z} = -1.$$

Solving for z, we have $z^* = \sqrt{2vL} - 2$.

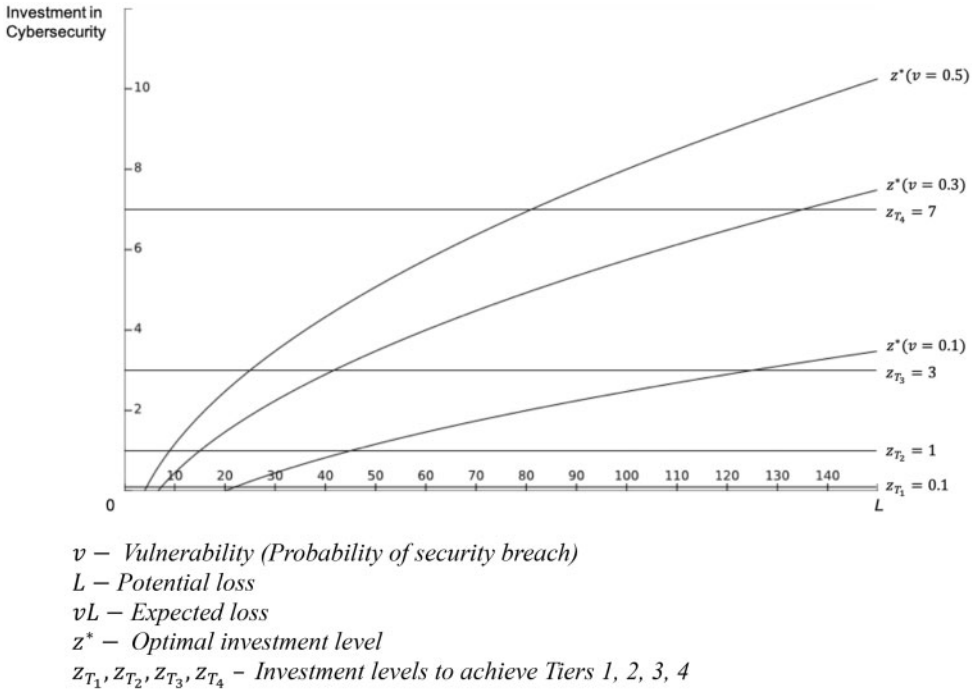

Figure 1. Optimal cybersecurity investments for different values of *L* and *v*, and NIST tier levels.

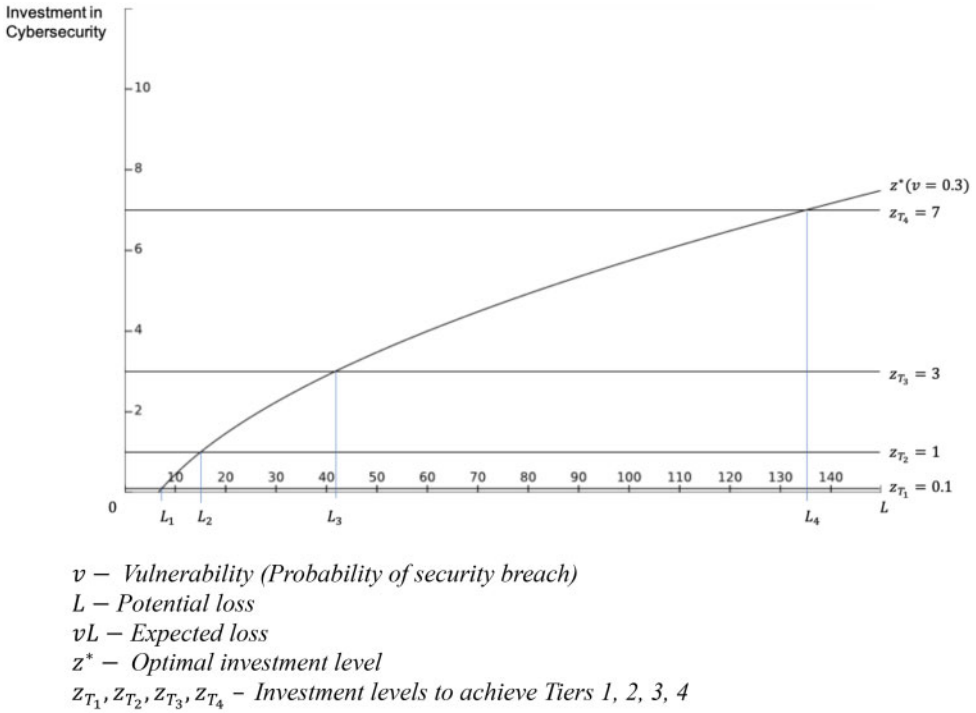

Figure 2. Determining critical *L* in applying NIST framework.

An insightful aspect of the NIST Cybersecurity Framework is its explicit recognition that the activities associated with managing cybersecurity risk are organization-specific. NIST also recognized that organizations need to evaluate their cybersecurity risk management needs on a cost–benefit basis [i.e., "...prioritize investments to maximize the impact of each dollar spent" ([10], p. 2)]. The NIST Cybersecurity Framework does not, however, provide guidance on how to carry out the above-noted cost–benefit analysis.

The objective of the analysis contained in this article has been to provide an approach for integrating cost–benefit analysis into the NIST Cybersecurity Framework. The focus of this integration has been on using the GL Model [11, 12] for cybersecurity investments as a basis for deriving a cost-effective level of spending on cybersecurity activities and selecting the NIST Implementation Tier level based on this cost-effective spending level. Specifically, it was shown that the GL Model provides a logical approach to use when

considering the cost–benefit aspects of cybersecurity investments during the process of selecting the most appropriate NIST Implementation Tier level for an organization. In fact, it was shown that the cost-effective NIST Implementation Tier level for a firm depends on the same three major components that form the basis of the GL Model: (i) the value of the information being protected, (ii) the vulnerability (or probability) of a cybersecurity breach to that information, and (iii) the productivity of the investments in cybersecurity activities. If additional benefits from achieving a higher NIST Implementation Tier were available, then an organization would be incentivized to consider moving to a higher Tier. Although not a panacea, combining the GL Model with the NIST Cybersecurity Framework could go a long way toward facilitating NIST's recommendation that cost–benefit analysis be used in decisions about an organization's appropriate Implementation Tier level.

As organizations gain more experience with the NIST Cybersecurity Framework, it seems natural to expect best practices to emerge. It is important, however, for these best practices to incorporate the cost–benefit aspects of implementing the NIST Framework. It is hoped that the analysis provided in this article will help to identify these best practices from a cost–benefit perspective.

Acknowledgements

We thank Gerald Ward, Victoriya Zotova, two anonymous referees, and the editors for their comments on an earlier version of this article.

References

1. Agrarafiotis I, Nurse J, Goldsmith M *et al*. A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. *J Cybersecur* 2018;**4**:1–15.
2. Campbell K, Gordon LA, Loeb MP *et al*. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *J Comput Secur* 2003;**11**:431–48.
3. Gordon LA, Loeb MP, Zhou L. The impact of information security breaches: has there been a downward shift in costs? *J Comput Secur* 2011; **19**:33–56.
4. Romansky S. Examining the costs and causes of cyber incidents. *J Cybersecur* 2016;**2**:121–35.
5. Spanos G, Angelis L. The impact of information security events to the stock market: a systematic literature review. *Comput Secur* 2016;**58**:216–29.
6. Bush GW. *U.S. National Strategy to Secure Cyberspace*. February 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (21 February 2020, date last accessed).
7. Obama B. *The White House, Presidential Executive Order 13636, Improving Critical Infrastructure Cybersecurity*. 12 February 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (21 February 2020, date last accessed).
8. National Institute for Standards and Technology (NIST). 2014. *Framework for Improving the Critical Infrastructure Cybersecurity*. Version 1.0, 12 February 2014. https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf (21 February 2020, date last accessed).
9. Trump D. *Executive Order 13800. 2017. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. 11 May 2017. https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure (21 February 2020, date last accessed).
10. National Institute for Standards and Technology (NIST). 2018. *Framework for Improving the Critical Infrastructure Cybersecurity*. Version 1.1, 16 April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (21 February 2020, date last accessed).
11. Gordon LA, Loeb MP. The economics of information security investment. *ACM T Inform Syst Sec* 2002;**5**:438–57.
12. Gordon LA, Loeb MP, Zhou L. Investing in cybersecurity: insights from the Gordon-Loeb model. *J Inform Secur* 2016;**07**:49–59.
13. Bodin L, Gordon LA, Loeb MP. Information security and risk management. *Commun ACM* 2008;**51**:64–8.
14. Böhme R, Laub S, Riek M. A fundamental approach to cyber risk analysis. *Variance* 2008;**12**:161–84.
15. Shameli-Sendi A, Aghababaei-Barzegar R, Cheriet M. Taxonomy of information security risk assessment (ISRA). *Comput Secur* 2016;**57**:14–30.
16. Meszaros J, Buchalcevova A. Introducing OSSF: a framework for online service cybersecurity risk management. *Comput Secur* 2017;**65**:300–13.
17. Flowerday SV, Tuyikeze T. Information security policy development and implementation: the what, how and who. *Comput Secur* 2016;**61**:169–83.
18. Laube S, Bohme R. The economics of mandatory security breach reporting to authorities. *J Cybersecur* 2016;**2**:29–41.
19. Anderson R, Moore T. The economics of information security. *Science* 2006;**314**:610–13.
20. Cavusoglu H, Cavusoglu H, Raghunathan S. Economics of IT security management: four improvements to current security practices. *Commun Assoc Inform Syst* 2004;**14**:65–75.
21. Gordon LA, Loeb MP. Information security expenditures. *Commun ACM* 2006;**49**:121–25.
22. Gordon LA, Loeb MP. *Managing Cybersecurity Resources: A Cost-Benefit Analysis*. New York: McGraw-Hill, 2006.
23. Moore T, Dynes S, Chang F. Identifying how firms manage cybersecurity investment. In: *15th Workshop on the Economics of Information Security (WEIS)*. Berkeley, CA, 2016.
24. Moore T, Probst C, Rannenberg K *et al*. Assessing ICT security risks in socio-technical systems (Dagstuhl Seminar 16461). *Dagstuhl Rep* 2017;**6**: 63–89.
25. Ruan K. Introducing cybernomics: a unifying economic framework for measuring cyber risk. *Comput Secur* 2017;**65**:77–89.
26. Swaminatha T. *The Rise of the NIST Cybersecurity Framework*. 11 May 2018. CSO. https://www.csoonline.com/article/3271139/the-rise-of-the-nist-cybersecurity-framework.html (21 February 2020, date last accessed).
27. Gordon L, Loeb M. You may be fighting the wrong security battles. *The Wall Street Journal*, **26** September 2011.
28. AFCEA International Cyber Committee. The economics of cybersecurity: a practical framework for cybersecurity investments. Appendix a: models to assess investments in cyber security, 2013. https://www.afcea.org/committees/cyber/documents/cybereconfinal.pdf (6 February 2020, date last accessed).
29. Fanelli B, Pessanha R, Gwiazdowski A *et al*. 2017 *State of Cybersecurity among Small Businesses in North America*. Council of Better Business Bureau. https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf (6 February 2020, date last accessed).
30. Fielder A, Konig E, Panaousis S *et al*. Risk assessment uncertainties in cybersecurity investments. *Games* 2018;**9**:34.
31. Iannacone MD, Bridges RA. A holistic approach to evaluating cyber security defensive capabilities. *ACM Comput Surv* 2018;**9**:1–33.
32. Baryshnikov Y. IT security investment and Gordon-Loeb's 1/e rule. In: *11th Workshop on the Economics of Information Security (WEIS)*, Berlin, Germany, 2012.
33. Lelarge M. Coordination in network security games. In: *Proceedings IEEE INFOCOM*. pp. 2856–60, 2012.
34. Lelarge M. Coordination in network security games: a monotone comparative statics approach. *IEEE J Sel Area Commun* 2012;**30**:2210–19.
35. Wang SS. Integrated framework for information security investment and cyber insurance. *Pac Basin Finance J* 2019;**57**:101173.