Risk Analysis, Vol. 41, No. 10, 2021 DOI: 10.1111/risa.13713

The Benefits and Costs of Cybersecurity Risk Reduction: A Dynamic Extension of the Gordon and Loeb Model

Kerry Krutilla,[1,*] Alexander Alexeev,[1] Eric Jardine [2] and David Good[1]

This article develops a dynamic extension of the classic model of cybersecurity investment formulated by Gordon and Loeb. In this dynamic model, results are influenced by the rate at which cybersecurity assets depreciate and the rate of return on investment. Depreciation costs are lower in the dynamic model than is implicitly assumed in the classic model, while the rate-of-return threshold is higher. On balance, the user cost of cybersecurity assets is lower in the dynamic model than is implicitly assumed in the classic model. This difference increases the economically efficient size of the cybersecurity system in value terms, increasing the efficient level of risk reduction.

KEY WORDS: Benefit-cost analysis; cybersecurity investment; dynamic decision-making

1. INTRODUCTION

Improving cybersecurity is a significant challenge as vulnerabilities evolve and risks increase to individuals and organizations, and threats emerge to public goods like the integrity of elections and critical infrastructures (Anderson et al., 2013; Anderson et al., 2019; Coburn, Leverett, & Woo, 2019; Geer, Jardine, & Leverett, 2020). Denial of service attacks, the theft of data and information, property damage, and other cyber risks impose significant direct and indirect costs to individuals (Riek & Böhme, 2018), companies, and governments (Coburn et al., 2019). A study by the Council of Economic Advisers found that malicious cyber activity cost the U.S. economy between $57 and $109 billion in 2016 (Council of Economic Advisors, 2018). Economic costs from cybersecurity breaches are likely to have increased in the period since.

[1]O'Neill School of Public and Environmental Affairs Indiana University, Bloomington, IN, USA.
[2]Virginia Polytechnic Institute, Blacksburg, VA, USA.
*Address correspondence to Kerry Krutilla, O'Neill School of Public and Environmental Affairs Indiana University, Bloomington; krutilla@iu.edu

The evolving cybersecurity environment requires strategies to reduce risks and to increase the resiliency of IT systems. At the federal level, the National Institute of Standards and Technology (NIST) has developed a "Cybersecurity Framework" to address this need (NIST, 2018). The NIST framework offers guidance for improving risk management in critical infrastructures, but is relevant to other sectors and contexts (NIST, 2018). The implementation of the NIST Cybersecurity Framework is required for all federal agencies (Executive Order 13800, 2017).

The NIST framework emphasizes return on investment as a criterion for selecting cyber risk reduction strategies, and a research literature has emerged that addresses this issue (Anderson & Moore, 2006; Baggott & Santos, 2020; Gordon & Loeb, 2006; Oughton et al., 2019; Paté-Cornell, Kuypers, Smith, & Keller, 2018). A significant strand of this literature focuses on the economic conditions required to optimize the level of cybersecurity investment, for example, Gordon and Loeb (2002, 2005), Gordon, Loeb, and Zhou (2016, 2020), Farrow (2007), and Farrow and Szanton (2016). Blended approaches that optimize the mix of cybersecurity investment and the

purchase of insurance have also been assessed (Mazzoccoli & Naldi, 2020).

A model by Gordon and Loeb (2002) is foundational in the literature on the benefits and costs of reducing cybersecurity risks (hereafter the "GL Model)." The GL model uses "breach" functions to represent the functional link between cybersecurity security expenditures and expected damages from cyberattacks. Comparing expected damages with and without expenditures shows the benefit of using resources to reduce risks. In this model, the expected damage in the without-any-expenditure scenario is a function of two parameters: the firm's inherent vulnerability, and the value of the assets at risk from a system's breach. Assuming a one-period decision problem and continuous functional forms giving interior maximums, the economically efficient cybersecurity investment level occurs at the point where the marginal benefits of the expected avoided damages equal the marginal costs. For the convex cybersecurity breach functions used in the original GL model, the efficient investment for a risk neutral firm as a fraction of total expected damages turns out to never be more than about 37% ($1/e$, with $e \approx 2.7182$).[1]

The GL model and the associated literature on cybersecurity investment are based on one-period models. The objective of this article is to develop a dynamic extension of the GL model, enabling the benefits and costs of cybersecurity investment to be evaluated over an extended horizon. The next section starts with background about the relevant research literature and our research motivation. Section 3 then develops a dynamic model of cybersecurity investment, and Section 4 solves the model to give steady-state solutions for the economically efficient level of cybersecurity assets. Section 5 compares this solution to that from the standard GL model on the assumption that the standard solution can be interpreted as a steady state associated with repeated decision-making over time. Section 6 evaluates the user costs that the two models imply for the opportunity cost of cybersecurity assets. Section 7 compares the steady-state solutions in the two models for the economically efficient level of cybersecurity risk reduction. Section 8 then establishes and compares the economically efficient maximums in the two models for the level of cybersecurity assets, user cost, and cyber risk reductions. Section 9 offers two extensions that indicate how dynamic considerations can be represented in one-period models. Section 10 offers a discussion and research recommendations. Section 11 offers a conclusion.

[1]Two regulatory conditions are also stated; see Gordon and Loeb (2002, p. 443).

2. BACKGROUND

The literature on the benefits and costs of cybersecurity investment has explored various extensions of the original GL model. Formalizations and extensions of cybersecurity breach functions have been assessed (e.g., Willemson, 2010), and studies have been made of the implications of functional forms for optimal investment levels and the 37% result. In Hausken (2006), the second derivative of the cybersecurity breach function is explored using concave, convex, logistic, and linear functional forms. These functional forms give different results in terms of the existence of interior maxima, the parameter values that give corner solutions, and whether investment levels change smoothly or jump noncontinuously with changes in an organization's vulnerability (Hausken, 2006, 2014). For nonconvex functional forms, investment can exceed 37% of expected damages for parameter configurations in which investment is positive. Additional work by Baryshnikov (2012) shows that log convexity is a necessary condition for the 37% result. A review by Farrow and Szanton (2016) concludes that the functional form of breach functions is an empirical question, with numerous candidates that could lead to maximum optimal expenditures above the 37% limit.

Farrow and Szanton (2016) extend the GL framework using a cost-minimizing model developed from Farrow (2007). The objective is to establish the conditions for efficient allocations from a limited budget among a cluster of at-risk sites. Costs include budget expenditures and inconvenience costs from changing security procedures (i.e., on and off-budget costs), and social costs in the event of an attack. Optimality conditions are established for budget allocations that minimize total social costs for a number of different cases. They include that attacks on sites are independent; the attacks on sites are interdependent (investment to protect one site displaces attacks to other sites); expenditures can reduce both the probability of attacks and the severity of the damages; sites are differentially difficult to protect; site protection may offer external benefits; and detection may be imperfect.

The original GL model has also been extended to incorporate the effects of external economic damages from breaching an organization's cybersecurity system (Gordon, Loeb, Lucyshyn, & Zhou, 2015). To the extent that legal liability does not fully internalize these damages, organizations will underinvest from a societal point of view. This modified GL model shows that the maximum optimal social investment will be higher than the organization's expected losses (i.e., rather than a 37% limit, the limit is more than 100%) when external damages are 172% or more higher than an organization's expected losses. Gordon et al. (2015) and Farrow and Szanton (2016) suggest that this threshold is likely to be empirically relevant. The upshot of this research is that there is a role for public policy to incentivize investments to reduce cybersecurity risks.

Insurance markets are a possible mechanism for transferring cybersecurity risks (see Gordon, Loeb & Sohail, 2003; Marotta, Martinelli, Nanni, Orlando, & Yautsiukhin, 2017; Meland, Tondel, & Solhaug, 2015; Shackelford, 2012). A recent article incorporates insurance into the GL framework (Mazzoccoli & Naldi, 2020). This model links investments to reduce cybersecurity risks to premium discounts for three types of insurance policies: a policy that covers all losses, a policy that covers less than the total losses, and a third policy that also provides partial coverage (the same as the second) but includes a deductible provision. The level of security investment that optimizes the benefits from each of these insurance policies is established, and a sensitivity analysis is conducted to show the conditions under which the optimal investment to reduce cybersecurity risks is positive. It turns out that combining security investment with insurance coverage is optimal for some parameter configurations, and for others, insurance coverage alone is the optimal choice. When a mix of policies is optimal, the expenditure on the insurance premium is significantly higher than that for the security investment. Overall, Mazzoccoli and Naldi (2020) show that cybersecurity insurance can play an important role in an economically efficient risk management strategy.

The articles just discussed are based on one-period optimization models. In this context, expenditures to reduce cybersecurity risks might be construed as *de facto* operational expenses rather than as "investments" in the traditional sense, or as investments in cybersecurity assets that depreciate fully each period. In either case, intertemporal tradeoffs do not generally arise in this decision-making context, and a rate of return opportunity cost, or discount rate, is not relevant.[2]

Another possible interpretation of the conventional formulation is that the model implicitly represents the steady-state level of investment to maintain a cybersecurity asset in a context where the discount rate is zero, and the value of the cybersecurity asset and the associated depreciation rate are not specified. This implies a particular interpretation of the parameters in the standard GL model (discussed in Section 9). To our knowledge, this interpretation of GL model has not been considered in the literature.

The contribution of this article is to explore the implications of a modified GL model that addresses the benefits and costs of cybersecurity investment within a dynamic analysis over an extended horizon. In this framework, the depreciation and discount rates are explicit, reflecting the fact that software, human capital, and IT equipment do not fully depreciate each period and that the discount rate is a relevant parameter for longer-run decision-making. The motivation is to explore the consequences of these parameters on the optimal level of cybersecurity investment and the implications for the efficient level of risk reduction. This topic has not been modeled in the theoretical GL literature. The depreciation and discount rate parameters are also relevant in the applied benefit-cost analysis of cybersecurity decision-making.

3. DYNAMIC MODEL

This section develops a stylized dynamic investment model of cybersecurity risk reduction to formalize the distinction between shorter- and longer-range investment perspectives. Following the literature on cybersecurity investment, the model is developed from the perspective of an organization that faces the decision problem to choose a cybersecurity system that maximizes the net benefits of cybersecurity risk reductions.

Expenditures on cybersecurity are needed to cover operational inputs, such as labor and utilities, and to finance assets such as software and equipment. Training is also needed to develop the human capital of IT staff and/or organizational employees to maintain best practice communication and security protocols.

[2]The exception is when costs and values are changing over time. In this situation, an intertemporal evaluation is needed.

To sharpen the distinction between the static and dynamic contexts, the model developed here makes the assumption that cybersecurity depends exclusively on an aggregated asset, $K(t)$ ("cybersecurity capital"), which can be thought of as a combination of software, hardware, and human capital. (We will return to the implications of this assumption in later sections of the article). For convenience, it will also be assumed that this asset will be purchased and owned, so that the discount rate and estimates of depreciation come from the organization making the decision about the cybersecurity investment—rather than from a cybersecurity services firm leasing the asset (this assumption will be revisited).

The model will be developed under the assumption that the investment horizon is infinitely long, a temporal perspective embodying the notion that organizations have long lives and think of investments as reoccurring over the long run. The infinite horizon perspective is commonly assumed in the dynamic modeling literature (Arrow & Kruz, 2013; Carlson, Haurie, & Leizarowitz, 2012). In our context, it provides a boundary case on the other end of spectrum from the myopic investment perspective embodied in one period models. This assumption has the benefit of clarifying the distinction between dynamic and static models without fundamentally affecting the results of the comparison.

It is assumed that an organization is certain to experience a cybersecurity attack in each instant, denoted as time "*t*."[3] As in the standard GL model, a boundary case vulnerability, V, for an organization's assets at risk from cybersecurity attacks is defined, with $0 \leq V \leq 1$. The parameter "V" is interpreted as the fraction of the value of an organization's assets that is expected to be damaged in the event of an unprotected breach of the cybersecurity system.

Define "D" as the total value of assets and information, measured in dollars, that the cybersecurity system is designed to protect. To maintain consistency with the standard GL model, this parameter is interpreted as a flow value, and it is assumed to be constant over time. This allows the steady state for the dynamic solution to be compared to the solution from the standard GL model, with the latter interpreted as a steady state arising from repeated decisions. Given this interpretation of "D" and the definition of "V," the combination "VD" represents the total expected monetary losses to an organization at each instant without any cybersecurity measures.

Let "$L(t)$" represent the monetary losses that an organization characterized by VD will incur at time t with cybersecurity assets of $K(t)$ as follows:

$$L(t) = \frac{VD}{(1+\alpha K(t))^{\beta}}, \alpha > 0; \beta \geq 1. \quad (1)$$

$L(t)$ is a convex cybersecurity breach function of the "Type 1" class in Gordon and Loeb (2002). It is chosen for its analytical tractability and the clarity of the comparisons it yields to the standard GL model. The only difference between Equation (1) and the standard formulation is that cybersecurity capital, $K(t)$, is substituted for investment, $I(t)$. While seemingly a minor distinction, this difference has significant implications for the results.

Note that in Equation (1), the α parameter is measured in units per dollar, the β parameter is unitless, and $K(t)$, VD, and $L(t)$ are all measured in dollars. $L(t)$ monotonically declines in $K(t)$, and also monotonically declines in the α and β parameters.

Given Equation (1), the expected reduction in monetary losses, $R(t)$, from reducing cybersecurity risks at time t for an organization having $K(t)$ is:

$$R(t) = VD\left(1 - \frac{1}{(1+\alpha K(t))^{\beta}}\right), \alpha > 0; \beta \geq 1, \quad (2)$$

Using this specification, a continuous time, dynamic extension of the static GL model can be described as:

Maximize wrt $I(t)$

$$\int_0^{\infty} e^{-rt}\left(VD\left(1 - \frac{1}{(1+\alpha K(t))^{\beta}}\right) - I(t)\right)dt, \quad (3)$$

Subject to

$$\frac{\partial K}{\partial t} = I(t) - \delta K(t), \quad (4)$$

with

$$K(0) = K_0, K(t) > 0, \quad r \geq 0, \quad 0 \leq \delta \leq 1. \quad (5)$$

The new variable, $I(t)$, is the level of investment; the new parameters are the discount rate, r, and the depreciation rate, δ. The restrictions $K(0) = K_0$ and $K(t) > 0$ are boundary conditions. Equation (4) shows that the change in the level of the cybersecurity asset, $\partial K/\partial t$, reflects a balance between new investment, $I(t)$, and the depreciation of the asset, $\delta K(t)$. The expression

[3]It is assumed that this threat comes from an amorphous group of attackers whose identities are not known. Hence, a game theoretic dimension where attackers face reprisals is not relevant for this context.

$VD(1-1/(1+\alpha K(t))^{\beta})-I(t)$ in Equation (3) indicates the net flow benefit at time t from reducing cybersecurity risks, measured as the reduction in expected monetary losses, $VD(1-\frac{1}{(1+\alpha K(t))^{\beta}})$, less the costs of new investment, $I(t)$. The dynamic investment decision is to choose $I(t)$ to maximize the sum of the discounted stream of net flow benefits shown in Equation (3), given the effects of $I(t)$ on $K(t)$ as expressed through the equation for $\frac{\partial K}{\partial t}$ in (4).

As noted, the decision problem described in Equations (3)–(5) follows the cybersecurity literature in assuming that the decision-making perspective is that of an organization investing in its own cybersecurity needs. It is worth noting, however, that the described model could also be interpreted as representing the decision problem of a security services firm choosing $I(t)$ to maximize profits from the sale or leasing of cybersecurity security products and services. The willingness to pay for such services would be derived from the expected reduction in monetary losses an organization would accrue from purchasing them. In this case, $R(t)$ in Equation (2) could be construed as the expected willingness to pay of an organization to purchase the services of a security firm having $K(t)$. The firm could monetize this willingness to pay as revenue received. Interpreted as such, the goal for the cybersecurity services firm would be to choose $I(t)$ to maximize the stream of net profits, $R(t)-I(t)$ Equation (3) subject to Equation (4) and the boundary conditions in Equation (5). With this possible interpretation noted, we will continue to maintain the interpretation in the GL literature that the decision problem is conducted from the perspective of an organization investing in its own cybersecurity needs.

It is convenient to use optimal control theory to solve the optimization problem described in Equations (3)–(5), and in this particular context, to combine Equation (2) and (3) into a "current value Hamiltonian:"[4]

$$H(t) = VD\left(1-\frac{1}{(1+\alpha K(t))^{\beta}}\right)-I(t) + \lambda(t)\left(I(t)-\delta K(t)\right). \quad (6)$$

The new variable, $\lambda(t)$, is a Lagrangian type multiplier. It can be interpreted as a shadow price that indicates the marginal value of the cybersecurity asset at time t, expressed in current period terms.

[4]See Kamien and Schwartz (2012) and Chiang (1992). Dorfman (1969) offers an intuitive explanation.

4. STEADY-STATE SOLUTIONS

Suppressing the time subscripts to reduce notational clutter, the first order conditions for this problem can be stated as:

$$\frac{\partial H}{\partial I} = -1+\lambda = 0 \rightarrow \lambda = 1, \quad (7)$$

$$\frac{\partial \lambda}{\partial t} = r\lambda - \frac{\partial H}{\partial K} \rightarrow \frac{\partial \lambda}{\partial t} = r\lambda - \left(\frac{\alpha\beta VD}{(1+\alpha K)^{(1+\beta)}}\right)+\lambda\delta \quad (8)$$

The constraint in Equation (4) also has to hold.[5]

Note that the constant value $\lambda = 1$ from Equation (7) implies that $\partial\lambda/\partial t = 0$. Substituting $\lambda = 1$ and $\partial\lambda/\partial t = 0$ into Equation (8) gives:

$$\left(\frac{\alpha\beta VD}{(1+\alpha K)^{(1+\beta)}}\right) = r+\delta. \quad (9)$$

Equations (7) and (9) and the constraint in (4) define the solution conditions for the optimal level of investment (I_d^*) and the size of cybersecurity asset (K_d^*). Equation (7) shows that investment should be continued up to the point that the marginal cost it imposes in lost current net benefits, which is "1" in this case, just equals the current value of the marginal gain, λ, from increasing the cybersecurity asset, $\frac{\partial K}{\partial t}$. Equation (9) says that investment should be carried to the point that the marginal value of the additional cybersecurity asset in reducing expected monetary losses, $(\frac{\alpha\beta VD}{(1+\alpha K)^{(1+\beta)}})$, is equal to its rate of return and depreciation opportunity costs, $(r+\delta)$.

Equation (9) implies that the optimal level of cybersecurity capital is constant for all t. Solving Equation (9) for this constant gives:

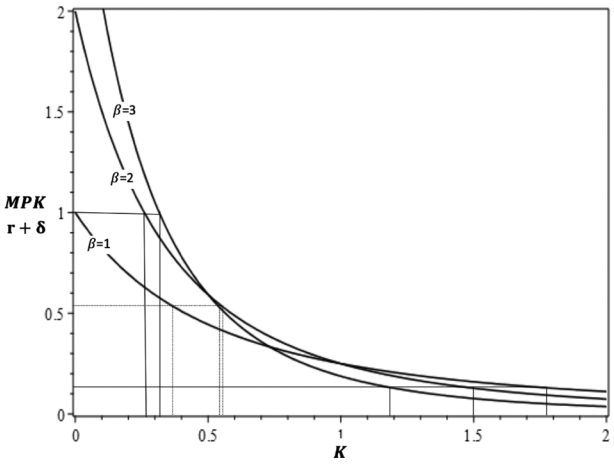
$$K_d^* = \frac{1}{\alpha}\left[\left(\frac{\alpha\beta VD}{(r+\delta)}\right)^{\frac{1}{(1+\beta)}}-1\right], \text{for all } t. \quad (10)$$

The time subscript is suppressed for convenience.[6]

[5]See Kamien and Schwartz (2012). The concavity of the Hamiltonian implies that the first orders are sufficient for a maximum. A sufficient transversally condition for this type of problem is that $K(t) \geq 0$ in the limit as $t \rightarrow \infty$(Chiang, 1992). This condition holds in our case by assumption (See Equation (4)). It is also consistent with the steady-state solution that results from the optimization.

[6]The condition in Equation (5) that $K_d^* > 0$ implies a positive profit condition has to be met for Equation (10) to hold. This implies that $(\alpha\beta VD/(r+\delta))^{1/(1+\beta)}-1>0$, or that $\alpha\beta VD > r+\delta$.

Panel A: ($VD = 1, \alpha = 1$; β at 1, 2, 3)



Panel B: ($VD = 1, \beta = 2$; α at .75, 1, and 1.25)

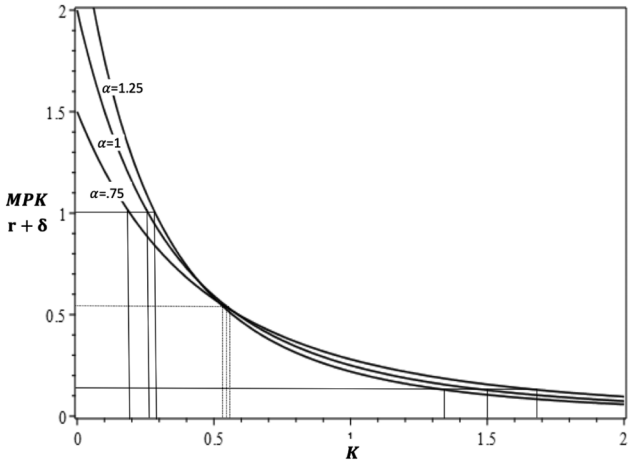


Fig 1. Cybersecurity capital with parameter variation.

Equation (10) shows that K_d^* will decline with a rise in the rate of return on capital, r, and the depreciation rate, δ, and increase with a rise in the level of expected monetary losses from an unprotected cybersecurity attack, VD. The relationship between K_d^* and the α and β parameters are ambiguous.[7]

5. CYBERSECURITY SYSTEM SIZE IN THE STANDARD AND DYNAMIC MODELS

Denoting variables with the subscript "s" as the solution values for the standard GL model, and using our notation, the solution for the GL model using a "type 1" security breach function is:

$$K_s^* = \frac{(\alpha\beta VD)^{\frac{1}{1+\beta}} - 1}{\alpha} \tag{11}$$

Note that this solution is the same as the dynamic solution in Equation (10) when $r + \delta = 1$. The particular case that $r = 0$ and $\delta = 1$ corresponds to the interpretation of the standard GL model as implicitly representing an operational expense, or the level of a cybersecurity asset that depreciates fully. Under these conditions, the investment equilibrium condition $I_s^* = \delta K_s^*$ reduces to $I_s^* = K_s^*$. In other words, with $\delta = 1$ there is no difference between the size of a cybersecurity asset and the level of investment needed to maintain it.

To provide some intuition, the left hand side of Equation (9), $(\frac{\alpha\beta VD}{(1+\alpha K)^{(1+\beta)}})$, representing the marginal value of additional cybersecurity capital (MPK), is plotted in Fig. 1, with MPK on the vertical axis and the value of cybersecurity capital, K, on the horizontal axis. The declining slope of the MPK curve (in absolute value terms) reflects the log convex form of the cybersecurity breach function. Panel A shows the impact of variation in the β parameter, letting $\alpha = 1$, while Panel B shows the variation in the α parameter, setting $\beta = 2$. In both panels the expected damages from cybersecurity risks without any cybersecurity system in place, VD, is set equal to 1.

The horizontal lines indicate different values for $r + \delta$ from the right-hand side of Equation (9). Because the equilibrium condition in Equation (9) is attained when $MPK = r + \delta$, the intersection of the MPK curves with the $r + \delta$ lines in Fig. 1 shows the equilibrium level of the cybersecurity capital (K). The benchmark case for the standard GL model is at the intersection of the MPK curves and the horizontal line for $r + \delta = 1$.

The other horizontal lines in Fig. 1 reflect assumptions for higher and lower bounds for $r + \delta$ relevant for dynamic investment evaluation. Real social discount rates of 3% and 7% are recommended for use in the regulatory impact analysis of federal regulations (U.S. Office of Management and Budget, 2003). The 7% rate is taken to represent the

[7]It can be shown that $\partial K_d^*/\partial\alpha > 0$ when $\alpha > (1+\beta)(r+\delta)/\beta^2(1+\beta/\beta)^\beta = X$, $\partial K_d^*/\partial\alpha = 0$ when $\alpha = X$, and $\partial K_d^*/\partial\alpha < 0$ when $\alpha < X$. Also, $\partial K_d^*/\partial\beta > 0$ when $\beta > 1/\mathrm{W}(1/e \cdot \alpha/r + \delta) = Y$, where W represents a lambert function; $\partial K_d^*/\partial\beta = 0$ when $\beta = Y$, $\partial K_d^*/\partial\beta < 0$ $\partial K_d^*/\partial\beta < 0$ when $\beta < Y$.

rate of return on private capital. Firms might also add transactions costs and risk premia to real discount rates, raising them further. We assume that different organizations will use discount rates falling in a range between 0.03 and 0.20.

Turning to depreciation, larger organizations typically replace IT equipment on three- to five-year cycles, while resources are scarcer in small or medium enterprises (SMEs) and equipment replacements may be stretched to up to 10 years (Hayes & Bodhani, 2013). SMEs are also less likely to regularly update software than large firms, under the mistaken assumption that smaller enterprises are less vulnerable to cybersecurity risks than larger organizations (Hayes & Bodhani, 2013). Lacking other information, it will be assumed that organizations are likely to face depreciation rates varying between about 0.1 and 0.33. Including the range noted for discount rates, this implies typical values for $r+\delta$ are likely to range from 0.13 ($r=0.03, \delta=0.1$) on the low side to 0.53 ($r=0.2, \delta=0.33$) on the high side. These bounds should be taken as illustrative, given the lack of empirical information about depreciation for all of the components that comprise cybersecurity assets, including software, hardware, and human capital.

Turning to Fig. 1 Panel A, the $r+\delta=1$ line represents the benchmark case—the standard GL model. It shows that the efficient level of cybersecurity capital is 0, 0.25, and 0.31 respectively for β values of 1, 2, and 3.[8] Because $VD=1$, these figures can be interpreted as the fraction of cybersecurity investment or capital (again investment and capital are equivalent when $\delta=1$) relative to total damages that would be expected from cybersecurity risks in the absence of any investment or capital (again, VD is interpreted as a flow value).

Turning to the dynamic model, consider first the case that $r+\delta=0.13$. For β values of 1, 2, and 3, the corresponding size of the capital asset is 1.77, 1.5, and 1.19. Three comments about these results are relevant. First, this pattern reflects the ambiguity in the sign of $\partial K_d^*/\partial\beta$ as noted before (see footnote 7). For the parametrization shown, $\frac{\partial K_d^*}{\partial\beta}>0$ for $r+\delta>0.7$, while $\frac{\partial K_d^*}{\partial\beta}<0$ for $r+\delta<0.25$. Given that $r+\delta$ value in the standard GL model is above the 0.7 threshold, while $r+\delta=0.13$ is beneath 0.25, increasing β has opposite effects on the size of the capital asset in the standard GL model and the dynamic GL model. The second point is that the size of cybersecurity capital in the dynamic model is larger than VD for all of the β permutations. This can occur because K_d^* is a stock while VD is a flow variable. Assuming the discount rate of 0.03, the present value of $VD=1$ is 1/0.03 or 33.33. The value of capital is a small fraction of this number for any of the β permutations. Finally, the size of the capital asset is higher in the dynamic model than in the standard model for any value of β, that is, by the amount 1.77 for $\beta=1$, 1.24 for $\beta=2$, and 0.88 for $\beta=3$.

Turning to the $r+\delta=.53$ case, the value of capital for β values at 1, 2, and 3 are 0.37, 0.56, and 0.54. These results show that $r+\delta=0.53$ is a range where the sign of $\partial K_d^*/\partial\beta$ is ambiguous (positive going from $\beta=1$ to $\beta=2$, but negative going from $\beta=2$ to $\beta=3$). The size of capital for any β permutation is higher in the dynamic model with $r+\delta<1$, than for the standard GL model with $r+\delta=1$.

Panel B of Fig. 1 shows variations in the α parameter letting $\beta=2$. The results are qualitatively the same as for the β permutations. In this case, $\partial K_d^*/\partial\alpha>0$ for $r+\delta>0.7$ and $\partial K_d^*/\partial\alpha<0$ for $r+\delta<0.4$. For the standard GL Model at $r+\delta=1$, capital values vary from 0.19 to 0.28 as α varies from 0.75 to 1.25, while for the dynamic model at $r+\delta=0.13$, capital values vary from 1.68 to 1.34 for α values between 0.75 and 1.25. In the neighborhood of intersection points of the MPK curve with the $r+\delta=0.53$ line, the values of all the permutations are quite close, with α values of 0.75, 1, and 1.25 corresponding to capital values of 0.55, 0.56, and 0.54.

To provide additional perspective on how discount and depreciation rates affect the economically-efficient size of cybersecurity capital, Fig. 2 plots cybersecurity capital (Panel A) and the relative comparison between the standard and dynamic models (Panel B) that correspond to isolines for constant sums for different combinations of r and δ. (It is assumed that $\alpha=1$ and $\beta=2$). The far-right corner on the horizontal axes for the $r+\delta=1$ isoline, where $r=0$ and $\delta=1$, is consistent with the standard GL model. The highlighted boxes encompass combinations ranging from $r+\delta=0.13$ to $r+\delta=0.53$. The southwest corner above and close to the $r+\delta=0.1$ isoline represents $r=0.03, \delta=0.1$, while the northeast corner lying above and near to the $r+\delta=0.5$ isoline represents $r=0.20, \delta=0.33$. The discount rate and depreciation rate combinations within the boxes lie on isolines between these points.

[8]The zero result arises from the fact that the positive profit condition $\alpha\beta VD>r+\delta$ is not satisfied, given the particular parameter values for this case, that is, $\alpha=1$, $\beta=1$, $VD=1$, and $r+\delta=1$.

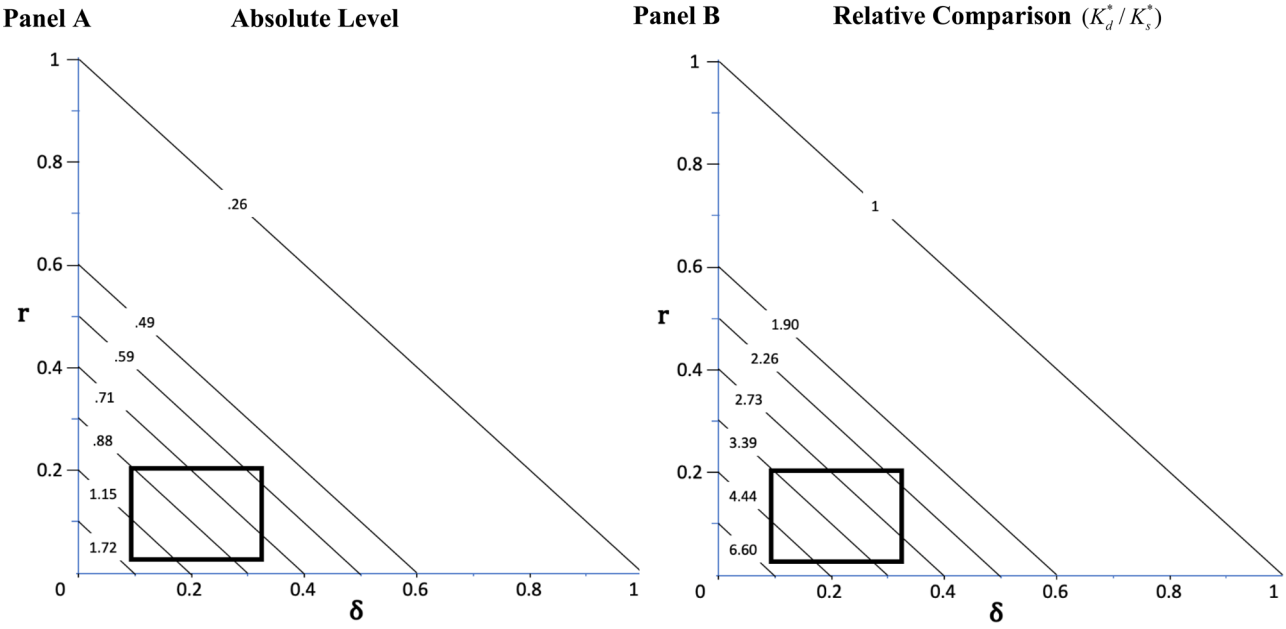


Fig 2. Cybersecurity capital in the dynamic and standard model ($VD = 1, \alpha = 1, \beta = 2$).

Turning to Panel A, the point on the northeast corner of the box gives a value for K_d^* of about 0.56. With $r = 0.20$ and $VD = 1$, the corresponding present value for the expected monetary losses avoided when cyber risks are reduced is (1/0.2), or 5. The southwest corner of the box gives a value for K_d^* of about 1.49. At the corresponding discount rate of $r = 0.03$, the present value of the expected monetary losses avoided is 33.3. The size of cybersecurity assets and their relationship to the present value of VD for other discount rate and depreciation rate combinations within the box will fall between these boundaries. The corresponding solution for the standard model is 0.26.

Panel B of Fig. 2 plots the ratios K_d^*/K_s^* to provide relative comparisons between the dynamic and standard GL models. This ratio varies from 5.72 at the southwest corner with $r = 0.03$ and $\delta = 0.1$ to 2.14 at the northeast corner with $r = 0.20$ and $\delta = 0.33$. The ratios for the other discount and depreciation combinations fall between these points.

6. USER COST IN THE STANDARD AND DYNAMIC MODELS

The user cost, C, of a capital asset, K, reflects rate of return (r) and depreciation (δ) components, with $C \equiv (r + \delta)K$(Dorfman, 1969; Hall & Jorgenson, 1967). The user cost gives the measure of the flow opportunity cost at time t from holding a capital stock. For example, if an organization borrowed to finance the purchase of a cybersecurity asset having value K, rK would be the interest charges required to service the loan, while δK would be the expenditure required to cover depreciation losses. If the asset was leased, C would be the lease payment charged to cover the rate of return and depreciation opportunity costs of the security services firm supplying the asset.

Given that $C^* \equiv (r + \delta)K^*$, user cost in the standard GL model reduces to K_s^*. In other words, with $r = 0$ and $\delta = 1$, $K_s^* = C_s^* = I_s^*$ (with the equivalence of $K_s^* = I_s^*$ coming from Equation (4) with $\delta = 1$) in the standard model. For the dynamic model, these variables are all different. Using Equation (10), user cost in the dynamic context is:

$$C_d^* = (r + \delta)K_d^* = \frac{r + \delta}{\alpha}\left[\left(\frac{\alpha\beta VD}{(r + \delta)}\right)^{\frac{1}{(1+\beta)}} - 1\right]. \quad (12)$$

The difference in magnitude between the user cost of capital in the dynamic model, C_d^*, and in the static model, C_s^*, will depend how C_d^* responds to changes in the values of $r + \delta$. Differentiating $C_d^* = (r + \delta)K_d^*$ with respect to $(r + \delta)$ gives:

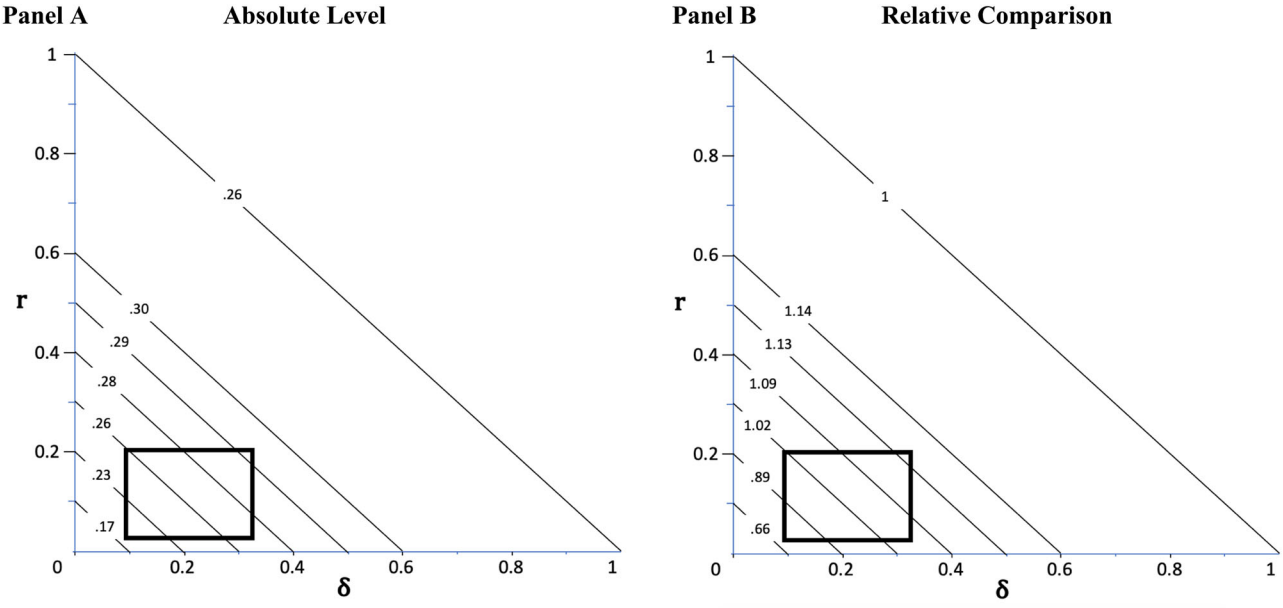


Fig 3. User cost in the dynamic and standard model ($VD = 1, \alpha = 1, \beta = 2$).

$$\frac{\partial C_d^*}{\partial(\delta + r)} = K_d^* + (\delta + r)\frac{\partial K_d^*}{d(\delta + r)}, \tag{13a}$$

$$\frac{\partial C_d^*}{\partial(\delta + r)} = K_d^*\left(1 + \frac{(\delta + r)}{K_d^*}\frac{\partial K_d^{*^*}}{\partial(\delta + r)}\right), \tag{13b}$$

$$\frac{\partial C_d^*}{\partial(\delta + r)} = K_d^*\left(1 + \eta_{r+d}\right). \tag{13c}$$

The expression $\eta_{r+d} \equiv \frac{(\delta+r)}{K_d^*}\frac{\partial K_d^*}{\partial(\delta+r)}$ in Equation (13c) is an "elasticity." It indicates the proportional change in the equilibrium level of the cybersecurity asset with a proportional change in $r + \delta$.[9] The sign of η_{r+d} is negative given that $\frac{\partial K_d^*}{\partial(\delta+r)} < 0$ (as evident in Equation (10) and Fig. 1). In terms of the effect of η_{r+d} on the sign of $\frac{\partial C_d^*}{\partial(\delta+r)}$, Equation (13c) shows that if $-1 < \eta_{r+d} \leq 0$, $\frac{\partial C_d^*}{\partial(r+\delta)} > 0$; if $\eta_{r+d} = -1$, $\frac{\partial C_d^*}{\partial(r+\delta)} = 0$, and if $-\infty \leq \eta_{r+d} < -1$, $\frac{\partial C_d^*}{\partial(r+\delta)} < 0$. These effects are driven by the two parts of Equation (13a). The first term, K_d^*, is positive. That is, holding the equilibrium level of the asset constant, (for example, letting the second term $\frac{\partial K_d^*}{d(\delta+r)} = 0$), user cost has to go up as $r + \delta$ increases. However, with the second term negative ($\frac{\partial K_d^*}{d(\delta+r)} < 0$), the base upon which r and δ are applied is reduced as $r + \delta$ increases. Whether the first or second terms dominate will determine the magnitude of $\eta_{r+\delta}$ and the sign of $\frac{\partial C_d^*}{\partial(\delta+r)}$.

Panel A in Fig. 3 shows user cost in the dynamic model (C_d^*) and static model (C_s^*), while Panel B indicates the relative comparison C_d^*/C_s^*. The user cost is about 0.19 in Panel A at the southeast corner of the box ($r = 0.03, \delta = 0.1$), and is slightly higher than 0.29 at the northeast corner ($r = 0.02, \delta = 0.33$). Comparing these to the user cost from the standard model, it evident that user costs in the dynamic model can be higher or lower than for the standard model. The relative comparison in Panel B indicates that user cost in the dynamic model is close to 0.68 of that in the standard model at the southeast corner ($r = 0.03, \delta = 0.1$) and slightly more than 1.13 times higher at the northeast corner ($r = 0.20, \delta = 0.33$).

These relative comparisons reflect the value of the elasticity, η_{r+d}. It is greater than 1 in absolute value from $r + \delta = 1$ to between $r + \delta = 0.54$ and $r + \delta = 0.53$. For $r + \delta < 0.53$, the absolute value of η_{r+d} is less than 1. Consistently with Panel A in Fig. 3, this implies that user cost will increase as $r + \delta$ declines from 1 to between 0.54 and 0.53, and starts to decrease as $r + \delta$ declines further. Or going in the opposite direction—starting at $r + \delta = 0.13$, for example, and increasing $r + \delta$—user costs will rise until

[9]For example, an elasticity of -2 implies that a 1% increase in $r + \delta$ will lower the equilibrium value of K_d^* by 2%.

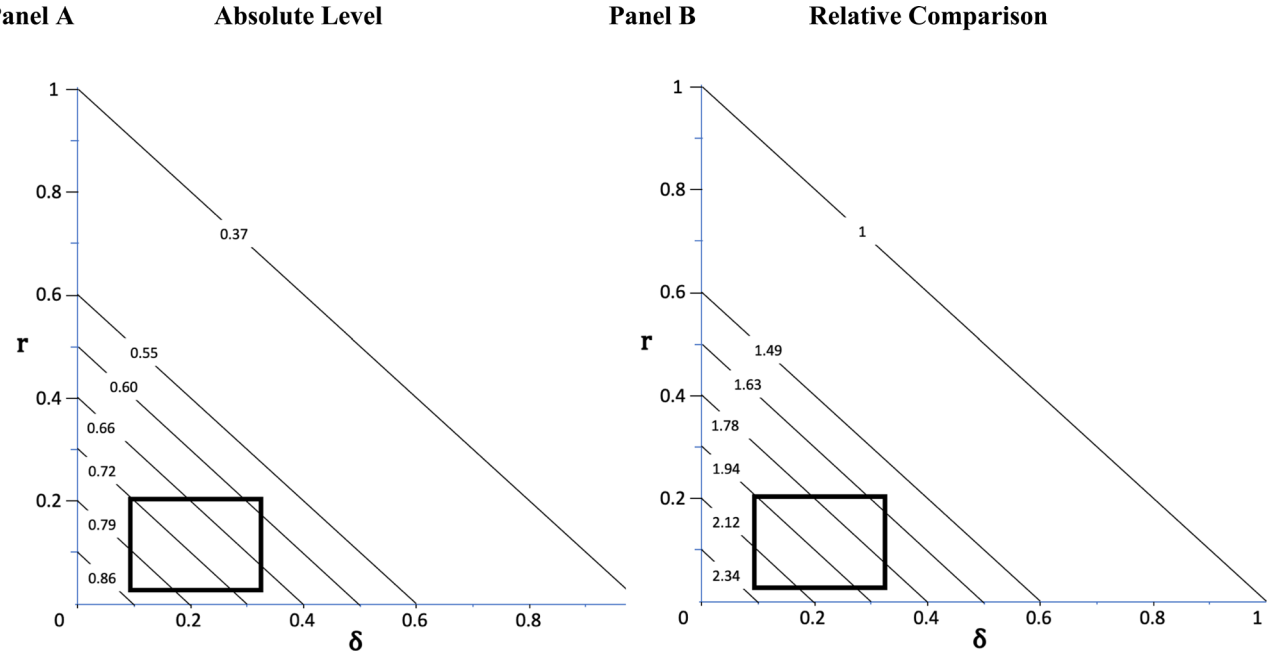


Fig 4. Expected value of monetary loss reduction from reducing cybersecurity risks in the dynamic and standard models ($VD = 1, \alpha = 1, \beta = 2$).

somewhere in the neighborhood of $r + \delta = 0.53$, and then begin to decline as $r + \delta$ increases further.

Regardless of whether user cost in the dynamic model is higher or lower than in the standard model, the associated level of cybersecurity capital will be different (again see Fig. 2). As an example, the parameter configuration $r + \delta = 0.3$ for the dynamic model gives about the same user cost, 0.26, as in the standard model. However, the cybersecurity capital associated with this user cost is $K_d^* = 0.26/0.3$, about 0.87—or 3.33 times larger than the capital stock/user cost of 0.26 in the static mode1.[10] In short, even when user costs in the dynamic and standard models are the same, they can correspond to significant differences in the size of cybersecurity assets. This possibility implies that equivalent flow expenditures on cybersecurity in the two models could correspond to significantly different cybersecurity risk reductions.

7. ECONOMICALLY EFFICIENT RISK REDUCTION IN THE STANDARD AND DYANAMIC MODELS

We now consider how steady states for cybersecurity assets translate into steady states for expected monetary loss reductions associated with reducing cybersecurity risks. These figures are derived from entering K_d^* and K_s^* into Equation (2) to get the reduced form for flow risk reductions in the standard and dynamic GL models. Panel A of Fig. 4 shows the associated monetary losses avoided in absolute terms. Again because $VD = 1$, these numbers also show the fraction of potential monetary losses avoided from reducing cybersecurity risks compared to the expected total damages with $K_d^* = 0$. The Figure shows that the expected monetary losses avoided range from about 0.59 for $r = 0.20, \delta = 0.33$ at the northeast corner of the box in the Figure to about 0.84 for $r = 0.03, \delta = 0.1$ at the southwest corner. The corresponding number for the static GL model is 0.37. These differences reflect the fact that the steady state levels for K_d^* vary with $r + \delta$, and with $r + \delta < 1$, $K_d^* > K_s^*$, providing greater risk reductions in the dynamic model than in the standard model. The ratio of expected monetary losses in the two models (measured as R_d^*/R_s^*) various from about 1.61 at $r = 0.20, \delta = 0.33$ to about 2.32 at $r = 0.03, \delta = 0.13$ (See Fig. 4 Panel B).

[10]The discrepancies between these numbers and those shown in Fig. 2 are due to rounding error.

8. EFFICIENT MAXIMUMUS FOR CYBER SYSTEM SIZE, USER COST, AND RISK REDUCTION

A common topic in the literature on cybersecurity investment is the maximum investment level that could be economically efficient as a share of the maximum expected monetary losses that could be avoided from risk reduction (Baryshnikov, 2012; Farrow & Szanton, 2016; Hausken, 2006; Willemson, 2010). To illustrate the conclusion from the standard GL model, divide both sides of Equation (11) by VD and substitute in $x_s \equiv \alpha VD$ to get:

$$\frac{K_s^*}{VD} = \frac{(x_s\beta)^{\frac{1}{(1+\beta)}} - 1}{x_s}. \tag{14}$$

Gordon and Loeb (2002) show that maximizing this expression for x_s gives the solution $x_s = (1+\beta)^{(1+\beta)}\beta^{(-2-B)}$. Substituting this solution into Equation (14) and letting $\beta \to \infty$ gives:

$$Max\frac{K_s^*}{VD} = \frac{1}{e} \approx .37. \tag{15}$$

As a point of comparison, this number compares to the K_s^* values for the standard GL model in Fig. 1 that range from to zero to 0.31 (for the parameter values indicated in Panels A and B).

Turning to the dynamic model, efficient maximums for both K_d^* and C_d^* can be computed (because $K_d^* \neq C_d^*$). For K_d^*, divide both sides of Equation (10) by VD and substitute $x_d \equiv \frac{\alpha VD}{(r+\delta)}$ giving:

$$\frac{K_d^*}{VD} = \frac{1}{(r+\delta)x_d}\left[(\beta x_d)^{\frac{1}{(1+\beta)}} - 1\right]. \tag{16}$$

This has the same functional form as Equation (14) with the multiplier $(r+\delta)$ in the denominator. Hence, in the limit, the efficient size of K_d^* goes to:

$$Max\frac{K_d^*}{VD} \approx \frac{0.37}{r+\delta}. \tag{17}$$

For the illustrative combinations $r+\delta = 0.53$ and $r+\delta = 0.13$, this implies maximums of about 0.70 and 2.84, respectively. As a point of comparison, these figures compare to about 0.56 and 1.49 respectively for the corresponding $r+\delta$ parameter configurations in Panel A Fig. 2, using the nonlimiting parameter values $\alpha = 1, \beta = 2$.

Given the functional relationship $C_d^* = (r+\delta)K_d^*$, multiplying both sides of (16) by $(r+\delta)$ will give the equivalent form for the expression for C_d^*/VD as for C_s^*/VD in Equation (14). In short, the efficient maximum for C_d^*/VD is also 0.37.

Lastly, it is possible to compute the maximum economically efficient expected reductions in monetary losses associated with reducing cybersecurity risks. Equation (2) implies:

$$\frac{R^*}{VD} = \left(1 - \frac{1}{(1+\alpha K(t))^{\beta}}\right). \tag{18}$$

Note that $\alpha > 0$ and $K(t) > 0$ by assumption (see (2) and (5)), so that $1+\alpha K(t) > 1$. This implies $(1+\alpha K(t))^{\beta} \to \infty$ as $\beta \to \infty$, implying that $\frac{1}{(1+\alpha K(t))^{\beta}} \to 0$, which implies that $\frac{R^*}{VD} \to 1$.

In other words, whatever level of cybersecurity capital is economically efficient, so long as it is positive the maximum level of risk reduction is 100% as $\beta \to \infty$. This does not seem like an informative result, and raises questions about the relevance of limiting parameter extremes for the evaluation of cybersecurity investment. Finding empirically reasonable parameter values to calibrate cybersecurity investment models would seem to be a more fruitful approach.

9. MODEL EXTENSIONS

The solutions for the dynamic model is a steady state, reflecting the assumption that parameter values such as expected damages from cybersecurity risks are constant over time. As such, the solution could be reproduced from a representative slice of the problem at time t. It is informative to compare this model to the standard GL model.

Suppressing the time subscripts, this formulation is:

$$\text{NB} = VD\left(1 - \frac{1}{(1+\alpha K)^{\beta}}\right) - (r+\delta)K. \tag{19}$$

NB in Equation (19) represents the flow net-benefits from cybersecurity risk reduction as the difference between expected damage reduction with cybersecurity capital, K, (first term on the right-hand side), less the user cost of cybersecurity capital, $C = (r+\delta)K$(second term). Maximizing Equation (19) with respect to K will reproduce the first order conditions in Equation (9) and the solution for K_d^* in Equation (10). As such, Equation (19) would be a convenient way to represent the dynamic optimization described in Equations (3)–(5).

In the special case that the discount rate is zero, it is also possible to reinterpret the standard GL model in order to construe its solution as representing the steady-state investment required to maintain some

level of cybersecurity capital. While the details of this translation are specific to the breach function used in this article, the point—that the GL model can have more than one interpretation—should be more general. To illustrate in our context, rewrite the standard GL model as:

$$\text{NB} = VD\left(1 - \frac{1}{(1+\theta I)^{\beta}}\right) - I. \tag{20}$$

In Equation (20), $\theta \equiv \alpha/\delta$, so that $\theta I = \alpha I/\delta = \alpha K$. (This makes use of the equilibrium relationship $I = \delta K$). Maximizing Equation (20) with respect to I will give a solution that has the equivalent form as Equation (11) for the standard GL model:

$$I^* = \frac{(\theta\beta VD)^{\frac{1}{1+\beta}} - 1}{\theta}. \tag{21}$$

The solution in Equation (21) might be interpreted as representing a steady-state level of investment required to maintain an unspecified level of capital stock with its associated depreciation rate. However, making the depreciation explicit and substituting back α/δ for θ in Equation (21) gives the solution $I^*/\delta = K^*$. This translation makes I^* in Equation (20) equivalent to the expression for user cost in Equation (12) in the dynamic model for the special case that $r = 0$. The interpretation of the GL model as representing a steady-state investment flow for some implicit depreciation rate in the special case that $r = 0$ might be useful in some contexts.

10. DISCUSSION

The preceding analysis shows that for the same definition of parameters in the cybersecurity breach function, a dynamic version of the GL model gives different results than the standard model with respect to user costs, the economically efficient level of cybersecurity assets, and the efficient level of cybersecurity risk reductions. In particular, the optimal level of cybersecurity assets and the degree of risk reduction are greater in the dynamic model than for the standard GL model. This follows from the fact that the price of cybersecurity assets, at $r + \delta < 1$, is less than the implicit price in the standard model, at $r + \delta = 1$. This difference makes additional investment and risk reductions economically efficient in the dynamic model.

This conclusion is based on a stylized model that highlights the implications of a dynamic investment evaluation. This formulation sharpens the distinction between short-term and long-term investment horizons. Future research could explore the effects of different timeframes on the economically efficient level of cybersecurity risk reductions.

The model also treats cybersecurity inputs as an asset. A useful research extension would be to embed a production process into the breach function that includes both operational expenditures and cybersecurity assets, allowing the parameter values for these two inputs to differ. In one study, the share of expenditures on operational inputs versus assets for IT as a category was about 0.45 and 0.55, respectively, with the latter broken down further as 0.26 for hardware and 0.29 for software (OMTCO, 2012). It would be desirable to differentiate these estimates for specific evaluation contexts, such as between SMEs and larger organizations, and to assess the implications for the economically efficient level of cybersecurity risk reduction.

The results in the study are based on particular log convex cybersecurity security breach function. As noted earlier, a number of other functional forms for breach functions have been considered in the literature. This suggests that formulating the dynamic model with different cybersecurity breach functions would be a useful research extension.

Cybersecurity risks, the performance of cybersecurity systems, and cybersecurity costs are all uncertain. The rate of depreciation of cybersecurity software is itself an uncertain parameter, given that obsolesce reflects the evolution of cybersecurity risks. An element of uncertainty is the possible irreversible consequences of cyberattacks, including damage to reputations, loss of data or intellectual property, or damage to physical systems. Incorporating uncertainty and irreversibility into the economic analysis of cybersecurity security risks would improve the economic assessment of cybersecurity investment.

Uncertainties and irreversibilities might also affect organizational choices about the decision to lease cybersecurity products and services rather than owning them. A "real options" framework might be used to assess the tradeoff involved, and the implications for the economically efficient level of risk reduction. As just one example, it might be economically efficient to lease IT equipment if technology performance is rapidly improving over time.[11]

[11] See Dixit and Pindyck (1994) and Farrow (2004) for a discussion of real options.

The article has followed the literature in treating cybersecurity investment from the perspective of the demand side of the market, that is, from the perspective of a "user" organization making decisions about investing resources to reduce its own cybersecurity risks. As noted before, cybersecurity services firms should be able to earn revenue equal to the expected damage reductions that user organizations would receive from the purchase and use of cybersecurity products and services. This equivalence allows the reinterpretation of the model in this article as the decision-making of a profit-maximizing cybersecurity services firm. In this context, it seems plausible that discount and depreciation rates for cybersecurity firms differ from those of organizations analyzing their own investment options, creating differences between the leasing rates that cybersecurity firms charge and the user costs of organizations making cybersecurity investments. The comparative advantage of leasing versus ownership, given these differences, and the implications for economically efficient cybersecurity risk reductions, would be another promising avenue for research.

11. CONCLUSION

This article has developed a dynamic extension of the influential model of cybersecurity investment formulated in Gordon and Loeb (2002). In this dynamic setting, the rate at which cybersecurity assets depreciate and the rate of discount are important parameters. All else constant, lower rates of depreciation reduce the cost of investing in cybersecurity assets, increasing the efficient size of the cybersecurity system, while higher discount rates impose higher rate-of-return opportunity costs, reducing the economically efficient size of the cybersecurity system. However, the sum of these cost-of-capital components are empirically likely to be lower than is implicitly assumed in the standard GL model. This difference increases the economically efficient level of risk reduction in the dynamic model compared to the standard model for the same definition of parameters in the cybersecurity breach function.

These results raise the possibility that the usual investment analyses of cybersecurity are underestimating the economically efficient level of cyber risk reduction, with the implication that the social benefits of cybersecurity are also larger than is commonly assumed in view of the spill-over effects from private investments. The results also suggest that the comparative economic evaluation of cybersecurity security investments with other risk management strategies such as the purchase of cyber insurance might be overestimating the relative value of these other strategies.

These are tentative conclusions based on the particular model developed. Modeling a cybersecurity production process that differentiates the risk-reducing effects of both operational expenses and cybersecurity assets would be a useful step forward. Empirical specification of this kind of production process would improve the use of applied benefit-cost analyses to help support the implementation of cybersecurity procedures, including the NIST cybersecurity framework of the U.S. federal government.

ACKNOWLEDGMENT

We greatly appreciate comments and suggestions from Nate Evans, Larry Gordon, and Scott Shackelford; exchanges with participants at NATO Workshop IST-153; and comments from the cybersecurity group at the Ostrom Workshop at Indiana University. Mike Bennett, Kevin Reynolds, and John Walker offered technical insights. Comments from two anonymous referees significantly improved the article. The usual disclaimer applies: the authors are solely responsible for the results, conclusions, and any errors in the article.

REFERENCES

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610–613.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., … Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 265–300). Berlin, Heidelberg: Springer.

Anderson, R., Barton, C., Böhlme, R., Clayton, R., Ganán, C., Grasso, T., … Vasek, M. (2019). Measuring the changing cost of cybercrime. Paper presented at the Workshop on the Economics of Information Security (WEIS), Boston, MA.

Arrow, K. J., & Kruz, M. (2013). *Public investment, the rate of return, and optimal fiscal policy*. New York: RFF Press.

Baggott, S. S., & Santos, J. R. (2020). A risk analysis framework for cybersecurity security and critical infrastructure protection of the U.S. electric power grid. *Risk Analysis*, *40*(9), 1744–1761. https://doi.org/10.1111/risa.13511

Baryshnikov, Y. (2012). IT security investment and Gordon-Loeb's 1/e Rule. Proceedings of the 11th Workshop on the Economics of Information Security (WEIS), Berlin, 25–26 June 2012.

Carlson, D. A., Haurie, A. B., & Leizarowitz, A. (2012). *Infinite horizon optimal control: Deterministic and stochastic systems*. Berlin, Heidelberg: Springer Science & Business Media.

Council of Economic Advisors, (2018). The Cost of Malicious Cybersecurity Activity to the U.S. Economy.

Chiang, A. (1992). *Elements of Dynamic Optimization*. New York: McGraw-Hill, Inc.

Coburn, A., Leverett, E., & Woo, G. (2019). *Solving cybersecurity risk: Protecting your company and society*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Dixit, A. K., & Pindyck, R.S. (1994). *Investment under uncertainty*. Princeton, N.J: Princeton University Press.

Dorfman, R. (1969). An economic interpretation of optimal control theory. *The American Economic Review*, *59*(5), 817–831.

Executive Order 13800 (2017). Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

Farrow, S. (2007). The economics of homeland security expenditures: Foundational expected cost-effectiveness approaches. *Contemporary Economic Policy*, *25*(1), 14–26.

Farrow, S. (2004). Using risk assessment, benefit cost analysis, and real options to implement a precautionary principle. *Risk Analysis*, *24*(3), 727–735.

Farrow, S., & Szanton, J. (2016). Cybersecurity investment guidance: Extensions of the Gordon and Loeb model. *Journal of Information Security*, *7*, 15–28.

Geer, D., Jardine, E., & Leverett, E. (2020). On market concentration and cybersecurity risk. *Journal of Cybersecurity Policy*, *5*(1), 9–29. https://doi.org/10.1080/23738871.2020.1728355

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*, 438–457.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cybersecurity-risk management. *Communications of the ACM*, *46*, 81–85.

Gordon, L. A., & Loeb, M. P. (2005). *Managing cybersecurity resources: A cost-benefit analysis* (1st Ed.). New York: McGraw-Hill Education.

Gordon, L. A., & Loeb, M. (2006). PEconomic aspects of information security: An emerging field of research. *Information Systems Frontiers*, *8*(5), 335–337.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the magnitude of cybersecurity security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security*, *6*(1), 24–30.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security*, *7*(02), 49–59.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1), tyaa005.

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers*, *8*, 338–349.

Hausken, K. (2014). Returns to information security investment: Endogenizing the expected loss. *Information Systems Frontiers*, *16*(2), 329–336.

Hall, R. E., & Jorgenson, D. W. (1967). Tax policy and investment behavior. *American Economic Review*, *57*(3), 391–414.

Hayes, J., & Bodhani, A. (2013). Cybersecurity security: Small firms under fire. *Engineering & Technology*, *8*(6), 80–83.

Kamien, M., & Schwartz, N. (2012). *Dynamic optimization: The calculus of variations and optimal control in economic management*. Mineola, NY: Dover Publications.

OMTCO, (2012). IT Costs: The Costs, Growth, and Financial Risk of Software Assets.

Oughton, E. J., Ralph, D., Pant, R., Leverett, E., Copic, J., Thacker, S., & Hall, J. W. (2019). Stochastic counterfactual risk analysis for the vulnerability assessment of cybersecurity-physical attacks on electricity distribution infrastructure networks. *Risk Analysis*, *39*(9), 2012–2031. https://doi.org/10.1111/risa.13291

Meland, P. H., Tondel, I. A., & Solhaug, B. (2015). Mitigating risk with cybersecurity insurance. *IEEE Security & Privacy*, *13*(6), 38–43.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cybersecurity-insurance survey. *Computer Science Review*, *24*, 35–61.

Mazzoccoli, A., & Naldi, M. (2020). Robustness of optimal investment decisions in mixed insurance/investment cybersecurity risk management. *Risk Analysis*, *40*(3), 550–564.

NIST. (2018). *Framework for improving critical infrastructure cybersecurity*. Versions 1.1. Gaithersburg, MD: National Institute of Standards and Technology.

U.S. Office of Management and Budget, (2003). Circular No. A-4: Regulatory Analysis. September.

Paté-Cornell, M.-E., Kuypers, M., Smith, M., & Keller, P. (2018). Cybersecurity risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis*, *38*(2), 226–241. https://doi.org/10.1111/risa.12844

Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybersecurity crime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy004

Shackelford, S. J. (2012). Should your firm invest in cybersecurity risk insurance? *Business Horizons*, *55*(4), 349–356.

Willemson, J. (2010). Extending the Gordon and Loeb model for information security investment. In *2010 International conference on availability, reliability and security* (pp. 258–261). IEEE.