ISSN: 2756-2638
Transactions on Engineering and Computing Sciences; Vol. 14 No. 04 (2026) (183-198)
https://doi.org/10.14738/tecs.1404.12106

Cybersecurity Budgeting: A Cyber Risk Perspective

Lawrence A. Gordon[1], Martin P. Loeb[2], Lei Zhou[3]

1. Ernst and Young Alumni Professor of Managerial Accounting and Information Assurance, Affiliate Professor in UMD Institute for Advanced Computer Studies, Robert H. Smith School of Business, University of Maryland
2. Professor Emeritus of Accounting and Information Assurance, Robert H. Smith School of Business, University of Maryland
3. Research Scholar of Accounting and Information Assurance, Robert H. Smith School of Business, University of Maryland

Abstract: Given the prominence of cyber risk, executives in organizations must address the following question: How much should be budgeted for cybersecurity? The primary objective of this paper is to provide a rigorous economic framework for analyzing and addressing the critical challenges associated with developing a cybersecurity budget, with particular emphasis on investments to prevent cyber breaches. The proposed framework is grounded in the Gordon–Loeb Model, which provides a theoretical basis for deriving the optimal level of investment in cybersecurity (Gordon and Loeb, 2002). The paper makes four contributions to the existing literature on cybersecurity budgeting. First, it identifies a comprehensive list of challenges associated with budgeting for cybersecurity activities within an organization. Second, it demonstrates that cybersecurity budgeting is best viewed from a cyber risk perspective and that this perspective is consistent with the U.S. Securities and Exchange Commission (SEC) rules concerning Cybersecurity Risk management, Strategy, and Governance (SEC, 2023). Third, it provides insight into the economic rationale for placing an upper-bound on initial cybersecurity budgets. Fourth, it examines the frequent misalignment between authority and responsibility for cybersecurity spending and proposes mechanisms to better align the incentives.

Keywords: Cybersecurity, Budgeting, Cyber, Risk

INTRODUCTION

The computer-based, interconnected digital economy has made *cyber risk* one of the, if not the, top risk concerns confronting organizations around the globe. For example, according to the Allianz Risk Barometer 2025, "Cyber incidents such as ransomware attacks, data breaches and IT outages are the top global risk for 2025, marking its fourth consecutive year at the top" (Allianz, 2025). Aon's Global Risk Management Survey found that "Cyber risk tops the global risk agenda in 2025 — and is forecast to retain the number one position through to 2028" (Aon, 2025). Numerous other studies confirm the findings concerning the importance of cyber risk to organizations globally (e.g., PwC, 2025; World Economic Forum, 2025).

Although cyber risk has become one of the most significant risks confronting organizations, managers still lack a rigorous economic framework for determining how much should be budgeted for cybersecurity. Nevertheless, organizations must continually address the following question: *How much should be budgeted for cybersecurity*? Addressing this

question requires recognizing that cybersecurity budgeting is an *ex-ante* process through which organizations determine their planned spending on cybersecurity during a given budgeting cycle. From a holistic perspective, this process encompasses the allocation of funds for preventing, detecting, and responding to successful cyber incidents, as well as investments in risk transfer mechanisms such as cyber insurance. Determining a cybersecurity budget is inherently challenging because it extends well beyond the standard financial constraints confronting all organizational budgets. Some of these challenges are unique to cybersecurity, whereas others are common to budgeting decisions more generally.

The primary objective of this paper is to provide a rigorous economic framework for analyzing and addressing the critical challenges associated with developing a cybersecurity budget, with particular emphasis on investments to prevent cyber breaches. The proposed framework builds upon the Gordon–Loeb Model (hereafter, GL Model), which provides a theoretical basis for deriving the optimal level of investment in cybersecurity (Gordon and Loeb, 2002). This model has been widely cited by both academicians and practitioners as a foundational approach for cybersecurity investment decisions.

This paper makes four contributions to the existing literature on cybersecurity budgeting. First, it identifies the major economic and organizational challenges associated with cybersecurity budgeting. Second, based on a rigorous mathematical economic framework for addressing these challenges, it demonstrates that cybersecurity budgeting is best viewed from a cyber risk perspective and that this perspective is consistent with the U.S. Securities and Exchange Commission (SEC) rules concerning Cybersecurity Risk management, Strategy, and Governance (SEC, 2023). Third, it provides insight into the economic rationale for placing an upper-bound on initial cybersecurity budgets, explaining why such a constraint may be optimal rather than arbitrary. Fourth, it analyzes the organizational problem created by the separation of authority and responsibility for cybersecurity spending and proposes mechanisms for better aligning managerial incentives.

The remainder of this paper is organized as follows. The second section reviews the foundations of budgeting and highlights the distinct features of cybersecurity budgeting in today's interconnected digital world. The third section presents the GL Model as an economic framework for analyzing the key challenges associated with developing a cybersecurity budget. The fourth section applies the framework to analyze and address the challenges of cybersecurity budgeting. The fifth section presents the steps involved in developing and allocating the actual cybersecurity budget based on the GL Model framework. The sixth section discusses the implications of the analysis and offers some concrete suggestions for improving cybersecurity budgeting. The seventh and final section of the paper offers some concluding comments and directions for future research.

BACKGROUND

The concept of budgeting has been around for centuries. For example, Urso (2024) traces the use of the modern concept of budgets to King Henry I in 1100. However, writings that frame budgeting as a contemporary management tool did not surface until the early 1900s. The book *Budgetary Control,* by McKinsey (1922), provided one of the influential discussions that focused on budgeting in businesses (Ursu, 2024). As noted by Marciano (2024),

Budgetary Control "…established McKinsey as the father of business budgets."[*] The early writings about budgeting frequently focused on the financial aspect of planning and control and were often considered part of managerial or cost accounting. In other words, budgeting was viewed from an accounting and economic perspective.

By the mid-1900s, a significant portion of the literature was emphasizing the behavioral and political aspects of budgeting. Issues like participative budgeting, Zero-Based Budgeting as an alternative to incremental budgeting, and the political nature of organizational budgets were popular topics covered in a plethora of articles (e.g., Brownell, 1981, 1982,1983; Pyhrr, 1973; Gordon et al., 1984, Covaleski and Dirsmith, 1986). The importance of treating budgets as part of the control system that aligns with an organization's business strategy was also a topic that received a lot of attention in the latter part of the 20th century (e.g., Simon, 1987). Otley (1999, p. 371), for example, explicitly raises the question: "How can budgeting be better tied into the achievement of strategic goals?" Otley (1999) also raises the concern that the traditional annual budget process fails to properly adapt to dynamic environments.

Budgeting in the 21st Century has been heavily influenced by technological advances related to the Internet, data science (especially data analytics), and AI (especially natural language processing and text analysis). The rise of the interconnected digital environment has also played an important role in the way budgeting is approached today. Contemporary budgeting emphasizes flexibility, risk management, continuous feedback, and adaptability to unpredictable events.

A unifying feature of the technologies being used today is that nearly everything is done via cyberspace (i.e., electronic communication through computer networks). As a result, cybersecurity has become a critical concern to the economic survivability of organizations. In fact, as noted earlier, cyber risk is one of the major risk concerns confronting organizations around the globe. This concern brings us back to the fundamental question: *How much should be budgeted for cybersecurity*?

Addressing the above question requires a framework that explicitly links cybersecurity expenditures to reductions in cyber risk. The framework also needs to recognize that 100% cybersecurity is not feasible and that organizations should not overspend on cybersecurity (i.e., scarce resources need to be allocated in an economically efficient manner). Additionally, the framework needs to be able to address the challenges that are unique to spending on cybersecurity activities, such as the uncertainty associated with cyber-attacks. The framework also needs to be able to address the more traditional challenges confronting resource allocation decisions by organizations, such as diminishing marginal returns. One framework that is consistent with the above requirements, which is employed in this paper, is the GL Model. The GL Model has been widely cited as providing a rigorous theoretical foundation for deriving the optimal level of cybersecurity investment by both academicians (e.g., Carfora and Orlando, 2024; Ebel and Mitra, 2024; Ermicioi and

[*] James McKinsey was an accountant, consultant, and professor of accounting at the University of Chicago in the early 1900s (https://en.wikipedia.org/wiki/James_O._McKinsey). He was also the founder of the consulting firm, McKinsey & Company (https://en.wikipedia.org/wiki/McKinsey_%26_Company).

Liu, 2021; Fedele and Roner, 2021; Fiedler, 2018; Krutilla et al., 2018; Skeoch, 2022) and practitioners (e.g., AFCES, 2013; Fanelli et al., 2017). As Skeoch (2022, p. 4) notes, "The GL model laid the foundations for a rigorous quantitative structured analysis of information security investment problems."

CYBERSECURITY BUDGETING FRAMEWORK

The GL Model provides the framework for linking cybersecurity spending to reducing an organization's cyber risk, as well as for analyzing and addressing the challenges associated with cybersecurity budgeting. The model is applicable to all private sector and public sector organizations.[†] It also provides a clear path for improving cybersecurity budgeting, emphasizing that the goal is to invest the right amount in cybersecurity. The model also emphasizes the importance of not overinvesting in cybersecurity.

The GL Model treats cyber risk as the expected loss from a successful cyber-attack (i.e., cyber incident), defined as the probability (referred to as vulnerability in the GL Model) of a successful attack multiplied by the potential loss from the attack. Investments in cybersecurity reduce the probability of a successful cyber-attack, thereby lowering the expected loss. Accordingly, the focus of the GL Model is on reducing the risk associated with future cyber incidents via cybersecurity investments. The reduction in expected loss (i.e., cyber risk) represents the benefits from cybersecurity investments. From an economic perspective, the objective is to find the optimal level of cybersecurity investments, which occurs at the point where the marginal cost associated with cybersecurity investments is equal to marginal benefit from the associated reduction in expected loss.

The basic GL Model can be explained in terms of the potential loss associated with a cyber incident, the probability that such a loss will occur, and the productivity of cybersecurity investments.[‡] The expected benefits of an investment in cybersecurity,[§] denoted by EBIS, are equal to the reduction in the firm's expected loss attributable to the extra security:

$$EBIS(z) = [v - s(z,v)]L, \qquad [1]$$

where z is the investment level, v is the initial probability (vulnerability) of a cyber incident occurring, L is the maximum potential loss due to a cyber incident, and $s(z,v)$ is the *security breach probability function*, which yields a revised value for v for a given z. In essence, $s(z,v)$ represents a mathematical function that describes the productivity of cybersecurity investments (i.e., the way cybersecurity investments reduce the probability that a cyber incident will occur). Thus, vL is the expected loss from a cyber breach, prior to making an investment in cybersecurity. Since the investment in cybersecurity is the firm's only decision variable (v and L are parameters of the information set), EBIS is written above

[†] The focus in this paper, however, is on budgeting for large publicly traded corporations.
[‡] The following description of the Gordon-Loeb Model is adapted from Gordon and Loeb (2002) and Gordon et al. (2016).
[§] The original model used the term information security rather than cybersecurity.

as a function of z, the investment. The expected net benefits from an investment in information security, denoted by ENBIS, equal EBIS less the cost of the investment, or:

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

Maximizing $ENBIS(z)$ is equivalent to minimizing the sum of the expected breach loss after the cybersecurity investment and the investment in cybersecurity:

$$s(z, v)L + z \quad [3]$$

An Interior maximum $z^* > 0$ is characterized by the first-order condition for maximizing [2] (or minimizing [3]):

$$-s_z(z^*, v)L = 1 \quad [4]$$

For two broad classes of security breach probability functions, Gordon and Loeb were able to show that the optimal level of investment, z*, as a function of vulnerability, satisfies:

$$z^*(v) \leq (1/e)\, vL. \quad [5]$$

That is, the optimal level of investment will be less than or equal approximately 37% (1/e) of the expected loss.

APPLYING THE FRAMEWORK TO THE CYBERSECURITY BUDGETING CHALLENGES

There are eight critical cybersecurity budgeting challenges associated with preventing cyber breaches. These challenges are as follows. First, cybersecurity spending generates invisible (i.e., unobservable) cost savings. Second, the probability of cyber incidents is widely viewed as being subject to extreme uncertainty and is therefore highly unstable. Third, estimating the magnitude of the potential loss associated with a cyber incident presents significant difficulties.[**,††] Fourth, it is extremely difficult to determine the productivity of investments in cybersecurity. Fifth, the number and sophistication of cyber-attacks targeting organizations are increasing at an alarming rate. Sixth, often there are significant externalities associated with cyber incidents that are either ignored or significantly undervalued. Seventh, incentive misalignment exists between those responsible for making decisions regarding cybersecurity spending and those responsible for cybersecurity performance. Eighth, cybersecurity disclosure regulations impose significant compliance issues for publicly traded companies.

As discussed below, the GL Model provides a framework for analyzing and addressing these eight challenges. Table 1 summarizes the linkages between these challenges and the GL Model.

[**] The term *cyber incident* is used in this paper to refer to a successful cyber-attack (i.e., an attack that penetrates an organization's defenses).

[††] The potential for an inordinately high loss resulting from a cyber incident is because the probability distribution for losses due to cyber-attacks has a fat-tail, meaning that extreme losses from a cyber incident have a higher probability than would be predicted by a normal (bell curve) probability distribution.

Invisible Cost Savings

The benefits derived from cybersecurity spending primarily come from the reduction in the *ex-ante* probability of having a cyber incident.[‡‡] This reduction, when multiplied by the potential loss from a cyber incident, yields an estimate of the cost savings resulting from spending on cybersecurity. Unfortunately, spending on cost savings endeavors is generally less attractive than spending on projects that generate revenue growth. This latter point is particularly true for publicly traded companies where the growth (decline) of a company's stock price is closely associated with the company's revenue growth (decline).

A further complication associated with cybersecurity expenditures is that the benefits from cybersecurity investments are invisible. Unlike investments that generate observable reductions in operating costs or measurable revenue increases, cybersecurity investments primarily create value by preventing losses that would have occurred from cyber incidents. In other words, if funds allocated to cybersecurity-related activities are effective, they prevent cyber incidents and the benefits associated with the prevented cyber incidents are unobservable. As a result, the link between cybersecurity spending and benefits (i.e., outcomes) is inherently weak, at best.

The GL Model reframes the cost savings (i.e., the benefits from cybersecurity investments) in terms of a reduction in the expected loss, which is equal to $[v - s(z, v)]L$. Thus, the model focuses on the change in the probability of a cyber incident $[v - s(z, v)]$ and facilitates the use of empirical proxy metrics for measuring the benefits derived from cybersecurity investments rather than the illusive notion of cost savings.

Estimating the Probability of a Cyber Incident

The probability of a cyber incident occurring, multiplied by the dollar value of the potential loss, is commonly thought of as an organization's dollar value of the cyber risk.[§§] Unfortunately, it is extremely difficult to estimate the probability that a cyber incident will occur in the future. Moreover, the distribution of cyber incidents is often characterized as fat-tailed, since a small number of cyber incidents have resulted in extraordinarily large losses.[***] Furthermore, unlike the massive amount of actuarial data available to support the pricing of life insurance policies, there exists only a relatively limited amount historical data associated with cyber incidents. This challenge is further compounded by the fact that the likelihood of future cyber incidents varies across industries and among firms within the same industry (e.g., Shevchenko, et al., 2023; Eling et al., 2022).

[‡‡] Although not addressed in this paper, the ability to transfer part of a firm's cybersecurity risk via such mechanisms as cybersecurity insurance or hedging, further complicates the issues surrounding cybersecurity budgeting.

[§§] Although this definition of cyber risk is common, there are other ways to define cyber risk (see Bodin et al., 2008).

[***] Fat-tailed probability distributions means that extreme outcomes have a much greater probability than would be the case with a normal (i.e., bell curve) distribution. Thus, there is a higher probability for a cyber incident to result in an extreme (or extraordinarily large) loss that a normal probability distribution would suggest.

When budgeting for cybersecurity activities, it is necessary to estimate not only the current probability of a cyber incident, but also the impact that additional spending will have on reducing that probability.[†††] In fact, this reduction in the probability of a cyber incident, multiplied by the potential loss associated with a cyber incident, represents the benefits resulting from cybersecurity expenditures.

The GL Model explicitly recognizes the subjective nature of the initial probability, v, of a cyber incident. Furthermore, the model explicitly considers how v is lowered as investments in cybersecurity, z, increase. It is this reduction (i.e., change) of the probability, $[v - s(z, v)]$ multiplied by the potential loss, L, that represents the expected benefits (i.e., savings) from cybersecurity investments. In sum, the model explicitly considers the initial probability of a cyber incident as well as the probability of a cyber incident after cybersecurity investments, thereby providing a direct link between cybersecurity budgeting and cyber risk.

Estimating Potential Losses

The potential loss from a cyber incident multiplied by the probability of the incident occurring represents the *expected loss* from a cyber incident occurring. This amount is commonly referred to as the dollar estimate of the cyber risk and plays a crucial role in budgeting for cybersecurity because it represents the potential benefit that could be derived from additional spending on cybersecurity.[‡‡‡] Unfortunately, there is substantial difficulty in estimating the magnitude of potential losses associated with a cyber incident, including the possibility of catastrophic losses. Thus, traditional incremental budgeting does not work well when it comes to cybersecurity budgeting.[§§§]

One way to address the issues related to estimating the potential loss from a cyber incident is to develop a probability distribution of different possible losses and solve for the expected loss rather than using a point estimate. This approach explicitly recognizes that there are several possible outcomes, including extreme losses, when it comes to the potential loss from a cyber incident.

The GL Model explicitly considers the potential maximum loss, L. In fact, it is this amount multiplied by the probability of a cyber incident, v, which yields the expected loss and is usually referred to as the dollar value associated with a firm's cyber risk. The model also lends itself to considering an array of possible losses as a probability distribution, including extreme losses (i.e., tail risks).

[†††] Although 100% cybersecurity is theoretically conceivable — implying zero probability of a breach — it is unachievable in practice unless all computers are eliminated.
[‡‡‡] As noted in the previous footnote, 100% cybersecurity is unrealistic, especially from an economics perspective. If it were possible, then investments in cybersecurity could reduce the expected loss to zero.
[§§§] Incremental budgeting refers to the process of starting with the last period's budget and adding or subtracting an incremental amount based on changes in activities to derive the budget for the next period.

Expected Benefits from Cybersecurity Investments

A unique aspect of deriving the appropriate budget for cybersecurity related activities is understanding how productive cybersecurity investments are in reducing the initial probability of a cyber incident occurring. Technically speaking, the link between cybersecurity spending and the revised probability of a cyber incident can be expressed as a mathematical function. Determining this mathematical function is, however, as much an art as it is a science. The above notwithstanding, effective cybersecurity budgeting depends on understanding this relationship.

The expected benefits of cybersecurity investments are derived by determining the expected loss from a cyber incident prior to the investments minus the expected loss from a cyber incident after the investments. The objective is to maximize these benefits after deducting the amount spent to achieve such a reduction. In most real-world scenarios, the benefits will be increasing at a decreasing rate, thereby indicating that there are diminishing marginal returns to cybersecurity investments. An alternative way of looking at the goal of cybersecurity budgeting is to determine the budget amount that minimizes the sum of the expected loss from a cyber incident plus the cost of the cybersecurity spending.

A fundamental aspect of the GL Model is the link between cybersecurity spending and the revised probability of a cyber incident. This link is the mathematical function that describes how cybersecurity investments reduce the initial probability of a cyber incident, v, to derive the revised probability of a cyber incident, $s(z,v)$. The GL Model refers to this mathematical function as the *security breach probability function*, represented by The probability security breach function can be thought of as a mathematical function that describes the productivity of cybersecurity investments. As shown in equation [3] in section III above, this goal of cybersecurity investments can be expressed as minimizing $s(z,v)L + z$.

The GL Model considered two broad classes of security breach probability functions $[s(z,v)]$. Both assume that additional investments in cybersecurity will reduce the expected loss based on the economic principle of diminishing marginal returns. Thus, as the firm spends more on cybersecurity, the benefits (in terms of reducing cyber risk) will increase at a decreasing rate (i.e., each additional dollar spent on cybersecurity will reduce risk by less than the previous dollar).

Growing Number and Sophistication of Cyber-attacks

The number and sophistication of cyber-attacks are rapidly growing worldwide. This growth is driven in large part by the rate of growth in technology related to the interconnected digital environment. As noted by the World Economic Forum (2025), “The rapid advancements and increasing adoption of digital platforms globally is matched by an equally evolving cyberthreat landscape. Cybercrime today is increasing not just in scale but also in sophistication” (p. 14).

When budgeting for cybersecurity it is necessary to take into consideration this rapid growth in the digital environment, as well as the changes that are accompanying this growth. In addition, the cybersecurity budget needs to be flexible, taking into consideration

both the growth and changes in the digital environment. Continuous monitoring of differences between actual and budgeted spending is a necessity rather than a luxury.

Although the GL Model is a static approach to investing in cybersecurity, the estimates used in the model can easily be updated as new information becomes available thereby facilitating a dynamic approach to cybersecurity budgeting. Indeed, the probability of a cyber incident, the maximum potential loss, and the security breach probability function can all be thought of as part of a continuous, flexible budget that incorporates a cybernetic feedback control feature.

Externalities

Externalities refer to costs and benefits to individuals and organizations that are not directly involved in the transaction or economic event. Accordingly, they are often referred to as spill-over effects. In terms of cyber incidents, externalities represent the spill-over effects on individuals and organizations that had nothing to do with causing the incident (e.g., the impact of a company's cyber incident on a supply-chain partner). In contrast, *private costs* are the costs borne by the company directly responsible for the economic activity to occur (e.g., the costs of a cyber incident borne by the company that experienced the cyber incident). Social costs are the sum of private costs and externalities.

Unfortunately, most firms focus on the private costs associated with cyber incidents (i.e., the costs that the firm will bear from an incident). However, given the interconnectivity of computer-based systems, there are significant externalities (spill-over effects) associated with cyber incidents. These externalities include spill-over costs that are absorbed by customers, supply chain partners, and possibly even national security. Externalities associated with cyber incidents are one of the main reasons it is often argued that companies underinvest in cybersecurity.

Ideally, when budgeting for cybersecurity activities, externalities should be considered, although they are frequently ignored. Ignoring externalities creates a free-rider problem when shared benefits are associated with computer networks. Trying to resolve the free-rider problem associated with cybersecurity investments has been addressed in the literature, although a commonly accepted solution doesn't exist (Gordon et al., 2003).

Although the GL Model focuses on private costs, a direct extension is to redefine the potential loss L to include externalities (Gordon et al., 2015a). Since the sum of private costs plus externalities equal social costs, this approach would facilitate having firms consider the full costs of cyber incidents when budgeting for cybersecurity.

Incentive Misalignment

In most organizations, those responsible for cybersecurity performance are usually the CISO (Chief Information Security Officer) or CIO (Chief Information Officer). However, it is usually the organization's CFO (Chief Financial Officer) who has final authority over the budget for cybersecurity. This situation frequently creates an incentive misalignment between those responsible for making decisions regarding cybersecurity spending and those responsible for

cybersecurity performance. More specifically, those responsible for cybersecurity performance usually advocate for higher spending on cybersecurity than those responsible for authorizing the cybersecurity budget. Although not unique to cybersecurity, this problem is clearly prevalent in budgeting for cybersecurity activities. In fact, one reason many firms underinvest in cybersecurity is because those who ultimately determine the budget for cybersecurity activities do not bear the responsibility for cyber incidents (Banker, 2017). Treating cybersecurity as a cost center exacerbates the incentive misalignment problem.

One way to improve the alignment between those who have authority over the cybersecurity budget with those who have responsibility for cybersecurity performance is to make the firm's cybersecurity performance a firm-wide responsibility, including linking the performance to the compensation of senior executives like the CFO and CEO (Chief Executive Officer). Some firms have already moved in this direction. For example, as reported by CNBC, Microsoft has launched a new Secure Future Initiative that includes linking executive compensation to cybersecurity performance (https://www.cnbc.com/2024/05/22/after-a-big-hack-microsoft-is-tying-top-executive-pay-to-cyberthreats.html?utm_source=chatgpt.com).

By expressing the objective of cybersecurity budgeting in terms of the potential maximum loss L, probability of a cyber incident v, and security breach probability function $s(z,v)$, the GL Model helps to align cybersecurity budgets with the technical aspects of cybersecurity. The model could also be used to establish a formal financial executive compensation plan based on the performance (e.g., in terms of reducing v) of those responsible for executing cybersecurity.

Regulatory Requirements

Regulatory requirements often result in a company focusing on compliance rather than the efficient allocation of resources. When this happens, a company will often devote a portion of its cybersecurity budget to complying with a checklist of items. This can lead to a situation where complying with the rules contained in the regulation becomes the dominant consideration rather than efficiently allocating the budget to minimizing the risk associated with the expected loss from a cyber incident. In addition, focusing on compliance can lead to spending an excessive portion of the cybersecurity budget on administrative concerns, such as personnel, reporting systems, and legal counsel. In essence, focusing on regulatory requirements could shift a company's emphasis away from the technical and economic aspects of cybersecurity toward an emphasis on an excessive amount of compliance administration.

By using the GL Model as the framework for cybersecurity budgeting, it puts the economic and technical aspects of cybersecurity at the center of budgeting process. Indeed, the GL Model makes it clear the primary goal is to derive the level of spending that minimizes the sum of the dollar amount of cyber risk plus the amount invested in cybersecurity $[s(z,v)L + z]$, as shown in Equation [3], section III. Thus, although U.S. publicly traded companies (as well as foreign companies listed with the U.S. SEC) need to comply with the 2023 SEC rules related to cybersecurity, using the GL Model as a framework for meeting this challenge makes it clear that the goal is not compliance for the sake of compliance.

IMPLICATIONS

Using the GL Model as the framework for analyzing and addressing the challenges associated with cybersecurity budgeting yields several important implications.

First, and of key importance, the focus of cybersecurity budgeting is best viewed from a cyber risk perspective rather than in terms of unobservable cost savings. Framing cybersecurity investments around reductions in cyber risk, rather than measuring the invisible cost savings, clarifies the need to treat cybersecurity risk as an integral part of the overall enterprise risk management (ERM) program. This shift in perspective is directly in line with the SEC's concern for having a registrant's cybersecurity risk management "…integrated into the registrant's overall risk management system or processes…" (SEC, 2023, Item 106b).

Moreover, this shift in perspective highlights the fact that cybersecurity performance is more appropriately evaluated and controlled using risk-based metrics (e.g., cyber intrusions detected and prevented, response times to cyber incidents, and the severity of cyber incidents) rather than traditional accounting metrics (e.g., budget variances).

A second implication is that by using the GL Model as the framework for analyzing and addressing the challenges associated with cybersecurity budgeting it provides an excellent example of how a static budget can easily lend itself to a changing, dynamic environment. The key parameters of the GL Model [i.e., the L, v, and $s(z,v)$] can be continuously updated as new information becomes available, thereby providing a dynamic approach to the cybersecurity budgeting process. Thus, the GL Model can facilitate a transition from what starts off as a static approach to cybersecurity budgeting to a dynamic budgeting approach for cybersecurity expenditures. Furthermore, AI and data analytics can play an important role in improving the estimation of key parameters and facilitating real-time adjustments to cybersecurity investment decisions.

A third implication concerns the social costs of cyber incidents. Most firms tend to ignore the externalities associated with cyber incidents when determining their cybersecurity budget. This leads to an underestimation of the true social costs of cyber risk. Although this tendency reflects the natural focus by firms on self-interest, it is also driven by the inherent difficulties of quantifying externalities. Nevertheless, the GL framework provides a straightforward and tractable way to incorporate the effects of externalities into the cybersecurity budget. More to the point, externalities can be approximated by adjusting the estimated maximum loss (L) upward to reflect the broader social impact of cyber risks (see Gordon et al., 2015b). Incorporating an adjustment to the estimated loss from a cyber incident into the cybersecurity budgeting process results in a more socially efficient level of cybersecurity investment.

A fourth implication follows from the fact that the GL Model assumes that there are diminishing marginal returns to cybersecurity investments and, for two broad classes of security breach probability functions, Gordon and Loeb (2002) were able to show that the maximum amount that should be spent on cybersecurity, denoted as z^*, should not exceed roughly 37% of the expected loss [$z^*(v) \leq (1/e)\, vL$]. These two factors provide support for the observed practice that managers in charge of cybersecurity spending often adopt a

conservative approach to the initial cybersecurity budget, while remaining prepared to make an additional investment in response to actual cyber incidents.[****]

A fifth implication is that the GL Model helps to align the financial aspects of cybersecurity budgets with the technical aspects of cybersecurity. This alignment should facilitate a stronger dialogue between the financially oriented people (e.g., CFO and Controller) and the cybersecurity experts (e.g., CIO and CISO) within a company.

STEPS IN DEVELOPING AND ALLOCATING THE CYBERSECURITY BUDGET

There are four basic steps in developing the actual cybersecurity budget. These steps utilize the economic foundation provided by the GL Model, while maintaining a focus on reducing the cyber risk.

Step 1: Estimate the maximum potential loss (i.e., L in the GL Model) that would result from a cyber incident. In other words, what would be the maximum potential cost to the organization if it were to be the victim of a successful cyber-attack.

Step 2: Estimate the initial probability of a cyber incident occurring (i.e., v in the GL Model). It is worth keeping in mind that vL is the expected loss from a cyber incident before budgeting additional funds for cybersecurity.

Step 3: Determine the optimal amount to invest in cybersecurity activities (i.e., z in the GL Model) to reduce v, which in turn reduces the expected loss. This step requires an estimate of how additional spending (i.e., the budget amount) on cybersecurity activities will reduce the probability of a cyber incident occurring. The GL Model refers to the mathematical relationship between additional spending on cybersecurity and the revised value of breach probability, as the *security breach probability function* [i.e., $s(z,v)$]. Although it is unlikely that an organization will be able to determine the exact mathematical relationship between additional spending and the revised probability, the GL Model shows that the optimal amount of investment in cybersecurity, z^*, will likely be less than approximately 37% of the initial expected loss [i.e., $z^*(v) \leq (1/e)\, vL$]. Knowledge of this result places an upper bound on the amount that should be invested in cybersecurity.

Step 4: Allocate the cybersecurity budget across different activities. This step involves assessing the marginal benefits per dollar of investment for different activities. At a macro level, the different activities could include such categories as preventing cyber incidents, detecting cyber incidents, and responding to cyber incidents. At a micro level, the different activities could include such categories as encryption, prevention intrusion systems, detection systems, employe hiring and training, and AI models. Ideally, the fourth step should be interactive with the third step (i.e., a sequential feedback loop) because the marginal benefit per dollar of investment will influence the security breach probability function derived in step 3.

[****] There is a well-established body of literature that argues that due to the real option known as the deferment option, it may be economically rational for a firm to take a wait-and-see approach to major cybersecurity investments (Gordon et al., 2003; Gordon et al., 2015).

CONCLUDING COMMENTS

The computer-based, interconnected digital economy has made cyber risk a critical concern to organizations around the globe. Recent advances in artificial intelligence (AI) have increased the importance and complexity of cyber risk. As a result, budgeting for cybersecurity has become a key managerial and policy concern.

Table 1: Linking Cybersecurity Budgeting Challenges to the Gordon-Loeb Model*

Cybersecurity Budgeting Challenges	**Linkages to the Gordon-Loeb Model**	**Comments**
Invisible Cost Savings	Cost savings result from the reduction in expected loss = $[v - s(z,v)]\,L$	Focuses on the change in the probability of a cyber incident $[v - s(z,v)]$ rather than the illusive notion of cost savings
Estimating the Probability of a Cyber Incident	Initial vulnerability (or probability of cyber incident) = v Security breach probability function = $s(z,v)$ results in revised probability	Provides direct link between cybersecurity budgeting and cyber risk Change in probability, $[v - s(z,v)]$, multiplied by L, represents benefits from z
Estimating Potential Losses	Maximum Loss = L	L multiplied by the probability of a cyber incident, v, is the initial expected loss
Expected Benefits from Cybersecurity Investments	Security breach probability function $s(z,v)$ results in revised reduction in expected loss $[v - s(z,v)\,]\,L$ The expected benefits from Cybersecurity Investments = $[v - s(z,v)]L - z$	Provides link between cybersecurity spending, z, and expected net benefit from cybersecurity investments, $[v - s(z,v)]L - z$
Growing Number and Sophistication of Cyber-attacks	The parameters, v, L, and $s(z,v)$ can easily be changed	Facilitates moving from a static cybersecurity budget to an adaptive, dynamic cybersecurity budget
Externalities	L can be redefined to include externalities	Facilitates having firms consider the total costs of cyber incidents when budgeting for cybersecurity
Incentive Misalignment	Minimize $s(z,v)L + z$	Helps align cybersecurity budgets with the technical aspects of cybersecurity
Regulatory Requirements (SEC, 2023)	Utilizing the model is consistent with SEC's requirements for disclosing firm's cybersecurity risk management, strategy, & governance.	Provides a structured process for managing cybersecurity risk, taking into consideration cost of reducing such risk.

*Legend: v = initial probability of cyber incident; L = potential maximum loss; $s(z,v)$ security breach probability function = revised probability after investment; z = cybersecurity investment.

The primary objective of this paper has been to provide a rigorous economic framework for analyzing the key challenges associated with cybersecurity budgeting. The proposed framework is grounded in the Gordon–Loeb Model for deriving the optimal level of investment in cybersecurity (Gordon and Loeb, 2002). Using this framework, we show that cybersecurity budgeting is best viewed from a cyber risk perspective rather than from a purely technical or compliance driven perspective. The framework also lends itself to easily incorporating externalities during the cybersecurity budgeting process and provides insight into why it is often economically justified for firms to initially underinvest in cybersecurity.

Although this study provides new insights into the issues surrounding cybersecurity budgeting aimed at preventing cyber incidents, it has limitations. Three of the most significant limitations are as follows. First, this study focuses solely on preventing cyber incidents. However, a holistic approach to cybersecurity budgeting should consider not only expenditures directed at preventing cyber incidents, but also resources allocated to responding to cyber incidents, transferring cyber risk through mechanisms such as cybersecurity insurance, and the possibility of gaining a competitive advantage through cybersecurity spending. Second, the study does not include any empirical testing of the arguments presented. It would be valuable to examine whether the eight challenges to cybersecurity budgeting discussed in this paper are, in fact, the dominant sources of difficulty for organizations, or whether other challenges play a more significant role in practice. Third, the study relies on simplifying assumptions inherent in the static Gordon–Loeb Model for investing in cybersecurity.

Future research could address the above limitations in several ways. For example, future research could develop specific hypotheses related to the challenges associated with cybersecurity budgeting and gather empirical data to statistically test the hypotheses. Future research could also extend the framework to include the dynamic and evolving nature of cyber risk, especially in environments influenced by developments related to AI. In addition, future research could consider the way game-theoretic strategic interactions between cyber defenders and attackers affect cybersecurity budgeting decisions. Finally, future research could also consider the behavioral, organizational, strategic, governance, and regulatory factors that potentially influence cybersecurity budgeting decisions.

Declaration of generative AI and AI-assisted technologies in the manuscript preparation process. During the preparation of this work the authors used ChatGPT to suggest ways to sharpen the focus of specific sections of the paper. After using this tool, the authors reviewed and edited the content as needed and accept full responsibility for the content of the published article.

REFERENCES

AFCEA (Armed Forces Communications and Electronics Association) Cyber Committee, 2013. The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment. See: https://www.afcea.org/mission/intel/documents/EconomicsofCybersecurityFinal10-24-13.pdf , pp. 1-15.

Allianz, 2025. Allianz Risk Barometer 2025 - Global risk #1: Cyber incidents (38%). See: https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2025-cyber-incidents.html?utm_source=chatgpt.com).

Aon, 2025. Global Risk Management Survey. See: https://www.aon.com/en/insights/reports/global-risk-management-survey/top-10-global-risks?collection=18a5358e-4f8c-4e2d-8fb3-291c7672dfaa&parentUrl=/en/insights/reports/global-risk-management-survey#aon-collection-detail-item-{29CAED57-3308-4475-9864-638B107B0D5B.

Bodin, L.D., Gordon, L.A. and Loeb, M.P., 2008. Information security and risk management. Communications of the ACM. Vol. 51(4), pp.64-68.

Brownell, P., 1981. Participation in budgeting, locus of control and organizational effectiveness. The Accounting Review, 56 (October), pp. 844-860.

Brownell, P., 1982. The role of accounting data in performance evaluation, budgetary participation and organizational effectiveness, Journal of Accounting Research (Spring), pp. 12-27.

Brownell, P., 1983. Leadership style, budgetary participation and managerial behavior. Accounting, Organizations and Society, Vol. 8, No.4, 307-321.

Carfora, M. F. and A. Orlando, 2024. Application of the Gordon Loeb model to security investment metrics: a proposal. Data Science in Finance and Economics, Vol. 4, No. 4, pp. 601-614, See: https://www.aimspress.com/article/doi/10.3934/DSFE.2024025?viewType=HTML.

Covaleski, M. A. and M. W. Dirsmith, 1986. The budgetary process of power and politics. Accounting, Organizations and Society, Vol. 11, No. 3, pp. 193–214.

Ebel, A. and D. Mitra, 2024. Economics and optimal investment policies of Attackers and Defenders in cybersecurity. Journal of Cybersecurity, Vol. 10, Issue 1 (see: https://academic.oup.com/cybersecurity/article/10/1/tyae019/7900094).

Eling, M., K. Jung, and J. Shim, 2022. Unraveling heterogeneity in cyber risks using quantile regressions. Insurance: Mathematics and Economics, Vol. 104, pp. 222-224.

Ermicioi, N. and X. Liu, 2021. An Interdisciplinary Study of Cybersecurity Investment in the Nonprofit Sector. American Journal of Management, Vol. 21(5), pp. 39-50.

Fanelli, B. R. Pessanha, A. Gwiazdowski, A. Chng-Castor, and G. Auger, 2017. 2017 State of Cybersecurity Among Small Businesses in North America. Better Business Bureau. See: http://saginllc.com/wp-content/uploads/2017/10/Cybersecurity_FINAL_LoRes_Embargoed.pdf.

Fedele, A. and C. Roner, 2022. Dangerous Games: A literature review of cybersecurity investments. Journal of Economic Surveys, Vol. 36, No. 1, pp. 157-187.

Fielder, A, S. Konig, E. Panaousis, S. Shauer, and S. Rass, 2018. Risk assessment uncertainties in cybersecurity investments. Games, 9(34), pp. 1-14. See: https://www.researchgate.net/publication/325681751_Risk_Assessment_Uncertainties_in_Cybersecurity_Investments.

Gordon, L. A., S. Haka, and A. G. Schick, 1984. Strategies for information systems implementation: The case of zero-base budgeting. Accounting, Organizations and Society, Vol. 9, No. 2, pp. 111-123.

Gordon, L. A. and M.P. Loeb, 2001. A Framework for Using Information Security as a Response to Competitor Analysis Systems. Communications of the ACM, September, pp.

Gordon, L. A. and M. P. Loeb, 2002. The Economics of Information Security Investment. ACM Transactions on Information and System Security, 5 (4), pp. 438–457.

Gordon, L. A., M. P. Loeb and W. Lucyshyn, 2003. Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy, Vol. 22, No. 6, pp. 461-485.

Gordon, L.A., M.P. Loeb and W. Lucyshyn, 2003. Information Security Expenditures and Real Options: A Wait-and-See Approach. Computer Security Journal, Vol. 19, No. 2, pp. 1-7.

Gordon, L.A., M.P. Loeb, W. Lucyshyn, and L. Zhou, 2015a. The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective. Journal of Accounting and Public Policy, Vol. 34, No. 5, pp. 509-519.

Gordon, L.A., M.P. Loeb, W. Lucyshyn, and L. Zhou, 2015b. Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. Journal of Information Security, pp. 24-30.

Gordon, L.A., M.P. Loeb, and L. Zhou, 2016. Investing in Cybersecurity: Insights from the Gordon-Loeb Model. Journal of Information Security, pp. 49-59.

Krutilla, K., A. Alexeev, E. Jardine, and D. Good, 2021. The Benefits and Costs of Cybersecurity Risk Reduction: A Dynamic Extension of the Gordon and Loeb Model. Risk Analysis, Vol. 41, No. 10, pp. 1795-1808.

Marciano, 2024. The amazing history, present, and future of business budgeting. Updated May 29, 2024. See: https://www.datarails.com/then-and-now-business-budgets/#:~:text=The%20evidence%20for%20the%20traditional,taking%20from%204%2D6%20months.

Otley, D., 1999. Performance management: a framework for management control systems research. Management Accounting Research, 10, pp. 363-382.

PwC, 2025. 2026 Global Digital Trust Insights: C-suite playbook and findings -- New world, new rules: Cybersecurity in an era of uncertainty. See: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html.

Pyhrr, P., 1973. Zero-Base Budgeting, New York: John Wiley and Sons, Inc., 1973.

Skeoch, H. R., 2022. Expanding the Gordon-Loeb Model to Cyber-Insurance. Computers & Security, Vol. 112, 1025333.

Securities and Exchange Commission, 2023. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Final Rule, see: https://www.sec.gov/files/rules/final/2023/33-11216.pdf.

Securities and Exchange Commission, S-K 106, 1/22/2026. See: https://www.ecfr.gov/current/title-17/chapter-II/part-229/subpart-229.100/section-229.106.

Shevchenko, P. V., J. Jang, M. Malavasi, G. W. Peters, G. Sofronov, and S. Truck, 2023. The nature of losses from cyber-related events: risk categories and business sectors. Journal of Cybersecurity, Vol. 9, No. 1, pp. 1-12.

Simons, R., 1987. Accounting Control Systems and Business Strategy: An Empirical Analysis. Accounting, Organizations and Society, Vol. 12, No. 4, pp. 357–374.

Ursu, I., 2024. The History of the Business Budgeting to the Present: A Literature Review. Journal of Eastern Europe Research in Business and Economics. See: https://ibimapublishing.com/articles/JEERBE/2024/342438/342438.pdf.

World Economic Forum, 2025. “Global Cybersecurity Outlook 2025. See: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.