Journal of Accounting and Public Policy 37 (2018) 527–544

Contents lists available at ScienceDirect

Journal of Accounting and Public Policy

journal homepage: www.elsevier.com/locate/jaccpubpol

Full length article

Cybersecurity insurance and risk-sharing

Lawrence D. Bodin[a], Lawrence A. Gordon[b], Martin P. Loeb[b,*], Aluna Wang[c]

[a] Emeritus Professor of Management Science, Robert H. Smith School of Business, University of Maryland, College Park, MD 20742-1815, USA
[b] Accounting and Information Assurance, Robert H. Smith School of Business, University of Maryland, College Park, MD 20742-1815, USA
[c] Tepper School of Business, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15217, USA

ARTICLE INFO

Keywords:
Cybersecurity insurance
Cybersecurity risk management

ABSTRACT

In today's interconnected digital world, cybersecurity risks and resulting breaches are a fundamental concern to organizations and public policy setters. Accounting firms, as well as other firms providing risk advisory services, are concerned about their clients' potential and actual breaches. Organizations cannot, however, eliminate all cybersecurity risks so as to achieve 100% security. Furthermore, at some point additional cybersecurity measures become more costly than the benefits from the incremental security. Thus, those responsible for preventing cybersecurity breaches within their organizations, as well as those providing risk advisory services to those organizations, need to think in terms of the cost-benefit aspects of cybersecurity investments. Besides investing in activities that prevent or mitigate the negative effects of cybersecurity breaches, organizations can invest in cybersecurity insurance as means of transferring some of the cybersecurity risks associated with potential future breaches.

This paper provides a model for selecting the optimal set of cybersecurity insurance policies by a firm, given a finite number of policies being offered by one or more insurance companies. The optimal set of policies for the firm determined by this selection model can (and often does) contain at least three areas of possible losses not covered by the selected policies (called the Non-Coverage areas in this paper). By considering sets of insurance policies with three or more Non-Coverage areas, we show that a firm is often better able to address the frequently cited problems of high deductibles and low ceilings common in today's cybersecurity insurance marketplace. Our selection model facilitates improved risk-sharing among cybersecurity insurance purchasers and sellers. As such, our model provides a basis for a more efficient cybersecurity insurance marketplace than currently exists. Our model is developed from the perspective of a firm purchasing the insurance policies (or the risk advisors guiding the firm) and assumes the firm's objective in purchasing cybersecurity insurance is to minimize the sum of the costs of the premiums associated with the cybersecurity insurance policies selected and the sum of the expected losses not covered by the insurance policies.

1. Introduction

In today's interconnected digital world, cybersecurity risks and resulting cybersecurity breaches are a fundamental concern to organizations (e.g., see Straub and Welke, 1998; Campbell et al., 2003; Cavusoglu et al., 2004; Gal-Or and Ghose, 2005; Gordon et al., 2010; Wang et al., 2013; and Spanos and Angelis, 2016) and public policy setters (e.g., see SEC, 2011, 2018; CEA, 2018). The importance of cybersecurity risks and incidents, from a public policy perspective, became a critical concern in the U.S. as a result of

* Corresponding author.
E-mail address: mloeb@rhsmith.umd.edu (M.P. Loeb).

https://doi.org/10.1016/j.jaccpubpol.2018.10.004

Available online 26 November 2018

the terrorist attacks on September 11, 2001. In fact, President Bush initiated a National Strategy to Secure Cyberspace, as a component of the U.S. National Strategy for Homeland Security, in response to the terrorists' attacks.[1] Accounting researchers, who have an interest in such issues as disclosure, internal control, and information sharing have also been concerned with cybersecurity (e.g., see Ettredge and Richardson, 2003; Gordon et al., 2003a; Gordon et al. 2006; Hilary et al., 2016; Amir et al., 2018).

While organizations would like to eliminate cybersecurity risks, they can never achieve 100% security. Furthermore, cybersecurity investments ultimately become more costly than the benefits derived from the incremental security (e.g., see Gordon and Loeb, 2002). Thus, those responsible for preventing potential cybersecurity breaches within their organization (e.g., the Chief Information Security Officer, the Chief Information Officer, the Chief Financial Officer), as well as firms (including accounting firms) providing advisory risk services to those organizations, need to think in terms of the cost-benefit aspects of cybersecurity investments.[2,3,4] In addition, auditors and other stakeholders are seeking reasonable assurance that firms are making rational investment decisions concerning cybersecurity risk management.

Besides investing in activities that prevent or mitigate cybersecurity breaches (e.g., firewalls, intrusion prevention and detection systems, encryption, employee training, etc.), organizations can invest in cybersecurity insurance as means of transferring some of the cybersecurity risks associated with potential future breaches (e.g., see Böhme and Schwartz, 2010; Gordon et al., 2003b; Herath and Herath, 2011).[5] More to the point, cybersecurity insurance allows an organization to transfer, at a cost, some of the risk associated with actual cybersecurity breaches. However, since insurance companies seek to earn profits, they set the cybersecurity insurance premiums in line with the risks they assume in writing the insurance policies. In an efficient cybersecurity insurance marketplace, the risks to insurance companies associated with potential cybersecurity breaches are aligned with the premiums of the cybersecurity insurance policies.

The importance of cybersecurity insurance as a means of helping organizations to manage their cybersecurity risks is clearly noted by Joe Nocera, a Principal in PwC's US Advisory practice, who writes:

> Cyber insurance can be an effective tool to help reduce information security risks, and companies should consider it within the context of their enterprise risk-management programs. As a first step, businesses should proactively evaluate available cyber-insurance products and understand pricing and coverage. (Nocera, 2014)

Similarly, Mark Millard writing as a senior manager in the Insurance and Claims Practice of Ernst & Young LLP, notes:

> Short of turning off your computers and using the postal service as your sole method of communication, no level of security protection is guaranteed to completely mitigate exposure to cyber damage and liability. It is critical that companies evaluate their frequency and severity exposure to cyber claims, and understand how to mitigate that exposure through insurance and contractual risk transfer. (Millard, 2015)

The importance of cybersecurity risks and incidents, from a public policy perspective, became a critical concern in the U.S. as a result of the terrorist attacks on September 11, 2001. In fact, President Bush initiated a National Strategy to Secure Cyberspace, as a component of the U.S. National Strategy for Homeland Security, in response to the terrorists attacks.

Cybersecurity insurance has also been a specific issue of concern to public policy-makers tasked with improving the level of cybersecurity within private sector organizations (e.g., Department of Homeland Security, 2012; European Union Agency for Network and Information Security, 2016). In this latter regard, Woods and Simpson (2017, p. 209) point out that, "…the underlying principle that the insurance industry will improve information security management is fundamental to a public-private partnership for cyber insurance."

Unfortunately, there are several impediments to the development of an efficient cybersecurity insurance marketplace. These impediments include inadequate actuarial data, asymmetric information between firms seeking insurance and the insurance companies offering insurance policies, and cybersecurity interdependency among Internet users. In addition, many executives incorrectly believe that cybersecurity risks are sufficiently covered by traditional commercial general liability and property insurance policies. Furthermore, many insurers are overly conservative in pricing their cybersecurity premiums because they fear the occurrence of a "cyber hurricane" (i.e., a situation where an insurance company is overwhelmed by claims due to correlated risks).[6] The impediments to an efficient cybersecurity insurance market have created a situation whereby cybersecurity insurance policies are commonly viewed as having high deductibles and low ceilings, relative to the premiums charged for these policies. In other words, cybersecurity insurance premiums are commonly viewed as being poorly aligned with the risks and coverage needs of private sector firms.

[1] See https://www.presidency.ucsb.edu/node/216254.

[2] While few would question the fact that the number of cybersecurity breaches is increasing at a rapid rate, there is less agreement on the actual cost of these breaches to companies, especially firms in the private sector (e.g., see Gordon et al., 2011; Romanosky, 2016).

[3] There is a lot of anecdotal evidence indicating that data breaches, especially highly visible ones, result in the firing or resignation of the persons responsible for protecting the information and information systems of corporations. For example, shortly after the data breach at Target Corporation in 2013 and the data breach at Equifax, the Chief Information Officers of those companies were no longer in their positions.

[4] Real options models offer a creative approach to addressing the cost-benefit aspects of investing in cybersecurity activities (e.g., see Benaroch, 2018; Gordon et al., 2015; Herath and Herath, 2008).

[5] Although cybersecurity insurance would be of value to public sector organizations, as well as individuals, our focus in this paper is on cybersecurity insurance for profit oriented private sector corporations.

[6] A more complete discussion of the impediments to the development of an efficient cybersecurity marketplace is provided in the next section of this paper.

The objective of the research contained in this paper is to develop a model that facilitates risk-sharing, among insurer and those being insured, that directly addresses the frequently expressed concern that cybersecurity insurance policies have high deductibles and low ceilings, relative to the premiums being charged for the policies. Our model can be used to determine an optimal set of cybersecurity insurance policies that a firm should purchase, where these optimal policies are selected from a finite set of insurance policies offered by insurance companies.

Our model is developed from the perspective of a firm purchasing the cybersecurity insurance policies. A fundamental assumption underlying the model is that a firm's objective in purchasing cybersecurity insurance is to minimize the sum of the total cost of the premiums associated with the purchased cybersecurity insurance policies and the weighted sum of the risk-adjusted potential losses over the loss areas that are not covered by these insurance policies (hereafter referred to as the Non-Coverage areas of possible losses). In essence, the model assumes that a firm self-insures over these Non-Coverage areas.

If a firm purchases a single insurance policy (the most common situation), then this policy has one Coverage area and, at most, two Non-Coverage areas. If the firm purchases more than one insurance policy, then the set of policies purchased by the firm can have more than one Coverage area and more than two Non-Coverage areas. The model developed in this paper explicitly considers the fact that the purchasing firm may find it advantageous to select a set of policies in a manner that results in more than two Non-Coverage areas.

A significant contribution of the analysis contained in this paper is that it shows from a risk-sharing perspective, how a firm could more efficiently evaluate available cybersecurity insurance products and determine the best insurance policies to purchase. Our analysis demonstrates that it is often in a firm's best interest to select policies that result in the firm being exposed to potential losses over at least three Non-Coverage areas. This approach to risk-sharing also provides the basis for a more efficient cybersecurity insurance marketplace by helping to alleviate the concern that cybersecurity insurance policies have high deductibles and low ceilings, relative to the premiums charged for the policies.[7] Besides providing an analytical procedure for determining the optimal set of insurance policies, examples are presented in this paper to demonstrate that the optimal set of policies may contain at least three Non-Coverage areas of potential losses.

The remainder of this paper is organized as follows. In the second section of the paper, we provide a brief review of the relevant literature on cybersecurity insurance and describe the general nature of insurance policies. In Section 2, we also provide a discussion of the assumptions used in our analysis and define the properties of an insurance ladder. In the third section of the paper, we develop the criterion for evaluating an insurance ladder. In the fourth section, we develop a process for evaluating the expected loss, given that a breach occurs, for any ladder regardless of the number of insurance policies on the ladder. In the fifth section of the paper, we develop a parametric procedure for determining the optimal ladder according to the criterion that we use for evaluating an insurance ladder over different ranges of the probability that a breach occurs. In the sixth and final section of the paper, we provide some concluding remarks regarding how a firm could use the model described in this paper, as well as some limitations of the model.

2. General nature of insurance policies

2.1. Literature review

Cybersecurity insurance is a means by which firms can transfer some of the risk (i.e., expected loss) associated with potential cybersecurity breaches. In addition, an efficient cybersecurity insurance marketplace would encourage firms to increase their investments in cybersecurity activities, so as to allow them to purchase cybersecurity insurance at the most attractive price (i.e., similar to the way an efficient automobile insurance marketplace encourages car owners to purchase anti-theft auto devices). Accordingly, an efficient cybersecurity insurance marketplace is considered an important mechanism for improving the overall level of cybersecurity protection within firms (e.g., see Department of Homeland Security, 2012). Unfortunately, there are several impediments to the development of an efficient cybersecurity insurance marketplace.

Adverse selection and moral hazard are two fundamental impediments to the development of an efficient cybersecurity insurance market (e.g., see Gordon et al., 2003a, 2003b; Böhme and Schwartz, 2010; U.S. DHS, 2012; Marotta et al., 2017). Both of these impediments stem from conflicting objectives and asymmetric information between insurance companies and the organizations being insured. Adverse selection refers to the situation where the purchaser of the insurance has valuable pre-contracting information that is not available to the insurer. For example, assume an organization that is seeking cybersecurity insurance has a formal set of cybersecurity processes in-place and tells the insurer about these processes. However, an adverse selection problem arises because the organization knows about certain existing problems associated with some of its cybersecurity related personnel who have been reluctant to follow the above-noted corporate cybersecurity processes, but these problems are not discussed with the insurance company prior to purchasing the cybersecurity insurance policies. Moral hazard refers to the situation where a firm purchasing insurance has post-contracting information that is not available to the insurer. For example, assume a particular corporation has a formal set of cybersecurity processes and strictly enforces these procedures prior to purchasing cybersecurity insurance. However, once the cybersecurity insurance is purchased, the corporation becomes lax in enforcing these processes. Hence there is a moral hazard problem.[8]

[7] Although our model is discussed in the context of cybersecurity insurance in this paper, the model could also be applied to other types of insurance.

[8] The moral hazard problem is intensified due to the interdependencies among Internet users (Shetty et al., 2010).

The aforementioned asymmetric information issues are not the only impediments to an efficient cybersecurity insurance marketplace. As pointed out by the U.S. Department of Homeland Security's (DHS) National Protection and Programs Directorate, in its 2012 report, three other impediments to the development of an efficient cybersecurity insurance market are:

> … (1) a lack of actuarial data which results in high premiums for first-party policies that many firms cannot afford; (2) the widespread, mistaken belief that standard corporate insurance policies/or general liability policies already cover most cyber risks; and (3) the fear that a so-called "cyber hurricane" will overwhelm insurance companies who might otherwise enter the market before they build up sufficient reserves to cover large losses.[9] (U.S. DHS, 2012, p. 1)

The above noted impediments to an efficient cybersecurity insurance marketplace are responsible for creating insurance policies that are frequently viewed (especially by corporate executives) as having high deductibles and low ceilings, relative to the premiums being charged (e.g.,see Bandyopadhyay et al., 2009; Biener et al., 2015; Finkle, 2015; Rechtman and Rashbaum, 2015).[10] High deductibles and low ceilings, relative to the premiums, is essentially a problem of deriving mutually beneficial risk-sharing among insurers and firms seeking cybersecurity insurance.

Risk-sharing among insurance companies is common. Although deriving risk-sharing arrangements between insurers and firms seeking cybersecurity insurance is problematic, two of the generic approaches to risk-sharing that are frequently used by insurance companies are *Pro Rata Liability* (PRL) and the *Increased Limits Factor* (ILF) packages for combining individual insurance policies. The PRL may be thought of as proportional insurance (or splitting the pie) formed by a group of insurance companies that join together to insure a firm against a potential cybersecurity breach. Each insurance company accepts a share of the agreed upon risk (i.e., the potential loss resulting from a cybersecurity breach) and receives a corresponding share of the insurance premium paid by the firm purchasing the insurance. This packaging arrangement is commonly accomplished via a reinsurance arrangement by a third party.[11]

Under the ILF approach, K insurance policies are combined and ordered from the smallest ceiling coverage to the largest ceiling coverage, where the ceiling of insurance policy i equals the deductible of insurance policy $i+1$, $i = 1, 2, \cdots, K-1$. This arrangement of the policies under the ILF approach is an example of what is often called an insurance tower or insurance ladder.[12] If the firm employs the ILF approach in connection with cybersecurity insurance, the insurance policy with the smallest ceiling covers the claim resulting from a security breach from its deductible to its ceiling. If there were a remaining loss, then, the second policy (i.e., the one with the second lowest ceiling) kicks in and covers the claim from its deductible to its ceiling, and so on. With an ILF tower described above, the first policy in the ordering of the policies in the ILF is more likely to have to pay a claim than the second policy in this ordered insurance tower and so forth. Hence, the premium attached to each of the policies in this ordering is reduced by a constant factor referred to as the ILF (Palmer, 2006), assuming that the term of each policy in the ILF is the same.[13]

A modified, and more complicated, version of the insurance tower described above, hereafter called an insurance ladder, allows for the deductible of a policy i in the tower to be strictly greater that the ceiling of policy $i-1$, creating multiple deductibles and Non-Coverage areas (i.e., coverage gaps) from the ceiling of policy $i-1$ to the deductible of policy i. In other words, the set of policies in the ladder could have more than two Non-Coverage areas. As noted in the introduction, we demonstrate situations where the optimal set of cybersecurity insurance policies that a firm should purchase would have more than two Non-Coverage areas. In essence, deriving the optimal set of cybersecurity insurance policies with more than two Non-Coverage areas makes the firm purchasing the insurance policies an active participant in sharing of risk with the insurers.

2.2. Insurance policy profile

Every insurance policy is characterized by its insurance policy profile or *representation* (D, C, P) where D is the *deductible* of the policy, C is the *ceiling* of the policy, and P is the *premium* (or cost) that a firm pays the insurance company for purchasing the policy. The *Coverage area* of an insurance policy with representation (D, C, P) is the interval (D, C) and represents the area of possible losses that are covered by the insurance policy. The *span* of the Coverage area associated with this policy is $C - D$. Furthermore, the *Non-Coverage areas* of this insurance policy are $(0, D)$ and (C, L_{max}), where L_{max} is the maximum loss that the firm assumes it can possibly suffer in any breach.[14]

For example, the insurance policy with representation $(5, 15, .5)$ has a deductible of \$5 million, ceiling of \$15 million, and premium of \$0.5 million.[15] The Coverage area of this policy is $(5, 15)$ with span equal to 15–5 = 10. The two Non-Coverage areas of

[9] DHS' National Protection and Programs Directorate held a series of workshops from 2012 to 2014 that addressed many issues related to the important role that an efficient cybersecurity insurance marketplace could play in facilitating improved cybersecurity, as well as the impediments to developing such a marketplace.

[10] Personal discussions between one of the authors of this paper and several corporate executives have confirmed the fact that high deductibles and low ceilings, relative to premiums being charged, are key executive concerns associated with cybersecurity insurance policies.

[11] See https://thismatter.com/money/insurance/multiple-insurance-coverage.htm for a more complete example of the use of pro rata liability insurance.

[12] For the purposes of this paper, we use the term *insurance ladder* in a more general sense explained in the subsequent paragraph of the paper.

[13] See Miccolis (1977) and Palmer (2006) for a further discussion and analysis of the use of increased limit factors.

[14] Although beyond the scope of this paper, determining the actual loss of a cybersecurity breach has been the subject of many empirical studies (e.g., Campbell et al., 2003; Gordon et al., 2011; Spanos and Angelis, 2016).

[15] All deductibles, ceilings, premiums, Coverage regions, losses, and risks in this paper are in millions of dollars to indicate the magnitude of the cost of a breach. However, it can scale in any way the firm desires.

this policy are (0, 5) with span equal to 5 and (15, L_{max}) with span equal to $L_{max} - 15$. We assume that $L_{max} = 100$ in the examples in this paper.

A basic assumption in this paper is that every insurance policy has the same fixed and common Coverage period (or *term*). For example, the term of an insurance policy could be the calendar year 2019.[16]

2.3. Insurance ladder profile

Assume an insurance ladder is made up of K insurance policies where the representation of policy i is (D_i, C_i, P_i), $i = 1, 2, \cdots, K$. An insurance ladder is assumed to have the following properties:

- The policies in the ladder are ordered from the smallest ceiling to the largest ceiling.
- The Coverage areas of the policies on the ladder do not overlap, i.e., $C_i \leq D_{i+1}$, for $i = 1, 2, \cdots, K-1$.
- Define $C_0 = 0$ and $D_{K+1} = L_{max}$, where as noted above, L_{max} denotes the largest loss the firm believes it would suffer in the event of a cybersecurity breach. The *Non-Coverage areas* for this insurance ladder are (C_i, D_{i+1}), $i = 0, 1, 2, \cdots, K$. In this definition, we assume that C_0 is the ceiling of policy 0 with representation (0, 0, 0) and D_{K+1} is the deductible of policy $K + 1$ with representation (L_{max}, L_{max}, 0). Policies 0 and $K + 1$ are introduced to specify the bounds of the Non-Coverage areas and play no further role in the analysis in this paper.

For simplicity and tractability, we focus on the case in which a firm can suffer at most one breach with losses during the term of the policies. If a breach were to occur, the firm could submit claims to the appropriate insurance company (or companies) that sold the insurance policy (or policies) to the firm. After this breach is detected and the corresponding claim(s) is (are) submitted, we assume the policies are no longer in effect regardless of whether a particular policy had a payout and the firm would need to purchase other insurance policies in order to continue its insurance protection from losses that may be suffered due to a subsequent breach.

The *Null Ladder* and the *One Policy Ladder* are important special cases of an insurance ladder. In our analysis, the *Null Ladder* is an insurance ladder made up of zero insurance policies and represents the situation where the firm decides to self-insure against all possible losses and not buy any insurance policies. The Non-Coverage area of the Null Ladder is (0, L_{max}). A *One Policy Ladder* contains one insurance policy with realization (D, C, P) where this policy has Coverage area (D, C) and Non-Coverage areas (0, D) and (C, L_{max}).

2.4. Example

Assume Policy 1 with representation (5, 15, 2), Policy 2 with representation (25, 45, 2.5), and Policy 3 with representation (50, 80, 1.5) make up an insurance ladder.[17] The Coverage areas for this insurance ladder are (5, 15), (25, 45), and (50, 80). The Non-Coverage areas for this ladder are (0, 5), (15, 25), (45, 50), and (80, 100). Fig. 1 provides a picture of this insurance ladder where the Coverage areas are shaded.

Assume that a firm purchased all the policies on the ladder shown in Fig. 1. Then, the firm would pay the insurance companies 6 units, where 6 is the sum of the premiums of the three policies in this ladder. The *ex post* benefit of purchasing all the policies depends on the size of the losses that the firm incurs due to a breach. If the losses due to the breach were 5 units or less, then the firm would be worse off, *ex post*, by 6 units, the size of the premiums purchased by the firm. If the loss due to the breach were between 5 and 11, then *ex post* the firm would still have been worse off purchasing the insurance. If a breach were to cause losses greater than 11, the firm would have been better off having purchased all the policies rather than self-insuring. In this case, the size of the *ex post* benefit would depend on the magnitude of the loss due to the breach suffered by the firm.

For example, if the firm purchased the three policies on this ladder and suffered a breach causing a loss of 70 during the term of these policies, then the firm must cover losses equal to the sum of the spans of all Non-Coverage areas up to 70. In this situation, the loss is equal to $20 = 5 + 10 + 5$; where (i) the first 5 equals the deductible of Policy 1 (ii) 10 equals the deductible of Policy 2 minus the ceiling of Policy 1 and (iii) the second 5 equals the deductible of Policy 3 minus the ceiling of Policy 2. On the other hand, if the firm self-insured against a breach, the firm's loss would have been 70. Thus, *ex post*, the firm would have saved $70 - (6 + 20) = 44$ by having purchased the policies.

The firm's *ex ante* benefit from purchasing any set of insurance policies will depend not only on the deductibles, ceilings, and premiums charged, but also on the firm's subjective probability distribution defined over the range of possible losses that the firm can suffer and the degree to which the firm is risk averse. The uncertainty stemming from whether a breach will occur during the term of the purchased policies and the magnitude of the loss associated with such a breach are essential stochastic components to the evaluation of any insurance ladder. These stochastic components are discussed in Sections 3, 4, and 5 of this paper as part of the development of a process for evaluating a collection of insurance ladders.

[16] Dropping this assumption would make the analysis much more complicated but the basic argument contained in this paper would remain unchanged.

[17] The premiums are set by the insurance companies offering the policies and depend on the probability distribution of losses assumed by the actuaries of the companies offering the policies. Thus, although Policy 3 has the largest span and hence the largest exposure, the lower premium would be explained by the actuarial determination that the probability of the insuree having a loss greater that 50 is relatively small. Accordingly, a small expected loss justifies a low premium price.

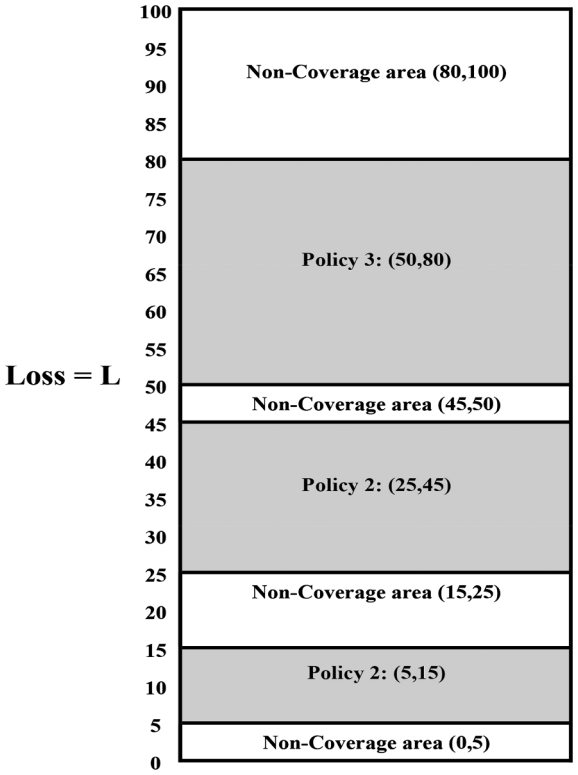

Fig. 1. Display of the Ladder Consisting of Policies 1, 2, and 3.

3. Criterion for evaluating an insurance ladder

In developing the criterion for evaluating an insurance ladder, we assume that the firm has set the value of L_{max}, the maximum loss that the firm believes it would encounter if a breach were to occur. We further assume that if a breach were to occur during the term of the policies that the firm has purchased, the firm would be able to detect the breach, and, along with all insurers, be able to measure and agree on the size of the loss. As noted earlier, however, before the insurance policies are purchased, neither the firm nor the insurers know with certainty if a breach will occur during the term of the policies, nor do they know the magnitude of the loss that would arise if a breach were to occur.

Any criterion for evaluating an insurance ladder needs to take into account (i.e., measure) the risk that remains with the purchaser after purchasing the insurance ladder. There are many possible measures of risk appropriate in a cybersecurity management context (Bodin et al., 2008). We use the simple, but popular, risk measure of *expected loss*. To do so, we assume the firm purchasing the insurance (the *insuree*) is risk-neutral. Given the well-known principal-agent literature (e.g., Shavell, 1979) showing that a risk-neutral agent is willing to bear all risk without additional compensation, one may wonder why a *risk-neutral* firm would ever wish to purchase cyber (or any other type) of insurance. A *risk-neutral* firm would wish to purchase insurance whenever the firm perceived the insurance policy to be underpriced (i.e., when the premium charged is less than the actuarial expected loss *based* on the firm's prior probabilities). A risk-neutral (or risk-averse) insurance company may offer such a policy when the insurance company's probability assessment of breach losses is less than the purchasing firm's probability assessment of breach losses.[18]

In this section, we develop a function that the firm can use for evaluating and comparing insurance ladders. This function, along with the analysis developed later in this paper using this function, can assist the firm in deciding upon the insurance ladder that best satisfies its needs. As noted above, a unique aspect of this model and analysis is that it allows a firm to analyze ladders with more than two Non-Coverage areas, thereby removing an implicit constraint of traditional insurance analysis. Accordingly, it expands the way cybersecurity insurance could be used to mitigate cybersecurity risk.

[18] Denoting the (unconditional) cumulative probability distribution of losses as assessed by the purchasing firm as $F_P(L)$ and the (unconditional) cumulative probability distribution of losses as assessed by the insurance company as $F_I(L)$, the condition can be written as follows: $F_P(L) \leq F_I(L)$ for all L and $F_P(L) < F_I(L)$ over some interval. That is, $F_P(L)$ first-order stochastically dominates $F_I(L)$. The insurance company may have a lower probability distribution of losses relative to the firm purchasing the insurance because the insurance company's estimate of a breach occurring during the term of the policy is less that the purchasing firm's estimate or for any given breach, the insurance firm's cost to address the breach's consequences would be lower for the insurance company due to economies of scale than the cost that would be incurred by the purchasing firm.

3.1. Terms, notation, and assumptions

The following terms, notation, and assumptions play an integral part of this development:

- λ is a random variable that designates the firm's prior probability that a breach occurs during the term of the insurance policies. Since λ is a probability, $0 \leq \lambda \leq 1$.
- BR is a Bernoulli random variable that equals 1 if a breach occurs during the term of the policies on a ladder and equals 0 if no breach occurs over this term. Thus, $P[BR = 1] = \lambda$ and $P[BR = 0] = 1 - \lambda$.
- The policies on a ladder that contains more than one insurance policy are ordered from the policy with the smallest ceiling to the policy with the largest ceiling.
- Every policy i in this analysis has a known representation (D_i, C_i, P_i).
- The Coverage areas of the policies on the ladder do not overlap, i.e., $C_i \leq D_{i+1},\ i = 1, 2, \cdots, K$ where K is the number of policies on the ladder and there are at least two policies on the ladder, i.e., $K \geq 2$.
- The following notation is used for defining the different types of insurance ladders.

a. π_0 denotes the Null Ladder.
b. π_f denotes a one-policy ladder made up of policy f.
c. $\pi_{e,f}$ denotes a two-policy ladder with policies e and f, where $C_e \leq D_f$.
d. $\pi_{b,c,d}$ denotes a three-policy ladder where C_b is no greater than D_c and C_c is no greater than D_d.
e. A generic ladder is a ladder where the policies are not specified. A generic ladder is denoted as π_{GEN}. If more than one generic ladder is part of the discussion, then the ladders will be denoted using some other subscript that identifies the policies (e.g., π_{GEN1} and π_{GEN2}).
f. L is a continuous random variable that denotes the loss suffered by the firm given that a breach has occurred for the Null Ladder.

We assume that λ, the firm's subjective probability that a breach will occur, may differ from the probability assessment of the insurance company, which we denote as λ_I. The insurance company's prior probability that a breach will occur is based on an overall population of firms sharing a limited number of characteristics (e.g., industry, type of firewalls employed). The firm's estimate λ, is the specific firm's assessment and is not only based on the characteristics known by the insurer, but on a host of characteristics privately known to the firm. As noted earlier, a risk-neutral firm would wish to purchase insurance whenever the firm perceived the insurance policy to be underpriced. Having $\lambda > \lambda_I$ could lead the insurance firm to offer a policy that the purchasing firm views as being under priced.

3.2. Ladder valuation function

Let π_{GEN} be any ladder and $E[L(\pi_{GEN})|BR = 1]$ be the expected value of the random variable $L(\pi_{GEN})$ given that a breach has occurred. Let $\varphi(\pi_{GEN},\ \lambda)$ denote the total premium plus the expected loss for ladder π_{GEN}. Then, $\varphi(\pi_{GEN},\ \lambda)$ is given in Eq. (1).

$$\varphi(\pi_{GEN}, \lambda) = \sum_{j=1}^{Q} P_j + E[L(\pi_{GEN})|BR = 1] * P(BR = 1) + E[L(\pi_{GEN})|BR = 0] * P(BR = 0). \tag{1}$$

In Eq. (1), $\sum_{j=1}^{Q} P_j$ is the sum of the premiums for the Q policies on the ladder. Further, $E[L(\pi_{GEN})|BR = 0] = 0$. Thus, the evaluation of $\varphi(\pi_{GEN}, \lambda)$ is given in Eq. (2).

$$\varphi(\pi_{GEN}, \lambda) = \sum_{j=1}^{Q} P_j + E[L(\pi_{GEN})|BR = 1] * P(BR = 1) \tag{2}$$

Eq. (3) is formed by substituting λ for $P(BR = 1)$ in Eq. (2).

$$\varphi(\pi_{GEN}, \lambda) = \sum_{j=1}^{Q} P_j + E[L(\pi_{GEN})|BR = 1] * \lambda \tag{3}$$

It is important to note that Eq. (3) is the Eq. of a straight line where λ is the independent variable, $\varphi(\pi_{GEN},\ \lambda)$ is the dependent variable, and $E[L(\pi_{GEN}|BR = 1]$ is the coefficient of λ and the slope of this straight line. We use the fact that Eq. (3) is a straight line in the procedure described in Section 5 for determining the insurance policy that minimizes $\varphi(\pi_{GEN},\ \lambda)$ as a function of λ. $RISK(\pi_{GEN})$ for ladder π_{GEN} is defined in Eq. (4).

$$RISK(\pi_{GEN}) = E[L(\pi_{GEN})|BR = 1]. \tag{4}$$

Eq. (5) is formed by substituting Eq. (4) into Eq. (3).

$$\Phi(\pi_{GEN}, \lambda) = \sum_{j=1}^{Q} Pj + RISK(\pi_{GEN}) * \lambda. \tag{5}$$

In this paper, we use $RISK$ in all capital letters to be the term defined in Eq. (4) to denote the computed risk for any ladder GEN. We use risk without capitals to denote risk in a more general manner. The last term in Eq. (5), $RISK(\pi_{GEN}) * \lambda$, will sometimes be referred to as the weighted RISK.

4. Evaluating the *RISK* of a ladder

In this section, we describe a process for evaluating *RISK* for any ladder π_{GEN} containing one or more insurance policies. Central to this process is a procedure for computing $RR(\pi_{GEN})$, the *Reduction in RISK* for ladder π_{GEN}. The equation for computing $RR(\pi_{GEN})$ for any ladder π_{GEN} is given in Eq. (6) and the equation for computing $RISK(\pi_{GEN})$ for ladder π_{GEN} is given in Eq. (7).

$$RR(\pi_{GEN}) = \sum \textit{ Reduction in RISK for all policies on the ladder}. \tag{6}$$

$$RISK(\pi_{GEN}) = RISK(\pi_0) - RR(\pi_{GEN}). \tag{7}$$

Eqs. (6) and (7) are important results that are proven later in this section. According to Eqs. (6) and (7) and under the conditions stated earlier in this paper, $RISK(\pi_{GEN})$ for any ladder π_{GEN} is computed by subtracting the sum of the *Reduction in RISK* for all policies making up ladder π_{GEN} from $RISK(\pi_0)$, the *RISK* of the Null Ladder. To implement these results, $RISK(\pi_i)$ and the *Reduction in RISK*, $RR(\pi_i)$, for all single policy ladders must be computed before evaluating $RISK(\pi_{GEN})$ and $RR(\pi_{GEN})$ for any ladder π_{GEN} containing two or more policies. In the remainder of Section 4, we describe how to compute $RISK(\pi_{GEN})$ and $RR(\pi_{GEN})$ for any ladder π_{GEN} and illustrate this procedure with two examples.

4.1. Evaluating $RISK(\pi_0)$, the RISK for the Null Ladder

Since the Null Ladder π_0 contains no insurance policies, the premium cost for the Null Ladder is zero. Also, the Null Ladder has one Non-Coverage area , $(0, L_{max})$, and no Coverage areas. Therefore, $RISK(\pi_0)$ for the Null Ladder can be calculated using Eq. (8) and $\varphi(\pi_0, \lambda)$ can be computed using Eq. (9).

$$RISK(\pi_0) = E[L(\pi_0)|BR = 1] = \int_0^{L_{max}} x*f(x)dx, \quad \text{where } f(x) \text{ is the density function of the random variable L.} \tag{8}$$

$$\varphi(\pi_0, \lambda) = RISK(\pi_0)*\lambda \tag{9}$$

Define $R(a, b)$ as the *RISK* for the Null Ladder in the interval (a, b) where $0 \le a \le b \le L_{max}$. Then, $R(a, b)$ is given in Eq. (10).

$$R(a, b) = \int_a^b x*f(x)dx, \ 0 \le a \le b \le L_{max}. \tag{10}$$

Since $R(0, L_{max}) = \int_0^{L_{max}} x*f(x)dx$, $R(0, L_{max})$ equals $RISK(\pi_0)$ for the Null Ladder π_0.

4.2. Evaluating *RISK* and *Reduction in RISK* for a one-policy ladder π_i

Let ladder π_i be a one-policy ladder made up of Policy i, with representation (D_i, C_i, P_i). Then, Ladder π_i has Non-Coverage areas $(0, D_i)$ and (C_i, L_{max}) and Coverage area (D_i, C_i). $RISK(\pi_0)$, the RISK of the Null Ladder, is given in Eq. (11).

$$RISK(\pi_0) = R(0, D_i) + R(D_i, C_i) + R(C_i L_{max}) \tag{11}$$

In Eq. (11), $RISK(\pi_0)$ is broken down into three components based on the deductible and the ceiling of Policy i, given that a breach is assumed to have occurred (i.e., $BR = 1$). When the firm purchases policy π_i, $RISK(\pi_i)$ is equal to the following:

$$\begin{aligned} RISK(\pi_i) = \ & E[L(\ \pi_i) \text{ and the loss due to the breach falls in Non-Coverage area } (0, D_i)|BR = 1] \\ & + E[L(\pi_i) \text{and the loss due to the breach falls in Coverage area } (D_i, C_i)|BR = 1] \\ & + E[L(\pi_i) \text{ and the loss due to the breach falls in Non-Coverage area } (C_i, L_{max})|BR = 1] \end{aligned} \tag{12}$$

We now show how to evaluate each of the three terms on the right-hand side of Eq. (12) for ladder π_i.

4.2.1. Evaluating $\boldsymbol{E[L(\pi_i)}$ *and the breach falls in Non-Coverage area* $\boldsymbol{(0, D_i)|BR = 1]}$

Under ladder π_i, if the loss due to a breach is between 0 and D_i, the firm pays for this loss since the Coverage of the policy on ladder π_i begins when the loss suffered by the firm is equal to the deductible D_i. Thus, the *RISK* for the Null Ladder π_0 and the *RISK* for ladder π_i are both equal to $R(0, D_i)$. Hence, the *Reduction in RISK* for ladder π_i in Non-Coverage area $(0, D_i)$ equals zero.

4.2.2. Evaluating $\boldsymbol{E[L(\pi_i)}$ and the breach falls in coverage area $\boldsymbol{(D_i, C_i)|BR = 1]}$

Under ladder π_i, i f the loss due to the breach is between D_i and C_i, then the firm covers the D_i units of loss since this loss is attributable to Non-Coverage area $(0, D_i)$. However, the firm pays for no additional loss when the loss is between D_i and C_i because this loss is covered by the insurance policy on ladder π_i. Thus, the expected loss that the firm incurs by purchasing the policy on ladder π_i is equal to $D_i*[F(C_i) - F(D_i)]$ where $[F(C_i) - F(D_i)]$ is the probability that the loss due to the breach lies between D_i and C_i. Hence, the *Reduction in RISK* for ladder π_i in Coverage area (D_i, C_i) is equal to $R(D_i, C_i) - D_i*[F(C_i) - F(D_i)]$.

4.2.3. Evaluating $\boldsymbol{E[L(\pi_i)}$and the breach falls in coverage area$\boldsymbol{(C_i, L_{max})|BR = 1]}$

Under ladder π_i, if the loss due to a breach is between C_i and L_{max}, then the insurance company covers $C_i - D_i$ units of loss and the firm covers the remaining loss. Thus, the expected loss for the firm is this situation is equal to the following :

$$R(C_i, L_{max}) - (C_i - D_i)*[F(L_{max}) - F(C_i)] = R(C_i, L_{max}) - (C_i - D_i)*[1 - F(C_i)]$$

In the above expression for expected loss, $F(L_{max}) - F(C_i)$ is the probability that the breach occurred in interval (C_i, L_{max}), and $F(L_{max}) = 1$. Hence, the *Reduction in RISK* in this situation is equal to $(C_i - D_i)*[1 - F(C_i)]$. A tabular representation of these computations is given in Table 1.

Table 1
RISK and *Reduction in RISK* for a One-Policy Ladder $\boldsymbol{\pi_i}$ with a Deductible of $\boldsymbol{D_i}$ and a Ceiling of.$\boldsymbol{C_i}$

	Non-Coverage Area $R(0, D_i)$	Coverage Area (D_i, C_i)	Non-Coverage Area (C_i, L_{max})
RISK - Null Ladder	$R(0, D_i)$	$R(D_i, C_i)$	$R(C_i, L_{max})$
RISK $- \pi_i$	$R(0, D_i)$	$D_i*[F(C_i) - F(D_i)]$	$R(C_i, L_{max})$–$[(C_i - D_i)*[F(L_{max}) - F(C_i)]$, where $F(L_{max}) = 1$
Reduction in RISK $- \pi_i$	0	$R(D_i, C_i) - D_i*[F(C_i) - F(D_i)]$	$((C_i - D_i)*[F(L_{max}) - F(C_i)]$ where $F(L_{max}) = 1$

Using the above results, $RISK(\pi_i)$ and *Reduction in RISK* (π_i) for ladder π_i are given in Eqs. (13) and (14).

$$RISK(\pi_i) = R(0, D_i) + \{D_i*[F(C_i) - F(D_i)]\} + \{R(C_i, L_{max}) - (C_i - D_i)*[1 - F(C_i)]\} \tag{13}$$

$$RR(\pi_i) = \{R(D_i, C_i) - D_i*[F(C_i) - F(D_i)]\} + \{(C_i - D_i)*[1 - F(C_i)]\}. \tag{14}$$

4.3. Computation of RISK and Reduction in RISK for a two-policy ladder

The computations of *RISK*, $R(\pi_{i,j})$, and *Reduction in Risk*, $RR(\pi_{i,j})$, for any two-policy ladder made up of Policies i and j are based on the following theorem. The results from this theorem serve as the prototype for computing the *Reduction in RISK* for any ladder containing at least two insurance policies where we assume that no pair of policies on this ladder overlaps in coverage.

4.3.1. Theorem

Assume π_i is a one-policy ladder made up of Policy i, π_j is a one-policy ladder made up of Policy j, and $\pi_{i,j}$ is a two-policy ladder composed of Policies i and j. Policy i has representation (D_i, C_i, P_i), Policy j has representation (D_j, C_j, P_j), and $C_i < D_j$ (i.e., no-overlap assumption). Then, the relationship between the corresponding *Reductions in RISK* of ladders π_i, π_j, and $\pi_{i,j}$ is presented in Eq. (15):

$$RR(\pi_{i,j}) = RR(\pi_i) + RR(\pi_j) \tag{15}$$

Proof of the theorem:

Ladder $\pi_{i,j}$ has Non-Coverage areas $(0, D_i)$, (C_i, D_j), and (C_j, L_{max}) and Coverage areas (D_i, C_i) and (D_j, C_j) and these policies do not overlap in coverage. The *Reduction in RISK* for each of the Non-Coverage areas and Coverage areas for ladder $\pi_{i,j}$ are given in Eqs. (16a) to (16e):

$$\textit{Reduction in RISK} \text{ in Non-Coverage area } (0, D_i) = 0. \tag{16a}$$

$$\textit{Reduction in RISK} \text{ in Coverage area } (D_i, C_i) = R(C_i, D_i) - D_i*[F(C_i,) - F(D_i)] \tag{16b}$$

$$\textit{Reduction in RISK} \text{ in Non-Coverage area } (C_i, D_j) = (C_i, -D_i)*[F(D_j) - F(C_i)]. \tag{16c}$$

$$\textit{Reduction in RISK} \text{ in Coverage area } (D_j, C_j) = \{R(Dj, C_j) - D_j*[F(C_j) - F(D_j)]\} + \{(C_i - D_i)*[F(C_j) - F(D_j)]\}. \tag{16d}$$

$$\textit{Reduction in RISK} \text{ in Non-Coverage area } (C_j, L_{max}) = \{(C_j - D_j)*[F(L_{max}) - F(C_j)]\} + \{(C_i - D_i)*[F(L_{max}) - F(C_j)]\} \tag{16e}$$

The *Reduction in Risk* for $\pi_{i,j}$ is calculated by summing the right-hand sides of Eqs. (16a) to (16e). Eq. (17) reorders the terms in those Eqs. (16a) to (16d) so that all terms related to ladder π_i are shown first and all terms related to ladder π_j are shown subsequently:

$$\begin{aligned} RR(\pi_{i,j}) = {} & \{R(D_i, C_i) - D_i*[F(C_i) - F(D_i)]\} + (C_i - D_i)*\{[\boldsymbol{F(D_j)} - \boldsymbol{F(C_i)}] + [\boldsymbol{F(C_j)} - \boldsymbol{F(D_j)}] + [\boldsymbol{F(L_{max})} - \boldsymbol{F(C_j)}]\} \\ & + \{R(D_j, C_j) - D_j*[F(C_j - F(D_j)]\} + \{(C_j - D_j)*[F(L_{max}) - F(C_j)]\}. \end{aligned} \tag{17}$$

Since $\boldsymbol{F(D_j) - F(C_i) + F(C_j) - F(D_j) + F(L_{max}) - F(C_j) = F(L_{max}) - F(C_i)}$, Eq. (17) simplifies to:

$$\begin{aligned} RR(\pi_{i,j}) = {} & \{R(D_i, C_i) - D_i*[F(C_i) - F(D_i)]\} + (C_i - D_i)*[F(L_{max}) - F(C_j)] + \{R(D_j, C_j) - D_j*[F(C_j) - F(D_j)]\} \\ & + \{(C_j - D_j)*[F(L_{max}) - F(C_j)]\} \end{aligned} \tag{18}$$

Using Eq. (14) for $RR(\pi_i)$ and $RR(\pi_j)$, one readily sees that Eq. (18) can be rewritten as Eq. (15), thus completing the proof.

4.3.2. Discussion of the theorem

The theorem provides the basis for a more general result. The theorem shows that the *Reduction in RISK* for the two policy ladder

$\pi_{i,j}$ is equal to the sum of the *Reductions in RISK* for the single policy ladders π_i and π_j, where the policy on ladder π_i and the policy on ladder π_j do not overlap in coverage. It is easy to show the more general result that the *Reduction in RISK* for any ladder containing two or more non-overlapping policies is the sum of the *Reductions in RISK* for the policies in the ladder (i.e., Eq. (15) generalizes to Eq. (6)). The proof of this result is analogous to the above theorem's proof.

Based on the above theorem, the Increased Limits Factor (ILF) policy containing K insurance policies labeled Policy 1, Policy 2, ⋯, Policy K can be replaced by a single policy with representation $(D_1, C_K, P_1 + P_2 + \cdots + P_K)$, where $C_j = D_{J+1} + 1$, for $j = 1, 2, \cdots, K-1$. An example illustrating this result is given at the end of Section 4. Depending upon the organization forming the ILF, the firm may be allowed to create subsets of these policies as smaller ILFs or break up the ILF into individual policies in its analysis. In other cases, the ILF may not be able to be divided into smaller policies.

Eqs. (6) and (15) generated from the theorem play an important role in the analysis presented in Section 5 of this paper in the following manner. If there are a large number of insurance ladders that can be formed from subsets of the available insurance policies where the policies on each ladder do not overlap in coverage, then the computation of the *Reduction in RISK* for each ladder can be simplified by using Eqs. (6), (7), and (15) as follows:

- In Step 1, the *Reduction in RISK* is computed for all available ladders containing one policy.
- In Step 2, $RISK(\pi_{GEN})$ for any insurance ladder π_{GEN} is equal to the $RISK(\pi_0)$ minus the sum of the *Reduction in RISK* for all policies on the ladder π_{GEN}.

This two-step process simplifies the enumeration and evaluation of the insurance ladders formed for a collection of available insurance ladders.

4.3.3. Example of computing *RISK* (π_0), the risk of the Null Ladder

Let L_{max} equal 100 and $f(x)$ be the density function for the random variable x, as given below:

$$f(x) = -.0002x + .02,\ 0 \le x \le L_{max} \text{ and } f(x) = 0, \text{ otherwise.} \tag{19}$$

A plot of $f(x)$ is given in Fig. 2.

Using $f(x)$, the Cumulative Distribution Function (CDF) is $F(x) = P(L \le x)$, is given in Eq. (20) and $RISK(\pi_0)$, the risk of the Null Ladder, is given in Eq. (21).

$$F(x) = \int_0^x f(y)dy = -.0001x^2 + .02x,\ 0 \le x \le 100. \tag{20}$$

Further, $F(x) = 0$ for $x < 0$ and $F(x) = 1$ for $x > 100$.

$$RISK(\pi_0) = \int_0^{100} x*f(x)dx = -.0002*\frac{10^6}{3} + .01*10^4 = -\frac{200}{3} + 100 = 33.33 \tag{21}$$

Since $RISK(\pi_0) = 33.\bar{3}3$, $RISK(\pi_0)$ is an upper bound on the value of *RISK* for any ladder π_{GEN} generated from any set of policies that do not overlap in coverage, assuming the firm uses the density function $f(x)$, CDF $F(x)$, and $RISK(\pi_0)$ defined above and $L_{max} = 100$.

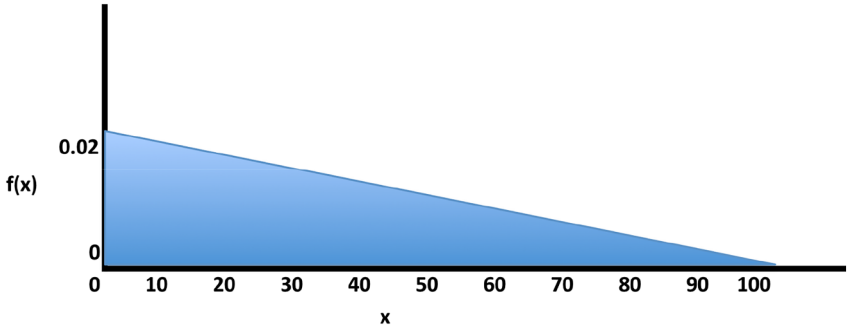

Fig. 2. Plot of the Density Function f(x) as a function of x.

4.3.4. Example of computing Reduction in RISK for a one-policy ladder

We now compute the *Reduction in RISK* for a ladder containing one policy, called Policy A, where Policy A has realization $(5, 15, -)$, $L_{max} = 100$, the density function $f(x)$ is defined in Eq. (19), and the CDF is computed in Eq. (20). Moreover, $R(a, b)$ is computed in Eq. (22) for the Null Ladder π_0 for any interval (a, b) where $0 \le a < b \le L_{max}$.

$$R(a, b) = \int_a^b x*f(x)dx = (-.0002/3)*(b^3 - a^3) + .01*(b^2 - a^2). \tag{22}$$

Using, Eqs. (19), (20) and (22), the *Reduction in RISK* for ladders π_A is equal to 8.103 and the $RISK(\pi_1)$ is equal to 25.223. The *RISK*

Table 2
RISK and *Reduction in RISK* for a One-Policy Ladder π_A with a Deductible of 5 and a Ceiling of 15.

	Non-Coverage Area (0,5)	Coverage Area (5,15)	Non-Coverage Area (15,100)	Totals
$RISK(\pi_0)$	0.242	1.783	31.308	33.333
$RISK(\pi_A)$	0.242	0.9	24.088	25.23
$RR(\pi_A)$	0	0.883	7.22	8.103

and the *Reduction in RISK* for ladder π_1 are displayed in Table 2.

It is important to note that in this example, $C_1 - D_1 = 10$ and $RR(\pi_A) = 8.103$, the *Reduction in RISK* for this example is not as large as $C_1 - D_1$, the coverage, of Policy A. This situation holds for the following reason. Since we are dealing with expected values, it is possible for the firm to receive less than $C_1 - D_1$ from the insurance company since the amount that the firm receives is based on the losses suffered by the firm. The maximum that the firm can receive from the insurance company under ladder π_A due to a breach is equal to $C_1 - D_1$. Therefore, $RR(\pi_A)$ will be no greater than (and, most likely, less than) $C_1 - D_1$.

4.3.5. Example of computing Reduction in RISK for a ladder containing at least two policies

We now illustrate how to compute the *Reduction in RISK* for a three-policy ladder using the density function and CDF described in Eqs. (19) and (20). The representations of the three policies on the ladder are as follows: Policy A has representation (5, 15, P_A), Policy B has representation (15, 35, P_B), and Policy C has representation (35, 65, P_C). In this analysis, it is not necessary to assign specific numerical values for the premium costs, P_A, P_B, andP_C, of each policy. The insurance ladder composed of Policies A, B, and C represent a three-policy ILF since the ceiling of Policy A equals the deductible of Policy B and the ceiling of Policy B equals the deductible of Policy C.

We use the following notation in this example. π_0 represents the Null Ladder, π_A represents the ladder made up of Policy A, π_B represents the ladder made up of Policy B, π_C represents the ladder made up of Policy C, and $\pi_{ILF} = \pi_{A,B,C}$ represents the ladder containing the ILF policy made up of Policies A, B, and C.

The Reduction in RISK and *RISK* for these ladders can be calculated as follows:

$RISK(\pi_0) = 33.333.$
$RR(\pi_A) = 8.103$ and $RISK(\pi_A) = 33.333 - 8.103 = 25.23.$
$RR(\pi_B) = 11.316$ and $RISK(\pi_B) = 33.333 - 11.316 = 22.017.$
$RR(\pi_C) = 7.725$ and $RISK(\pi_C) = 33.333 - 7.725 = 25.608.$
$RR(\pi_{ILF}) = RR(\pi_{A,B,C}) = 27.15$ and $R(\pi_{ILF}) = RISK(\pi_{A,B,C}) = 33.333 - 27.15 = 6.183.$

Using Eq. (15), π_{ILF} has a *Reduction in RISK* equal to 27.15 and *RISK* equal to 6.183. The sum of the *Reductions in RISKS* for the single policies ladders π_A, π_B, and π_C is equal to 8.103 + 11.316 + 7.725 = 27.144, differing only by 0.006 from the $RR(\pi_{ILF}) = 27.15$ due to rounding error necessitated by the density function (19). Details of this analysis are shown in Tables 3 through 5. This example shows that the policies making up the ladder π_{ILF} can be replaced by one policy with representation:(D_A, C_C, $P_A + P_B + P_C$).

5. The optimal insurance ladder as a function of λ

In Sections 3 and 4 we developed a procedure for evaluating $RISK = E[L(\pi_{GEN})|BR = 1]$, a key component in evaluating $\varphi(\pi_{GEN}, \lambda)$. In this section we present a procedure that determines the insurance ladder that minimizes $\varphi(\pi_{GEN}, \lambda)$ for intervals of λ between 0 and 1 where these intervals are non-overlapping and cover all possible values of λ between 0 and 1. This parametric solution of the optimal insurance ladder as a function of λ allows the firm to consider the tradeoff between the total premium costs of the insurance policies on the ladder being analyzed versus the risk associated with the insurance policies on these ladders. This analysis can benefit the firm in making an intelligent decision as to the insurance policies to purchase.

The steps in finding this parametric solution of the optimal insurance ladder as a function of λ are now described. Then, two examples are presented to illustrate this approach.

5.1. Finding a set of dominating insurance ladders

The procedure first enumerates all insurance ladders that can be formed from a collection of available insurance policies where

Table 3
RISK and *Reduction in RISK* for ladder π_B with a Deductible of 15 and a Ceiling of 35.

	Non-Covered Area (0,15)	Covered Area (15,35)	Non-Covered Area (35,100)	Totals
$RISK(\pi_0)$	2.025	7.367	23.941	33.333
$RISK(\pi_B)$	2.025	4.5	15.492	22.017
$RR(\pi_B)$	0	2.867	8.449	11.316

Table 4
RISK and *Reduction in RISK* for Ladder π_C with a Deductible of 35 and a Ceiling of 65.

	Non-Covered Area (0,35)	Covered Area (35,65)	Non-Covered Area (65,100)	Totals
$RISK(\pi_0)$	9.393	14.55	9.39	33.333
$RISK(\pi_c)$	9.393	10.5	5.715	25.608
$RR(\pi_C)$	0	4.05	3.675	0.725

Table 5
RISK and *Reduction in RISK* for ladder π_{ILF} with a Deductible of 5 and Ceiling of 65.

	Non-Covered Area (0,5)	Covered Area (5,65)	Non-Covered Area (65,100)	Totals
$RISK(\pi_0)$	0.242	23.7	9.391	33.333
$RISK(\pi_{ILF})$	0.242	3.9	2.042	6.183
$RR(\pi_{ILF})$	0	19.8	7.349	27.15

the policies on the ladder do not overlap. As a new insurance ladder is enumerated, the *inferior insurance ladder test* (described in the next section) is applied to determine if this new insurance ladder is an inferior or dominating insurance ladder. Any ladder determined by the *inferior insurance ladder test* to be inferior is discarded. If there are only a few available insurance policies, it may be easier to enumerate all insurance ladders first and then apply the inferior insurance ladder test to the ladders that are enumerated to generate the set of dominating insurance ladders. We use the approach of enumerating all ladders before applying the inferior insurance ladder test in the examples at the end of Section 5, since there are only eight ladders in each example.

After the *inferior insurance ladder test* is applied to all enumerated insurance ladders, the dominating ladders that have not been discarded comprise the initial set of *dominating insurance ladders*. This set of dominating insurance ladders is further reduced by discarding all dominating insurance ladders that have the same value of $\varphi(\pi, \lambda)$ except for the ladder with the smallest value of *RISK*. At the end of this process of discarding inferior ladders, the final set of dominating insurance ladders has been found.

5.1.1. The inferior insurance ladder test

Let π_{GEN1} and π_{GEN2} be two generic insurance ladders where the following holds:

$$\varphi(\pi_{GEN1}, \lambda) \leq \varphi(\pi_{GEN2}, \lambda) \text{ when } \lambda = 0. \tag{23a}$$

$$\varphi(\pi_{GEN1}, \lambda) \leq \varphi(\pi_{GEN2}, \lambda) \text{ when } \lambda = 1. \tag{23b}$$

Either (23a) or (23b) (or both) must be a strict less than relationship. (23c)

If the three conditions given above are satisfied, π_{GEN2} is discarded as it is an inferior ladder to π_{GEN1}. Further, π_{GEN1} may not end up being a dominating ladder even if π_{GEN1} dominates $\pi_{GEN2,}$ since another insurance ladder π_{GEN3} can dominate insurance ladder π_{GEN1} and insurance ladder π_{GEN3} has not been enumerated and/or examined at this point in the enumeration.

5.1.2. Ordering the dominating insurance ladders

After the set of dominating insurance ladders have been enumerated, these ladders are ordered from smallest premium to largest premium; i.e., these ladders are ordered from the smallest value of $\varphi(\pi_{GEN}, \lambda)$ to the largest value of $\varphi(\pi_{GEN}, \lambda)$ when $\lambda = 0$. Since these insurance ladder are dominating insurance ladders, the insurance ladder with the smallest premium has the largest value of $\varphi(\pi_{GEN}, \lambda)$, when $\lambda = 1$. Further, the insurance ladder with the second smallest value of $\varphi(\pi_{GEN}, \lambda)$ when $\lambda = 0$ has the second largest value of $\varphi(\pi_{\mathrm{GEN}}, \lambda)$ when $\lambda = 1$ and so forth. This ordering of the insurance ladders plays a crucial role in the procedure that finds the optimal dominating insurance ladder as a function of λ.

5.1.3. Computing the value of λ where two dominating insurance ladders intersect

Given that the set of dominating ladders are ordered from smallest to largest premium, let π_{GENF} and π_{GENG} be two dominating insurance ladders where the following holds:

- $\varphi(\pi_{GENF}, \lambda) = PREM(\pi_{GENF}) + RISK(\pi_{GENF}) * \lambda$,
- $\varphi(\pi_{GENG}, \lambda) = PREM(\pi_{GENG}) + RISK(\pi_{GENG}) * \lambda$,
- $PREM(\pi_{GENF})$ is the sum of the premiums of all policies on ladder π_{GENF}.
- $PREM(\pi_{GENG})$ is the sum of the premiums of all policies on ladder π_{GENG}.

$$PREM(\pi_{GENG}) < (or \leq) PREM(\pi_{GENF}) \tag{24a}$$

$$RISK(\pi_{GENG}) \geq (or >) RISK(\pi_{GENF}). \tag{24b}$$

Then, the value of λ where $\varphi(\pi_F, \lambda) = \varphi(\pi_G, \lambda)$, denoted as $\lambda(\pi_{GENG}, \pi_{GENF})$ λ, is the following:

$$\lambda(\pi_{GENG}, \pi_{GENF}) = [PREM(\pi_{GENF}) - [PREM(\pi_{GENG})]/[RISK(\pi_{GENG}) - RISK(\pi_{GENF})] \quad (25)$$

$\lambda(\pi_{GENG}, \pi_{GENF}) \geq 0$ as the numerator and denominator of Eq. (25) are positive. If $\lambda(\pi_{GENG}, \pi_{GENF}) \geq 1$, ladder π_{GENF} is discarded because ladder π_{GENG} dominates ladder π_{GENF} for all value of λ between 0 and 1 as specified in Eqs. (24a) and (24b).

5.2. Procedure for finding the optimal insurance ladder as a function of λ

We now describe the steps that are taken to find the dominating insurance ladder that minimizes the value of $\varphi(\pi_{GEN}, \lambda)$ as a function of λ for all values of λ from $\lambda = 0$ to $\lambda = 1$. This procedure begins at $\lambda = 0$.

5.2.1. Create the matrix of intersection points of the dominating ladders

Assume there are Q dominating insurance ladders, denoted as $GEN1, GEN2, \cdots, GENQ$. These ladders are ordered from the smallest premium to the largest premium. Thus, $GEN1$ has the smallest premium; $GEN2$ has the second smallest premium, etc. Let Q^* be a QxQ matrix called the *Matrix of Intersection Points*. The (i, j) element of Q^* is equal to $\lambda_{GENi,GENj}$, where $\lambda_{GENi,GENj}$ is the value of λ where $\varphi(\pi_{GENi}, \lambda) = \varphi(\pi_{GENj}, \lambda)$, *for* $i = 1, 2, \cdots, Q-1$, and $j = 2, 3, \cdots, Q$. $\lambda_{GEN1,GENj}$ is found using Eq. (25). Q^* is an upper triangle matrix since the other entries in this matrix are not used in this analysis.[19]

If the value of λ for any entry in Q^* using Eq. (25) is greater than 1, this value can be disregarded because λ is a probability and, thus, can be no larger than 1. As noted previously, the value of λ determined using Eq. (25) is nonnegative because both the numerator and denominator of Eq. (25) are positive. At the end of this procedure, the upper triangular portion of Q^* contains the value of λ for each pair of dominating insurance ladders that have been found where λ is between 0 and 1.

5.2.2. Generating the parametric solution

5.2.2.1. Initialization Step. The parametric solution begins with ladder $GEN1$ since the ladders have been ordered with respect to their premiums and $GEN1$ had the smallest premium value. Generally, $GEN1$ is the Null Ladder π_0. The procedure then examines the entries in the first row of Q^* to find the ladder $GENk1$ that minimizes the value of $\lambda(\pi_{GEN1}, \pi_{GENk})$ of where $GENk$ goes from $GEN2$ to $GENQ$. In other words, the procedure scans the first row of the Matrix of Intersection Points and finds the dominating ladder $GENk1$ that is the first ladder to intersect with $GEN1$.

5.2.2.2. Recursion Step 1. We now analyze the $k1$ row of the matrix Q^* to find the ladder $GENk2$ that minimizes the value of $\lambda_{GENk1,GENk}$ where $GENk$ goes from $GEN(k1 + 1)$ to $GENQ$. In other words, the procedure scans the $GENk1$ row of the Matrix of Intersection Points and finds the dominating ladder $GENk2$ that is the first ladder to intersect with $GENk1$.

5.2.2.3. Recursion Step 2. We repeat Recursion Step 1, except that we are looking for the dominating ladder $GENk3$ that is the first ladder to intersect with $GENk2$ as given in entries in the matrix Q^*. We repeat the Recursion Step until we have examined either explicitly or implicitly all of the rows of Q^*.

Additional considerations in carrying out the Initialization Step and the Recursion Steps are as follows:

a. As described previously, if $\lambda(\pi_{GENi}, \pi_{GENj}) \geq 1$ for any ladder π_{GENj} in the execution of the Recursion Step, then ladder π_{GENj} is not a viable candidate for entry into the parametric solution since λ is a probability and can only take on values between 0 and 1.

b. If $\lambda(\pi_{GENi}, \pi_{GENj}) \geq 1$, where $\lambda(\pi_{GENi}, \pi_{GENj})$ is the minimum value of λ in row $GENi$ in either the Initialization or Recursion Step, the procedure terminates since the optimal parametric solution from $\lambda = 0$ to $\lambda = 1$ has been found. $GENi$ is the optimal ladder from the minimum value of λ determined on the previous Recursion Step or until $\lambda = 1$.

c. If more than one ladder have the same minimum value of λ, when carrying out the aforementioned Initialization Step or Recursion Step, then the ladder with the minimum value of *RISK* (and largest premium cost) becomes the best ladder at this point in the generation of the parametric solution.

5.2.2.4. Termination condition. The Recursion Steps are carried out until all rows in Q^* are examined or the procedure with the maximum premium cost becomes the ladder that is the next ladder to be scanned. In either case, the last ladder that is determined to be part of the optimal solution is found and the procedure terminates.

5.3. Two examples of the parametric procedure

We now present two examples that illustrate the parametric procedure developed in this paper and an analysis of the results generated by this procedure.

5.3.1. Parametric procedure example 1

Example 1 is a direct application of the parametric procedure described above. The three available policies in Example 1 are the following: π_1 whose Policy $P1$ has representation (5, 15, 2), π_2 whose Policy $P2$ has representation (25, 45, 2.5), and π_3 whose Policy $P3$ has representation (50, 80, 1.5). Also, $L_{max} = 100$.

[19] Tables 8 and 12 will provide examples of a Q^* matrix.

The random variable L is assumed to be uniformly distributed over the interval (0, 100). Under these assumptions, the following holds:

- The density function for the random variable L given that a breach has occurred is $f(x) = .01$, for $0 \le x \le 100$ and $f(x) = 0$, otherwise.
- The CDF for the random variable L given that a breach occurs, is $F(x) = .01x$ for $0 \le x \le 100$. Further, $F(x) = 0$ for $x \le 0$ and $F(x) = 1$ for $x \ge L_{max}$, where $L_{max} = 100$.
- $RISK(\pi_0)$ for the Null Ladder π_0 is equal to $\int_0^{100} x*f(x)dx = 50$.

The parametric procedure systematically determines the optimal ladder as a function of λ, when λ ranges from 0 to 1. As shown below, when $\lambda = 0$, there is one Non-Coverage area. Then, as λ increases from 0 to 1, the optimal ladder has two Non-Coverage areas, then three Non-Coverage areas and, finally, four non-Coverage areas. We now apply the parametric procedure to this three insurance policies example.

5.3.1.1. Computing the Reduction in RISK for the one-policy ladders π_1, π_2, **and** π_3. The *Reduction in RISK* for Policies 1, 2, and 3 are the following:

$$\text{Reduction in } RISK(\pi_1) = \{R(5, 15) - 5*[F(15) - F(5)]\} + (15 - 5)*(1 - .15)$$

$$= \int_5^{15} x*f(x)dx - 5*(.15 - .05) + 10*(1 - .15)$$

$$= 1.0 - .5 + 8.5 = 9.0$$

$$\text{Reduction in } RISK(\pi_2) = \{R(25, 45) - 25*[F(45) - F(25)]\} + (45 - 25)*(1 - .45)$$

$$= \int_{25}^{45} x*f(x)dx - 25*(.45 - .25) + 20*(1 - .45)$$

$$= 7 - 5 + 11 = 13$$

$$\text{Reduction in } RISK(\pi_3) = \{R(50, 80) - 50*[F(80) - F(50)]\} + (80 - 50)*(1 - .8)$$

$$= \int_{50}^{80} x*f(x)dx - 50*(.8 - .5) + 30*(1 - .8)$$

$$= 19.5 - 15 + 6 = 10.5$$

5.3.1.2. Enumerating and evaluating the ladders. Eight ladders (including the Null Ladder) can be generated from π_1, π_2 and π_3. These eight ladders are denoted by π_0, π_1, π_2, π_3, $\pi_{1,2}$, $\pi_{1,3}$, $\pi_{2,3}$, and $\pi_{1,2,3}$, as shown in the first column of Table 6. The calculations of the *RISK* for ladders π_0, π_1, π_2, and π_3 were shown above, and the calculation of the *RISK* for ladders $\pi_{1,2}$, $\pi_{1,3}$, $\pi_{2,3}$, and $\pi_{1,2,3}$ are easily calculated by applying the theorem given in Section 4.3.1. The *RISK* for all eight ladders are shown in the second column of Table 6. The values of $\varphi(\pi_{GEN}, \lambda)$, each ladder's total premium plus the expected loss (the ladder's *RISK* weighted by the firm's prior probability that a breach will occur, λ), is shown in the third column of Table 6. Further, the two ladders, π_1 and $\pi_{1,2}$, in Table 6, are identified as inferior ladders according to the Inferior Ladder Test and are discarded. The six dominating ladders, ordered by premium, are given in Table 7.

5.3.1.3. Creating the matrix of intersection points. The Matrix of Intersection Points is created using the ladders in Table 7 where the rows and columns in Table 8 are ordered by non-decreasing premium cost. In Table 8, the value of λ where $\varphi(\pi_{GEN1}, \lambda) = \varphi(\pi_{GEN2}, \lambda)$ for all pairs of dominating insurance ladders, π_{GEN1} and π_{GEN2}, are generated using Eq. (25). This matrix is filled in before entering the algorithm for determining the parametric solution, which is described next. The bold elements in Table 8 are described in the next step as the algorithm for determining the parametric solution is carried out.

Table 6
Enumerated Ladders with **their *RISK* and their** Overall Premium + Weighted *RISK* for Parametric Procedure Example 1.

Ladder	*RISK*	Premium + Weighted RISK
π_0	$RISK(\pi_0) = 50$	$\varphi(\pi_0, \lambda) = 0 + 50*\lambda$
π_1	$RISK(\pi_1) = 50 - 9 = 41$	$\varphi(\pi_1, \lambda) = 2 + 41*\lambda$, dominated by π_3
π_2	$RISK(\pi_2) = 50 - 13 = 37$	$\varphi(\pi_2, \lambda) = 2.5 + 37*\lambda$
π_3	$RISK(\pi_3) = 50 - 10.5 = 39.5$	$\varphi(\pi_3, \lambda) = 1.5 + 39.5*\lambda$
$\pi_{1,2}$	$RISK(\pi_{1,2}) = 50 - 22 = 28$	$\varphi(\pi_{1,2}, \lambda) = 4.5 + 28*\lambda$, dominated by $\pi_{2,3}$
$\pi_{1,3}$	$RISK(\pi_{1,3}) = 50 - 19.5 = 30.5$	$\varphi(\pi_{1,3}, \lambda) = 3.5 + 30.5*\lambda$
$\pi_{2,3}$	$RISK(\pi_{2,3}) = 50 - 23.6 = 26.5$	$\varphi(\pi_{2,3}, \lambda) = 4 + 26.5*\lambda$
$\pi_{1,2,3}$	$RISK(\pi_{1,2,3}) = 50 - 32.5 = 17.5$	$\varphi(\pi_{1,2,3}, \lambda) = 6 + 17.5*\lambda)$

Table 7
Dominating Ladders and their Total Premium Cost plus Weighted *RISK* for Parametric Procedure Example 1.

Ladder	Overall Premium + Weighted *RISK*
π_0	$\varphi(\pi_0, \lambda) = 0 + 50*\lambda$
π_3	$\varphi(\pi_3, \lambda)=1.5 + 39.5*\lambda$
π_2	$\varphi(\pi_2, \lambda)=2.5 + 37*\lambda$
$\pi_{1,3}$	$\varphi(\pi_{1,3}, \lambda)=3.5 + 30.5*\lambda$
$\pi_{2,3}$	$\varphi(\pi_{2,3}, \lambda)=4 + 26.5*\lambda$
$\pi_{1,2,3}$	$\varphi(\pi_{1,2,3}, \lambda)=6 + 17.5*\lambda$

Table 8
Value of λ where $\varphi(\pi_{GEN1}, \lambda) = \varphi(\pi_{GEN2}, \lambda)$ for Parametric Procedure Example 1.

	π_0	π_3	π_2	$\pi_{1,3}$	$\pi_{2,3}$	$\pi_{1,2,3}$
π_0	–	**0.143**	0.193	0.179	0.170	0.185
π_3	–	–	0.4	0.222	**0.192**	0.205
π_2	–	–	–	0.143	0.115	0.179
$\pi_{1,3}$	–	–	–	–	0.125	0.192
$\pi_{2,3}$	–	–	–	–	–	**0.222**
$\pi_{1,2,3}$	–	–	–	–	–	–

5.3.1.4. Algorithm for determining the parametric solution. We now generate the parametric solution for this example using the algorithm described previously in this section and the data in Table 8. This procedure consists of an Initialization Step, two Recursion Steps, and a Termination Step.

5.3.1.4.1. Initialization Step. The Null Ladder π_0 is the optimal ladder since the premium cost of π_0=0 and all other dominating ladders have positive premium costs. The entry with the minimum value in the π_0 row in Table 8 is equal to the *Min*{.143, .193, .179, .170, .185} = .143 so that π_0 is the optimal ladder from $\lambda = 0$ to $\lambda = .143$. This decision is indicated in Table 8 by bolding the (π_0, π_3) cell in Table 8. We begin Recursion Step Pass 1 by examining the π_3 row in Table 8.

5.3.1.4.2. Recursion Step Pass 1. The entry with the minimum value in the π_3 row in Table 8 is equal to the *Min*{.4, .222, .192, .205} = .192. Thus, the (π_3, $\pi_{2,3}$) cell in Table 8 is bolded and π_3 is the optimal ladder from $\lambda = .143$ to $\lambda = .192$. Ladder π_3, has two Non-Coverage areas, (0, 50) and (80,100), and one Coverage area, (50, 80). We begin Recursion Step Pass 2 by examining the $\pi_{2,3}$ row in Table 9.

5.3.1.4.3. Recursion Step Pass 2. The entry with the minimum value in the $\pi_{2,3}$ row in Table 8 is equal to the *Min*{.222} = .222. Thus, the ($\pi_{2,3}$, $\pi_{1,2,3}$) cell in Table 8 is bolded and $\pi_{2,3}$ is the optimal ladder from $\lambda = .192$ to $\lambda = .222$. Ladder $\pi_{2,3}$ has three Non-Coverage areas, (0, 25), (45, 50) and (80, 100), and two Coverage area, (25, 45) and (50, 80). We next examine the $\pi_{1,2,3}$ row in Table 8.

5.3.1.4.4. Termination. After Recursive Step Pass 2 is completed, the procedure terminates since ladder $\pi_{1,2,3}$ is the ladder with the largest premium, so $\pi_{2,3}$ is the optimal ladder for $\lambda = .222$ to $\lambda = 1$. Ladder $\pi_{1,2,3}$ has four Non-Coverage areas, (0, 5), (15, 25), (45, 50) and (80, 100), and three Coverage areas, (5, 15), (25, 45), and (50, 80).

5.3.1.5. Further analysis of the solution to this example. A summary of the results of this example is presented below and summarized in Table 9.

- π_0 is the optimal ladder for λ between $\lambda = 0$ and $\lambda = .143$. The overall cost plus weighted *RISK* at $\lambda = 0$ is $\varphi(\pi_0, \lambda = 0) = 0$ and the overall cost plus weighted risk at $\lambda = .143$ is $\varphi(\pi_0, \lambda = .143) = 7.15$. The ladder π_0 has one Non-Coverage area, (0, 100), and no Coverage areas.
- λ between $\lambda = .143$ and $\lambda = .192$ so that $\varphi(\pi_3, \lambda = .143) = 7.15$ and $\varphi(\pi_3, \lambda = .192) = 9.0845$. The ladder π_3 has two Non-Coverage areas, (0, 50) and (80, 100), and one Coverage area, (50, 80).
- $\pi_{2,3}$ is the optimal ladder for λ between $\lambda = .192$ and $\lambda = .222$ so that $\varphi(\pi_{2,3}, \lambda = .192) = 9.0845$ and $\varphi(\pi_{2,3}, \lambda = .222) = 9.885$. The

Table 9
Summary of the Solution for Parametric Procedure Example 1.

Beginning Ladder	Minimum λ	Maximum λ	Ending Ladder	φ at Minimum Value of λ	φ at Maximum Value of λ
π_0	0	0.143	π_3	0	7.15
π_3	0.143	0.192	$\pi_{2,3}$	7.15	9.0845
$\pi_{2,3}$	0.192	0.222	$\pi_{1,2,3}$	9.0845	9.885
$\pi_{1,2,3}$	0.222	1	–	9.885	23.5

Table 10
Enumerated Insurance Ladders and their Properties for Parametric Procedure Example 2.

Ladder	Premium	RR	*RISK*	Dominance Check
π_0	0	0	33.333	
π_a	0.5	8.103	25.23	
π_c	1	7.73	25.603	Dominated by π_a
π_b	1.5	11.317	22.016	Dominated by $\pi_{a,c}$
$\pi_{a,c}$	1.5	15.833	17.5	
$\pi_{a,b}$	2	19.42	13.913	
$\pi_{b,c}$	2.5	19.049	14.284	Dominated by $\pi_{a,b}$
$\pi_{a,b,c}$	3	27.152	6.181	

ladder $\pi_{2,3}$ has three Non-Coverage areas, (0, 25), (45, 50) and (80, 100), and two Coverage areas, (25, 45) and (50, 80).

- $\pi_{1,2,3}$ is the optimal ladder for λ between . 222 and 1 so that $\varphi(\pi_{1,2,3}, \lambda = .222) = 9.885$ and $\varphi(\pi_{1,2,3}, \lambda = 1) = 23.5$. The ladder $\pi_{1,2,3}$ has four Non-Coverage areas, (0, 5), (15, 25), (45, 50), and (80, 100), and three Coverage areas, (5,15), (25, 45), and (50, 80).

5.3.2. Parametric procedure example 2

Example 2 illustrates the following situation. An ILF insurance ladder is made up of three insurance policies called Policy a, Policy b, and Policy c. In this ILF, the ceiling of Policy a equals the deductible of Policy b and the ceiling of Policy b equals the deductible of Policy c. Further, these policies are ordered from smallest ceiling to largest ceiling. The two Non-Coverage areas of positive span for the ILF ladder are (0, Policy a's Deductible) and (Policy c's Ceiling, L_{max}), and one Coverage area, (Policy a's Deductible, Policy c's Ceiling). In this example, Policy a has realization (5, 15, 0.5), Policy b has realization (15, 35, 1.5) and Policy c has realization (35, 65, 1). Define π_a, π_b, and π_c to be the associated one-policy insurance ladders for Policies a, b, and c. The ILF ladder $\pi_{a,b,c}$ can be thought of as a single insurance policy with realization (5, 65, 3).

The firm wishes to determine if any ladder made up of one or two policies from the policies on this ILF ladder can generate an optimal dominating ladder for some range of λ between 0 and 1. In particular, the firm is interested in knowing if ladder π_{ac}, the ladder comprised of Policies a and c, is optimal for some range of λ between 0 and 1.

Using the density function given in Eq. (19) and the example illustrating the computation of *RISK* for the ILF ladder $\pi_{a,b,c}$ given in Section 4 of this paper, the computation of the *Reduction in RISK* (RR) and *RISK* are given in Table 10.[20] Also, in Table 10, three ladders that are inferior ladders are identified and discarded from consideration in the parametric procedure. Then, in Table 11, a listing of the dominating ladders ordered by premium from smallest to largest is presented. Finally, in Table 12, the parametric solution is presented.

A more detailed analysis of the solution found in Table 12 is the following:

- π_0 is the optimal ladder for λ in the interval (0, .0617), where $\varphi(\pi_0, \lambda = 0) = 0$ and $\varphi(\pi_0, \lambda = .0617) = 2.123$. The ladder π_0 has one Non-Coverage area, (0, 100), and no Coverage areas.
- π_a is the optimal ladder for λ in the interval (.0617, .12937), where $\varphi(\pi_a, \lambda = .0617) = 2.123$ and $\varphi(\pi_a, \lambda = .12937) = 3.764$. The ladder π_a has two Non-Coverage areas (0, 5) and (15, 100), and one Coverage area, (15, 25).
- $\pi_{a,c}$ is the optimal ladder for λ in the interval (.12937, .1325), where $\varphi(\pi_{a,c}, \lambda = .12937) = 3.764$ and $\varphi(\pi_{a,c}, \lambda = .1325) = 3.819$. The ladder $\pi_{a,c}$ has three Non-Coverage areas, (0, 5), (15, 35), and (65,100), and two Coverage areas, (5,15) and (35, 65).
- $\pi_{a,b,c}$ is the optimal ladder for λ in the interval (.1325, 1), where $\varphi(\pi_{a,b,c}, \lambda = .1325) = 3.819$ and $\varphi(\pi_{a,b,c}, \lambda = 1) = 9.181$. The ladder $\pi_{a,b,c}$ has two Non-Coverage areas, (0, 5) and (65, 100), and one Coverage area, (5, 65).

Example 2 illustrated that when offered an ILF, there is often a range of values of λ (the firm's prior probability of a breach occurring) for which the firm would be better off deleting an interior policy (i.e., inserting an interior Non-Coverage area) and saving

Table 11
Dominating Ladders Ordered by their Premiums for Parametric Procedure Example 2.

Ladder	Premium	RR	*RISK*
π_0	0	0	33.333
π_a	0.5	8.103	25.23
$\pi_{a,c}$	1.5	15.833	17.5
$\pi_{a,b}$	2	19.42	13.913
$\pi_{a,b,c}$	3	27.152	6.181

[20] Note that the density function given in equation (19) necessitates some rounding in the subsequent calculations.

Table 12
Values of λ where Pairs of Dominating Ladders Intersect for Parametric Procedure Example 2.

	π_0	π_a	$\pi_{a,c}$	$\pi_{a,b}$	$\pi_{a,b,c}$
π_0	–	**0.0617**	0.0947	0.1030	0.1105
π_a	–	–	**0.1294**	0.1325	0.1312
$\pi_{a,c}$	–	–	–	0.1394	**0.1325**
$\pi_{a,b}$	–	–	–	–	0.1738
$\pi_{a,b,c}$	–	–	–	–	–

on premium costs. That is, for Example 2, the insuree is better off (*ex ante*) purchasing the Ladder $\pi_{a,c}$ made up of Policies a and c than purchasing the entire ILF Ladder $\pi_{a,b,c}$ for $.12937 < \lambda < .1325$. In other words, for a range of values of λ, by considering sets of insurance policies with three Non-Coverage areas, the insuree is better able to address the frequently cited problems of high deductibles and low ceilings common in the current cybersecurity insurance marketplace.

6. Concluding comments

The uncertain and complex nature of cybersecurity attacks is one of the key challenges confronting organizations in today's interconnected digital world. Organizations cannot, however, realistically eliminate all cybersecurity risks to achieve 100% security. Furthermore, cybersecurity investments ultimately become more costly than the benefits derived from the incremental security. Thus, those responsible for preventing cybersecurity breaches (i.e., securing the information and information systems within their organizations), as well as firms providing risk advisory services (e.g., accounting firms and other risk management consulting firms), need to think in terms of the cost-benefit aspects of cybersecurity investments. Cybersecurity insurance is one way to consider the cost-benefit aspects of cybersecurity investments. More to the point, cybersecurity insurance allows an organization to transfer, at a price, some of the risk associated with a cybersecurity breach. Of course, for such a strategy to be effective, there needs to be an efficient cybersecurity insurance marketplace.

In addition to transferring the risk of cybersecurity breaches, an efficient cybersecurity insurance market would, or at least should, reduce the actual number of data breaches. As noted by the Department of Homeland Security (DHS): "…A robust cybersecurity insurance market could help reduce the number of successful cyberattacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection" (see: https://www.dhs.gov/cybersecurity-insurance). The belief that an efficient cybersecurity insurance market would improve cybersecurity within organizations is at the heart of why public policy-makers have devoted a significant amount of attention to the topic (see Woods and Simpson, 2017).

The objective of the research contained in this paper has been to develop a model that facilitates risk sharing among insurers and those being insured in a manner that directly addresses the frequently expressed concern that cybersecurity insurance policies have high deductibles and low ceilings, related to the premiums being charged for the policies. The model developed in this paper can be used to derive the optimal set of cybersecurity insurance policies that a firm should purchase, from a finite set of insurance policies offered by insurance companies. The model is based on finding an appropriate cost-adjusted risk-sharing arrangement among cybersecurity insurers and firms being insured. The model is developed from the perspective of a firm purchasing the insurance policies and assumes that the firm's goal in purchasing cybersecurity insurance is to select a set of policies to minimize the total expected costs of the insurance premiums plus the expected loss from a breach.

The model proposed in this paper explicitly considers the fact that the purchasing firm may select a set of policies in a manner that can result in more than two Non-Coverage areas. The model allows a firm to systematically evaluate various insurance policies as a function of the probability that a cybersecurity breach occurs during the term of the policies and the premiums associated with the policies. Most importantly, the proposed model provides a risk-sharing approach that helps firms select cybersecurity insurance policies in a manner that should help to facilitate an efficient cybersecurity insurance marketplace. As such, our model can be thought of as a response to the call by Marotta et al. (2017), where they note that "Novel approaches and treatments are required to ensure the positive effect of cyber insurance on society as well as new standards and practices required for the maturation of the market" (p. 22).

As with all papers based on an analytical model, this paper makes several assumptions. Changing these assumptions would, of course, result in a different risk-sharing solution among firms and insurance companies. For example, if the assumption that all insurance policies begin and end on the same date or the assumption that companies and insurance firms are risk neutral were to change, then the optimal set of insurance policies that firms would purchase to make up an insurance ladder (i.e., tower) would be more difficult to derive. The risk term would measure the firm's certainly equivalent loss over the set of policies in the ladder. We also assumed that purchasing firms could identify, at no cost, the relevant set of cybersecurity policies to examine. To the extent that this assumption was not valid, the cost of identifying such policies would have to be considered.

In addition to the above noted assumptions, our model did not take into consideration pricing strategies that might be employed by companies selling cybersecurity insurance. For example, given the fact that cyber insurance offers tremendous growth opportunities for insurance firms, there could be strong incentives for such firms to employ limit pricing as a means of obtaining a large share of the potential cybersecurity insurance market. Although beyond the scope of this paper, examining the effects of different pricing strategies on the development of the cybersecurity marketplace offers a fertile area for future research.

Our assumptions, however, do not negate the logic underlying the analysis presented in this paper. Accordingly, we believe the analysis contained in this paper provides a meaningful step forward in the development of a more robust cybersecurity insurance market. One way for a government agency to facilitate the development of an efficient cybersecurity insurance marketplace might be to develop a database that lists various insurance carriers together with generic information concerning the policies available from these carriers.

Acknowledgements

We wish to thank Thomas Finan for his assistance in structuring the problem discussed in this paper and for discussing this problem with us. We also want to thank Jin Choi, Hemantha Herath, Cody Hyman, Laurel Mazur, Gerald Ward, and Lei Zhou for their comments on an earlier draft of this paper.

References

Amir, E., Levi, S., Livne, T., 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. Rev. Account. Stud. 1–30.
Bandyopadhyay, T., Mookerjee, V.S., Rao, R.C., 2009. Why IT managers don't go for cyber-insurance products. Commun. ACM 52 (11), 68–73.
Benaroch, M., 2018. Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. Inf. Syst. Res. February 22, 2018 (on-line).
Biener, C., Eling, M., Wirfs, J.H., 2015. Insurability of cyber risk: an empirical analysis. Geneva Pap. Risk Insurance-Issues Pract. 40 (1), 131–158.
Bodin, L.D., Gordon, L.A., Loeb, M.P., 2008. Information security and risk management. Commun. ACM 51 (4), 64–68.
Böhme, R., Schwartz, G., 2010. Modeling Cyber-Insurance: Towards a Unifying Framework. WEIS (June).
Campbell, K., Gordon, L.A., Loeb, M.P., Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J. Comput. Secur. 11 (3), 431–448.
Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. Int. J. Electronic Commerce 9 (1), 70–104.
CEA (The Council of Economic Advisors), 2018. The Cost of Malicious Cyber Activity to the U.S. Economy. < https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf > .
Department of Homeland Security Department of Homeland Security, 2012. Cybersecurity Insurance Workshop Readout Report, from < http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf > (accessed 4 August 2015).
Gal-Or, E., Ghose, A., 2005. The economic incentives for sharing security information incentives for sharing security information. Inf. Syst. Res. 16 (2), 186–208.
Ettredge, M.L., Richardson, V.J., 2003. Information transfer among internet firms: the case of hacker attacks. J. Inf. Syst. 17 (2), 71–82.
European Union Agency for Network and Information Security (ENISA), 2016. Cyber Insurance: Recent Advances. Good Practices and Challenges, Available at: https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges.
Finkle, J., 2015. Cyber Insurance Premiums Rocket after High-profile Attacks. Reuters, Boston, MA. < www.reuters.com/article/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012 > (accessed 07 June 2018).
Gordon, L.A., Loeb, M.P., 2002. The economics of information security investment. ACM Trans. Inf. Syst. Security (TISSEC) 5 (4), 438–457.
Gordon, L.A., Loeb, M.P., Lucyshyn, W., 2003a. Sharing information on computer systems security: an economic analysis. J. Account. Public Policy 22 (6), 461–485.
Gordon, L.A., Loeb, M.P., Lucyshyn, W., Sohail, T., 2006. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. J. Account. Public Policy 25 (5), 503–530.
Gordon, L.A., Loeb, M.P., Lucyshyn, W., Zhou, L., 2015. The impact of information sharing on cybersecurity underinvestment: a real options perspective. J. Account. Public Policy 34 (5), 509–519.
Gordon, L.A., Loeb, M.P., Sohail, T., 2003b. A framework for using insurance for cyber-risk management. Commun. ACM 46 (3), 81–85.
Gordon, L.A., Loeb, M.P., Sohail, T., 2010. Market value of voluntary disclosures concerning information security. MIS Q. 567–594.
Gordon, L.A., Loeb, M.P., Zhou, L., 2011. The impact of information security breaches: Has there been a downward shift in costs? J. Comput. Secur. 19 (1), 33–56.
Herath, H.S., Herath, T.C., 2008. Investments in information security: a real options perspective with Bayesian postaudit. J. Manage. Inf. Syst. 25 (3), 337–375.
Herath, H., Herath, T., 2011. Copula-based actuarial model for pricing cyber-insurance policies. Insurance Markets Companies: Analyses Actuarial Comput. 2 (1), 7–20.
Hilary, G., Segal, B., Zhang, M.H., 2016. Georgetown McDonough School of Business Research Paper No. 2852519. Available at SSRN: < https://ssrn.com/abstract=2852519 > or https://doi.org/10.2139/ssrn.2852519.
Marotta, A., Martinelli, F., Nanni, S., Orlando, A., Yautsiukhin, A., 2017. Cyber-insurance survey. Comput. Sci. Rev. 24, 35–61.
Miccolis, R.S., 1977. On the theory of increased limits and excess of loss pricing. PCAS LXIV 27.
Millard, M., 2015. Make sure your company has adequate insurance for cyber incidents, (2015 Ernst & Young LLP), accessed at < http://www.ey.com/Publication/vwLUAssets/ey-maintaining-adequate-insurance-for-cyber-incidents/$File/ey-maintaining-adequate-insurance-for-cyber-incidents.pdf > on 16 June 2017.
Nocera, J., 2014. How cyber insurance can help you better manage security risks. (2014 pwc Cybersecurity and Privacy blog), accessed at < http://usblogs.pwc.com/cybersecurity/how-cyber-insurance-can-help-you-better-manage-security-risks/ > on 16 June 2018.
Palmer, Joseph, 2006. Increased Limits Ratemaking for Liability Insurance, accessed on the Internet at 6 May 2018 at < https://www.casact.org/library/studynotes/palmer.pdf > .
Rechtman, Y., Rashbaum, K.N., 2015. Cybersecurity risks to CPA firms. CPA J. 85 (5), 54.
Romanosky, S., 2016. Examining the costs and causes of cyber incidents. J. Cybersecurity 2 (2), 121–135.
SEC (Securities and Exchange Commission), 2011. CF Disclosure Guidance: Topic No. 2. Cybersecurity. < https://www.sec.gov/divisions/corpfin/guidance/cfguidancetopic2.htm > .
SEC (Securities and Exchange Commission), 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. 17 CFR Parts 229 and 249 [Release Nos. 33-10459; 34-82746] Available at: < https://www.sec.gov/rules/interp/2018/33-10459.pdf > .
Shavell, S., 1979. Risk sharing and incentives in the principal and agent relationship. Bell J. Econ. 55–73.
Shetty, N., Schwartz, G., Felegyhazi, M., Walrand, J., 2010. Competitive cyber-insurance and internet security. In: Economics of Information Security and Privacy. Springer, Boston, MA, pp. 229–247.
Spanos, G., Angelis, L., 2016. The impact of information security events to the stock market: a systematic literature review. Comput. Security 58, 216–229.
Straub, D.W., Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. MIS Q. 441–469.
U.S. Department of Homeland Security, 2012. National Protection and Programs Directorate, Security, Cybersecurity Insurance Workshop Readout Report. Washington, DC.
Wang, T., Kannan, K.N., Ulmer, J.R., 2013. The association between the disclosure and the realization of information security risk factors. Inf. Syst. Res. 24 (2), 201–218.
Woods, D., Simpson, A., 2017. Policy measures and cyber insurance: a framework. J. Cyber Policy 2 (2), 209–226.