J. Account. Public Policy 34 (2015) 509–519

Contents lists available at ScienceDirect

J. Account. Public Policy

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

Journal of Accounting and Public Policy

The impact of information sharing on cybersecurity underinvestment: A real options perspective

Lawrence A. Gordon [a], Martin P. Loeb [a,*], William Lucyshyn [b], Lei Zhou [a]

[a] Robert H. Smith School of Business, University of Maryland, College Park, MD 20742-1815, USA
[b] Center for Public Policy and Private Enterprise, School of Public Policy, University of Maryland, College Park, MD 20742-1815, USA

ABSTRACT

Maintaining adequate cybersecurity is crucial for a firm to maintain the integrity of its external and internal financial reports, as well as to protect the firm's strategic proprietary information. This paper demonstrates how information sharing could encourage firms to take a more proactive, as compared to a reactive, approach toward cybersecurity investments. In particular, information sharing could reduce the tendency by firms to defer cybersecurity investments. The basic argument presented in this paper is grounded in the *real options* perspective of cybersecurity investments. More to the point, the value of an option to defer an investment in cybersecurity activities increases as the uncertainty associated with the investment increases. To the extent that information sharing reduces a firm's uncertainty concerning a cybersecurity investment, it decreases the value of the deferment option associated with the investment. As a result of this decrease in the deferment option value, it may well make economic sense for the firm to make the cybersecurity investment sooner than otherwise would be the case.

* Corresponding author. Tel.: +1 301 405 2209; fax: +1 301 314 9414.
E-mail address: mloeb@rhsmith.umd.edu (M.P. Loeb).

http://dx.doi.org/10.1016/j.jaccpubpol.2015.05.001
0278-4254/© 2015 Elsevier Inc. All rights reserved.

1. Introduction

Improving cybersecurity is a key concern in the current digital world of computers, industrial control systems, tablets, and smart phones. Maintaining adequate cybersecurity is crucial for a firm to maintain the continuity of its services, integrity of its external and internal financial reports, as well as to protect the firm's strategic proprietary information. The U.S. Securities and Exchange Commission (U.S., 2011) issuance of the ''Disclosure Guidance on Cybersecurity Risks and Cyber Incidences'' provides evidence of the essential role cybersecurity plays in successful corporations. In addition, in order to comply with sections 302 and 404 of the Sarbanes-Oxley Act of 2002 (SOX) dealing with providing an adequate internal control system to ensure reliable financial reports and the protection of assets, auditors and firms' executive officers recognize the essential role of cybersecurity. Given the relevance of cybersecurity to accounting and public policy, accounting researchers (e.g., see Gordon and Loeb, 2002, 2006; Gordon et al., 2003a, 2003b, 2006, 2011), as well as computer scientists (e.g., see Anderson and Moore, 2006; Böhme and Moore, 2009), have recognized the importance of cybersecurity investments in a modern digital economy.

Corporations around the world are currently making significant investments in various cybersecurity related activities.[1] These investments relate to such things as encryption techniques, access controls, firewalls, anti-malware software, intrusion prevention and detection systems, data segregation, and personnel training. Clearly, the amount a firm should invest in cybersecurity activities depends (in part) on the cost-benefit (i.e., economic) aspects of such investments (e.g., see Gordon and Loeb, 2002, 2006). However, no matter how much a firm invests in cybersecurity, 100% security is not achievable.

Viewing cybersecurity investments through an economic lens has its strengths and weaknesses. The key strength is that it facilitates an efficient allocation of resources within a firm. In contrast, a fundamental weakness is that there are several key impediments to quantifying the economic benefits of cybersecurity investments. These impediments include the fact that the benefits are largely in terms of potential cost savings, which are riddled with significant uncertainty. A firm can only estimate the cost savings based on the difference between the *ex ante* estimated costs of security breaches assuming an incremental cybersecurity investment under consideration were not made, and the *ex post* costs associated with actual cybersecurity breaches after making the investment.[2] Thus, the cost savings from preventing security breaches are not directly observable.

As a result of the difficulties associated with estimating the benefits from cybersecurity investments, there is a widespread belief that private sector firms tend to underinvest in cybersecurity activities.[3] Furthermore, firms tend to defer much of their cybersecurity investments unless reacting to a major cybersecurity breach. That is, firms tend to take a reactive, rather than proactive, approach toward cybersecurity investments related to their organizations. While this observation has been noted elsewhere (e.g., Gordon et al., 2003a), the future capital investments section of the Management's Discussion and Analysis of Financial Condition and Results of Operation (item 7) section of the 10-K for Target Corporation for the fiscal year ended February 1, 2014 (Target Corporation Annual Report, 2014), provides a striking illustration of this phenomenon.[4] Under the *Future Capital Investments* section of the company's 2013 Data Breach discussion on page 18, the company states, ''We plan to accelerate a

[1] Although the exact amount being invested in cybersecurity is not known because firms do not disclose this item in their financial reports, it is well known that the level of investments in cybersecurity is extensive. For example, Target, Inc.'s Chief Financial Officer and Neiman Marcus, Inc.'s Chief Information Officer both noted, during Congressional hearings on February 4, 2014 (e.g., see the C-Span.org coverage of the Senate hearing, at: http://www.c-span.org/video/?317553-1/hearing-cybercrime-privacy), that their respective companies made significant cybersecurity related investments (e.g., at Target, Inc., the company invested hundreds of millions over the past several years) prior to their well publicized major cybersecurity breaches.

[2] Determining the actual costs of cybersecurity breaches is also problematic due to the fact that there are implicit, as well as explicit, costs. Furthermore, there are also indirect, as well as direct, costs (see Gordon and Loeb, 2006).

[3] For example, Mathews (2013) refers to a Forrester Consulting report in his article titled, ''Companies Not Budgeting Enough for Cybersecurity, Study Says,'' and another 2013 Accenture study of CIOs (Accenture High Performance Report, 2013) found ''45% concede they have been underinvesting in cybersecurity. See page 13 of the report available at: http://www.accenture.com/Microsites/high-performance-it/Documents/media/Accenture-High-Performance-IT-Research.pdf.

[4] Target Corporation was the victim of a major cybersecurity breach that was discovered in December 2013.

previously planned investment of approximately $100 million to equip our proprietary REDcards and all of our U.S. store card readers with chip-enabled smart-card technology by the first quarter of 2015."

The objective of this paper is to show how sharing cybersecurity related information among firms has the potential to offset the tendency by firms to defer much of their cybersecurity investments until a cybersecurity breach occurs. The basic argument presented in this paper is grounded in the *real options* perspective of cybersecurity investments.[5] The value of an option to defer an investment in cybersecurity activities increases as the uncertainty of the investment increases. Thus, to the extent that information sharing reduces the uncertainty associated with a firm's cybersecurity investment decision, it decreases the value of the deferment option. As a result, it makes rational economic sense for the firm to make the cybersecurity investment sooner than otherwise would be the case. In other words, information sharing is likely to reduce the incentive for firms to defer their cybersecurity investments.

The remainder of this paper will proceed as follows. In the next, second, section of the paper, we will briefly review the literature on information sharing, with particular focus on sharing information related to the cybersecurity risks and incidents affecting a firm. We discuss the basic argument underlying this paper, which is grounded in real options framework, in the third section of the paper. By revisiting and extending the real options approach to a cybersecurity investment decision provided by Gordon et al. (2003a), we illustrate how a real options perspective sheds new light on the value of information sharing in addressing issues related to cybersecurity investments. The fourth section of the paper discusses the implications of the analysis concerning information sharing and cybersecurity investments. The fifth section of the paper provides some concluding comments and directions for future research.

2. Information sharing and cybersecurity

Information sharing is a concept supported by most corporate executives and government officials/agencies responsible for reducing and responding to cybersecurity breaches related to their organizations.[6] In the U.S., for example, the Department of Homeland Security (DHS) is responsible for the federal government's overall national strategy for cybersecurity and information sharing is an important component of this strategy. More specifically, the 2011 DHS' document entitled "Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise" advocates "Information sharing with trusted partners, including peer and interdependent organizations, government agencies, and vendors through risk-mitigating fusion centers, sector-designated Information Sharing and Analysis Centers (ISACs), Sector Coordinating Councils, security and/or network operations centers, computer incident response teams, and consumers and suppliers in a supply chain" (DHS, 2011, p. l7). In President Obama's February 12, 2013 Executive Order #13636 entitled, "Improving Critical Infrastructure Cybersecurity" (Obama, 2013), Section 4, part (a), entitled "Cybersecurity Information Sharing," the executive order specifically states that: "It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats."

The U.S. federal government established and promoted security-based information sharing organizations, such as the industry-based Information Sharing and Analysis Centers (ISACs), as a means of facilitating voluntary information sharing among private sector firms related to cybersecurity activities.[7] Information sharing of cybersecurity related activities holds the promise of being a cost-effective way for firms to improve their overall cybersecurity. In fact, Gordon et al. (2003b) show that information sharing related to cybersecurity could reduce the overall costs associated with achieving any particular level of cybersecurity, while at the same time enhancing social welfare. Moreover, Gal-Or and Ghose (2005) show that information sharing related to computer security activities may also positively affect

[5] *Real options* refer to the opportunity, but not the obligation to initiate, defer or abandon a capital investment project.

[6] Although beyond the scope of this paper, information sharing can also help prevent cybersecurity breaches affecting individuals.

[7] It is worth noting that the European Union is moving toward more mandated actions, as contrasted to voluntary actions concerning cybersecurity activities (e.g., see High Representative of the European Union for Foreign Affairs and Security Policy European Commissions, 2013).

the demand for a firm's products. Both Gordon et al. (2003b) and Gal-Or and Ghose (2005) also point out the importance of having appropriate economic incentives to share information in order for the benefits of sharing to be realized.[8] In addition to the analyses by Gordon et al. (2003b) and Gal-Or and Ghose (2005), Schechter and Smith (2003) also point out that that information sharing could help prevent cyber-information security breaches.

As noted earlier, most corporate executives and government officials (i.e., senior administrators and politicians) advocate information sharing as one way of reducing and responding to cybersecurity breaches. Today, most of the current information sharing is based on nation-centric organizations. However, in today's global environment, with its transnational firms and threats, there is good reason to extend this concept to include international partners.

Of course, the virtues of information sharing are not restricted to the cybersecurity arena. Indeed, there is an extensive body of literature extolling the benefits of information sharing in a variety of fields. Of particular relevance to this paper is the economics-based research on information sharing.

The economics-based literature on information sharing focuses on such issues as the role of information sharing in facilitating the activities of trade-associations and joint ventures, as well as the smooth functioning of various economic markets (e.g., oligopolies). Some of the important papers, in this regard, are the ones by Novshek and Sonnenschein (1982), Fried (1984), Gal-Or (1985), Shapiro (1986), Kirby (1988), Vives (1990), Kamien et al. (1992), and Ziv (1993). Although these papers, as well as others, address many issues related to information sharing, the following two issues are of particular importance to this paper. First, information sharing helps to reduce the uncertainty surrounding the supply and demand for a firm's products and/or services. Thus, information sharing enables a firm to generate higher expected profits via improved pricing and production decisions. Second, the economics-based literature clearly notes that information-sharing arrangements are often associated with a free-rider problem.[9]

Although not previously discussed in the cyber/information security literature, information sharing among firms clearly has the potential for reducing the uncertainty associated with cyber/information security investment decisions and, in turn, influencing the level of cybersecurity investments made by firms. One way to consider this influence is via a real options modeling approach. We now turn to such an approach.

3. Real options and cybersecurity investments

3.1. Cybersecurity investments and the deferral option

Investment decisions related to cybersecurity activities are frequently treated as if the decision at hand is either to invest now or lose the investment opportunity (i.e., invest now or never). In reality, however, a large portion of cybersecurity investment decisions can be postponed in total, or in part, to a later date. That is, there is an option to defer the investment. This *deferment option*, as it is called, is part of what is referred to in the investment literature as a real option. When the opportunity to postpone all, or part, of a cybersecurity investment exists, organizations should take into account the costs and benefits of deferring the investment during the process of considering the investment decision. In other words, organizations should consider the value of the deferment option before making an investment decision.

The valuation of the option to defer an investment decision has been part of the study of real options by economists for several decades (e.g., McDonald and Siegel, 1986; Dixit and Pindyck, 1994). Furthermore, there have been several papers addressing the application of real options to

[8] Gordon et al. (2003b) write that although "…information sharing does indeed offer the *potential* to reduce overall information security costs and raise social welfare, some pitfalls exist that may well prevent the realization of the full potential benefits. These pitfalls revolve around the need to create economic incentives to facilitate effective information sharing" (Gordon et al., 2003b, p. 481).

[9] The free-rider problem refers to a situation where a firm (or individual) is able to benefit from a situation irrespective of the magnitude of the firm's (or individual's) contribution. A free-rider situation becomes a problem when it creates an inefficient allocation of resources. See Varian (2002) for an analysis of how the free-rider problem affects decisions to invest in cybersecurity.

the generic issue of information technology investments over the past few decades (e.g., Benaroch and Kauffman, 1999, 2000; Taudes et al., 2000; Benaroch et al., 2006; Fichman, 2004; Ghosh and Li, 2013). The application of real options theory to cybersecurity investments, however, is relatively new.[10] To our knowledge, the paper by Gordon et al. (2003a) was the first article to explicitly discuss the application of real options theory to cybersecurity investments. Later articles that have addressed cybersecurity investments, based on the real options perspective, include those by Daneva (2006), Herath and Herath (2008), Tatsumi and Goto (2010), and Demetz and Bachlechner (2013).

As discussed in the real options literature, the value of a deferment option is positively associated with the degree of uncertainty associated with the investment decision's payoff. In terms of a cybersecurity investment decision, this means that the greater the uncertainty associated with the potential payoff from a cybersecurity investment, the greater the expected value of the option to defer the investment. The value of the option to defer an investment, including a cybersecurity investment, is also positively associated with the irreversibility of the investment decision. In other words, the larger the probability of the irreversibility of an investment decision, the more valuable the option to defer such an investment.[11] Thus, the economic rationality for firms to take a wait-and-see (i.e., defer) approach to part, or all, of a cybersecurity investment opportunity is positively associated with the uncertainty and/or irreversibility of the investment opportunity.[12]

3.2. *Gordon et al. (2003a) real options example without information sharing*

Gordon et al. (2003a) illustrated, via a hypothetical example based on real options theory, why rational managers might decide to defer part, or all, of a cybersecurity investment until some sort of a cybersecurity breach occurs. In their example, the value of the deferment option created a situation whereby waiting to invest helped to address the uncertainty associated with the size of the security breaches, as well as the irreversibility aspects of the cybersecurity investment decision. Although not discussed by Gordon et al. (2003a), the real options view of cybersecurity investments could shed new light on the benefits of information sharing. More to the point, information sharing could reduce the uncertainty associated with a cybersecurity investment opportunity and, in turn, reduce the deferment option value related to cybersecurity investments. A reduction of the deferment option value makes it economically rational for the firm to make a cybersecurity investment sooner than otherwise would be the case. In other words, information sharing would facilitate a more proactive, rather than reactive, approach to cybersecurity investments. To illustrate this latter point, we revisit the Gordon et al. (2003a) example and then extend it to include information sharing.

In the Gordon et al. (2003a) example, the GLL Company has tentatively budgeted $2,500,000 for next year's expenditures on cybersecurity related activities. The example assumes that 60% of the budget, or $1,500,000, is already earmarked for basic cybersecurity activities (e.g., anti-malware software, firewalls, employee training, etc.) and the Chief Security Officer (CSO) has already been authorized to use these funds. However, the remaining, discretionary, $1,000,000 (or 40%) of the cybersecurity budget cannot be spent without the approval by the firm's Chief Financial Officer (CFO).

The CSO at GLL Company wants to use the remaining portion of the firm's cybersecurity budget to hire a consulting firm that specializes in enhancing the cybersecurity operations of its clients.[13] The outside consulting firm will charge GLL $1,000,000 for one fiscal year, or any part thereof.[14]

[10] Cybersecurity investments did not become a major issue of concern until around turn of the century, when the Internet became an important factor in the economies of industrialized countries and the personal lives of their citizens.

[11] If an investment opportunity were completely reversible, from an economics perspective, this would mean that a firm could recover the full value of its investment through some sort of sale of the assets associated with the cybersecurity investment. Under this unlikely scenario, there would be no economic incentive for the firm to defer an otherwise attractive investment opportunity (i.e., there is no real option).

[12] The option to defer an investment is one of several real options. See Dixit and Pindyck (1994) for a comprehensive discussion of the history and development of the theory of real options, as well as a technical discussion of the theory.

[13] From the CSO's perspective, hiring the cybersecurity consulting firm now rather than later makes sense as the CSO is the one who bears the ultimate responsibility for actual security breaches. In other words, there is an agency problem between the CSO and the CFO.

[14] The time value of money is ignored in this example due to the fact that the example only covers a one-year time horizon.

Furthermore, the consulting firm's fee is assumed to be irreversible, once a contract is signed (i.e., cancellation of the consulting contract during the years does not result in a refund of a portion of the $1,000,000 consulting fees). In an effort to get the approval to spend the discretionary $1,000,000 portion of GLL's cybersecurity budget, GLL's CSO presents the firm's CFO with estimates of the cost savings that would result if the cybersecurity consulting firm were hired (i.e., the costs savings associated with the additional monthly security breaches that would be prevented if the consulting firm were hired).

The cost savings, by hiring the cybersecurity consulting firm, according to the CSO, would be either $40,000 or $200,000 a month, with an equal likelihood (i.e., 50% probability). Thus, GLL could hire the consulting firm now and save a total annual estimated expected cost of $1,440,000 (i.e., $[(.5 \times 40{,}000) + (.5 \times 200{,}000)] \times 12$). If GLL could hire the consulting firm at the beginning of the year, the expectant savings to the firm would be $440,000 (i.e., $1,440,000 – $1,000,000). However, a unique feature of this example is that the true cost savings per month will reveal itself after one month. That is, after one month GLL will know with certainty whether the cyber breaches prevented by hiring the cybersecurity consulting firm would be $40,000 to $200,000. Accordingly, GLL could wait one month to find out the true cybersecurity cost savings derived from hiring the consulting firm. Furthermore the opportunity to hire the consulting firm one month later would still be available, although the fee would still be $1,000,000 for the remaining 11 months.[15]

As shown in the Gordon et al. (2003a) paper, the expected net savings to the firm by deferring by one month the decision to hire the consulting firm would be $600,000 (i.e., $(11 \times \$200{,}000 - \$1,000,000) \times .5$), which is $160,000 greater than the $440,000 expected net savings from immediately hiring the consulting firm.[16] The $160,000 is the value of the deferment option in this example. Accordingly, in the Gordon et al. (2003a) basic example, it would be in GLL's best interest to defer the decision concerning the hiring of the cybersecurity consulting firm. Thus, at this point in time, GLL's CFO denies the CSO's request for approval to spend the remaining $1,000,000 in the cybersecurity budget. Of course, if the high cost savings turned out to be the actual state, the CSO's request to spend the remaining $1,000,000 in the cybersecurity budget could be approved in the following time period.[17]

3.3. Gordon et al. (2003a) real options example with information sharing

In the Gordon et al. (2003a) basic example, the uncertainty pertaining to the decision of whether or not to make the investment necessary to hire the cybersecurity firm was resolved by waiting for a month. However, it is possible that the uncertainty associated with the potential cost savings could be resolved, or at least reduced, without waiting a month due to information sharing. In other words, if GLL were actively involved in some sort of information sharing association (e.g., an industry-specific ISAC), information pertaining to how other firms prevented and/or responded to similar cybersecurity attacks, as well as the actual costs associated with such attacks when successful, would (or at least could) change the analysis of this example.[18] To demonstrate how this could unfold, we return to, and modify, the original Gordon et al. (2003a) basic example to include information sharing.

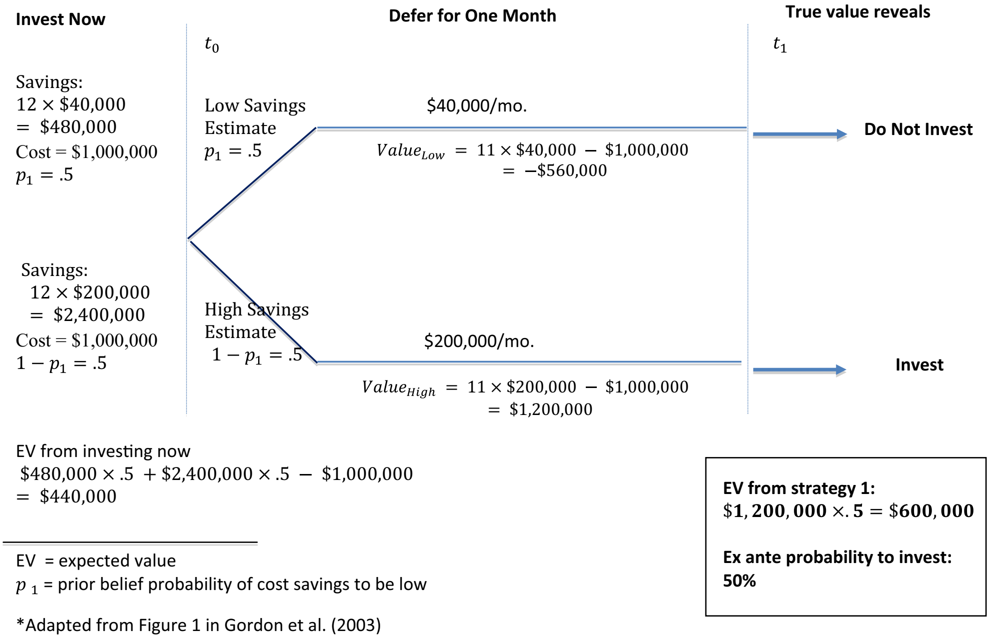
In the modified example, we refer to the company under consideration as M-GLL (i.e., the modified GLL). We assume that M-GLL is confronted with the same cybersecurity budget and cost savings possibilities given in the original Gordon et al. (2003a) example. That is, M-GLL has tentatively budgeted $2,500,000 for expenditures on cybersecurity activities. Once again, the firm has earmarked $1,500,000 (or 60%) of its total $2,500,000 budget for basic cybersecurity activities and this portion of the budget can be spent by the firm's CSO without any further approval. We also assume (as in

[15] Gordon et al. (2003a) assume that at the end of the year, GLL will re-evaluate its entire cybersecurity plan and budget, for purposes of moving forward.

[16] If the cost savings turned out to be $40,000 per month, then GLL would not hire the consulting firm because the cost savings would be only $440,000 (i.e., 11 × $40,000), which is below the $1,000,000 cost of hiring the consulting firm.

[17] This latter scenario is analogous to the situation referred to in the introduction to this paper, where a firm is investing more in cybersecurity activities as a reaction to a major cybersecurity breach.

[18] It is interesting to note that since experiencing its recent cybersecurity breach, Target joined the Financial Services Information Sharing and Analysis Center, FS-ISAC (see: https://corporate.target.com/discover/article/Target-joins-Financial-Services-Information-Sharin).



EV = expected value
p_1 = prior belief probability of cost savings to be low

*Adapted from Figure 1 in Gordon et al. (2003)

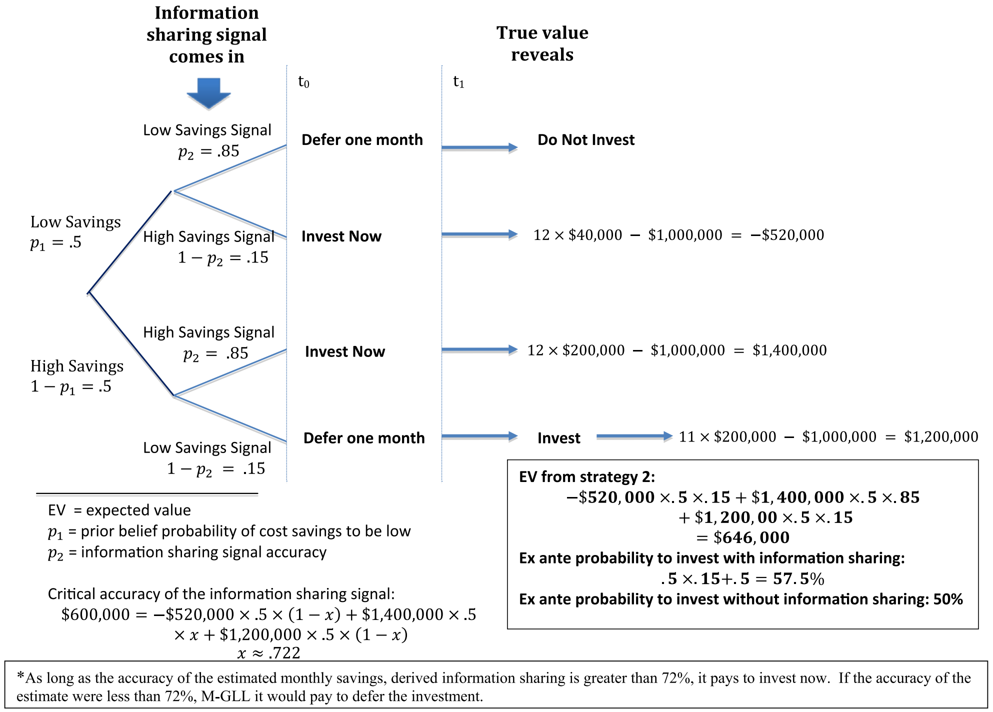
Fig. 1. Strategy 1: Ignore information sharing and defer the investment*.

the original example) that the firm's CSO needs the approval of the firm's CFO to spend the remaining (i.e., the discretionary) \$1,000,000 in the budget set aside for the current year's cybersecurity activities. As in the original example, the CSO of M-GLL wants to spend the remaining \$1,000,000 by hiring the cybersecurity consulting firm to enhance the firm's cybersecurity operations. Fig. 1 illustrates, in the absence of information sharing, the benefit to the firm of deferring the hiring of the cybersecurity consulting firm. We now, however, assume that M-GLL has joined an industry specific information-sharing group. We also assume that there is no charge to belong to this information-sharing group, providing a firm is willing to share cybersecurity related information with the group's members (i.e., free-riders are excluded from this group). Based on the agreement, all firms report to the group's members detailed information on their actual cybersecurity breaches, as well as steps taken to prevent and respond to cybersecurity breaches.

Since M-GLL is now a member of the information-sharing group, the CSO is able to present the firm's CFO a revised, more accurate analysis (i.e., a revised "business case"), for spending the discretionary \$1,000,000 in the cybersecurity budget. In other words, we now assume that M-GLL is able to use the information derived from the other members of the information-sharing group as an imperfect signal as to whether the cost savings from hiring the cybersecurity consulting firm will be high (i.e., \$200,000 per month) or low (i.e., \$40,000 per month.[19] Specifically, we assume that based on the information gleaned from the other members of the information-sharing group, M-GLL's CSO is now able to estimate the monthly savings with 85% accuracy.

Fig. 2 illustrates the revised value derived from deferring the discretionary cybersecurity investment of \$1,000,000 (i.e., hiring the cybersecurity consulting firm) for M-GLL. As shown in that figure, the revised expected value from making the incremental discretionary investment now, rather than deferring the investment, is \$646,000 compared to the \$600,000 (i.e., \$1,200,000 × .5) expected value derived from deferring the discretionary investment. Thus, with the new information gained from

[19] In reality, the information sharing would likely not provide a single signal concerning the high or low cost savings estimates. However, M-GLL could combine the information received into a single signal.


Information sharing signal comes in
True value reveals
t0
t1
Low Savings Signal
$p_2 = .85$
Defer one month
Do Not Invest
Low Savings
$p_1 = .5$
High Savings Signal
$1 - p_2 = .15$
Invest Now
$12 \times \$40{,}000 - \$1{,}000{,}000 = -\$520{,}000$
High Savings Signal
$p_2 = .85$
Invest Now
$12 \times \$200{,}000 - \$1{,}000{,}000 = \$1{,}400{,}000$
High Savings
$1 - p_1 = .5$
Defer one month
Invest
$11 \times \$200{,}000 - \$1{,}000{,}000 = \$1{,}200{,}000$
Low Savings Signal
$1 - p_2 = .15$
EV = expected value
p_1 = prior belief probability of cost savings to be low
p_2 = information sharing signal accuracy
Critical accuracy of the information sharing signal:
$\$600{,}000 = -\$520{,}000 \times .5 \times (1 - x) + \$1{,}400{,}000 \times .5 \times x + \$1{,}200{,}000 \times .5 \times (1 - x)$
$x \approx .722$
EV from strategy 2:
$-\$520,000 \times .5 \times .15 + \$1,400,000 \times .5 \times .85 + \$1,200,00 \times .5 \times .15 = \$646,000$
Ex ante probability to invest with information sharing:
$.5 \times .15 + .5 = 57.5\%$
Ex ante probability to invest without information sharing: 50%

*As long as the accuracy of the estimated monthly savings, derived information sharing is greater than 72%, it pays to invest now. If the accuracy of the estimate were less than 72%, M-GLL it would pay to defer the investment.

Fig. 2. Strategy 2: Invest when information sharing signal suggests high savings and defer investment when signal suggests low savings.

joining the information-sharing group, M-GLL is $46,000 better off hiring the cybersecurity consulting firm now rather than waiting to observe the actual costs associated with the security breach in the first month. Hence, the expected value derived from the information sharing in this example is $46,000. In other words, with more accurate information on the monthly cost savings from the cybersecurity investment derived from the information sharing group, it becomes cost efficient for M-GLL to immediately hire the cybersecurity consulting firm. Accordingly, in this scenario, the CFO of M-GLL should approve the request by the firm's CSO to hire the cybersecurity consulting firm. Since hiring the cybersecurity consulting firm is essentially making a cybersecurity investment, the increase in cybersecurity cost savings resulting from the information sharing has encouraged timelier cybersecurity investment.

As noted in Fig. 2, as long as the estimate of the accuracy of the estimated monthly savings derived from information sharing in the revised example is greater than 72%, it is economically rational to invest sooner rather than later. For our example, the value derived from information sharing is $46,000. However, it is important to note that this value is strongly dependent on the accuracy of the signal received from information sharing regarding the monthly cost savings. In general, the accuracy of the information sharing signal will likely be highest when the sharing arrangement is among firms within the same industry (as is the case with the industry-ISACs).

For the revised example that includes information sharing, there is a 57.5% probability of investing in cybersecurity versus a 50% probability of making such an investment without information sharing (see Fig. 2). Hence, the expected magnitude of the firm's cybersecurity investment is greater with information sharing than without information sharing ($1,500,000 + .575 [$1,000,000] versus $1,500,000 + .50 [$1,000,000]). One can easily demonstrate that the magnitude of the firm's expected cybersecurity investment will be greater with information sharing as long as the accuracy of the estimated monthly savings derived from information sharing is greater than 72%, but less than 100%. The expected investment level decreases as the accuracy of signal from information sharing increases. In the extreme case, when the signal is perfect (i.e., with 100% accuracy), the ex ante investment level is the same as in the case without information sharing. The investment, however, will be made sooner. From the firm's perspective, having the imperfect signal from information sharing makes the firm overinvest. The cost of the overinvesting is offset by the benefits from avoiding breaches earlier. What the firm considers overinvestment, however, would likely move the expected investment level towards the social optimal, given that the firm does not consider the externalities associated with breaches (e.g., costs to borne by the firm's customers, potential customers, and other firms not directly or indirectly borne by the firm experiencing the breach).

4. Implications

There are several implications of the analysis presented in the previous section of this paper. The first implication is that information sharing has the potential for reducing the uncertainty surrounding cybersecurity investment decisions. As a result of this reduction in uncertainty, the value of the option to defer cybersecurity investments is reduced. Thus, as shown in our example, information sharing is likely to have a calculable positive expected value on decisions to invest in cybersecurity activities now rather than to defer such investments. The ability to calculate such a metric should (or at least could) help to offset the costs typically associated with belonging to an information-sharing group. That is, the ability to calculate an expected value from the information received should serve as an incentive to encourage firms to share their information in return for receiving information from other firms.

Everything else equal, reducing the uncertainty surrounding cybersecurity investment decisions should encourage more timely, and more cost efficient, cybersecurity investments. Accordingly, a second implication of the analysis presented in the previsions section of this paper is that information sharing is likely to lessen the common tendency by firms to wait for a major cybersecurity breach before investing significant incremental funds for cybersecurity activities. Moreover, information sharing can result in an increase in the expected amount invested in cybersecurity.

A third implication of the analysis presented in the previous section of the paper has to do with similarities among the firms sharing cybersecurity information. The greater the similarities among the firms within a given information-sharing group, the more likely the information shared will be accurate (and thus more valuable) in terms of reducing the uncertainty surrounding cybersecurity investments. Accordingly, firms should seek to join an information-sharing group based on the similarities of the firm's characteristics to the characteristics of the other firms in the group. Some of the key characteristics to consider, in this regard, are the industry, average size of firms in the group, and the degree to which operations of the firms in the group are conducted via the Internet.

A fourth implication of the analysis provided in the previous section of the paper has to do with the prevalence, or lack thereof, of free-riding among members of an information sharing group. More specifically, the potential value of the information shared is inversely related to the amount of free-riding taking place by members of the group. Thus, in selecting an information-sharing group, firms would be wise to inquire as to the incentives and/or governing rules used to prevent firms from being a free-rider member of the group. Indeed, the extent to which an information-sharing group permits free-riding is one of the major reasons why firms are reluctant to share cybersecurity related information (Gordon et al., 2003b).

A fifth, albeit somewhat indirect, implication of the analysis provided in the previous section of this paper has to do with the potential for facilitating a vibrant cybersecurity insurance market. Insurance companies could provide discounts to firms actively engaged in sharing valuable cybersecurity information. Insurance companies could also develop better actuarial data and, in turn, develop more appropriate cybersecurity risk premiums based on collaboration with various information-sharing groups. The above would have the feedback effect of encouraging more firms to actively engage in the act of information sharing.

5. Concluding comments

Academicians, government officials/agencies, and corporate executives have advocated the sharing of information related to cybersecurity for some time. The argument for sharing information is based on the belief that firms can reduce their cybersecurity threats, vulnerabilities and, in turn, cyber incidences, based on the experiences of other (especially similar) firms. One aspect of sharing information related to cybersecurity not previously addressed in the literature has to do with its effect on the level of cybersecurity investment made by a firm. Based on a real options perspective, we demonstrated that information sharing, with its ability to reduce the uncertainty associated with cybersecurity investments may well result in reducing the tendency by private sector firms to underinvest in cybersecurity activities. This result was derived through the analysis of a hypothetical example that builds on the example provided in the paper by Gordon et al. (2003a). Furthermore, the demonstrated benefit gained from information sharing could provide the necessary incentive to overcome the reluctance by firms to actively share their private information.

As with most research related to cybersecurity, the research contained in this paper has its limitations. The most obvious of these limitations is the fact that our analysis is based on a hypothetical example. For our example, we provided a sufficient condition for information sharing to lead to a positive expected benefit for the firm and an expected increase in the magnitude of the firm's investments in cybersecurity. Accordingly, a natural extension of the research presented in this paper would be to provide a general model and sufficient conditions for information sharing to lead to positive expected benefits and an increase in the level of cybersecurity investments. Another extension of our research would be to empirically test the conceptual arguments. One way to conduct such a test would be via a laboratory experiment, where the participants were actual corporate managers in charge of cybersecurity activities within their firms. Conducting case studies of cybersecurity investment decisions by actual firms would represent another way to empirically test the arguments presented in this paper.

A second limitation of the research contained in this paper is that it looks at potential benefits of information sharing only in terms of the association between information sharing and the timing of cybersecurity investments. Of course, there are other factors that affect a firm's decision to share cybersecurity related information. For example, there are potential legal ramifications of sharing cybersecurity related information. Sharing cybersecurity related information could also have impact on a firm's competitiveness on a particular market space. The above limitations notwithstanding, we believe our analysis provides an important step in helping firms better understand the potential benefits of sharing information related to cybersecurity activities.

Acknowledgements

The authors gratefully acknowledge research support from the United States Department of Homeland Security (DHS) Science and Technology Directorate, the Netherlands National Cyber Security Centre (NCSC) and Sweden MSB (Myndigheten för samhällsskydd och beredskap) – Swedish Civil Contingencies Agency.

References

Accenture High Performance Research Report, 2013. <http://www.accenture.com/Microsites/high-performance-it/Documents/media/Accenture-High-Performance-IT-Research.pdf>.

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

Benaroch, M., Kauffman, R.J., 1999. A case for using real options pricing analysis to evaluate information technology project investment. Inform. Syst. Res. 10 (1), 70–86.

Benaroch, M., Kauffman, R.J., 2000. Justifying electronic banking network expansion using real options analysis. MIS Quart. 24 (2), 197–225.

Benaroch, M., Shah, S., Jeffery, M., 2006. On the valuation of multi-stage IT investments embedding nested real options. J. Manage. Inform. Syst. 23 (1), 239–261.

Böhme, R., Moore, T., 2009. The iterated weakest link: A model of adaptive security investment. In: 8th Workshop on the Economics of Information Security, June 24–25, London, UK. <http://weis09.infosecon.net/files/152/paper152.pdf>.

Daneva, M., 2006. Applying Real Options Thinking to Information Security in Networked Organizations. CTIT Technical Report TR-CTIT-06-11, Centre for Telematics and Information Technology, University of Twente. Enschede, The Netherlands.

Demetz, L., Bachlechner, D., 2013. To invest or not to invest? Assessing the economic viability of a policy and security configuration management tool. In: The Economics of Information Security and Privacy. Springer, pp. 25–47.

Department of Homeland Security (DHS), Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise, November 2011. <http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf>.

Dixit, A.K., Pindyck, R.S., 1994. Investment Under Uncertainty. Princeton University Press.

Fichman, R.G., 2004. Real options and IT platform adoption: Implications for theory and practice. Inform. Syst. Res. 15 (2), 132–154.

Fried, D., 1984. Incentives for information production and disclosure in a duopolistic environment. Quart. J. Econ. 99 (2), 367–381.

Gal-Or, E., 1985. Information sharing in oligopoly. Econometrica 53 (2), 329–343.

Gal-Or, E., Ghose, A., 2005. The economic incentives for sharing security information. Inform. Syst. Res. 16 (2), 186–208.

Ghosh, S., Li, X., 2013. A real options model for generalized meta-staged projects – valuing the migration to SOA. Inform. Syst. Res. 24 (4), 1011–1027.

Gordon, L.A., Loeb, M.P., 2002. The economics of information security investment. ACM Trans. Inform. Syst. Security 5 (4), 438–457.

Gordon, L.A., Loeb, M.P., 2006. Managing Cybersecurity Resources: A Cost-Benefit Analysis. McGraw-Hill, New York.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., 2003a. Information security expenditures and real options: a wait-and-see approach. Comput. Security J. 19 (2), 1–7.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., 2003b. 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., Zhou, L., 2011. The impact of information security breaches: has there been a downward shift in costs? J. Comput. Security 19 (1), 33–56.

Herath, H.S., Herath, T.C., 2008. Investments in information security: a real options perspective with Bayesian postaudit. J. Manage. Inform. Syst. 25 (3), 337–375.

High Representative of the European Union for Foreign Affairs and Security Policy, 2013. Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace. European Commission, July 2 2013.

Kamien, M.I., Muller, E., Zang, I., 1992. Research joint ventures and R&D cartels. Am. Econ. Rev. 82 (5), 1293–1306.

Kirby, A., 1988. Trade associations as information exchange mechanisms. RAND J. Econ. 29 (1), 138–146.

Mathews, C.M., 2013. Companies not budgeting enough for cybersecurity, study says. Wall Street J. Risk Compliance J., <http://blogswsj.com/riskandcompliance/2013/04/12/companies-not-budgeting-enough-for-cybersecurity-study-says/> April 12, 2013.

McDonald, R., Siegel, D., 1986. The value of waiting to invest. Quart. J. Econ. 101 (4), 707–727.

Novshek, W., Sonnenschein, H., 1982. Fulfilled expectations Cournot duopoly with information acquisition and release. Bell J. Econ. 13, 214–218.

Obama, B., Improving Critical Infrastructure Cybersecurity, Presidential Executive Order #13636, February 12, 2013 <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

Sarbanes-Oxley Act of 2002. <http://www.sec.gov/about/laws/soa2002.pdf>.

Schechter, S.E., Smith, M.D., 2003. How much security is enough to stop a thief? In: Financial Cryptography. Springer, Berlin, Heidelberg, pp. 122–137.

Shapiro, C., 1986. Exchange of cost information in oligopoly. Rev. Econ. Stud. 53 (3), 433–446.

Target Corporation Annual Report (Form 10-K) for the Fiscal Year ended February 1, 2014. <http://investors.target.com:phoenix.zhtml%3Fc=65828&p=irol-sec>.

Tatsumi, K., Goto, M., 2010. Optimal timing of information security investment: a real options approach. In: Moore, T., Pym, D., Ioannidis, C. (Eds.), Economics of Information Security and Privacy. Springer, US, pp. 211–228.

Taudes, A., Feurstein, M., Mild, A., 2000. Options analysis of software platform decisions: a case study. MIS Quart. 24 (2), 227–243.

U.S. Security and Exchange Commission Division of Corporation Finance, 2011. CF Disclosure Guidance: Topic No. 2 Cyber Security. <http://www.sec.gov/divisions/corpfin/guidance/ cfguidance-topic2.htm>.

Varian, Hal, 2002. System Reliability and Free Riding, Workshop on the Economics of Information Security, 2002 May 16–17, Berkeley, CA. <http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/49.pdf>.

Vives, X., 1990. Trade association disclosure rules, incentives to share information, and welfare. RAND J. Econ. 21 (3), 409–430.

Ziv, A., 1993. Information sharing in oligopoly: the truth-telling problem. RAND J. Econ. 24 (3), 455–465.